PTB mitteilungen

Fachorgan für Wirtschaft und Wissenschaft, Amts- und Mitteilungsblatt der Physikalisch-Technischen Bundesanstalt Braunschweig und Berlin

126. Jahrgang, Heft 4, Dezember 2016

Metrologische IT
Teil I

Titelbild: Quelle fotolia.com

Inhalt

Metrologische IT, Teil I

Metrologische IT, Teil II folgt in PTB-Mitteilungen 1/2017

Internationale Zusammenarbeit

Vorwort

Florian Thiel*

„*Digitalisierung ist der Motor für Innovation, der den Industriestandort Deutschland stärkt und zukunftsfähig macht.*“ Sigmar Gabriel, Bundesminister für Wirtschaft und Energie, Mai 2016

Durch die Digitalisierung der Wirtschaft werden wesentliche Impulse für den europäischen Binnenmarkt erwartet. Die Bundesregierung sieht entsprechend den Nutzen der Digitalisierung für Deutschland und hat die Informations- und Kommunikationstechnologie (IKT) im Jahr 2014 in die neue Hightech-Strategie aufgenommen und die „Digitale Agenda“ als nationales Pendant der europäischen Initiative initiiert.

Die deutsche IKT-Branche trägt heute schon deutlich mehr zur gewerblichen Wertschöpfung bei als traditionelle Branchen wie die Maschinen oder die Automobilindustrie. Diese „Digitale Transformation“ der Wirtschaft geht einher mit allgegenwärtigen Technologie-Begriffen wie *Cyber Security*, *Embedded Systems*, *Internet of Things*, Cyber-physische Systeme, intelligente oder virtualisierte Messsysteme, *Cloud Computing*, *Big Data*, *Smart Data* und *Smart Services* – um die wesentlichsten zu nennen.

All diese Technologien sind nicht dabei, neu erfunden zu werden, sondern haben im Zuge ihrer Evolution nun den Reifegrad erreicht, der sie ganz natürlich in neue Technologiefelder konvergieren lässt. Das prominenteste Beispiel für solch ein Technologiefeld ist „Industrie 4.0“.

Diese Ausgabe der PTB-Mitteilungen „Metrologische IT“ möchte die Frage nach den Herausforderungen und Chancen beleuchten, die sich für die Metrologie durch die neuen IT-Technologien eröffnen und welche Angebote sie im Rahmen der metrologischen Dienstleistungen bereits offerieren oder in Zukunft anbieten könnten.

Im Fokus des ersten Artikels steht das Technologiefeld Industrie 4.0 und er gibt auch Ausblicke darauf, wohin die Entwicklung – insbesondere zum Nutzen des gesetzlichen Messwesens – gehen könnte.

Es ist schon abzusehen, dass die IT-Sicherheit in Zukunft eine noch wichtigere Rolle spielen und sich zunehmend zu einem bedeutenden Wirtschaftsfaktor entwickeln wird. Daher haben wir uns um zwei Artikel von prominenten Experten auf diesem Gebiet bemüht. Der erste Artikel dazu stammt aus dem Referat „Cyber-Sicherheit in der Industrie“ des Bundesamts für die Sicherheit in der Informationstechnik (BSI). Der sich anschließende Artikel stammt aus der Abteilung *Hardware Security* des Fraunhofer-Instituts für Angewandte und Integrierte Sicherheit (AISEC) dessen Geschäftsführende Leiterin, Prof. Dr. Claudia Eckert, in diesem Jahr in das Kuratorium der PTB berufen wurde.

Wie bereitet sich die PTB auf diese Herausforderungen vor oder gibt es schon Angebote? Das soll in den folgenden fünf Artikeln detailliert dargestellt werden. Dabei gehen wir den Weg von der Systemkonfiguration zur individuellen, lokalen und über Netze verteilten Systemarchitektur. Wir beginnen bei der sicheren Konfigurierung von Betriebssystemen, gehen weiter zu einer Referenzarchitektur für eingebettete Systeme bzw. dem Internet der Dinge und von dort zu einer Referenzarchitektur für das Cloud Computing. Ziel ist hier, Herstellern von Messgeräten Angebote für rechtskonforme Lösungen bei der Nutzung neuer Technologien zu geben, die diese im Zuge des Technologietransfers nutzen können. Weiterhin werden diese Referenzarchitekturen einer Risiko-Analyse unterzogen und bieten einfache Verifikationsmöglichkeiten für die Marktaufsicht im Feld an.

* Dr. habil. Florian Thiel, Fachbereich 8.5 „Metrologische Informationstechnik“, E-Mail: florian.thiel@ptb.de

Daran schließt sich ein Artikel an, in dem eine Prozedur vorgeschlagen wird, wie sogenannte „adäquate“ Sicherheit – gefordert von europäischen und nationalen Rechtsnormen – möglichst objektiv „gemessen“ werden kann. Dieser Themen-Block wird abgeschlossen durch einen weiteren Artikel des BSI zu den aktuellen Anforderungen an intelligente Messsysteme, bei denen die PTB die metrologischen Aspekte in einer eigenen PTB-Anforderung festgelegt hat. Diesem Thema wurde im letzten Jahr eine eigene PTB-Mitteilung (3/2015) gewidmet. Hier endet Teil I dieser PTB-Mitteilung. Die im folgenden beschriebenen Artikel finden sich in Teil II, Heft 1/2017 der PTB-Mitteilungen.

In einem Umfeld mit solch hoher Innovationsrate wie der Informations- und Kommunikationstechnologie braucht die Metrologie entsprechende „Filter“, um wesentliche von unwesentlichen Entwicklungen zu trennen und um die metrologischen Dienstleistungen vorlauforientiert auch in Zukunft handlungsfähig zu halten. Solch ein wesentlicher Filter wird durch das ureigenste Bestreben der Industrie bereitgestellt, kommerziell zielführende Technologien zu identifizieren und den Bedarf an „akzeptablen Lösungen“ für diese in die Harmonisierungsgremien des gesetzlichen Messwesens einzubringen, bevor sie der PTB entsprechende technische Entwürfe zur Konformitätsbewertung vorlegt.

Wir halten es daher für angemessen, in diesem Kontext auch zwei große europäische Industrieverbände, CECOD und CECIP, zu Wort kommen zu lassen, um ihren zukünftigen Bedarf an die metrologischen Dienstleistungen zu formulieren.

Die Marktaufsicht, deren Sichtweise auf die neuen Technologien wir ebenfalls nachgefragt haben, fühlt sich durch die PTB gut beraten und überlässt daher einen fundierten Blick in die Technikmöglichkeiten gerne und notwendigerweise den Herstellern und den entwicklungsunterstützenden Fachkreisen der PTB.

Die Aktualisierung von Software, sei es um neue Programmversionen aus der Ferne aufzuspielen, Programmierfehler zu beseitigen oder das System gegen neue Manipulationsmöglichkeiten zu härten, ist eine der Möglichkeiten, die die Hersteller neben den oben genannten Technologien besonders interessiert. Daher scheint eine Darstellung der rechtlichen Möglichkeiten und Vorgehensweisen international, europäisch und national hier wichtig und wird in zwei Artikeln behandelt.

Um ganz konkret zu werden, schließen sich diesem Teil zwei Artikel an, die detailliert die Entwicklungen im Bereich der Gasrekonstruktionssysteme und in der Fertigungsmesstechnik im Hinblick auf Industrie 4.0 beleuchten.

Metrologie und die Angabe von Messunsicherheiten sind wie zwei Seiten ein und derselben Medaille. Hier kommen schon lange kommerzielle Softwareprodukte zum Einsatz. Daher soll abschließend noch auf die Vorgehensweise bei der Validierung solcher Softwareprodukte für die Berechnung von Messunsicherheiten nach GUM (*Guide to the Expression of Uncertainty in Measurement*) eingegangen werden. Die dort zum Einsatz kommenden und von der PTB entwickelten Testumgebungen (*Testbeds*) können zusätzliche Anregungen für die Prüfung komplexer Systeme geben.

Die Vorgehensweisen und Anforderungen zur Absicherung von IT-gestützten Systemen werden in vielen Bereichen der gesetzlichen Beauftragung der PTB immer ähnlicher, so z. B. im Gewerberecht und im gesetzlichen Messwesen.

Daher sollen zum Abschluss die gesteigerten IT-Sicherheitsanforderungen an Geldspielgeräten beleuchtet werden. Diese werden durch die Novellierung der Spielverordnung im Rahmen der Bauartzulassung gefordert und wurden von der PTB in einer technischen Richtlinie entsprechend technologisch interpretiert, um den Herstellern Rechts- und Handlungssicherheit zu geben. Die hier vorgestellten Vorgehensweisen sind möglicherweise für die Aufgaben der PTB im Rahmen ihrer Beauftragung in weiteren Rechtsnormen von Interesse.

Mit dieser Zusammenstellung hoffen wir, Ihr Interesse für diese Thematik zu wecken, Sie für die Fragen der Sicherheit in der Informationstechnik speziell in regulierten Bereichen zu sensibilisieren und hoffentlich einige Ihrer Fragen zu beantworten und neue Sichtweisen und Ideen anzustoßen.

In diesem Sinne wünschen wir Ihnen viel Spaß beim Lesen!

Digitalisierung im gesetzlichen Messwesen

Florian Thiel*, Marko Esche**

1.0 Einführung

Informations- und Kommunikationstechnologie (IKT) ist die ausschlaggebende Zukunftstechnologie für den deutschen Wirtschaftsstandort. Schon heute ist die IKT-Branche verantwortlich für eine gewerbliche Wertschöpfung von rund 85 Milliarden Euro pro Jahr. Damit ist sie bereits leistungsstärker als die traditionellen Industriezweige wie der Maschinenbau und die Automobilindustrie [1]. Die IKT kann als Innovationstreiber verstanden werden, der auch in der Zukunft wirtschaftliches Wachstum garantieren und damit Wohlstand und Arbeitsplätze sichern wird.

Die fortschreitende Digitalisierung der Gesellschaft hat in den vergangenen zwei Jahrzehnten zu neuen Formen der Kommunikation, der Arbeit und der Mediennutzung geführt. Die Innovationen und neue Geschäftsmodelle sind dabei nicht auf den Technologiesektor beschränkt, sondern umfassen neben der Industrie auch die Bereiche Energie, Gesundheit, Verkehr und Bildung [1, 2, 3]. Die weltweit unter dem Titel *Industrial Internet* bekannte technologische Veränderung, die in Deutschland unter der Überschrift „Industrie 4.0“ subsummiert wird, spielt in der „Digitalen Agenda“ der Bundesregierung [1] eine prominente Rolle. Darin wurde die IKT in die neue Hightech-Strategie integriert [4], die einen weiteren Schritt hin zur Industrie 4.0 darstellt.

„*Im Mittelpunkt von Industrie 4.0 steht die echtzeitfähige, intelligente, horizontale und vertikale Vernetzung von Mensch, Maschine, Objekten und IKT-Systemen zum dynamischen Management von komplexen Systemen*“ [5].

Aufgrund dieser Entwicklung entstehen neue Herausforderungen für die nationale und internationale Qualitätsinfrastruktur [6], deren wesentliche Komponente – das gesetzliche Messwesen – international ein bedeutender Wirtschaftsfaktor ist. Die in diesem Artikel dargestellte Betrachtung der Implikationen und Chancen von Industrie 4.0 für das gesetzliche Messwesen soll vor allem fruchtbare zukünftige Handlungsfelder identifizieren. Auf deren Grundlage können proaktiv technologische Lösungsvorschläge für die Industrie, die Konformitätsbewertungsstellen und die Markt- und Verwendungsaufsicht durch das nationale Metrologieinstitut, die Physikalisch-Technische Bundesanstalt (PTB), entwickelt und angeboten werden.

1.1 Historische Entwicklung und Blick nach vorne

Die anstehenden technologischen Veränderungen hin zur Industrie 4.0 können als logische Fortführung einer vierstufigen Entwicklung gesehen werden, die bis in das 17. Jahrhundert zurückverfolgt werden kann. Dabei stand die Umstellung auf mechanische Produktionsanlagen, die bspw. mit Wasser- oder Dampfkraft betrieben wurden, im Fokus der ersten industriellen Revolution (1784, erster mechanischer Webstuhl). Durch die Mechanisierung war der Weg geebnet für die Umstellung auf eine arbeitsteilige Massenproduktion, deren Hauptmerkmal die Fließbandarbeit war (1870, erste Fließbänder in Schlachthöfen von Cincinnati). Der flächendeckende Einsatz von elektronischen Systemen und von Informationstechnologie (IT) ab der Mitte des 20. Jahrhunderts mit dem Ziel einer weiteren Automatisierung der Produktion markiert in diesem Kontext die dritte industrielle Revolution (1969, erster Einsatz von speicherprogrammierbaren Steuerungen (SPS)). Weitere technologische Entwicklungen, die sich u. a. auf den Einsatz von cyber-physikalischen Systemen (CPS) gründen, sollen jetzt zur vierten industriellen Revolution führen. Hervorzuheben

* Dr. habil. Florian Thiel, Fachbereich 8.5 „Metrologische Informationstechnik“, E-Mail: florian.thiel@ptb.de

** Dr.-Ing. Marko Esche, Arbeitsgruppe 8.51 „Metrologische Software“, E-Mail: marko.esche@ptb.de

ist an dieser Stelle, dass hier eine Revolution ausgerufen wird, bevor diese eigentlich stattgefunden hat. Der Innovationsdruck den steigenden Anforderungen eines globalisierten, regionalisierten und personalisierten Marktes zu genügen, motiviert den Einsatz neuester IKT in der Produktion.

Von den Anfängen der Massenproduktion, bei der bspw. alle Model-T der Firma Ford identisch waren („People *can have the Model T in any colour – so long as it`s black*", Henry Ford 1913), hat sich die industrielle Produktion inzwischen deutlich weiterentwickelt. Heute ist die Industrie in der Lage, stark individualisierte Produkte mittels eines hoch flexibilisierten Produktionsprozesses herzustellen. So lassen sich längst PKW frei über das Internet konfigurieren oder ganz unterschiedliche individuelle Produkte über 3D-Drucker erzeugen. In der Zukunft werden immer mehr Unternehmen ihre weltweit existierenden Maschinen, Lagersysteme und Betriebsmittel sowie die dazugehörige IT in Form sogenannter CPS miteinander vernetzen. Die eigenständig agierenden und Informationen austauschenden CPS werden dann den Kern einer neuen *Smart Factory* bilden, in der die Prozesse der Produktion, der Entwicklung, der Materialverwendung sowie des Lieferketten- und des Lebenszyklus-Managements gemeinsam optimiert werden können. In der Smart Factory kann unter anderem die bisherige sequenzielle Produktion durch ein entkoppeltes, flexibilisiertes und hochgradig integriertes Produktionssystem ersetzt werden. Um dies zu erreichen, werden aus den bisherigen Fertigungsprodukten, die bisher nur eine passive Rolle während der Produktion einnahmen, sogenannte *Smart Products*, die zu allen Zeitpunkten eindeutig identifizier- und lokalisierbar sind. Zusätzlich verfügen die Smart Products über Informationen hinsichtlich ihres aktuellen Zustands und über verschiedene Alternativwege zum gewünschten Zielzustand. Dies erfolgt mithilfe des Konzepts eines virtuellen Produktabbildes, das zu jedem Zeitpunkt in digitaler Form den genauen Ist- und Soll-Zustand eines Produkts kennt und das Produkt während aller Lebensphasen begleitet.

Mit dem Ziel auch individuelle Kundenwünsche berücksichtigen und auch Einzelstücke herstellen zu können, werden die Produktionssysteme der Smart Factory in der Zukunft sowohl horizontal mit anderen in Echtzeit steuerbaren Wertschöpfungsnetzwerken, als auch vertikal mit den betriebswirtschaftlichen Prozessen der Smart Factory verknüpft sein. Sie sind damit in der Lage, die gesamte Wertschöpfungskette vom Bestellungseingang bis hin zur Ausgangslogistik abzubilden. In der Konsequenz werden betriebswirtschaftliche Prozesse und Entwicklungsprozesse dynamisch anpassbar, was gleichzeitig auch eine erhöhte Robustheit gegen Störungen und Ausfälle bedeutet. Die dadurch vollständig transparenten Produktionsprozesse ermöglichen nicht nur eine Optimierung der notwendigen Entscheidungsprozesse, sondern auch das Entstehen neuer Geschäftsmodelle und neuer Formen der Wertschöpfung.

Nur sichere, vertrauenswürdige und qualitativ hochwertige Produkte und Dienstleistungen bestehen langfristig auf den internationalen Märkten. Die Anforderungen an Produkte und Dienstleistungen werden in Europa zunehmend im Rahmen von sogenannten Konformitätsbewertungsverfahren überprüft. Innerhalb der EU ist die Konformitätsbewertung, bei der die Erfüllung vorgegebener grundlegender Anforderungen nachgewiesen wird, für bestimmte Produktgruppen (wie z. B. Messgeräte im gewerblichen Gebrauch, oder Medizinprodukte) notwendige Voraussetzung für das erstmalige Inverkehrbringen und kann den weltweiten Marktzugang deutlich beschleunigen. Für zahlreiche innovative Produkte ist ein leistungsstarkes Messwesen eine Grundvoraussetzung, denn letztendlich kann nur das mit hoher Qualität entwickelt und produziert werden, was auch sehr genau gemessen werden kann. Die Bundesregierung sieht daher u. a. die Konformitätsbewertung, Marktüberwachung und das Messwesen als wichtige Grundpfeiler der Wirtschaft und wird diese im Rahmen der Hightech-Strategie weiterentwickeln, international harmonisieren und damit auch zum Abbau nicht tarifärer Handelshemmnisse beitragen [4].

2.0 Überblick zum gesetzliche Messwesen

Grundsätzliche Aufgabe des gesetzlichen Messwesens ist es, das Vertrauen der Konsumenten in Messungen herzustellen, die im amtlichen oder geschäftlichen Verkehr durchgeführt werden. Dabei wird die Rückführbarkeit aller Messungen im gesetzlichen Messwesen auf nationale Normale bzw. auf die internationalen SI-Definitionen sichergestellt. Damit wird eine Voraussetzung für die Produktion qualitativ hochwertiger Produkte geschaffen [6]. Globale Produktionssysteme sowie der internationale Handel sind nur möglich, wenn alle beteiligten Parteien einheitliche Maßeinheiten verwenden. Gemäß Grundgesetzartikel 73 Absatz 1 Nummer 4 besitzt der Bund in Deutschland die alleinige Gesetzgebungskompetenz „für Maße, Gewichte sowie die Zeitbestimmung." Im Rahmen dieser hoheitlichen Aufgabe werden Anforderungen an Maßeinheiten, Messmethoden, Messgeräte und Fertigpackungen formuliert, wodurch dann angemessene Messrichtigkeit, -beständigkeit und -prüfbarkeit gewährleistet werden. Dementsprechend stellt das gesetzliche Messwesen eine fundamentale Voraussetzung für das Funktionieren der deutschen Wirtschaft dar.

Moderne IKT durchdringt schon heute weite Bereiche des privaten und gesellschaftlichen Lebens. Auch im gesetzlichen Messwesen ist diese Entwicklung spürbar und äußert sich in dem durch nationale und internationale Herstellerverbände geäußerten Bedarf und Wunsch, solche Technologien in ihren Messgeräten zu nutzen. Um das Vertrauen in das richtige Messen zu stärken und Verwender von Messgeräten sowie die Verbraucher zu schützen, wird es damit notwendig, rechtskonforme, transparente Lösungen für den Einsatz moderner IKT im gesetzlich geregelten Bereich zu entwickeln. Diesem Bedürfnis wurde im Gesetz zur Neuordnung des gesetzlichen Messwesens Rechnung getragen. Dies gilt insbesondere beim Einsatz komplexer Technologien, die sich zunehmend dem intuitiven Verständnis des technischen Laien entziehen (s. Bild 1). Insbesondere hier müssen geeignete Maßnahmen und Prozeduren entwickelt werden, um das Vertrauen des Nutzers zu sichern und damit Technologieoffenheit und Marktakzeptanz zu fördern. Eine Institutionalisierung dieser Vertrauensbildung kann z. B. über die PTB erreicht werden.

Das gesetzliche Messwesen in Deutschland umfasst rund 160 Millionen Messgeräte, die im geschäftlichen, im amtlichen Verkehr oder im öffentlichen Interesse eingesetzt werden. Sie untergliedern sich in 150 Gerätearten, Teilgeräte sowie in Zusatzeinrichtungen. Der größte Anteil entfällt dabei auf den Bereich der geschäftlich genutzten Verbrauchsmessgeräte wie Strom-, Gas-, Wasser- und Wärmezähler. Zu anderen alltäglichen Berührungspunkten mit dem gesetzlichen Messwesen zählen nicht nur Zapfsäulen an Tankstellen und Waagen im Einzelhandel, sondern auch Geschwindigkeits- und Atemalkoholmessgeräte. Wie wichtig ein hinreichender Manipulationsschutz der Software in Messgeräten ist, lässt sich anhand des durch das gesetzliche Messwesen erwirtschafteten Anteils am Bruttoinlandsprodukt (BIP) nachvollziehen: In den meisten Industrieländern sind gesetzlich geregelte Messungen verantwortlich für einen Anteil von 4 % bis 6 % am BIP. Dies entspricht in Deutschland einem erwirtschafteten jährlichen Umsatz von 104 bis 157 Milliarden Euro [7]. Die Konsequenzen einer erfolgreichen Manipulation lassen sich anhand dieser Zahlen leicht abschätzen. Gleichzeitig ist das gesetzliche Messwesen verantwortlich für rund 56 % des Steueraufkommens des Bundes. Im Jahr 2015 entfielen dabei rund 40 Milliarden Euro allein auf Einnahmen aus der Energiesteuer (Strom/Gas/Wärme/Mineralöl) [6].

Der rechtliche Rahmen für die Regulierung des gesetzlichen Messwesens wird dabei durch die europäische *Measuring Instruments Directive* (MID) 2014/32/EU aufgespannt [8]. In Deutschland ist diese Richtlinie durch das Mess- und Eichgesetz (MessEG) [9] bzw. durch die Mess- und Eichverordnung (MessEV) [10] im Jahr 2015 umgesetzt worden. Der sogenannte *New Approach*, der den Kerngedanken der neueren EU-Richtlinien bildet, zeigt sich dabei deutlich in einem bewussten Verzicht auf die bisherigen staatlichen Genehmigungs- bzw. Zulassungsverfahren. Stattdessen trägt der Hersteller eine deutlich größere Verantwortung, da er seine Messgeräte vor dem Inverkehrbringen lediglich von einer unabhängigen Drittstelle auf Übereinstimmung mit den gesetzlichen Anforderungen prüfen lassen muss. Nach Abschluss eines solchen Konformitätsbewertungsverfahrens stellt die durchführende Konformitätsbewertungsstelle, in Deutschland bspw. die Physikalisch-Technische Bundesanstalt, ein Zertifikat aus, auf dessen Grundlage der Hersteller dann die Konformität eines jeden Einzelgeräts erklärt. Auf europäischer Ebene darf nach einer erfolgreichen Konformitätsbewertung das CE-Kennzeichen auf dem Gerät angebracht werden, national wird bspw. bei Übereinstimmung mit dem Produktsicherheitsgesetz das GS-Zeichen angebracht.

Die gesetzlichen Anforderungen an Software sind eher allgemein formuliert. Mit dem Ziel die Vorgehensweisen der verschiedenen Konformitätsbewertungsstellen zu vereinheitlichen, werden

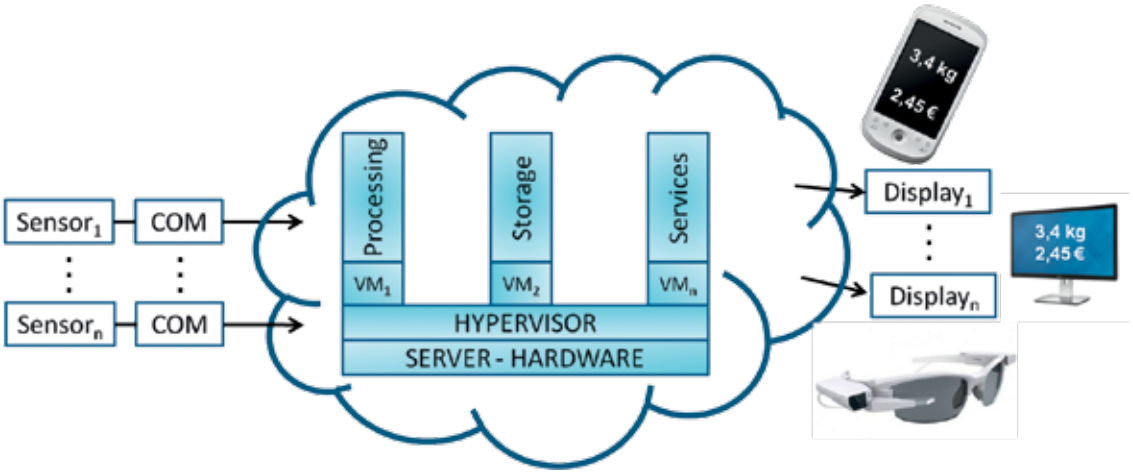

Bild 1:
Messgerät der Zukunft mit verteilten und virtualisierten Komponenten

daher im Rahmen harmonisierter Handlungshilfen spezielle Anforderungen für Software und IT-Komponenten ausgestaltet. Diese unterstützen gleichzeitig die Industrie bei der Entwicklung konformer Messgeräte. Auf nationaler Ebene werden vom Regelermittlungsausschuss [9] solche Dokumente identifiziert, die den Stand der Technik repräsentieren und damit bei Einhaltung der Dokumente die Vermutungswirkung hinsichtlich der Erfüllung der gesetzlichen Anforderungen auslösen. Für den Bereich der intelligenten Messsysteme stellen die PTB-Anforderungen 50.8 [11] ein solches ermitteltes Dokument dar, das metrologische Anforderungen an Smart Meter Gateways festlegt. Mit den PTB-A 50.8 werden die komplementären, metrologischen Anforderungen, die in der technischen Richtlinie und dem Schutzprofil des Bundesamts für Sicherheit in der Informationstechnik (BSI) noch nicht vollumfänglich umgesetzt sind, abgedeckt.

Bei der europaweiten Entwicklung von Anforderungsdokumenten zur Interpretation der MID ist die *European Cooperation in Legal Metrology* (WELMEC) federführend und veröffentlicht Handlungshilfen, die dann von der *Working Group Measuring Instruments* der EU-Kommission identifiziert werden können.

Der WELMEC Guide 7.2 „Software“ [12] interpretiert die wesentlichen Anforderungen der MID für Software und IT-Komponenten und bietet gleichzeitig akzeptable technische Lösungen. Auf internationaler Ebene stellt das Dokument D 31 „*General requirements for software controlled measuring instruments*“ [13] ein vergleichbares Dokument der *Organisation Internationale de Métrologie Légale* (OIML) dar. Diese veröffentlicht weltweit anerkannte Anforderungsdokumente, sogenannte *Recommendations*, für spezifische Messgeräte sowie Dokumente wie den D 31, die Empfehlungen für alle Messgerätearten darstellen. Als solches findet der D 31 Berücksichtigung bei der Neu- und Weiterentwicklung aller Recommendations, die dann jeweils spezifische Softwareanforderungen enthalten und den Rang eines normativen Dokuments von der Europäische Kommission erhalten. Durch die Mitarbeit in beiden Organisationen unterhält die PTB regen Kontakt sowohl zu anderen Konformitätsbewertungsstellen und Metrologieinstituten, zu den Marktaufsichtsbehörden, als auch zu den Industrieverbänden.

Mit den genannten Hilfsmitteln und Beteiligungen kann die PTB metrologierelevante technische Trends aus der Vielzahl innovativer Informations- und Kommunikationstechnologien herausfiltern und vorlauforientiert Lösungen vorschlagen. Diese werden dann in den obigen Gremien zur Harmonisierung eingebracht. Gleichzeitig werden so Handels- und Innovationshemmnisse abgebaut.

3.0 Basistechnologien von Industrie 4.0

Industrie 4.0 ist keine neue Technologie, sondern setzt sich aus mehreren sich weiterentwickelnden Technologiefeldern zusammen. Deren Reifegrad und ihr evolutionäres Zusammenwachsen hat ganz natürlich zur Industrie 4.0 geführt. Zu diesen Technologieelementen gehören im Wesentlichen die kostengünstige Hochintegration, robuste Netze, die Verwendung „eingebetteter Systeme“ (*embedded systems*), die durch Anbindung an das Internet zu cyber-physikalischen Systemen (CBS) werden und so das Internet der Dinge bilden (*Internet of Things*, IoT) sowie das Cloud Computing.

Industrie 4.0 umschreibt die Anbindung der Fabrik, der Logistik, ja der ganzen Wertschöpfungskette an das Internet der Dinge, was deutlich durch den äquivalenten US-amerikanischen Begriff *Industrial Internet* [14] oder *Industrial Internet of Things* (IIoT) ausgedrückt wird.

Die bereits heute existierenden lokalen Netzwerktechnologien in Industrieanlagen stellen den zentralen Baustein dieser vierten industriellen Revolution dar. Zukünftig müssen hier noch größere Datenmengen als bisher in nahezu Echtzeit übertragen werden. Dabei muss sowohl die steigende Zahl von Sensoren und Aktuatoren berücksichtigt als auch eine zuverlässige Steuerung und Regelung gewährleistet werden. Zentraler Ansatz von Industrie 4.0 ist daher die standortübergreifende Vernetzung der lokalen Produktionsnetzwerke über offene Weitverkehrsnetze. Dabei stoßen zwei offensichtlich gegensätzliche Paradigmen aufeinander; den auf Langlebigkeit ausgelegten Industrieanlagen mit hohen Anforderungen an Zuverlässigkeit steht auf der anderen Seite die sich schnell weiterentwickelnde Kommunikationsinfrastruktur gegenüber. Da Erstere sich nur selten aktualisieren und aufrüsten lassen und zumeist auf spezialisierter Hardware sowie spezialisierten Protokollen basieren, kommt es zu Insellösungen bzw. zum sogenannten „Lock-in-Effekt“ und schließlich zu Inkompatibilitäten zwischen den verschiedenen Kommunikationstechnologien. Verstärkt wird dieser Effekt durch die immer weiter verteilten Industrieanlagen, die schnell fortschreitende Industrieautomatisierung und durch die Anbindung einer großen Anzahl von Sensoren, Aktuatoren, Maschinen, Steuer- und Regeleinheiten.

Bislang gibt es nur wenige globale Ansätze, wie diese Inseln integriert, einheitlich konfiguriert und gemanagt werden können. Es existieren jedoch insbesondere im Bereich der Virtualisierung und der Cloud (*Edge-Cloud* [15]) Möglichkeiten, die Vielzahl der vorhandenen Systeme, Protokolle und der in sich geschlossenen Produktionsnetzte miteinander zu verbinden und so

Aktualisierungen und Nachrüstung zu ermöglichen [16]. Die Virtualisierungstechnik erlaubt es, Steuerungsfunktionen, die bisher durch Hardwarekomponenten direkt an den Messgeräten, Maschinen und Anlagen angebracht waren, in der Cloud virtuell zur Verfügung zu stellen und als Software-Dienste abrufbar zu halten. Cloud Computing ist inzwischen eine etablierte Technologie, die für die Verbraucher selbstverständlich geworden ist [17]. Als alltägliche Beispiele seien hier nur DropBox, Google Drive oder die Amazon *Elastic Compute Cloud* (EC2) genannt. Auch eingebettete Systeme stellen heute schon das Rückgrat der digitalen Gesellschaft dar. Mehr als 90 % der Computer in der ersten Welt sind nicht als PCs anzutreffen, sondern sind bspw. das Kernstück von ABS, ESP und Herzschrittmachern oder automatisieren kritische Infrastrukturen (Verkehr, Wasser, Energie) [18].

Selbstverständlich wird erwartet, dass diese Systeme unter allen Umständen korrekt funktionieren, weshalb für sie grundsätzlich das Konzept *Security by Design* verfolgt werden soll [19]. Gleichzeitig werden auch die bereits existierenden eingebetteten Systeme immer weiter miniaturisiert, da nur so die Vorstellung des IoT realisiert werden kann. Schätzungen der Firma Cisco zufolge dürften bis zum Jahr 2020 rund 50 Milliarden eingebetteter vernetzter Systeme in Betrieb sein. IPv6 mit einem um den Faktor $7{,}9 \cdot 10^{28}$ größeren Adressraum als IPv4 bildet eine dafür wichtige Voraussetzung [20]. Bereits heute können Verbraucher Bausätze für das *Smart Home* kaufen, mit denen sie nicht nur aus der Ferne den Energieverbrauch einzelner Geräte in ihrem Haushalt überwachen, sondern auch aktiv steuern können. Neben den offensichtlichen Vorteilen birgt diese Bidirektionalität selbstverständlich auch Sicherheitsrisiken.

Im Rahmen der Digitalisierung der Produktion werden zunächst Steuerungsprogramme von Automatisierungssensoren und -aktuatoren sowie die Software ganzer Produktionsanlagen auf externe Servern ausgelagert werden. Im Zuge dessen können dann Steuerungsfunktionen in der *Automation Cloud* als virtuelle Dienste zur Verfügung gestellt werden und brauchen nicht mehr vollständig als lokale Hardwaresteuerungen realisiert zu werden. Dadurch ist es nicht mehr notwendig, bei Änderungen am Produktionsprozess neue Hardware zu installieren und existierende Steuerungen umzuprogrammieren. Vielmehr werden die Produktionsstraßen zukünftig selbstständig auf bereits optimierte Steuerungsdienste in der Cloud zurückgreifen. Zu den offensichtlichen Vorteilen bei der Inbetriebnahme oder Erweiterung von Produktionsanlagen zählen dabei die Kostenreduktion sowie Speicherplatz- und Zeitersparnis.

Die durchgehende Vernetzung der IT-Systeme und die Autonomie der Produktionssysteme bei Industrie 4.0 bieten eine wesentlich erweiterte Angriffsfläche. IT-Sicherheit auf einem angemessenen Niveau in bestehende und erweiterte Anlagen zu integrieren, wird daher zu einem der wichtigsten Wettbewerbsfaktoren einer globalisierten Produktion und in der global vernetzten Dienstleistungslandschaft [21]. Aktuelle Fragestellungen der IT-Sicherheit im Kontext von Industrie 4.0 betreffen die Fernwartung im Maschinen- und Anlagenbau, den Unternehmens- und grenzüberschreitenden Datenaustausch zur Produktionsoptimierung in der Logistikbranche (Cloud-Sicherheit), die Inbetriebnahme produktionsrelevanter Systeme unter Zeitdruck in der Automobilindustrie (intrinsische Systemsicherheit, Plug&Play, *Zero-TouchConfiguration*) und die Netzwerksegmentierung von Produktionsnetzwerken z. B. in der chemischen Industrie (bspw. durch Virtualisierung und Kontrolle von cloudbasierten Anwendungen durch Attestation von virtuellen Maschinen) [19].

Abschließend lässt sich feststellen, dass abgesehen vom vollständigen IoT quasi alle notwendigen Technologien zur Realisierung von Industrie 4.0 bereits verfügbar sind. Die Initiative Industrie 4.0 ist daher auch als Treiber des IoT in der Produktion zu verstehen.

4.0 Bedeutung von Industrie 4.0 für das gesetzliche Messwesen

Mit dem neuen Mess- und Eichgesetz (MessEG) [9] wurde ein innovationsoffenes Gesetz geschaffen, das u. a. erstmals eine rechtliche Grundlage für an das Internet angebundene Messgeräte schafft. Fernabfragen über beliebige Endgeräte, Teilbefundprüfungen (*Remote Diagnostic*), Software-Aktualisierung, sogar Fernkalibrierung, -instandsetzung und -wartung (*Remote-Maintenance*) über das Internet sind auf dieser Grundlage möglich geworden. Das neue MessEG wirkt so als Innovationstrigger im Messwesen. Die sogenannten intelligenten Messsysteme, *vulgo Smart Meter*, stellen einen ersten Schritt in Richtung des „virtualisierten" Messgerätes dar, bestehend aus einem rudimentären physikalischen Sensor mit einer miniaturisierten Kommunikationseinheit und der Implementierung der Sensorfunktionalität in Software. In einem nächsten Schritt die Software, den Datenspeicher und die dazugehörige Anzeige virtuell in der Cloud verfügbar zu machen, ist nur folgerichtig. Erste Marketingkonzepte der Messgerätehersteller liegen hierfür bereits vor.

In der folgenden Analyse soll insbesondere zwischen den intelligenten Produktionsprozessen und dem intelligenten Produkt auf dem Markt unterschieden werden.

4.1 Smart Factory

In vielen Fällen stellt eine Prüfung eines Baumusters und der dazugehörigen technischen Unterlagen im Rahmen der Modul-B-Konformitätsbewertung [8] die Grundlage für ein gesetzeskonformes Inverkehrbringen eines Messgeräts dar. Aufbauend auf einem von der für dieses Modul verantwortlichen Konformitätsbewertungsstelle ausgestellten Zertifikats erklärt der Hersteller selbstständig die Konformität der individuellen Seriengeräte. Die Sicherstellung der Konformität dieser Seriengeräte erfolgt – bspw. bei großen Stückzahlen – mittels eines im Rahmen von Modul D [8] zertifizierten Qualitätsmanagementsystems (QMS), das den Produktionsprozess und die fertigen Messgeräte überwacht. Im Zuge der vierten industriellen Revolution ist eine Ausweitung dieser Überwachungsmechanismen auf im Verkehr befindliche Geräte denkbar. So könnten Produktdaten vom Messgerät in der Verwendung zeitnah in den Produktionsprozess zurückgekoppelt und dort zur Produkt- oder Prozessoptimierung genutzt werden. Dieses Szenario soll im nachfolgenden Kapitel Smart Products näher beleuchtet werden. Zur Aufrechterhaltung einer Modul-D-Zertifizierung sind regelmäßige Audits notwendig. Die Einführung von Industrie 4.0 stellt damit ganz neue fachliche Anforderungen an diese Auditoren.

Mit Einführung der neuen technologieoffen gehaltenen Rechtsnorm wird der Weg geebnet für Dienste wie Ferndiagnose bzw. Fernbefundprüfung (§ 39 Abs. 3 MessEV) [10], Fernwartung (Softwareaktualisierung/Patch-Management über Netze, § 37 Abs. 6 MessEG i. V. m. § 40 MessEV) [9, 10], Fernkalibrierung sowie Fernrezertifizierung. Gleichzeitig können Technologien zum Einsatz kommen, wie sie bereits im Mobilfunk Einsatz finden (Wahl von Ausweichknoten, Selbstheilung von Netzen, Ad-hoc-Netzwerke). Selbstverständlich steigt damit auch das Anforderungsniveau an die Konformitätsbewertung solcher Technologien. In der klassischen Sichtweise auf ein Messgerät, wie sie bisher bei der Konformitätsbewertung Anwendung findet, ist beim Baumuster die Kette zwischen Sensor, Datenerfassung, Datenverarbeitung, Speicherung, Übertragung und Anzeige der Messwerte geschlossen. Entweder wird dabei eine Sicherung der Hardware eingesetzt oder es kommen Methoden der Ende-zu-Ende-Sicherung bzw. des *Direct Trust* zum Einsatz.

Während der Produktion in einer Smart Factory kann das Messgerät oder -system ständig umkonfiguriert werden, um das individuelle Wunschziel zu erreichen. Bspw. kann das Gerät um zusätzliche Schnittstellen erweitert werden oder Teile der Funktionalität (Speicherung, Anzeige) werden in andere Komponenten ausgelagert. Damit verlieren die klassischen Sicherungsansätze ihre Wirksamkeit, da die Grenzen des Messgeräts bzw. des Systems nicht zu jeder Zeit klar definiert sind. Ein möglicher Ausweg bestünde in der Aufteilung des Messgeräts in Module bzw. Komponenten, die separat zur Konformitätsbewertung vorgestellt werden. Jede dieser Komponenten besäße dann eine Vielzahl von Kommunikationsschnittstellen, um eine schnelle Netzwerkanbindung und Interoperabilität mit anderen Komponenten zu erzielen. Jede Einzelkomponente müsste weiterhin die wesentlichen Anforderungen der MessEV bzw. der MID separat erfüllen. Gleiches würde jedoch auch für mögliche Kombinationen von Komponenten oder Modulen gelten. Diese müssen sich regelmäßig an neue Umgebungsbedinungen anpassen können, verfügbare Kommunikationspartner sowie anstehende Aufgaben identifizieren und ggf. Wege zum Zielknoten auswählen. Die ständige Neukonfiguration eines Messsystems erlaubt dabei das Weiterleiten von Daten über individuelle Netzknoten (Ad-hoc-Netzwerke), wodurch Engpässe vermieden werden und der Datenverkehr besser verteilt werden kann als in zentral gesteuerten Verteilnetzen. Hier sollte festgehalten werden, dass im Rahmen von Industrie 4.0 diese Neukonfiguration sowohl während der Produktion als auch nach dem Inverkehrbringen regelmäßig notwendig sein kann.

Selbstverständlich ergeben sich aus den gerade beschriebenen Szenarien auch neue Aufgabenstellungen für das gesetzliche Messwesen. Es müssen Regeln für Teilsysteme und Einzelkomponenten identifiziert werden. Weiterhin müsste die Konformitätsbewertung so ausgelegt werden, dass auch die Konformität von verschiedenen und ggf. im Vorhinein nicht bekannten Kombinationen von Komponenten stets gewährleistet ist. Schließlich wird es notwendig sein, neue Prüfverfahren für Seriengeräte im Markt zu etablieren, da diese möglicherweise nicht mehr nach der Inbetriebnahme aus ihrem „Ökosystem“ (siehe Smart Meter Gateway [22]) entfernt werden können.

4.2 Smart Products außerhalb der Smart Factory

Die in der Smart Factory entstandenen Produkte sind mit zusätzlichen Sensoren, Intelligenz und Kommunikationsmöglichkeiten ausgestattet. Intelligente Produkte sind damit eindeutig identifizierbar, jederzeit lokalisierbar, kennen ihre Historie, ihren aktuellen Zustand und alternative Wege zum Zielzustand. Die durch Sensoren bereitgestellten Umgebungsinformationen lassen sich über cloudbasierte Plattformangebote sammeln (*Big Data*), filtern, aggregieren und nutzergerecht präsentieren (*Smart Data*) und auf dieser Grundlage

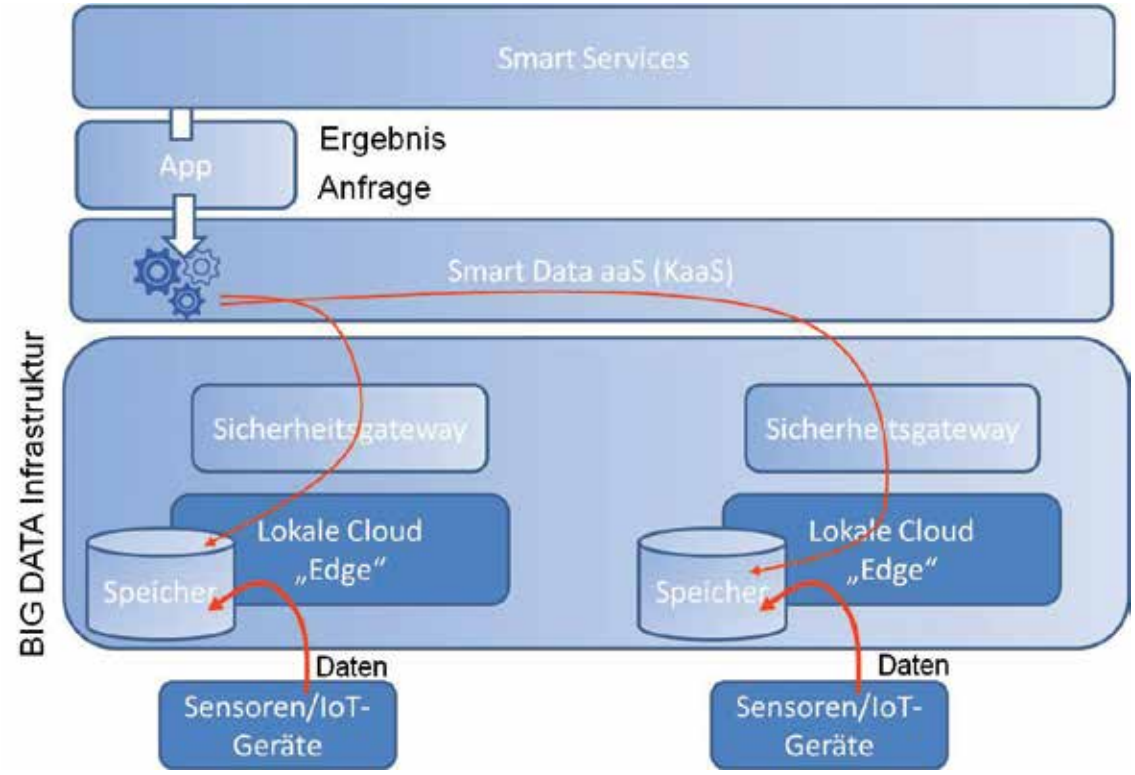

Bild 2:
Vom Sensor zum Smart Service

im Markt über *Smart Services* für neue Geschäftsmodelle nutzen (siehe Bild 2). Möglichkeiten für den Einsatz von Smart Services reichen dabei von spezifischen Einzelfunktionen über die Entscheidungsunterstützung bis hin zur Steuerung komplexer Systeme. Die Potenziale von Smart Services werden in Deutschland bisher erst in Ansätzen ausgeschöpft [23]. So könnten die Umgebungsbedingungen am Einsatzort durch zusätzliche, kostengünstige Sensoren, wie z. B. für Druck, Temperatur, Medienparameter wie die Wasserhärte, den Ort, etc., kontinuierlich ermittelt werden. Damit lassen sich z. B. Verschleißerscheinungen frühzeitig erkennen oder prognostizieren. Auf diese Weise könnte man die festen Eichgültigkeitsdauern durch dynamische, parameterabhängige Einsatzperioden der Messgeräte ersetzen (*predictive maintanance*).

Digitale Produktgedächtnisse zeichnen in Zukunft Daten aus Fertigung, Logistik, Nutzung und Entsorgung auf und stellen sie für die Produkt- und Prozessoptimierung zur Verfügung. Diese enthalten u. a. das Wissen des Herstellers über seine internen Optimierungsprozesse oder die Fertigungsabweichungen der einzelnen Prozessschritte und sind entsprechend wertvoll und damit schützenswert. Mit der Fragestellung, wie solche Geheimnisse mit informationstechnischen Maßnahmen kostengünstig zu schützen sind, beschäftigt sich das gesetzliche Messwesen bei der Konformitätsbewertung von Software in Messsystemen bereits heute. Solche wertvollen Daten nicht am Produkt, sondern in der Cloud verfügbar zu machen, ist naheliegend. Damit kann z. B. auch Produktpiraterie verhindert werden.

5.0 Lösungsangebote der Metrologie

5.1 Referenzarchitekturen für die virtualisierte Messtechnik

Quasi alle Bausteine von Industrie 4.0 gehören jetzt schon zum Betätigungsfeld der PTB. Unter anderem sind dabei eine Referenzarchitektur sowie Handlungshilfen für eingebettete Systeme als Bestandteil von Messgeräten entstanden [24]. Diese Systemarchitektur ist in der Lage, die intrinsische Sicherheit des Messgeräts zu garantieren und damit eine hohe Widerstandsfähigkeit gegen äußere Angriffe zu gewährleisten. Durch den Einsatz eines formal verifizierbaren Separationskerns mit darauf laufenden virtuellen Maschinen können Angriffe auf das Betriebssystem über Hardware- und Softwareschnittstellen (bspw. über das Internet) effektiv unterbunden werden. Dies ermöglicht zusätzlich eine schnelle Austauschbarkeit von Komponenten im Sinne eines *Plug&Measure* [24]. Weiterhin garantiert die Systemarchitektur, dass Einzelkomponenten, die aufgrund eines Angriffs ausfallen, nicht automatisch zum Ausfall des Gesamtsystems bzw. der Messung führen. Gleichzeitig können Ausfälle, die das Hauptziel von Hackerangriffen auf netzwerkangebundene Geräte darstellen, durch eine dynamische Rekonfiguration oder durch den Ersatz von virtuellen Komponenten schnell kompensiert werden. In ähnlicher Art und Weise wie bei den eingebetteten Systemen, erarbeitet die PTB derzeit sichere Referenzarchitekturen für den Einsatz des Cloud Computings im gesetzli-

chen Messwesen [25]. Mit der Referenzarchitektur selbst soll den Konformitätsbewertungsstellen und Marktaufsichtsbehörden eine rechtskonforme Lösung und harmonisierte Prüfanweisungen bereitgestellt werden, während die Architektur dem Hersteller hinreichend Spielraum für eigene Innovationen und somit Raum zur Abgrenzung gegenüber Mitbewerbern einräumt.

Eine vollständige Konformitätsbewertung des gesamten *Software-Stacks* eines Cloud-Dienstleisters erscheint schon aufgrund des Aufwandes als unrealistisch. Stattdessen kann Vertrauen in die Cloud-Infrastruktur bspw. durch die Berücksichtigung von Zertifikaten (ISO 2700X, Notfallbehandlung, Verfügbarkeit, Vertraulichkeit, etc.) sowie durch eine sinnvolle Vertragsgestaltung (*Service Level Agreement*, Serverlokalisierung, Datentransfer, etc.) zwischen Cloud-Nutzern und Cloud-Dienstleistern gewonnen werden [25].

Zusätzlich können existierende technische Sicherungsmethoden genutzt werden, um bspw. eine vertrauenswürdige, vertrauliche Kommunikation zwischen Messgeräte- und Softwarekomponenten zu garantieren (TLS, VPN, Virtualisierung, *Sensor-Device-Pairing*, etc.), ohne den Software-Stack berücksichtigen zu müssen [25]. Damit kann das System dann unabhängig von der Hardware bewertet werden, während zukünftig neue Sicherungsmechanismen gegen sich ständig weiterentwickelnde Bedrohungsszenarien (Manipulation durch nicht vertrauenswürdige Administratoren, Angriff aus einer virtuellen Maschine heraus in eine benachbarte virtuelle Maschine) zu entwickeln sein werden.

5.2 Durchbrechen des Rezertifizierungskreislaufs

Die fortgeschrittene Hochintegration kann genutzt werden, um die Rezertifizierungskette zu ersetzen und dynamisch zu halten. Dieser Prozess soll hier kurz beschrieben werden. Nach vorbestimmten Zeiten müssen gesetzlich geregelte Messgeräte einer Prüfung, einer sogenannten Nacheichung, unterzogen werden. Dazu werden die Messgeräte oftmals ausgebaut und bei öffentlichen Stellen geprüft, nachjustiert oder repariert und danach wieder verwendet. Diese Re-Kalibrierung/Re-Zertifizierung ist kosten- und logistikintensiv. Heute sind jedoch ganze Labore auf einer Platine integrierbar, sogenannte *Lab on a Chip* [26]. Bspw. hat das NIST die Initiative *NIST on a Chip* gestartet [27], um rückgeführte Standards für die SI-Einheiten in einzelnen Messgeräten zur Verfügung zu stellen. So sind heute schon Atomuhren auf Chip-Größe kommerziell erhältlich (Symmetricom CSAC SA.45s chip scale atomic clock) [28]. Solche selbstkalibrierenden Systeme sparen Zeit und Kosten. Ein Messgerät könnte sich so regelmäßig rekalibrieren und die Kalibrierdaten via Internet an die Überwachungsbehörde senden, welche dann anhand der übermittelten Daten und durch Abgleich bspw. mit einem virtuellen Modell des Messgeräts selbst entscheiden kann, ob eine Befundprüfung vor Ort noch zusätzlich notwendig ist.

5.3 Eine virtualisierte Qualitätsinfrastruktur: die Metrology Cloud

Auch Messgeräte, die im europäischen Binnenmarkt jeweils nationalen oder europäischen Regelwerken unterliegen, werden in Zukunft im Rahmen von Industrie 4.0 gefertigt und werden ihre Intelligenz und Kommunikationsmöglichkeiten, die sie im Produktionsprozess einsetzen, auch im Markt verwenden. Konformitätsbewertungsprozeduren, Wartung und Instandsetzungsmaßnahmen, Markt- und Verwendungsüberwachung oder Befundprüfungen werden internetbasiert vereinfacht werden, da dies durch neue nationale und europäische Rechtsnormen unterstützt wird. Damit bietet sich die Chance, sowohl Fertigungsprozesse in der Industrie, als auch die Tätigkeit der Marktaufsichtsbehörden effizienter zu machen. Die Qualität und das Vertrauen in die Messgeräte im europäischen Binnenmarkt wird sich erhöhen, da sich deren Wartung und Reparatur sowohl erheblich vereinfacht, als auch zeitnah und ortsabhängig erfolgt und nicht mehr unspezifisch anhand fester Zeiten: Eingebettete Systeme stellen zukünftig vollständige Transparenz über den Zustand aller Messgeräte her; bevor oder sobald Verschleißerscheinungen auftreten, bestellen diese ihre Ersatzteile selbstgesteuert oder kalibrieren sich neu (predictive maintenance). Alle Marktakteure, Konformitätsbewertungsstellen und Marktaufsichtsbehörden könnten intern über die Metrology Cloud agieren, einer virtualisierten Qualitätsinfrastruktur, die als Informationsbasis und sicherer Zugriffsort auf die netzangebundenen Messgeräte in der Verwendung fungiert (s. Bild 3). Qualitätsinfrastruktur bezeichnet dabei die Gesamtheit aller Elemente des Mess-, Normen- und Prüfwesens, des Qualitätsmanagements, der Zertifizierung und der Akkreditierung, die besonders für die Konformitätsbewertung wesentlich sind. Qualitätsinfrastruktur ist notwendig, um technische Handelshemmnisse überwinden zu können. Sie schafft damit wichtige Voraussetzungen zur verstärkten Integration der Partnerländer in das internationale Handelssystem [6]. Die PTB könnte mit ihrer herausragenden Stellung in der europäischen Metrologielandschaft den Aufbau einer solchen Metrology Cloud für das Mess- und Prüfwesen koordinieren und weitere entscheidende Impulse liefern. Die dabei anfallenden Daten der Messgeräte (allein 160 Mio. in

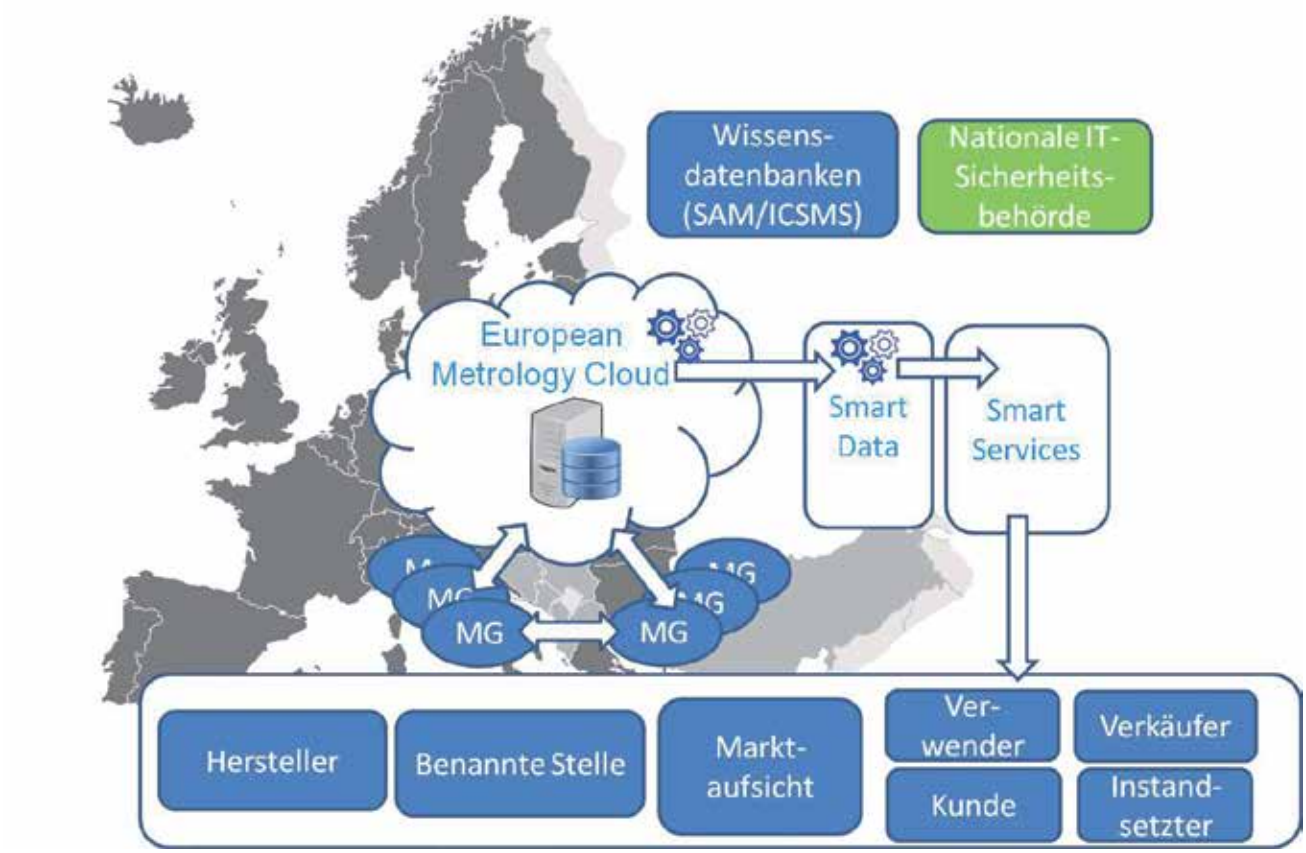

Bild 3:
Die Metrology Cloud – eine virtualisierte Qualitätsinfrastruktur für Messgeräte (MG)

Deutschland) und der Marktteilnehmer könnten genutzt werden, um die Prozesse bei allen Beteiligten, z. B. über Smart Services, weiter zu verschlanken, neue Geschäftsmodelle anzubieten und die Harmonisierung in Europa weiter voranzutreiben.

Im Rahmen einer Konformitätsbewertung kann das in der Industrie 4.0 vorgesehene digitale Abbild eines Messgeräts oder einer Komponente bereits genutzt werden, um den Prüfvorgang in logische Gruppen zu zerlegen und auf mehrere verfügbare Prüfer zu verteilen. So ließen sich erhebliche Zeitersparnisse gegenüber der bisherigen Prüfpraxis realisieren, bei der bspw. jeweils ein Softwareprüfer ein in sich geschlossenes Gerät oder System beurteilt. Weiterhin ließen sich die virtuellen Messgerätemodelle bei der Verwendung von Standardlösungen in Teilen selbst automatisch prüfen. Dabei läge die eigentliche Hauptaufgabe nicht mehr in der Konformitätsbewertung des Modells, sondern in der Überprüfung, ob virtuelles Abbild und Messgerät bzw. -komponente tatsächlich identisch sind. Ist dieser Nachweis einmal erfolgt, ließe sich eine Diskrepanz zwischen dokumentiertem und realem Messgerät, wie sie bisher regelmäßig auftritt, faktisch ausschließen. Weiterhin wären mithilfe eines virtuellen Messgeräts nun auch simulierte Prüfungen von Extremfällen für Hard- und Software denkbar, die bisher sowohl aus Zeit- als auch aus Kostengründen unmöglich waren.

5.4 Individualisierung der Produktion

Ein Ziel im Rahmen von Industrie 4.0 ist u. a. die individualisierte Produktion bis hin zur Losgröße 1. Die Konformitätsbewertung solcher Einzelstücke berücksichtigt sowohl die europäische Richtlinie als auch das nationale Recht über das sogenannte Konformitätsbewertungsmodul G (Konformität auf der Grundlage einer Einzelprüfung). Wird jedoch ein Massenprodukt wie bspw. ein Energiezähler oder eine Waage produziert, stellt sich die Frage, welcher Spielraum für Individualisierung bleibt. Hier könnten zusätzliche Eigenschaften durch die Teile der Software bereitgestellt werden, die neben der Messfunktion weitere Funktionen erfüllen. Es wird in der MessEV gefordert, dass u. a. die für die messtechnischen Merkmale entscheidende Software identifizierbar ist und durch die zugehörige Software nicht in unzulässiger Weise beeinflusst werden darf [8]. Wenn diese „Härtung“ der metrologischen Software sichergestellt ist, kann der Hersteller frei Individualisierungsmaßnahmen treffen, z. B. kundenspezifische Services anbieten, die auf Kopien der Messdaten aufsetzen. Der WELMEC Software Guide 7.2 : 2015 gibt hierfür wertvolle technische Hinweise zur Umsetzung solch einer Modularisierung [12]. Die Konformitätsbewertung würde im Fall von Massenprodukten über die gängige Kombination von Modul B (Prüfung des Entwurfs) + Modul D (Qualitäts-

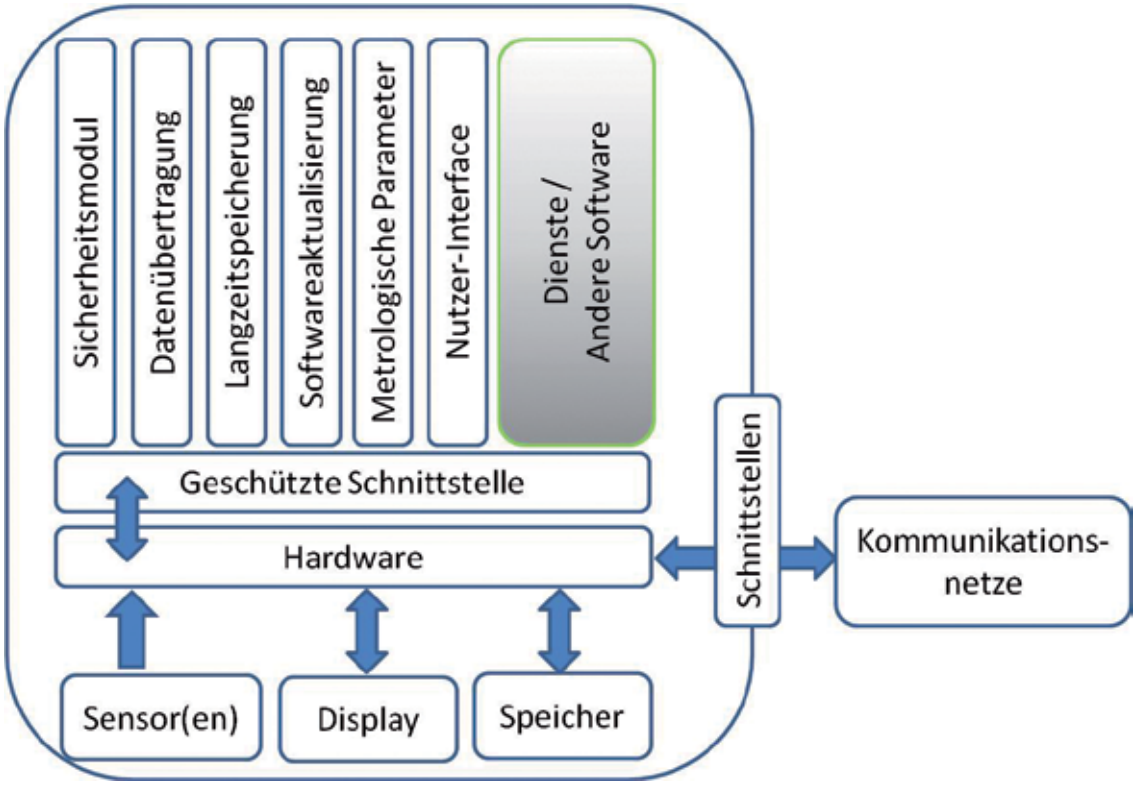

Bild 4:
Vorschlag einer modularen, individualisierten Systemarchitektur für Messgeräte

sicherung bezogen auf den Produktionsprozess) durchgeführt. Sollte eine Trennung der für die messtechnischen Merkmale entscheidenden Software und sonstiger Software nicht nachgewiesen werden können, so wird bisher die gesamte Software des Messgeräts festgeschrieben. Änderungen an der „sonstigen Software" sind damit nur mit erneutem Durchlaufen einer Konformitätsbewertung sowie einer kostenpflichtigen Rezertifizierung möglich. Auch wenn die rechtlichen Rahmenbedingungen zwischen beiden Softwareteilen die gleichen bleiben sollten, ließe sich doch das Konzept einer virtuellen Qualitätsinfrastruktur nutzen, um die erneute Konformitätsbewertung erheblich zu beschleunigen. So könnte wieder auf Basis des virtuellen Messgeräteabbilds eine Übereinstimmung des messtechnischen Teils der Software mit der ursprünglich bewerteten Software quasi automatisch nachgewiesen werden. Ebenso ließen sich schnell alle möglichen Interaktionen zwischen beiden Softwareteilen entdecken, sodass die Prüfung sich dann auf diesen Bereich allein beschränken würde.

5.5 Systemmodularisierung und Risikoindividualisierung

Eine Produktindividualisierung wird sich zunächst auf die Zusammenstellung von modularen technischen Einheiten und deren Funktionsvarianten beziehen. So lassen sich auch intelligente Messsysteme in grundlegende technische Einheiten zerlegen (s. Bild 4).

Beispielsweise kann die Verarbeitung der Messdaten auf unterschiedlichen Hardwaremodulen erfolgen. Entweder kommen hier Mikroprozessoren oder eingebettete Systeme zum Einsatz. Erstere sind für sehr spezifische Messgeräte und Messfunktionen vorbehalten, Letztere bieten die ganze Angebotspalette der heutigen Informationstechnologie an, womit eine Individualisierung noch einfacher ermöglicht wird. Weitere modulare Einheiten sind die Art der Messdatenspeicherung, insbesondere über längere Zeit, die Ausführung der Kommunikationseinheit(en) und die Übertragungseinheit zur Anbindung an offene Kommunikationsnetze sowie die Modularisierung der Software in den rechtlich relevanten und den nicht rechtlich relevanten – also freien – Teil (sonstige Software / Dienste). Diese beiden Teile kommunizieren über ein entsprechendes sicheres Interface. Für eine Fernwartung (Remote-Maintenance), insbesondere für ein *Patch-Management*, ist ein entsprechender Download-Mechanismus als Modul vorzusehen. Dazu können auch Module für die Berücksichtigung messgerätespezifischer Besonderheiten vorgesehen werden. So werden Gasmessgeräte andere Anforderungen an die Informations- und Kommunikationstechnolgie stellen als zum Beispiel Messgeräte für thermische Energie. Wird ein Messgerät nach obigem Schema entworfen, wird die Individualisierung im gesetzlichen Messwesen schon heute unterstützt (s. Bild 4).

Die WELMEC-Arbeitsgruppe 7 „Software“ hat einen auf europäischer Ebene harmonisierten Leitfaden zur metrologischen Sicherung von softwaregesteuerten Messgeräten entwickelt, der für die oben genannten Module entsprechende technische Umsetzungen anbietet [12]. Bei Einhaltung dieser Leitlinien wird zum einen die Einhaltung der wesentlichen Anforderungen der europäischen Richtlinie 2014/32/EU angenommen. Zum anderen wird sichergestellt, dass nach erfolgreicher Konformitätsbewertung die Messgeräte im Feld von der Markt- und Verwendungsaufsicht der europäischen Mitgliedsstaaten akzeptiert werden. Alle weiteren Funktionen und Services lassen sich um diesen Rahmen herum individualisieren.

5.6 Adäquate technische Sicherheitsanforderungen an Komponenten von Messsystemen

Durch die immer weiter fortschreitende Vernetzung der IT und durch die individuelle Autonomie der Produktionssysteme ergeben sich vielfältige Angriffsmöglichkeiten für Manipulationsversuche, für das Ausspähen vertraulicher Daten oder gleich für die Sabotage eines ganzen Produktionsprozesses. Der WELMEC Guide 7.2, welcher vorrangig einen angemessenen Manipulationsschutz zum Ziel hat, berücksichtigt das individuelle Bedrohungspotenzial einzelner Messgeräte und klassifiziert die unterschiedlichen Messgerätearten in Risikoklassen. Über diese wird dann das Schutzniveau des gesamten Gerätes einheitlich festgeschrieben. Aufgrund dieser Pauschalisierung und aus Furcht vor der falschen Einschätzung einer Bedrohung kann es bei den Konformitätsbewertungsstellen zu vier unterschiedlichen Reaktionen auf neue Technologien kommen: Ablehnung der Neuerung, Veränderung einer Lösung, sodass sie bekannten Lösungen entspricht, Überfrachtung mit Sicherheitsanforderungen oder schließlich – zu geringe und ungenügende Sicherheitsanforderungen. Alle vier Szenarien können, wenn sie unbegründet sind, Innovationshemmnisse darstellen.

Gemäß MID [8] und MessEG [9] bzw. der dazugehörigen Mess- und Eichverordnung ist für Messgeräte und -systeme ein angemessenes, vergleichbares und damit wirtschaftlich vertretbares Sicherheitsniveau herzustellen. Einen Baustein, der es ermöglicht, das Schutzniveau zu definieren, stellt die von MID und MessEG geforderte Risikoanalyse und -bewertung dar. Dabei ist zu beachten, dass metrologische und IT-Sicherheit zwar viele Methoden miteinander teilen, grundsätzlich aber unterschiedliche Anforderungen formulieren. Insbesondere bei der Konformitätsbewertung von Messsystemen, die neuartige Technologien verwenden und zu großen Teilen in Software realisiert werden, wird die Risikoanalyse zukünftig einen großen Teil der Bewertungsarbeit ausmachen. Um von Anfang an die Objektivität und Vergleichbarkeit dieser Analyse zu gewährleisten, erscheint die Verwendung internationaler Standards sowie einschlägiger EU-Richtlinien zur Sicherheits- und Risikobewertung von IKT-Systemen sinnvoll, z. B. der *Common Criteria* (ISO 15408), der ISO 27005, ISO 18045 und der RAPEX-Richtlinie (2010/15/EU). Auf diese Weise entstehen objektive Vorgehensweisen zur Bewertung aktueller Bedrohungen, die ein Risiko für Messgeräte darstellen, z. B. durch deren Anbindung an offene Kommunikationsnetze. Die PTB entwickelt aktuell auf Basis solcher akzeptierter Industriestandards ein innovationsoffenes, objektives und damit vergleichbares Verfahren zur Bewertung des aus aktuellen Bedrohungen resultierenden Risikos für Messgeräte und hat dieses bereits auf Bitten der Hersteller testweise in Konformitätsbewertungsverfahren angewendet [29]. Die schützenswerten Güter ergeben sich dabei aus den Anforderungen der Rechtsnormen, die zur Realisierung einer Bedrohung notwendigen technischen Schritte (Angriffsvektoren) ergeben sich aus Erfahrungswerten der Konformitätsbewertungsstellen, der Marktaufsicht und anderer kompetenter Stellen im Bereich der IT-Sicherheit, die Angriffsszenarien bspw. in Studien veröffentlichen. Es ist hier die Aufgabe, z. B. der PTB, die für das gesetzliche Messwesen aktuell relevanten Angriffsvektoren herauszufiltern, anzuwenden und auf einem aktuellen Stand zu halten [29].

Eine Risikobewertung von einzelnen funktionalen Modulen des Messgerätes und deren Kombinationen hat den Vorteil, dass einzelne Module in eine geringere Risikoklasse fallen können als andere Module. Weiterhin wäre es möglich, dass nur vereinzelt Module den Anforderungen einer erweiterten Risikoklasse genügen müssen, z. B. aufgrund neuer Bedrohungsszenarien. Insgesamt wird sich hier, neben Kostenersparnissen in der Entwicklung und Fertigung, eine realistischeres Abbild des notwendigen Schutzbedarfs versprochen. Zukünftig ließe sich auch die Risikobewertung deutlich vereinfachen, da virtuelle Messgeräte im Labor automatisch einer großen Anzahl von Angriffen ausgesetzt werden können, deren Einzelprüfung bisher die technischen Möglichkeiten einer Konformitätsbewertungsstelle übersteigt. Dadurch würde dann auch die bisherige Unsicherheit bei der Einschätzung des Risikos durch einen Bewerter ersetzt werden – durch ein fast hundertprozentig objektives Bewertungsmaß.

5.7 Patch-Management à la Industrie 4.0

Die Aktualisierung von Software in Messgeräten ist im neuen nationalen Rechtsrahmen geregelt

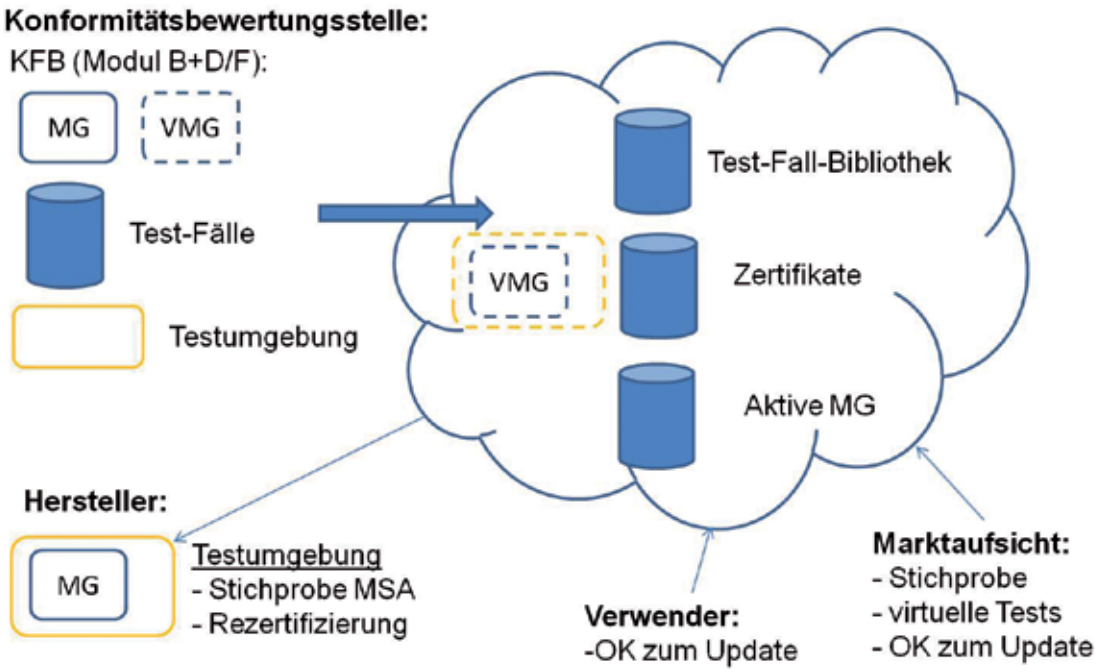

Bild 5:
Zusammenspiel beim Patch-Management à la Industrie 4.0

und orientiert sich an dem europäisch harmonisierten Verfahren, das im WELMEC Guide 7.2 beschrieben wird [12]. Darauf aufsetzend lässt sich unter Verwendung der oben angesprochenen Möglichkeiten durch IoT und Cloud Computing ein Patch Management à la Industrie 4.0 entwerfen.

Während der Konformiätsbewertung im Rahmen von Modul B wird dem Baumuster die Eignung für die Softwareaktualisierung bescheinigt und es erhält eine individuelle Kennung (ID). Die Bestätigung der Eignung für eine Softwareaktualisierung beinhaltet die Prüfung folgender Eigenschaften: selbstständiger Ablauf der Aktualisierung, Gewährleistung der Authentizität und Integrität eines Updates sowie die Protokollierung aller Aktualisierungsversuche, also die Existenz und Funktion eines gesicherten Logbuchs. Die individuelle ID des Messgerätes wird zusammen mit messgerätebezogenen Daten und den Ergebnissen der Konformitätsbewertung oder einem elektronischen Konformitätszertifikat, in der Metrologie-Cloud gespeichert.

Wird dieses Messgerät jetzt in Verkehr gebracht, meldet es sich selbstständig in dieser Metrologie-Cloud an und macht sich als aktives Messgerät in einer Datenbasis der Cloud kenntlich. Die Marktaufsicht wird in diesem Moment automatisch informiert, was ebenfalls über eine Datenbasis in der Metrologie-Cloud geschehen kann. In dieser Messgeräte-Datenbasis wird das Messgerät durch spezifische Daten repräsentiert. Dazu gehören insbesondere die ID, die GPS-Koordinaten, der Inhalt der Konformitätsbescheinigung, Verwenderdaten, Daten der Konformitätsbewertungsstelle, die aktuelle Softwareversion, etc. (MID Artikel 18 und Annex I 9.3). Zusätzlich wird ein virtuelles Modell, eine modellierte Repräsentation, des Messgerätes dort abgelegt. Diesem Model wurde im Rahmen der Konformitätsbewertung bescheinigt, eine äquivalente Repräsentation des Messgerätes darzustellen. Entsprechende Testfälle werden im Rahmen der Konformitätsbewertung festgelegt, die auf dem realen und dem virtuellen Messgerät ablaufen können. Wird nun eine Softwareaktualisierung dieses Messgerätes benötigt, greift der Antragsteller auf die Datenbasis der Messgeräte zu, indiziert diese und hinterlegt das entsprechende Update. Eine virtuelle Repräsentation des Updates wird an dem virtuellen Messgerät durchgeführt, d. h. es entsteht ein neues Messgerät. Über das automatische Durchspielen der Testfälle an diesem aktualisierten Modell wird die Konformität zu den grundlegenden Anforderungen nachgewiesen. Nach positiver Bestätigung und Zustimmung des Verwenders erfolgt die Aktualisierung aller indizierten Messgeräte. Stichprobenartig und randomisiert kann das Update zuvor auf reale Baumuster der Messgeräte beim Hersteller aufgespielt werden. Diese befinden sich in einer gesicherten Testumgebung, auf der automatisiert die obigen Testfälle durchgespielt werden. Die Landeseichbehörde hat hier Fernzugriff, um diesen Test zu initiieren und die Ergebnisse abzurufen. Ebenso lässt sich auf diese Weise eine Konformitätsbewertung der aktualisierten Bauart stichprobenartig durchführen, nachdem sie virtualisiert auf dem Model durchgeführt wurde. Ein Zugriffsmanagement der involvierten Partner ist hierfür Voraussetzung. Mit so einem Verfahren lassen sich Rezertifizierungen kostengünstig und flächendeckend im Feld durchführen (s. Bild 5).

6.0 Zusammenfassung

Das gesetzliche Messwesen schafft eine der Voraussetzungen, um überhaupt qualitativ hochwertige Produkte fertigen zu können [6]. Nur was gemessen werden kann, kann auch in gleicher Güte produziert werden. Industrie 4.0 birgt neue Herausforderungen und Chancen für das gesetzliche Messwesen in der Smart Factory und durch die neuen Funktionalitäten, die die Smart Products im Markt bereitstellen.

Dieser Artikel hat die Implikationen und Chancen von Industrie 4.0 für das gesetzliche Messwesen beleuchtet. Dazu wurden zunächst die wesentlichen Technologiefelder, die Industrie 4.0 ausformen, bzgl. ihres Reifegrades begutachtet. Danach wurden die neuen Herausforderungen an das gesetzliche Messwesen, die die Smart Factory und die dann im Markt befindlichen Smart Products mit sich bringen, diskutiert. Antworten des gesetzlichen Messwesens auf die von Industrie 4.0 formulierten Ziele, die heute schon gegeben werden können, wurden abschließend dargestellt.

Durch die Entwicklung und Bereitstellung rechtskonformer Referenzarchitekturen für die Technologiefelder, die Industrie 4.0 ausformen und ein adäquates Sicherheitsniveau garantieren, kann ein Beitrag zu deren Technologieakzeptanz geleistet werden. Damit haben Hersteller eine Orientierungsmöglichkeit, können den Prozess der Konformitätsbewertung zügiger durchlaufen und die Nachbaugeräte im Markt werden von den Marktaufsichtsbehörden akzeptiert. Solche Architekturen, wie sie zurzeit von der PTB entwickelt werden, tragen dazu bei, Innovationshemmnisse abzubauen und, sobald sie den europäischen Harmonisierungsprozess in der WELMEC durchlaufen haben, im europäischen Binnenmarkt nichttarifäre Handelshemmnisse zu verringern.

Auf Grundlage der technischen Möglichkeiten lassen sich Vorschläge für die Vereinfachung von etablierten Prozessen vorschlagen, wie eine virtualisierte Qualitätsinfrastruktur für Europa – die Metrology Cloud. Diese würde eine technologisch fixierte Harmonisierung der Prozesse aller Partner ermöglichen.

Referenzen

[1] Digitale Agenda 2014–2017, 2014; http://www.bmwi.de/DE/Mediathek/publikationen,did=650294.html (Letzter Zugriff am 28.11.2016)

[2] BDI Leitfaden – *Die Industrie auf dem Weg in die „Rechnerwolke", Cloud Computing – Wertschöpfung in der digitalen Transformation*, 2013; http://www.bdi.eu/download_content/InformationUndTelekommunikation/Cloud_Computing.pdf (Letzter Zugriff am 28.11.2016)

[3] Intel IT Center, *Big Data in the Cloud: Converging Technologies,* 2014; http://www.intel.com/content/dam/www/public/us/en/documents/product-briefs/big-data-cloud-technologies-brief.pdf (Letzter Zugriff am 28.11.2016)

[4] *Die neue Hightech-Strategie*, 2014; http://www.bmbf.de/pub_hts/HTS_Broschure_Web.pdf (Letzter Zugriff am 28.11.2016)

[5] *Umsetzungsstrategie Industrie 4.0,* Ergebnisbericht der Plattform Industrie 4.0, 2015; http://www.bmwi.de/BMWi/Redaktion/PDF/I/industrie-40-verbaendeplattform-bericht,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf (Letzter Zugriff am 28.11.2016)

[6] F. Thiel und M. Loy: *Die nationale und internationale Bedeutung einer Qualitätsinfrastruktur – Qualitätssicherung für Verbraucher*, Wirtschaft und Staat, Schlaglichter der Wirtschaftspolitik – Monatsbericht Dezember 2012, Bundesministerium für Wirtschaft und Technologie (BMWi), 14–20, 2012; https://www.bmwi.de/Dateien/BMWi/PDF/Monatsbericht/Auszuege/12-2012-I-3,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf (Letzter Zugriff am 1.12.2016)

[7] N. Leffler und F. Thiel: *Im Geschäftsverkehr das richtige Maß – Das neue Mess- und Eichgesetz*, Schlaglichter der Wirtschaftspolitik, November 2013, Bundesministerium für Wirtschaft und Technologie (BMWi), 2013; http://www.bmwi.de/DE/Mediathek/publikationen,did=599710.html (Letzter Zugriff am 28.11.2016)

[8] Directive 2014/32/EU of the European Parliament and of the Council from 26 February 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of measuring instruments, 2014; http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32014L0032 (Letzter Zugriff am 28.11.2016)

[9] Mess- und Eichgesetz vom 25. Juli 2013 (BGBl. I S. 2722, 2723); http://www.gesetze-im-internet.de/messeg/index.html (Letzter Zugriff am 28.11.2016)

[10] Mess- und Eichverordnung vom 11. Dezember 2014 (BGBl. I S. 2010, 2011); http://www.gesetze-im-internet.de/messev/index.html (Letzter Zugriff am 28.11.2016)
[11] PTB-A50.8 Smart Meter Gateway, 2014; https://www.ptb.de/cms/fileadmin/internet/fachabteilungen/abteilung_q/q.3_gesetzliches_messwesen/q.31/ptb-a/PTB-A_50-08.pdf (Letzter Zugriff am 28.11.2016)
[12] WELMEC Guide 7.2: Software Guide (Measuring Instruments Directive 2014/32/EU); http://www.welmec.org (Letzter Zugriff am 28.11.2016)
[13] Organisation Internationale de Métrologie Légale (OIML), *General requirements for software controlled measuring instruments*, OIML D-31, 2008; http://workgroups.oiml.org/tcsc/tc-05/tc-05-sc-02/archives/D031-e08.pdf (Letzter Zugriff am 28.11.2016)
[14] http://www.industrialinternetconsortium.org (Letzter Zugriff am 28.11.2016)
[15] H. Chang et al.: *Bringing the cloud to the edge*, IEEE Conference on Computer Communications (INFOCOM WKSHPS), 2014; DOI: 10.1109/INFCOMW.2014.6849256
[16] Förderung von Forschungsinitiativen auf dem Gebiet „5G: Industrielles Internet“ im Rahmen des Förderprogramms „IKT 2020 – Forschung für Innovationen“; http://www.bmbf.de/foerderungen/26953.php (Letzter Zugriff am 28.11.2016)
[17] *Gartners 2014 Hype Cycle for Emerging Technologies Maps the Journey to Digital Business*; http://www.gartner.com/newsroom/id/2819918 (Letzter Zugriff am 28.11.2016)
[18] ARTEMIS Strategic Research Agenda, ARTEMIS SRA WG, 2006
[19] Studie *IT-Sicherheit für die Industrie 4.0 – Produktion, Produkte, Dienste von morgen im Zeichen globalisierter Wertschöpfungsketten,* 2015; http://www.bmwi.de/DE/Mediathek/publikationen,did=764200.html (Letzter Zugriff am 1.12.2016)
[20] *Discover New Opportunities with Cisco IoT System*; http://www.cisco.com/web/solutions/trends/iot/portfolio.html (Letzter Zugriff am 28.11.2016)
[21] C. Eckert, N. Fallenbeck: *Industrie 4.0 meets IT-Sicherheit: eine Herausforderung*, Informatik Spektrum, Vol. **38**, Issue 3, 217–223, 2015
[22] BSI Smart Metering System; https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/SmartMeter/smartmeter_node.html (Letzter Zugriff am 1.12.2016)
[23] BMWi-Fördermaßnahme 2015, *Smart Service Welt*; http://www.bmwi.de/DE/Themen/Digitale-Welt/Digitale-Technologien/smart-service-welt.html (Letzter Zugriff am 28.11.2016)
[24] D. Peters, M. Peter, J.-P. Seifert und F. Thiel: *A Secure System Architecture for Measuring Instruments in Legal Metrology*, published in Computers, Open Access Journal (ISSN 2073-431X), 2015
[25] F. Thiel, M. Esche, D. Peters und U. Grottker: *Cloud Computing in Legal Metrology*, submitted to EPJ, 2015
[26] *Lab on a Chip*; http://pubs.rsc.org/en/journals/journalissues/lc#!recentarticles&adv (Letzter Zugriff am 28.11.2016)
[27] *NIST on a Chip*; http://www.nist.gov/director/vcat/upload/NIST-on-a-Chip-Revolution-in-Measurement-Services-VCAT-October-2012.pdf (Letzter Zugriff am 28.11.2016)
[28] *Quantum™ SA.45s Chip Scale Atomic Clock*; http://www.microsemi.com/products/timing-synchronization-systems/embedded-timing-solutions/components/sa-45s-chip-scale-atomic-clock (Letzter Zugriff am 28.11.2016)
[29] M. Esche und F. Thiel: *Software Risk Assessment for Measuring Instruments in Legal Metrology*, accepted for Federated Conference on Computer Science and Information Systems (FedCSIS), 2015

Cyber-Security in Industrie 4.0

Jens Mehrfeld*

1 Einleitung

Die Welt der Automatisierung befindet sich im Umbruch. Die Vernetzung der Produktion und der Unternehmen nimmt immer weiter zu und zusätzliche Technologien kommen in der Fertigung zum Einsatz. „Menschen, Maschinen, Anlagen, Logistik und Produkte kommunizieren und kooperieren in der Industrie 4.0 direkt miteinander. Produktions- und Logistikprozesse zwischen Unternehmen im selben Produktionsprozess werden intelligent miteinander verzahnt, um die Produktion noch effizienter und flexibler zu gestalten.“[1]

Diese Ziele und Veränderungen stehen im Vordergrund, wenn über Industrie 4.0 (I40) geredet wird. Ein Thema, welches meist nur am Rande angesprochen wird, ist Security – hier im Sinne der Abwehr von Bedrohungen aus der IT- und Cyber-Welt. Es geht nicht nur wie in der konventionellen IT um den Schutz vor Spionage oder Datendiebstahl, sondern auch um die Gewährleistung der Verfügbarkeit und Integrität von Produktionsanlagen. In erster Linie gilt es, die mit Industrie 4.0 aufgrund der starken Vernetzung einhergehende Komplexität der Systeme beherrschbar zu machen und Risiken durch Angriffe zu minimieren.

Insgesamt stellt das Thema Cyber-Sicherheit eine Herausforderung (nicht nur im Rahmen von Industrie 4.0) dar. Dynamische Prozesse und Abläufe erfordern eine Berücksichtigung der Security von Beginn an. Dies betrifft Planung, Umsetzung und den späteren Betrieb. Das ist notwendig, um einen in jeglicher Sicht sicheren und zuverlässigen Betrieb zu ermöglichen. Cyber-Sicherheit ist daher einer der wesentlichen Grundbausteine von Industrie 4.0.

2 Herausforderungen aus Security-Sicht

Auf einige der Veränderungen durch Industrie 4.0 und vorhandene Rahmenbedingungen wird im Folgenden genauer eingegangen. Dabei werden auch mögliche Implikationen für die Security berücksichtigt. Der Einstieg erfolgt dazu über die sich abzeichnenden Veränderungen in der Produktion, geht über die Wertschöpfungsnetzwerke und endet bei den Bestandsanlagen und einer Betrachtung der Produktionsdaten.

2.1 Veränderungen in der Produktion

Wie auch bei der IT im Büroumfeld steigt die Leistungsfähigkeit von Automatisierungskomponenten kontinuierlich. So können diese mittlerweile deutlich mehr und komplexere Aufgaben erfüllen. Komponenten bieten neue und erweiterte Funktionen und haben die Möglichkeit, zunehmend autonomer zu agieren. Durch diese zusätzlichen Anwendungen und Dienste steigt die Komplexität im Blick auf Entwicklung und Konfiguration. Es gibt mehr Möglichkeiten, Fehler in beiden Bereichen zu machen. Die hierdurch entstehenden Schwachstellen können zu einem Ausfall der Komponente oder Maschine führen oder können durch einen Angreifer ausgenutzt werden. Die Auswirkungen können in diesem Fall deutlich schwerwiegender sein, da Manipulationen nicht zwangsläufig direkt erkennbar sind.

Neben den intelligenteren Komponenten selbst liegt ein anderer Trend in weitreichenden Zugriffen innerhalb der verschiedenen Netze. Die Produktionsnetze wurden mit den Büronetzen verbunden, um z. B. eine direkte Anbindung der Maschinen an das Warenwirtschaftssystem zu ermöglichen. Die ehemals strikte Trennung beider Netze ist nicht mehr gegeben. Ähnliches gilt für die zunehmende weitere Vernetzung und weitrei-

* Jens Mehrfeld, Bundesamt für Sicherheit in der Informationstechnik (BSI)
Referat CK23 – Cyber-Sicherheit in der Industrie,
E-Mail: jens.mehrfeld@bsi.bund.de

chenderen Zugriffsmöglichkeiten, die zu Effizienzgewinnen führen können und z. B. Möglichkeiten für Fernzugriffe und -wartung bereitstellen. Vergessen werden sollte dabei nicht, dass auch ein Angreifer hiervon Gebrauch machen kann. Einzige Voraussetzung ist, dass er in das Unternehmen bzw. das Unternehmensnetz gelangt. Dies stellt jedoch keine echte Hürde dar, wie viele Beispiele in der jüngsten Vergangenheit gezeigt haben. Hier sei auf die Jahresberichte des BSI 2015 [2] verwiesen.

Zu guter Letzt soll an dieser Stelle auf die zentrale und integrierte Planung und Programmierung von Maschinen und Anlagen eingegangen werden. Hier kommen einheitliche Schnittstellen und ein Datenpool zum Einsatz, in dem alle relevanten Informationen von Abmessungen über Verkabelung bis hin zu Maschinen- und Safety-Programmen abgelegt sind. Dies vereinfacht die Planung deutlich und beschleunigt die Entwicklung. Auf der anderen Seite bedarf diese Informationssammlung eines besonderen Schutzes. Denn ein Angreifer findet dort, an einer Stelle gesammelt, geistiges Eigentum (*Intellectual Property*) und wertvolle Informationen für gezielte Manipulationen.

2.2 Vernetzung mit anderen Unternehmen

Die Veränderungen durch Industrie 4.0 beschränken sich nicht nur auf das Innere der Unternehmen. Sie werden auch die Zusammenarbeit zwischen Unternehmen beeinflussen. Die dynamischen (aus den bisherigen starren Wertschöpfungsketten entstehenden) Wertschöpfungsnetzwerke sind ein Ausdruck dafür. Dabei steht die Flexibilisierung der Produktion im Vordergrund, sodass dort Aufgaben aller Art dynamisch an möglicherweise spezialisierte Produktionsunternehmen oder Dienstleister vergeben werden können. Dies kann beispielsweise über Marktplätze erfolgen, die als Vermittler auftreten, oder im direkten Kontakt. Dies können aber auch Cloud-Dienste sein, in denen Daten gespeichert oder komplexe Berechnungen z. B. für Optimierungen durchgeführt werden. Die Anbindung und Durchführung von vorausschauender Wartung ist ein weiterer Bereich aus dieser Kategorie. Gemein haben diese Beispiele, dass sich für die Unternehmen bisher nicht oder nur indirekt vorhandene Abhängigkeiten und Risiken ergeben. Bei der dynamischen Auftragsvergabe ist das Unternehmen darauf angewiesen, permanent verfügbar zu sein, um Aufträge bestätigen zu können und diese in die Produktionsplanung einzubinden. Wenn innerhalb einer kurzen Zeitspanne keine Antwort erfolgt, wird der Auftraggeber sich für ein anderes Unternehmen entscheiden. Bisher war eine solche Verfügbarkeit der Planungssysteme nicht notwendig und stellt sich nun als Herausforderung dar. Gleiches gilt für die externe Anbindung an die Planungssysteme.

Ähnlich verhält es sich bei der Fernwartung. Der Maschinenbauer oder Integrator muss dafür Sorge tragen, dass er stets in der Lage ist, die Informationen der Maschine zu empfangen. Eine Störung des Wartungszugangs darf den Betrieb der Anlage nicht beeinflussen und es müssen Vorbereitungen getroffen werden, wie beispielsweise bei einem *Denial-of-Service-Angriff* reagiert wird. Die Gefahr hierfür hat in den letzten Jahren stark zugenommen. Betroffen ist dann nicht nur der Dienstleister, sondern auch dessen Kunden, die keine Überwachung und Unterstützung für den Betrieb der Anlage erhalten.

Um bei diesem Beispiel zu bleiben: Nicht nur die Verfügbarkeit ist ein zentraler Aspekt, sondern auch die Vertraulichkeit der Daten. Zu diesen Daten können Rezepturen oder andere Produktionsdaten gehören, aber auch Auslastungen von Maschinen. Diese können mögliche Rückschlüsse über die Auftragslage eines Unternehmens geben. Hier muss klar geregelt sein, welche Daten bei der Wartung übermittelt werden und wie die Speicherung bzw. Verarbeitung erfolgt.

Einen letzten Punkt stellt die Identifikation der Teilnehmer untereinander dar. Bevor irgendeine Art der Kommunikation stattfindet, muss eine sichere Authentisierung der Teilnehmer stattfinden. Die bisherigen Beispiele machen diese Notwendigkeit sehr deutlich, da entweder der Zugriff auf zum Teil sehr sensible Daten erfolgt oder es bei dem Beispiel der Marktplätze um Aufträge und damit Umsatz geht. Hierfür müssen geeignete Techniken zum Einsatz kommen und mit der entsprechenden Sorgfalt genutzt werden.

2.3 Bestandsanlagen

Trotz der Veränderungen und möglichen Optimierungen wird nicht jedes Unternehmen neue Anlagen und Maschinen beschaffen und einsetzen. In vielen Fällen werden bestehende Anlagen ertüchtigt. Problematisch ist, dass in vielen dieser alten Anlagen bisher nichts oder nur wenig in Bezug auf Security getan wurde. Dies muss bei der Umsetzung berücksichtigt werden. Es sind Migrationspfade von alt zu neu notwendig, um eine sichere Einbindung und einen sicheren Betrieb zu gewährleisten.

2.4 Daten in der Industrie 4.0

Neben den bereits angesprochenen Veränderungen ist zu beobachten, dass die Menge an Informationen, die entstehen und gesammelt werden, ebenfalls zunimmt. So gibt es in den *Smart Factories* eine Fülle von Sensoren, die Auskunft über den Zustand einer Maschine oder über den Herstellungsprozess eines Produktes geben. Ein Hersteller eines Produktes hat die Möglichkeit,

sehr detailliert nachzuvollziehen, unter welchen Bedingungen dieses hergestellt wurde. Gleichzeitig können neue intelligente Produkte die Möglichkeiten bieten, diese über den gesamten Lebenszyklus zu *tracken*. Dies ermöglicht bei Problemen eine schnelle Reaktion und Information der Kunden.

Bei all diesen Informationen muss selbstverständlich auf deren Speicherung geachtet werden. So können diese ggf. manipuliert oder offengelegt werden. Dies wäre gerade bei sensiblen Daten von Kunden sehr kritisch. Das gilt auch für den Zugriff durch andere Unternehmen, wie es zuvor bereits angesprochen wurde.

3 Security in Industrie 4.0

Man sieht, dass mit den vielen neuen Chancen auch viele Herausforderungen verbunden sind. Daher stellt sich direkt die Frage, wie dies bei Industrie 4.0 gehandhabt werden soll und wo darauf eingegangen wird.

Das Referenzarchitekturmodell Industrie 4.0 (RAMI4.0) stellt eine Sicht auf die funktionalen Aspekte der Produktionsautomation dar. Bei Security handelt es sich, wie z. B. auch bei Safety oder Datenschutz, um nicht-funktionale Bestandteile. Grundsätzlich wäre ein Betrieb ohne Security möglich, vorhandene Risiken und Gefahren erfordern jedoch eine Beschäftigung damit. Daher handelt es sich um eine grundlegende Anforderung, ohne die eine sinnvolle Realisierung und der sichere Betrieb nicht möglich ist (Bild 1).

3.1 Hierarchie-Level

Die Hierarchie-Level bilden die verschiedenen Funktionen/Komponenten der Automatisierungspyramide ab bzw. erweitern diese. Sie reichen vom Produkt bis hin zur Außenwelt (*Connected World*). Die verschiedenen Komponenten enthalten je nach Einsatzumgebung ihrem Schutzbedarf entsprechende Sicherheitsmaßnahmen und -mechanismen. Diese müssen ein dem Anwendungsfall ausreichendes Schutzniveau ermöglichen. Dabei gilt jeweils so viel wie möglich (für einen hohen Schutzgrad), aber auch so wenig wie nötig (um die Kosten und Aufwand gering zu halten) Security zu integrieren.

Um dies gewährleisten zu können, muss für die Komponenten jeweils eine Risikoanalyse durchgeführt werden. Dazu werden die Bedrohungen und Risiken bestimmt. Aus den Ergebnissen lassen sich Maßnahmen für die Komponenten selbst ableiten oder auch für die Funktionalitäten, die von untergeordneten Komponenten bereitgestellt werden müssen bzw. denen sich auf höherer Ebene gewidmet werden muss.

Exemplarisch sei eine Maschine (*Station*) bestehend aus verschiedenen speicherprogrammierbaren Steuerungen (SPS*; Control Devices*) in einer Produktionsumgebung (*work unit*) genannt. Beginnend bei der SPS muss diese eine korrekte und störungsfreie Verarbeitung gewährleisten und die Möglichkeit zum Schutz von Steuerprogrammen vor unberechtigtem Auslesen oder vor Veränderungen bieten.

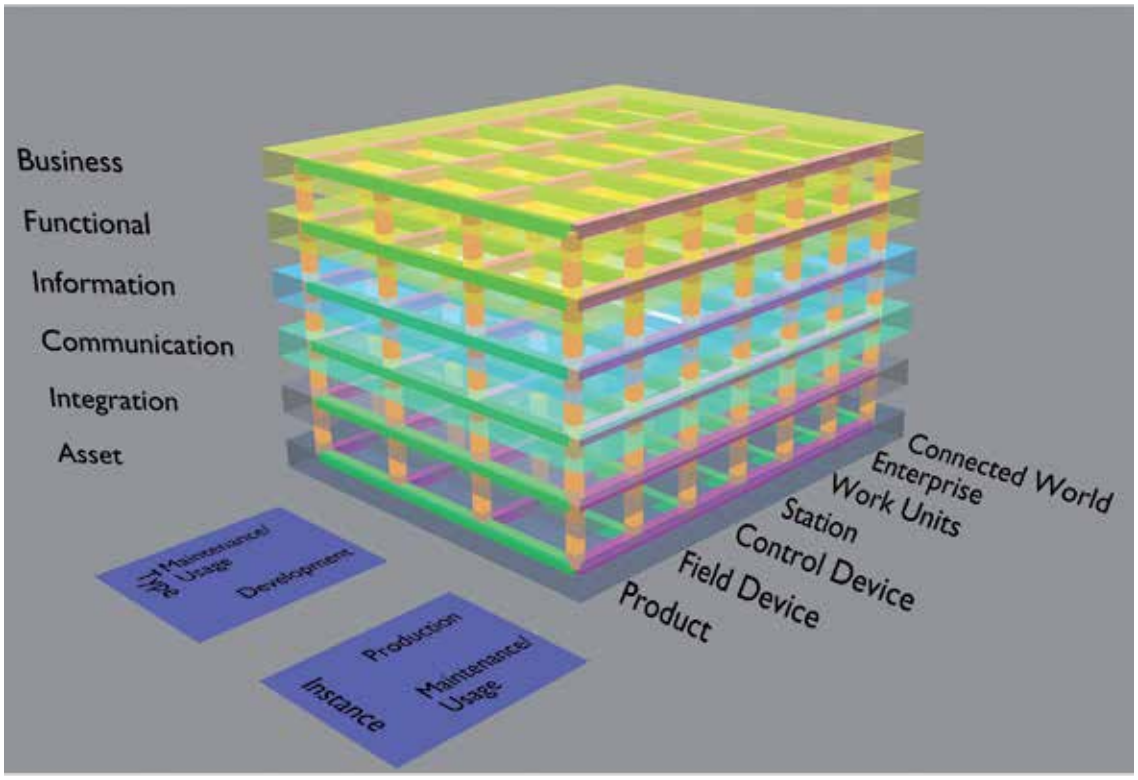

Bild 1:
Eine erweiterte Darstellung des RAMI4.0. Die parallel zu den drei Achsen eingezeichneten Linien stehen stellvertretend für die notwendigen Aktivitäten im Hinblick auf Security. Sie bilden eine Art Skelett, das sich durch sämtliche Ebenen zieht und die Funktionalitäten unterstützt. Diese Stützstruktur bezieht sich bei der Achse des *Hierarchy-Layer* auf die jeweilige Art der Komponente, bei der Achse des *Life-Cycle/Value-Stream* auf den Lebenszyklus und in den einzelnen Layern auf die verschiedenen Betrachtungsebenen. Die Darstellung zeigt den durchdringenden Charakter der Security in Industrie 4.0.

Die Maschine nutzt die SPS und deren Funktionen, um ein Produkt zu fertigen. Dazu müssen Steuerdaten auf vertrauenswürdigen Wegen an die SPS übertragen werden oder es müssen Bediener identifiziert und je nach Berechtigung unterschiedliche Eingriffsmöglichkeiten geboten werden.

Auf Produktionsumgebungsebene gilt es, die Mitarbeiter und deren Berechtigungen oder mehrere Maschinen zu verwalten und entsprechende Aufträge zu übermitteln sowie deren Abarbeitung zu kontrollieren. Auch hier ist eine sichere Identifizierung und Übertragung von Informationen und Maschinen notwendig.

3.2 Lebenszyklus

Allein die Betrachtung der Hierarchie und der Funktionalitäten reicht nicht aus. Security beginnt bereits bei der Planung und Entwicklung, setzt sich über die Produktion und den Betrieb bis hin zum Einsatz sowie zur Pflege und Wartung fort. Dies gilt grundsätzlich für alle Arten von Komponenten bzw. Funktionsbereiche.

Im Rahmen der Planung gilt es, die Risiken und Rahmenbedingungen für den Betrieb zu bestimmen und die dafür notwendigen Funktionen zu berücksichtigen oder als Anforderungen für andere Komponenten zu formulieren. Während der Entwicklung gilt es, konsequent Fehler zu vermeiden. Hierfür bildet ein *Secure Development Lifecycle* eine Basis, die die Entwickler unterstützt und Vorgaben für die Implementierung enthält.

Im weiteren Verlauf geht es um den sicheren Betrieb und auch um die Beseitigung von Fehlern durch Updates. Diese müssen entwickelt, an die Kunden verteilt und in deren Systeme eingespielt werden. Die Hersteller tragen somit auch über den Verkauf eine gewisse Verantwortung, um einen sicheren Einsatz zu ermöglichen.

3.3 Ebenen

Nach den zwei bereits beschriebenen Achsen von RAMI4.0 folgt die Letzte. Die Ebenen ermöglichen eine logische Unterteilung in verschiedene fachliche Themengebiete. Am einfachsten verständlich ist die Ebene der Kommunikation. Hier werden Maßnahmen wie Verschlüsselung ergriffen, wenn sensible Informationen über ungeschützte Netze übertragen werden. Aber auch hier gibt es wieder gewisse Zusammenhänge zwischen den Ebenen. Um die Entscheidung zu treffen, ob die Kommunikationsverbindung schutzbedürftig ist, muss klar sein, welche Daten aus dem *Information-Layer* darüber übertragen werden. Dies ist nur ein Beispiel für mögliche Abhängigkeiten.

3.4 Zusammenwirken

Im Rahmen der Beschreibung der einzelnen Bestandteile von RAMI4.0 wird deutlich, dass letztlich in allen Schnittpunkten der verschiedenen Achsen Security eine Rolle spielt und so eine querschnittliche und zentrale Aufgabe darstellt. Auch die Abhängigkeiten zwischen den einzelnen Ebenen und Schnittpunkten wurden angedeutet.

Für die Umsetzung kann in vielen Bereichen auf bereits vorhandene Standards zurückgegriffen werden. Der Austausch der Anforderungen zwischen Herstellern, Integratoren und Betreibern wird z. B. in der VDI 2182 und der IEC 62443 adressiert.

Die Ausführungen und Beispiele haben die Entwicklung und den Betrieb einer Produktionsanlage in den Fokus gestellt. RAMI4.0 enthält jedoch auch das Produkt selbst. Auf diese Weise kann die Herstellung intelligenter Produkte ebenfalls abgebildet werden.

4 Vorgehen

Unabhängig von der theoretischen Betrachtung und der Thematik Industrie 4.0 ist, dass sich Unternehmen überhaupt mit Security beschäftigen. Bei Industrie 4.0 rückt dies jedoch stärker in den Fokus. Vielfach wird in der Diskussion um Funktionen nicht daran gedacht oder es wird als nachrangiges Thema betrachtet, mit dem sich später beschäftigt wird. Daher wurde in der Vergangenheit nur wenig Aufwand investiert. Ein Grund hierfür ist häufig fehlendes Wissen über die möglichen Risiken und deren Konsequenzen.

Dies ist ein Ansatzpunkt der unter anderem durch die ICS Top 10 Bedrohungen des BSI [3] adressiert wird. Diese beschreiben wichtigste Bedrohungen und sollen zu einer ersten Beschäftigung mit Security anregen.

Wenn die Aufmerksamkeit geweckt wurde, gilt es, sich eingehender mit der Materie zu beschäftigen. Dies bedeutet, dass erste Bestandsaufnahmen stattfinden, um den aktuellen Status beurteilen zu können. In dieser Phase können Maßnahmen mit geringem Aufwand umgesetzt werden, um eine erste grundlegende Absicherung und Erhöhung des Sicherheitsniveaus zu ermöglichen. Ein Beispiel können Regelungen zum Umgang mit mobilen Datenträgern sein. Die Umsetzung erfordert keinen großen Aufwand und dient gleichzeitig als Einstieg in die Sensibilisierung der Mitarbeiter. Einschränkend muss gesagt werden, dass dies allein noch keinen umfassenden Schutz bietet. Es geht vielmehr um die sukzessive Umsetzung von Maßnahmen und die Steigerung des Sicherheitslevels.

Diese schrittweise Herangehensweise setzt sich mit der Ermittlung der schützenswerten Informationen und Systeme und in der dazugehörenden Risikoanalyse fort und geht in die Auswahl und Umsetzung von Schutzmaßnahmen über. Ein grundlegendes Verständnis der Bedrohungen und Risiken ist für eine erfolgreiche Abwehr zwingend notwendig, denn es gilt die vorhandenen Ressourcen optimal einzusetzen. Ziel ist es, mit den vorhandenen Mitteln eine optimale Wirkung zu erzielen. Viele solcher Maßnahmen sind im ICS-Security-Kompendium des BSI zusammengefasst.

Das Ziel dieser Maßnahmen ist ein geregelter Security-Prozess, der alle Aufgaben im Hinblick auf z. B. die Entwicklung von Produkten bei Herstellern, die Produktion von Komponenten, die Konstruktion, Aufstellung und Wartung von Anlagen oder deren Betrieb regelt. Als Basis hierfür können etablierte Verfahren auf Basis von IT-Grundschutz des BSI, ISO 27001 oder der ISO/IEC 62443 dienen.

Es gilt nicht nur den Produktionsprozess zu betrachten, sondern auch Security über den Lebenszyklus der Produkte im Auge zu behalten. So gilt es, die intelligenten Produkte (auch *Smart-Products* genannt) über die gesamte Nutzungsdauer zu schützen. Dabei steht die Vermeidung von Schwachstellen an erster Stelle. Dies sollte schon bei der Entwicklung berücksichtigt werden, um Aufwände für die spätere Beseitigung zu vermeiden. Dazu kommen die vertrauliche Verarbeitung von Sensordaten oder datenschutzrechtliche Vorgaben.

5 Ausblick

Der Artikel sollte einen Einblick in die Überlegungen zu Security für Industrie 4.0 geben. Auf konkrete Details konnte dabei aufgrund der Komplexität und zum Teil noch offener Festlegungen nicht eingegangen werden. Ziel war es, einen Anstoß zu geben, sich im Kontext von Industrie 4.0 mit Security zu beschäftigen und auf die gestiegenen Anforderungen hinzuweisen. Die zu bewältigenden Aufgaben orientieren sich an den bereits etablierten Vorgehensweisen aus ISO 27001, dem IT-Grundschutz des BSI und Verfahren zur sicheren Softwareentwicklung. In vielen Bereichen kann auf bestehende Technologien aufgebaut werden. In anderen Bereichen sind noch weitere Überlegungen anzustellen, um dort geeignete Festlegungen zu treffen.

Einer dieser offenen Punkte betrifft die Vernetzung und Kommunikation innerhalb der Unternehmen und auch zwischen diesen. Es ist häufig zu hören, dass alle Komponenten untereinander ohne Einschränkungen kommunizieren können müssen und die Trennungen der Netze aufgehoben werden. Diese sehr generelle Darstellung muss mit Blick auf die Security kritisch hinterfragt werden. Die Folge wäre, dass ein Angreifer – einmal im Unternehmen – Zugriff auf sämtliche Systeme hätte, und dass eine Anomalieerkennung unmöglich würde. Es sollte vielmehr von einer Zunahme des zulässigen Verkehrs gesprochen werden. Denn eine Kontrolle und Einschränkung auf diese erlaubte Kommunikation wird auch in Industrie 4.0 unabdingbar sein, um die bekannten Strategien der stufenweisen Absicherung umzusetzen. Denn nur so kann es Angreifern erschwert werden, ungehindert in die Produktionsumgebungen einzudringen und sich auszubreiten.

Die Umsetzung von Industrie 4.0 erfordert zusätzliches Wissen und ein Umdenken bei allen Verantwortlichen. Zusätzliches Wissen im Hinblick auf Security, Risiken und Techniken zum Schutz und ein Umdenken im Hinblick auf die Aufwände sind notwendig. Erfolgreiche Angriffe haben gezeigt, dass die Kosten für die Vorsorge und den Schutz vor Angriffen deutlich geringer sind als der Schaden, der durch einen solchen entsteht! Es liegt daher an allen Beteiligten, Security bei Industrie 4.0 einzufordern und umzusetzen. Es ist eine gemeinschaftliche Herausforderung. Die Hersteller müssen die notwendigen Funktionen bereitstellen, die Maschinenbauer und Integratoren müssen diese mit Sorgfalt nutzen und integrieren und die Betreiber müssen sie einfordern und etablieren.

Referenzen

[1] http://www.plattform-i40.de/I40/Navigation/DE/Industrie40/WasIndustrie40/was-ist-industrie-40.html
(Letzter Zugriff am 28.11.2016)

[2] https://www.bsi.bund.de/DE/Publikationen/Lageberichte/lageberichte_node.html
(Letzter Zugriff am 28.11.2016)

[3] https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/Empfehlungen/ICS-Betreiber/empfehlungen-betreiber_node.html
(Letzter Zugriff am 28.11.2016)

Herausforderungen für Informationssicherheit in eingebetteten Systemen bei Angreifern mit Hardware-Zugriff

Johann Heyszl*

Kurzfassung – Die Informationssicherheit von vernetzten eingebetteten Systemen in Anwendungen wie „Industrie 4.0“, dem Automobilbereich, dem intelligenten Stromnetz und dem Internet der Dinge, das sich zukünftig auch auf medizinische Geräte, Heimautomatisierung und auf das intelligente Messwesen erstrecken wird, ist einerseits ein besonders wichtiges Entwicklungsziel und andererseits auch eine besonders große Herausforderung. Die betreffenden Fragestellungen sind in den genannten Anwendungen sehr ähnlich. Der Kern der Herausforderung ist, Informationssicherheit für dort eingesetzte eingebettete Geräte zu gewährleisten, obwohl Angreifer physischen Zugang zu diesen Geräten haben könnten. Es besteht dabei meist die Gefahr, dass erfolgreiche Angriffe auf einzelne Geräte zu Verwundbarkeiten und Angriffen oder Auswirkungen auf alle vernetzten Geräte führen könnten. Schutzmaßnahmen gegen Angreifer mit Hardware-Zugriff benötigen oft Funktionen in Hardware, die nicht nachgerüstet werden können. Aufgrund der potenziell langen Lebenszeit von eingebetteten Geräten im Betrieb ist es aber eine große Herausforderungen, diese notwendigen Hardware-basierten Schutzmaßnahmen vorzusehen, um damit auch die Grundlage für die ebenfalls notwendige Software-Sicherheit zu bilden.

1 Einleitung

Seit einigen Jahren hat die Technologie-Entwicklung von stark integrierten Computer-Chips mit Vernetzungs- und Kommunikationsmöglichkeiten bei verbesserter Energieeffizienz deutlich zugenommen und kommt nun in wichtigen Anwendungen abseits der Konsumentenwelt an. Begriffe wie *Cyber-Physical Systems* (CPS), Industrie 4.0, *Internet of Things* (IoT) bzw. Internet der Dinge haben diesen Trend in den vergangenen Jahren als Schlagworte gekennzeichnet. Der Kern dieses Technologietrends ist, dass man signifikante Rechenleistung und Speicher mit attraktiven Funkkommunikationsmöglichkeiten in eingebettete Systeme integrieren kann und dabei nur einen vertretbaren Energiebedarf bewältigen muss. Massenprodukte wie Mobiltelefone und Tablets haben durch ihre hohen Volumina und Nachfrage die rasante Entwicklung solcher Chips ermöglicht. Für eingebettete Geräte sind daher Chips, die alle notwendigen Funktionen bereits integrieren, einfach, daher quasi aus dem Regal, verfügbar.

Anwendungsbereiche für eingebettete Systeme wie Industriekomponenten, die sich durch vergleichsweise geringe Stückzahlen kennzeichnen, können von diesem Hochvolumenmarkt profitieren und auf solchen Chips aufbauen. Diese üblicherweise leistungsstarken Rechnerplattformen ermöglichen es, anstatt von dediziert entwickelter Firmware, auf herkömmliche Linux-basierte Betriebssysteme zu setzen, worauf dann mit Betriebssystems-Unterstützung die benötigte Anwendungs-Software mit deutlich weniger Entwicklungsaufwand erstellt werden kann.

Die Anwendungsbereiche, die sich auf diese Art verändern, sind insbesondere die industrielle Produktion, der Automobilbereich im Zuge des Aufkommens des autonomen Fahrens und das Internet der Dinge ganz allgemein, das fast alle Bereiche des täglichen Lebens umfassen wird. Intelligente Messsysteme werden sich wohl zukünftig auch in ähnlicher Art entwickeln. Der treibende Aspekt der Entwicklung ist die starke Vernetzung zum Zweck des Informationsaustauschs. Die Zukunft der Wertschöpfung benötigt diese starke Vernetzung für ein zusätzliches Informationsangebot an Kunden zur Effizienzsteigerung, oder auch für gänzlich neue Geschäftsmodelle. Ein Beispiel für Effizienzsteigerung ist eine zukünftig vollvernetzte industrielle Produktion, aber auch selbstfahrende

* Dr. Johann Heyszl, Head of Hardware Security Department, Fraunhofer-Institut AISEC, Garching bei München, E-Mail: johann.heyszl@aisec.fraunhofer.de

Autos, die die Effizienz der Straßeninfrastruktur erhöhen werden. In einer ähnlichen Art wird auch das Messwesen Effizienzsteigerungen erfahren. Im Sinne neuer Geschäftsmodelle ist zu beobachten, dass zumeist versucht wird, möglichst viele Daten zu sammeln und auszuwerten. Es gibt gute Beispiele von Unternehmen, die es schaffen, einen beachtlichen Wertschöpfungsanteil an der Auswertung von Daten aufzuhängen.

Diese gesamte Entwicklung bringt allerdings signifikante Herausforderungen mit sich. Vernetzung bedeutet immer, dass Geräte an ein Kommunikationsnetzwerk angeschlossen werden. Dadurch wird die zu beachtende Angriffsfläche aber sofort drastisch vergrößert. Eine Verweigerung dieser Entwicklung wäre trotzdem nicht sinnvoll, weil das Sammeln, Verarbeiten und Bereitstellen von Informationen über solche Vernetzungen der Kern der Verbesserungen ist. Wenn es aber nicht gelingt, ein hohes Maß an Informationssicherheit zu gewährleisten, wird all diesen positiven Aspekten die Grundlage entzogen. Die möglichen negativen Auswirkungen von unzureichender Informationssicherheit sind signifikant. Sie reichen von dem Lahmlegen öffentlicher Infrastruktur, industrieller Produktion, und privatem Verkehr bis zur Verletzung von Privatsphäre und ganz konkret der systematischen Manipulation von Messdaten.

Informationssicherheit in vernetzten eingebetteten Systemen ist eine vielschichtige Herausforderung. Gefahren durch Netzwerk-basierte Angriffe aus der Ferne sind schon relativ bekannt und werden in der Entwicklung häufig adressiert. Der große Paradigmenwechsel ist nun aber, dass man Angreifer mit physischem Zugriff in hohem Maß ernst nehmen muss, da durch die Vernetzung auch einzelne kompromittierte Geräte Relevanz für ein gesamtes Netzwerk besitzen können. Beispielsweise könnte man aus einem Gerät Informationen oder Schlüsselmaterial extrahieren, um über die Vernetzung einen Angriff auf viele weitere Geräte und das Netzwerk durchzuführen. Denkbar ist so etwas zum Beispiel bei den verteilten Teilen der öffentlichen Schieneninfrastruktur oder der Energieversorgung. Informationssicherheit gegen lokale Angreifer auf eingebettete Geräte ist daher dringend notwendig und benötigt Vorkehrung in Hardware. Anders als im Kontext von PCs und Servern können dafür notwendige Hardware-basierte Schutzmaßnahmen allerdings nicht per Update nachgerüstet werden. Es ist daher nicht möglich, ein eingebettetes System auszurollen, und danach im Betrieb per Software-Aktualisierungen Schwachstellen zu schließen, um die Sicherheit zu erhöhen. Bereits während des Systemdesigns müssen die richtigen Entscheidungen getroffen und die richtigen Komponenten bzw. Chips ausgewählt werden. Diese Hardware muss Möglichkeiten bieten, sensible Daten wie kryptografische Schlüssel, Zertifikate und Passwörter sicher zu speichern und die Manipulationssicherheit der Software auf dem System mithilfe von Hardware-Mechanismen zu gewährleisten. In der Folge werden diese Zusammenhänge näher beleuchtet.

2 Gemeinsamkeiten eingebetteter Systeme

Vernetzte eingebettete Systeme in der Industrie 4.0, im Automobilbereich, im intelligenten Stromnetz, in intelligenten Messwesen und im Internet der Dinge teilen gemeinsame Eigenschaften und haben abstrakt gesehen die gleichen Bestandskomponenten. Dies ist auch der Grund dafür, warum die Herausforderungen bezüglich Informationssicherheit sehr ähnlich sind.

Jedenfalls ist eine Haupt-CPU entweder einzeln oder zusammen mit peripheren Komponenten wie Rechenbeschleunigern und Schnittstellen als System-on-Chip (SoC) auf einer Platine zu finden. Zusätzlich werden darauf jedenfalls noch ein Baustein als Arbeitsspeicher und ein weiterer als Festspeicher verbaut. Nachdem Vernetzung ein wesentlicher Bestandteil solcher Systeme ist, ist üblicherweise noch ein Modem-Chipsatz für Mobilfunk oder WLAN integriert. An dem System hängen außerdem Sensoren und Aktoren für die eigentliche Funktion des Systems. Die Vernetzung aller Geräte erfolgt üblicherweise zu einer zentralen Server-Infrastruktur.

3 Sicherheit eingebetteter Systeme

Informationssicherheit lässt sich generell nie vollumfänglich lösen. Anstatt dessen versucht man, den Aufwand für Angreifer auf realistisch prohibitive Niveaus zu heben. Im Kontext von kryptografischen Algorithmen bedeutet dies, dass die notwendige Rechenleistung zum Brechen von Schlüsseln von aktuell als sicher geltenden Algorithmen auch in vielen Jahrzehnten trotz Supercomputern und großer Rechenzentren (*Cloud-Computing*) unrealistisch ist[1].

Im Kontext von realen Geräten zählen allerdings nicht nur kryptografische Algorithmen. Angreifer nutzen immer den einfachsten Weg, um an ein Ziel zu gelangen. Anstatt die verschlüsselte Kommunikation zu brechen, könnte der Angreifer zum Beispiel versuchen, direkt in das System einzubrechen und Daten auszulesen. Allgemeine Angriffsziele sind jedenfalls sensible Daten wie Schlüssel und Passwörter. Außerdem ist Manipulation der laufenden Software eines Geräts, beispielsweise zur systematischen Manipulation von Messdaten, immer ein mögliches Ziel.

Zumeist stellt sich daher die Frage nach dem Sicherheitsniveau, das für jeden möglichen Angriffspfad angestrebt werden sollte. Dies erfordert immer auch eine Abwägung zwischen not-

1 Für gewisse Algorithmen stellen Quanten-Computer mit individuellen dafür entwickelten Algorithmen eine Gefahr dar, die früher eintreten könnte.

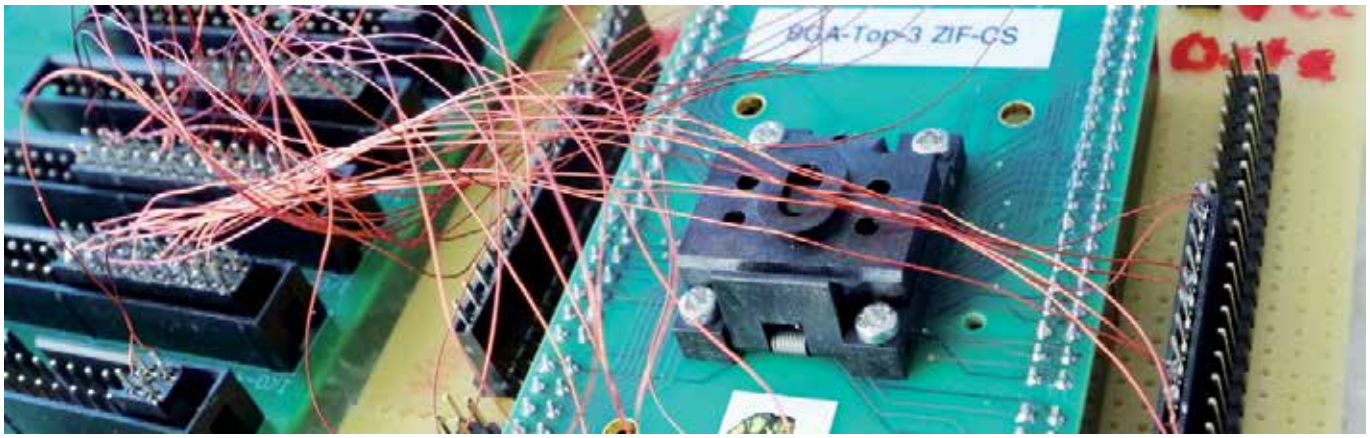

Bild 1: Auslesen eines abgelöteten BGA-Speicherchips

wendigem Ressourceneinsatz und erhöhten Kosten für ein höheres Sicherheitsniveau. Hochsicherheit, wie sie etwa bei hoheitlichen Dokumenten gefordert und sinnvoll ist, scheint in vielen Fällen nicht unbedingt erforderlich. Nichtsdestotrotz muss das Sicherheitsniveau auf die Bedrohungslage insofern angepasst sein, als dass die Kosten-Nutzen-Rechnung für mögliche Angreifer unattraktiv wird. Dabei muss man eine Vielzahl von verschiedenen Angriffsvektoren getrennt berücksichtigen. Kein denkbarer Angriffsvektor darf für einen Angreifer zu einem positiven Kosten-Nutzen-Verhältnis führen. Dafür gilt es, an vielen Stellen den notwendigen Entwicklungs- und Materialkosten-Aufwand zu investieren, um dies zu gewährleisten.

4 Angreifer auf eingebettete Systeme

Um die Gefahren zu adressieren, ist es wichtig, sich über die Möglichkeiten bzw. Eigenschaften möglicher Angreifer im Klaren zu sein. Diese Eigenschaften erfasst man üblicherweise in Form eines Angreifermodells für alle weiteren Überlegungen. Im Kontext vernetzter eingebetteter Systeme ist ein besonders wichtiger Punkt des Angreifermodells, dass der Angreifer physischen Zugriff auf die eingebetteten Systeme in den Gerätenhaben wird. Dieser wichtige Aspekt wird oft unterschätzt. Kombiniert mit den üblich vorauszusetzenden Fähigkeiten von Angreifern führt das zu wichtigen Angriffsmöglichkeiten. Diese Fähigkeiten umfassen typischerweise Kenntnisse in Elektronik, Entwicklung von eingebetteten Systemen, daher Platinen, Hardware, Software, Firmware und Schaltungen, *Reverse-Engineering* Mikrokontrollerbasierter Systeme, Nachrichtentechnik und Kenntnisse in Kryptografie und Angriffsmethoden gegen kryptografische Implementierungen. Ein Beispiel für die Auswirkung des physischen Zugangs ist, dass Angreifer verschiedene Speichermodule eingebetteter Systeme auslesen und jegliche sensible Information extrahieren können. Das Bild 1 zeigt einen Speicherchip in einem BGA-Package, der aus einem eingebetteten System abgelötet wurde und individuell ausgelesen wird. Alle Informationen, die im Speicher abgelegt wurden, fallen dem Angreifer damit in die Hände.

Abgesehen vom physischen Zugriff setzt man üblicherweise an, dass Angreifer relativ viel Zeit investieren können. Insbesondere können sich Angreifer üblicherweise mit einem deutlich höheren Zeitaufwand auf einen einzelnen Teilaspekt des Systems konzentrieren, der sich für einen Angriff eignet, als die an der Entwicklung beteiligten Personen. Während der Entwicklung ist gewöhnlich nicht absehbar, auf welche Aspekte ein Angreifer sich konzentrieren wird. Dies liegt oft an fehlenden Kenntnissen in angewandter Informationssicherheit. Der Angreifer muss typischerweise nur einen Angriffsvektor identifizieren, der am erfolgversprechendsten ist.

Häufige fehlerhafte Annahmen

In vielen Fällen bestehen falsche Hoffnungen, dass die konkrete Sicherheit eines Systems in der Praxis aus überbewerteten Gründen ausreichen wird. Beispielsweise wird oft davon ausgegangen, dass die Systemkomplexität zu hoch ist, als dass ein Angreifer relevante Teile nachvollziehen könnte. Angreifer müssen allerdings nur eine einzige nutzbare Schwachstelle finden und haben dazu üblicherweise signifikante Zeitbudgets zur Verfügung. Ähnlich falsch ist die Hoffnung, dass Angreifer praktisch nicht in der Lage seien, Speicherbausteine (z. B. BGA-Packages) auszulesen (siehe Bild 1), oder Busse mitzuhören. Dass der Aufwand dazu aber vertretbar ist, wurde oft gezeigt. Auch das Reverse-Engineering von Software aus Speicher-Abbildern mithilfe von leistungsfähigen Werkzeugen ist in vertretbarer Zeit möglich.

5 Aspekte der Sicherheits-Herausforderung

Konkret besteht die Herausforderung, die Informationssicherheit von vernetzten eingebetteten Systemen auf ein hohes Niveau zu heben, hauptsächlich aus den folgenden wichtigen Aspekten:

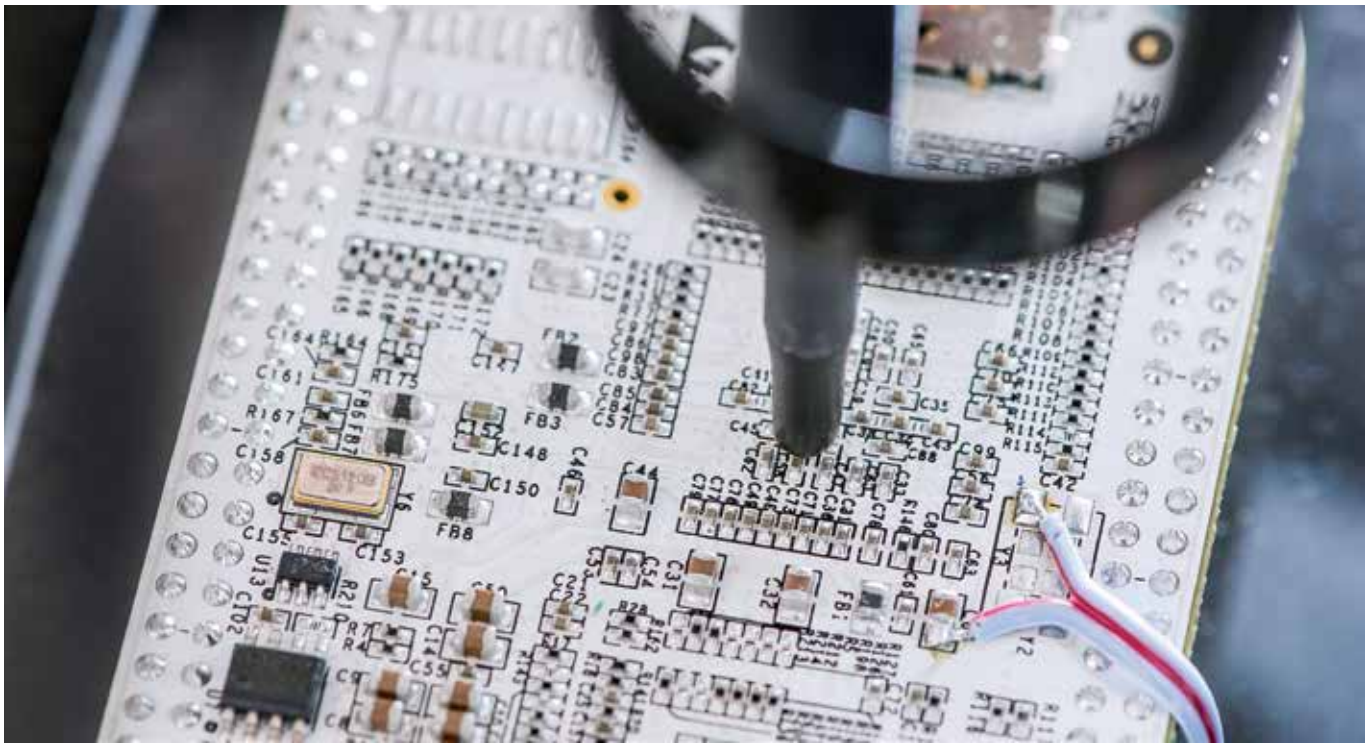

Bild 2:
Angriff durch Messung des Stromverbrauchs

A. Anwendung von Verschlüsselung und Schlüsselmanagement
B. Sicheres Speichern auf eingebetteten Systemen
C. Debug-Schnittstellen
D. Kommunikation zu zentralen Ressourcen
E. Manipulationsschutz der Software beim Start
F. Aktualisierungsmechanismen
G. Isolation von Funktionen und Software

Diese Aspekte werden nachfolgend einzeln diskutiert und es werden jeweils Empfehlungen abgeleitet.

A. Anwendung von Verschlüsselung und Schlüsselmanagement

Sicherheit für Informationen, die über öffentliche bzw. zugängliche Übertragungswege ausgetauscht werden, ist ohne Verschlüsselungstechnologie, daher Kryptografie, unmöglich. Heutzutage sind kryptografische Algorithmen auf einem sehr ausgereiften Stand, sodass man bei Einsatz von standardisierten Algorithmen und unter Einhaltung von einschlägigen Empfehlungen zu Parametern und Schlüssellängen eine hohe Sicherheit erreichen kann. Das Bundesamt für Informationssicherheit (BSI) erstellt einen jährlich erneuerten sogenannten Algorithmenkatalog [1], der von der Bundesnetzagentur veröffentlicht wird und in dem sichere Algorithmen und Schlüssellängen beschrieben sind. Für eingebettete Systeme sind AES-128, elliptische Kurven-Kryptografie mit zumindest 256 Bit, und SHA-2 bzw. SHA-3 jedenfalls eine zu empfehlende Wahl.

Die folgenden zwei Aspekte sind allerdings im Zusammenhang mit dem Einsatz von Verschlüsselung besonders kritisch:

5.1 Sicherheit von Implementierungen der Algorithmen

Kryptografische Algorithmen müssen in Software oder Hardware implementiert und auf dem eingebetteten System berechnet werden. Im Unterschied zu Angreifern aus der Ferne, kann der Angreifer mit physischem Zugriff auf das eingebettete System sogenannte Implementierungsangriffe durchführen. Das bedeutet, dass er beispielsweise während der Berechnung des Algorithmus' Messungen anstellt oder gezielt Störungen einbringt, anstatt nur das Ergebnis zu analysieren. Ein wichtiger Vertreter solcher Angriffe ist ein sogenannter Seitenkanalangriff, bei dem von einem Angreifer beispielsweise der Stromverbrauch während kryptografischer Berechnungen gemessen wird. Bild 2 zeigt, wie der Stromverbrauch eines eingebetteten Systems während der Berechnung eines kryptografischen Algorithmus' mithilfe einer Magnetfeldsonde gemessen wird. In einer statistischen Analyse vieler Messungen kann danach der geheime Schlüssel gewonnen werden, obwohl der Algorithmus (z. B. AES-128) – kryptografisch gesehen – absolut einwandfrei sicher ist. Bild 3 zeigt einen Teil der grafischen Darstellung eines solchen Analyseprogramms. So ist es beispielsweise möglich, die Festplattenverschlüsselung eines eingebetteten Systems zu brechen, was im Bild 2 gezeigten Messaufbau der Fall war.

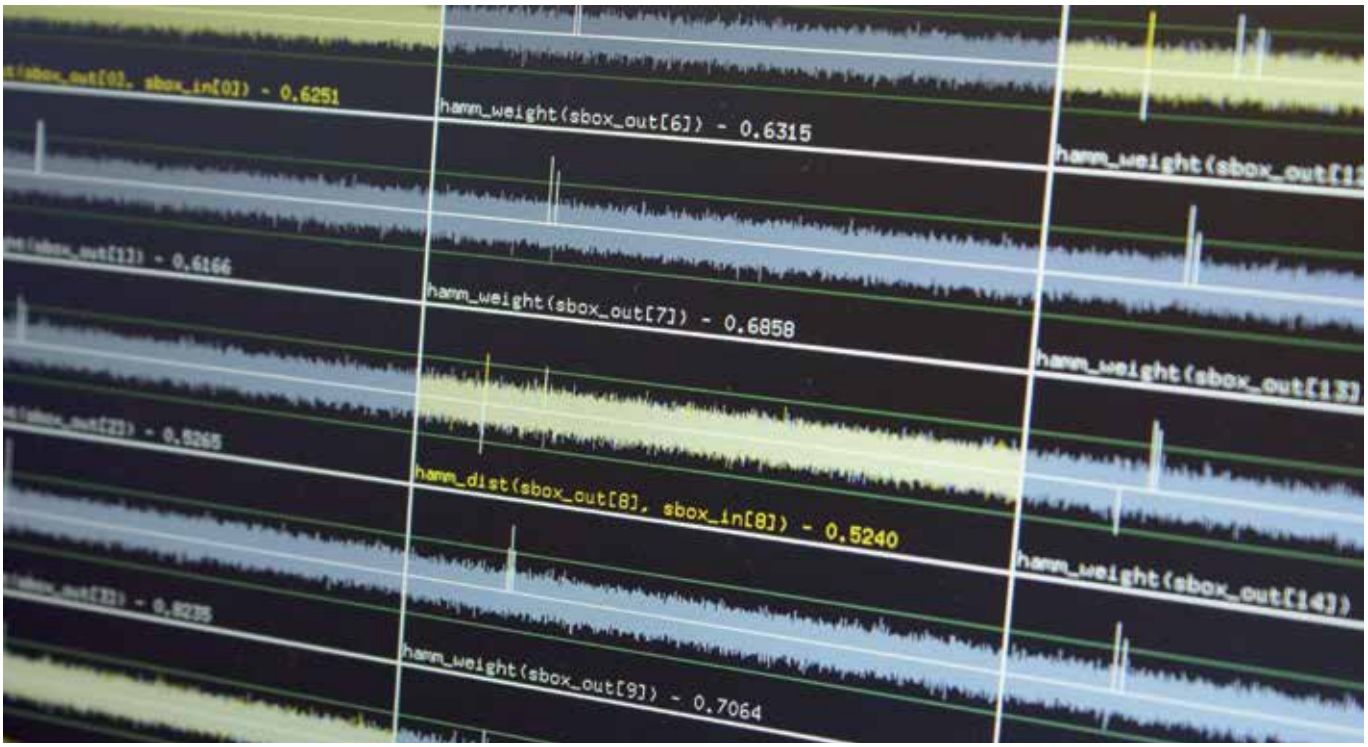

Bild 3:
Analyse von Messdaten zum Brechen kryptografischer Implementierungen

Schutzmaßnahmen gegen solche Angriffe sind teilweise sehr aufwendig. Daher kann es sinnvoll sein, geschützte Implementierungen zu lizenzieren bzw. Verschlüsselungen auf dedizierten, geschützten Sicherheitschips auszuführen, die dediziert geschützte Implementierungen anbieten.

Aus diesen Umständen lassen sich zwei Erkenntnisse ableiten. Erstens ist die sichere Implementierung von kryptografischen Algorithmen, die kryptografisch einwandfrei sind, trotzdem eine Herausforderung, sodass man idealerweise auf ausgereifte Implementierungen, beispielsweise Software-Bibliotheken, die regelmäßig aktualisiert werden, oder dedizierte Implementierungen in Sicherheitschips, setzen sollte. Andererseits kann gerade bei Software-Implementierungen selten ausgeschlossen werden, dass Implementierungsschwachstellen auftreten, die im Nachhinein im Rahmen einer Aktualisierung geschlossen werden müssen.

5.2 Schlüsselmanagement

Bei der Auswahl von kryptografischen Algorithmen muss man sich grundsätzlich zwischen sogenannten symmetrischen Algorithmen, wobei ein Schlüssel von zwei an einer Übertragung teilnehmenden Seiten geteilt wird, und asymmetrischen Algorithmen, wobei jeder Teilnehmer ein Paar aus öffentlichem und geheimem, privatem Teil besitzt, entscheiden. Asymmetrische, oder auch sogenannte *Public-Key-Verfahren*, ermöglichen, dass jeder Teilnehmer nur **einen** individuellen Schlüssel geheim halten muss. Sie sind aber rechenintensiver, was in vielen Fällen prohibitiv ist. Diese Verfahren werden üblicherweise durch sogenannte *Public-Key-Infrastrukturen* (PKI) bzw. Zertifikate und Zertifikatshierarchien angereichert, um Vertrauensverhältnisse zu schaffen. Jede verschlüsselte Verbindung zu Internetseiten basiert auf diesen Prinzipien. Zusätzlich dazu, dass ein individueller Schlüssel geheim gehalten werden muss, müssen Zertifikate zum Prüfen der Kommunikationsgegenstellen zwar nicht geheim, aber manipulationssicher gespeichert werden. Symmetrische Algorithmen zwingen dazu, geheime Schlüssel auf jeweils beiden Seiten sicher zu speichern, sind dafür aber weniger rechenintensiv. Auch mit symmetrischen Schlüsseln kann man jedoch Angriffsflächen verringern, indem symmetrische Schlüssel jeweils nur für ein einzelnes Gerät und die zentrale Stelle verwendet werden, und somit jedes Gerät trotzdem einen individuellen Schlüssel erhält. Geräteindividuelle Schlüssel dürfen allerdings auch keine Schädigung des Gesamtsystems erlauben, indem sie für Angriffe gegen die zentrale Stelle verwendet werden. Dazu müssen in der zentralen Stelle entsprechende Vorkehrungen getroffen werden.

Die Entscheidungen, welche Algorithmen zu bevorzugen sind, ist stark von der Anwendung und den damit verbundenen Eigenschaften abhängig. Sie beeinflusst dann aber in einem hohen Maß die Angriffsfläche, indem Geräte beispielsweise nur individuelle geheime Schlüssel speichern, anstatt im schlechtesten Fall sogar einen symmetrischen Generalschlüssel. So kann mit der Wahl der Algorithmen das notwendige Schlüsselmanagement und die konkrete Anforderung an das Sicherheitsniveau des Speichers entscheidend beeinflusst

werden. Es ist zu empfehlen, möglichst keine Generalschlüssel in Geräten zu speichern, sondern stattdessen nur Geräte-individuelle Schlüssel.

B. Sicheres Speichern auf eingebetteten Systemen

Eingebettete Systeme müssen Informationen austauschen. Damit Informationen am Übertragungsweg nicht manipuliert bzw. umgeleitet (Authentizität) oder abgehört (Vertraulichkeit) werden können, wird Verschlüsselungstechnologie verwendet. Beispielsweise werden standardisierte Verfahren wie *Transport Layer Security* (TLS) [2] angewendet. Für diese vertraulichen Übertragungen werden geheime kryptografische Schlüssel benötigt, die sicher gespeichert werden müssen. Auch für manipulationsgeschützte Übertragung werden Schlüssel benötigt, die beim Speichern zumindest gegen Manipulation geschützt werden müssen, selbst wenn es sogenannte öffentliche Schlüssel sind. Abgesehen von kryptografischen Schlüsseln gibt es weitere Informationen, die vertraulich und manipulationsgeschützt gespeichert werden müssen. Beispiele sind aggregierte Messdaten, Software-Implementierungen proprietärer Algorithmen oder Passwörter zum Zugriff auf Ressourcen.

Sicheres Speichern in eingebetteten Systemen ist allerdings schwierig zu lösen. Angreifer können Speicherbausteine auf der Platine eingebetteter Systeme relativ problemlos abnehmen (auslöten) und auslesen (siehe dazu Bild 1). Daher ist es unmöglich, Schlüssel bzw. Passwörter für Speicherverschlüsselung in solchen Speichern abzulegen. In eingebetteten Systemen steht auch kein Nutzer für Eingaben von Passwörtern zur Verfügung. Auf PCs und Mobiltelefonen ist die Verschlüsselung der Festspeicher durch eben solche Passwort-Eingaben gelöst. Abhängig von dem Sicherheitsverständnis des Benutzers bei dem Wählen eines Passworts kann auf diese Art ein sehr solides Sicherheitsniveau erzielt werden. Ein Beispiel dafür ist der im Frühjahr 2016 öffentlich gewordene Versuch des FBI in den USA, den Speicher eines iPhones auszulesen, was sich als außerordentlich schwierig herausstellte.

Ein möglicher Ansatz, dieses Speicherproblem zu lösen, ist, vertrauliche Informationen in dedizierten Sicherheitschips abzulegen und die Schnittstelle zu diesen Chips im Rahmen der gewünschten Funktion möglichst einzuschränken, sodass kein Extrahieren möglich ist. Ein Beispiel für solche Sicherheitschips sind zwar grundsätzlich sogenannte *Trusted- Plattform-Modul-Chips* (TPM-Chips), diese eignen sich allerdings in der verbreiteten Version 1.2 [3] nicht unbedingt dafür, weil ein Angreifer mit physischem Zugang diesen Chip nach Belieben belauschen kann, und auch Kommunikation manipulativ einspielen kann, um den Chip zur Herausgabe des Schlüssels zu bewegen. In der Version 2.0 des TPM-Standards wird es dafür geeignetere Lösungen geben. Programmierbare CPU-basierte Sicherheitschips, die bisher hauptsächlich in Anwendungen wie hoheitlichen Dokumenten (Reisepässe) und Pay-TV eingesetzt wurden, sind nun auch für eingebettete Systeme verfügbar und erlauben es, relevante Teile der eigentlichen Systemfunktion, daher Software-Teile, gemeinsam mit schützenswerter Information und Schlüsseln in den Sicherheitschip zu ziehen und damit abzukapseln. Dies ist in vielen Fällen eine besonders solide Methode für sicheres Speichern. Es gibt auch einige System-on-Chips, die zusätzliche und weitgehend isolierte Mikrokontroller mit eigenem Speicher zusätzlich zu dem Hauptsystem für Sicherheitszwecke integrieren. Diese Plattformen sind auch geeignet, um sicheres Speichern zu gewährleisten.

Sollte es nicht möglich sein, Schlüsselmaterial auf einem Gerät ausreichend zu sichern, kann versucht werden, im Zentralsystem Routinen vorzusehen, die es ermöglichen, kompromittierte Geräte zu detektieren und auszuschließen. In diesem Kontext sind Methoden relevant, die darauf abzielen, kompromittiertes bzw. anomales Verhalten von Geräten mithilfe von maschinellen Lernverfahren zu detektieren.

C. Debug-Schnittstellen

Während der Entwicklung und zur Fehleranalyse von Chips aus der Produktion ist es notwendig, Möglichkeiten zur Analyse bzw. zum *Debugging* vorzusehen. Allerdings sind genau solche Zugänge im Betrieb ein Sicherheitsproblem, weil damit sensible Speicherinhalte ausgelesen werden können. In vielen Fällen gibt es Möglichkeiten, diese Zugänge für den Feldeinsatz zu schließen, was absolut notwendig ist. Daher ist es wichtig, geeignete Chips auszuwählen, die dies vorsehen. Außerdem ist es wichtig, dass keine weiteren, nicht dokumentierten Hersteller-Zugangsfunktionen bestehen, die zu einem späteren Zeitpunkt öffentlich werden, was beispielsweise für einen FPGA-Chip 2012 öffentlich bekannt wurde [4].

D. Kommunikation zu zentralen Ressourcen

Zentrale Ressourcen spielen eine wichtige Rolle in vernetzten eingebetteten Systemen. Daher ist es immens wichtig, dass die Authentizität dieser sichergestellt ist. Der Nachweis der Authentizität des Server wird üblicherweise per Zertifikat erbracht, das ein Server dem Gerät beim Verbindungsaufbau präsentiert. Das Gerät muss dann allerdings die Authentizität des Zertifikats prüfen. Das kann anhand eines übergeordneten Zertifikats geschehen. Empfehlenswert ist, ein sogenanntes *Zertifikats-Pinning* umzusetzen, bei dem nur schon dem Gerät bekannte Zertifikate akzeptiert werden,

um zu verhindern, dass ein Angreifer dem Gerät ein Zertifikat präsentiert, das zwar aufgrund von Fehlkonfiguration als echt verifiziert wird, aber zu einem anderen Server gehört.

Der Verbindungsaufbau erfolgt mithilfe von umfangreichen kryptografischen Protokollen wie TLS [2]. Dabei sollte man allerdings darauf achten, immer die aktuellen Versionen, daher z. B. TLS 1.2, zu verwenden, da in neuen Versionen bekannte Sicherheitsschwachstellen geschlossen wurden. Da die Implementierung typischerweise komplex ist, treten immer wieder Schwachstellen aus Implementierungsfehlern auf. Aus Gründen der Rückwärtskompatibilität stellt TLS außerdem eine größere Anzahl an möglichen Algorithmen-Kombinationen (*Cipher Suites*) an, wobei nicht mehr alle einem zeitgemäßen Sicherheitsanspruch genügen (RC4, 512 Bit RSA). Diese müssen daher dringend deaktiviert werden.

E. Manipulationsschutz der Software beim Start

Nach dem Einschalten der Spannungsversorgung läuft eine CPU üblicherweise mit dem ersten Code los, der fest in dem CPU-Chip hinterlegt ist (ROM Maske). Danach springt die CPU in einen der Speicher, um sich dort den nächsten ausführbaren Code zu holen. Ist der Speicher bzw. die Schnittstelle nicht gesichert, kann ein Angreifer dem System manipulierte Software unterschieben. Dies lässt sich durch sogenannte Secure-Boot-Mechanismen verhindern. Dabei wird nur der Code ausgeführt, der von dem davor laufenden Code kryptografisch auf Authentizität geprüft bzw. gemessen wird. Dazu ist es allerdings notwendig, dass bereits der erste in der CPU laufende Code diesen Mechanismus unterstützt und über entsprechendes Schlüsselmaterial verfügt. Man nennt dies dann einen *Core Root of Trust*. Diese Funktion lässt sich nicht nachrüsten und ist einer der Punkte, an dem die Auswahl des Chips eine hohe Auswirkung auf die spätere Systemsicherheit hat. Es ist zu empfehlen, CPUs mit integriertem Secure Boot zu wählen.

F. Aktualisierungsmechanismen

Ein charakteristisches Merkmal von eingebetteten Systemen ist, dass sie in vielen Anwendungsfällen für viele Jahre im Feld im Betrieb sind. Dabei kann die elektronische Hardware nicht verändert werden. Die Möglichkeiten, Software zu aktualisieren, sind bisher auch meist stark begrenzt. Dies steht im Gegensatz zu Endnutzergeräten wie Mobiltelefonen, die nach drei bis fünf Jahren mit hoher Wahrscheinlichkeit aus dem Feld verschwunden sind und üblicherweise bereits laufend Aktualisierung erfahren. Ein langer Einsatzzeitraum bedeutet auch, dass Angreifer viele Jahre Zeit haben, um Angriffspunkte zu entdecken und untereinander zu verbreiten. Mögliche Angriffspunkte resultieren oft aus Fehlern in der Entwicklung. Allerdings scheint es unmöglich, fehlerfreie Software zu entwickeln, obwohl seit vielen Jahren an entsprechender Entwicklungsunterstützung geforscht wird. Selbst bei hohem Entwicklungsaufwand kann eine gewisse Fehlerrate wohl nie ausgeschlossen werden. Aus diesem Grund ist es alternativlos, Aktualisierungsmöglichkeiten vorzusehen. Aktualisierung erfordert sichere Kommunikationskanäle zur Verteilung der Updates (wie zuvor beschrieben) und Möglichkeiten, die Authentizität der neuen Software zu prüfen, was im Zuge eines Secure Boot Mechanismus durchgeführt werden kann.

Aktualisierungsfunktionen sind im Kontext von Anwendungen, die Zertifizierungen und Zulassungen benötigen, zusätzlich herausfordernd, da beispielsweise Teile der Zulassung wiederholt werden müssen, wenn sich die Software ändert. Außerdem ist die Verfügbarkeit bzw. Laufzeitstabilität delikat, da es in kritischen Anwendungen keinesfalls zu Ausfällen kommen darf, wenn beispielsweise verschiedene Geräte eines Geräteverbunds zu unterschiedlichen Zeiten aktualisiert werden. Trotzdem ist eine Möglichkeit zur Aktualisierung aus Informationssicherheits-Gesichtspunkten als absolut notwendig zu betrachten.

G. Isolation von Funktionen und Software

Auf einem eingebetteten System gibt es Software und Daten von unterschiedlicher Kritikalität. Den höchsten Schutz benötigen beispielsweise geheime Schlüssel und Verschlüsselungsroutinen. Wie zuvor erläutert, ist es unrealistisch, dass die gesamte Software eines Systems fehlerfrei entwickelt wurde. Man muss daher davon ausgehen, dass Schwachstellen in gewissen Teilen der Software auftreten und potenziell ausgenutzt werden könnten. Wenn eine Software-Schwachstelle zur Laufzeit genutzt wird, kann der Angreifer üblicherweise mit den Rechten im System agieren, die dieser Teil der Software bzw. dieser Prozess innehatte. Um das Gesamtsystem oder kritische Teile dagegen zu schützen, versucht man, diese Teile der Software zu isolieren, sodass erfolgreiche Angriffe auf nicht-kritische Teile eines Systems davon isoliert bleiben. Dies gelingt am überzeugendsten durch zusätzliche Hardware-basierte Mechanismen. Beispiele dafür sind die Trust-Zone-Technologie von ARM, die eine isolierte und sichere Laufzeitumgebung durch eine Hardware-Erweiterung schafft, oder ähnlich auch Intels Software *Guard Extensions* (SGX). Es ist allerdings notwendig, Chips mit der entsprechenden Technologie zu wählen, weil sie nicht nachgerüstet werden kann.

Hersteller von System-on-Chip-Plattformen bieten bereits Architekturen an, die abgesehen von der hauptsächlichen (multi-Prozessor)

Anwendungs-CPU und angebundenen peripheren Komponenten auch einen weiteren Mikrokontroller mit eigenem Speicher integrieren, der nur durch eine minimale Schnittstelle an das Bussystem angebunden wird, um ein hohes Maß an Isolation zu erreichen (beispielsweise Infineon oder Freescale). So kann auf dieser weitgehend isolierten Recheneinheit eine Form eines Hardware-Secure-Modules (HSM) mit minimaler API realisiert werden auf das die Software auf der Haupt-CPU nur eingeschränkten Zugriff hat. So bleiben geheime Schlüssel zum Beispiel unberührt, weil sie im getrennten Speicher des HSM liegen.

Es gibt auch weitere Mechanismen zur Isolation, genannt Virtualisierung, bei denen die CPU-Hardware in einem zusätzlichen komplexeren Software-System (*Virtual Machine Manager* oder *Hypervisor*) mithilfe von etwas Hardware-Funktion abstrahiert wird, und mehreren darauf laufenden regulären Systemen voneinander isoliert zur Verfügung gestellt wird. Die Ansätze unterscheiden sich in ihren Eigenschaften, und sind jeweils einer Verbesserung der Systemsicherheit zuträglich. Ansätze, die auf komplexeren Software-Architekturen, wie Virtualisierung und Kernel-Level-Isolation, basieren, bieten eine etwas größere Angriffsfläche für Software-Angriffe, weil Schwachstellen in den Implementierungen eben dieser Software-Architekturen enthalten sein könnten.

Empfehlenswert ist jedenfalls, kritische und geheime Teile des Systems möglichst zu isolieren, wobei die konkrete Methode in Abhängigkeit der konkreten Umstände ausgewählt werden muss.

6 Zusammenfassung und Empfehlungen

Die konkret notwendigen Informations-Schutzmaßnahmen für ein eingebettetes System im Internet der Dinge werden immer von den individuellen Umständen einer Anwendung abhängen. Trotzdem ist zusammenfassend zu betonen, dass Hardware-basierte Sicherheit einen hohen Stellenwert einnimmt, da die Angreifer Hardware-Zugriff haben. Daher ist es notwendig, gewisse Hardware-basierte Schutzmaßnahmen wie einen sicheren Boot-Prozess durch Auswahl eines geeigneten Prozessors, sichere Speicher für Schlüssel beispielsweise durch Integration eines Sicherheitschips, deaktivierbare Debug-Schnittstellen und Isolierungsunterstützung durch Auswahl des Prozessors schon beim Systemdesign vorzusehen, weil kein nachträgliches Umrüsten möglich ist. Zu empfehlen ist, das Sicherheitskonzept schon früh im Entwicklungsprozess zu erarbeiten und auf entsprechende Produkteigenschaften bei der Auswahl der Komponenten zu achten. Aktualisierungsmöglichkeiten für die Software des Systems ist aus Sicht der Informationssicherheit ebenfalls definitiv notwendig. Bei der Anwendung von kryptografischen Algorithmen sollte auf etablierte oder geprüfte Implementierungen gesetzt werden, um Implementierungsangriffe zu verhindern. Dabei kann mit einem vorteilhaften Schlüsselkonzept die Angriffsfläche der Einzelgeräte entscheidend verringert werden.

Zusammenfassend ist die zentrale Herausforderung für Informationssicherheit von eingebetteten Systemen, diese von Beginn an mit ausreichenden Schutzmaßnahmen in den unveränderlichen Hardware-Komponenten auszurüsten, sodass eine langfristige Gewährleistung von Informationssicherheit im Betrieb gelingt.

Referenzen

[1] BSI, *Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung*, Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, BAnz AT 01.02.2016 B5, Dezember 2015

[2] RFC 5246: *The Transport Layer Security (TLS) Protocol Version 1.2*, IETF, August 2008

[3] ISO/IEC 11889-1:2009, *Information technology — Trusted Platform Module*, ISO/IEC, 2009

[4] Skorobogatov et al. *Breakthrough Silicon Scanning Discovers Backdoor in Military Chip*, Proceedings of the 14th International Conference on Cryptographic Hardware and Embedded Systems, Springer, 2012

Konfigurationsanforderungen an Betriebssysteme

Ulrich Grottker*, Reinhard Meyer**

1 Einleitung

Neue Technologien wie das *Internet of Things* (IoT) (siehe „Digitalisierung im gesetzlichen Messwesen", Seite 5 und „Sichere Architekturen für eingebettete Systeme im gesetzlichen Messwesen", Seite 45) benötigen kleine Komponenten, die dennoch hohe Rechenleistung liefern, damit sie die komplexe Kommunikation mit der Infrastruktur und immer anspruchsvollere Funktionen bewerkstelligen können. Die fortschreitende Miniaturisierung der Mikroprozessoren bei gleichzeitiger Steigerung der Rechenleistung ermöglicht den Einsatz von Betriebssystemen mit all ihren Vorzügen selbst in sehr kleinen Geräten wie z. B. Messgeräten.

Werden Messgeräte im gesetzlich geregelten Bereich eingesetzt, müssen sie die gesetzlichen Vorgaben einhalten. Es existieren bereits mehrere nationale [1, 2], europäische [3, 4, 5] und internationale Leitfäden [6], die die gesetzlichen Vorgaben hinsichtlich Software interpretieren. Der Schwerpunkt bei diesen Leitfäden liegt auf den Anforderungen an die eigentliche metrologische und eichrechtlich relevante Anwendungssoftware, der Unterbau wie Betriebssysteme wird nur punktuell behandelt. Dies ist gerechtfertigt, wenn die gesetzlich geforderten Sicherungsmaßnahmen allein von der Anwendungssoftware realisiert werden.

Nun bieten Betriebssysteme – insbesondere *Multiuser*-Betriebssysteme – neben den bekannten Vorzügen von grafischen Benutzeroberflächen und komplexen Kommunikationsprotokollen (*Protokoll-Stacks*) Hilfsmittel zur Sicherung von Daten und Programmen gegen unzulässige Beeinflussung durch die verschiedenen Benutzer des Systems. In eichpflichtigen Messgeräten lassen sich diese Schutzmechanismen, die bei normaler Nutzung des Betriebssystems dazu dienen, die den jeweiligen Benutzerrollen zugeordneten Bereiche für Programme und Daten (Domänen) gegen unzulässige Beeinflussung durch andere Nutzer zu schützen, sehr gut zur Umsetzung verschiedener Anforderungen im gesetzlichen Messwesen verwenden.

Eine akzeptable technische Lösung für die Absicherung eines Messgerätes beinhaltet immer ein Bündel von Schutzmaßnahmen im Betriebssystem, in Software-Anwendungen und in der Hardware, die sich geeignet ergänzen. Der Hersteller des Messgerätes bestimmt die Wahl der Mittel, aber das Messsystem als Ganzes muss die folgende grundlegende Anforderung erfüllen:

Sämtliche Schutzmaßnahmen bestehend aus der Funktionalität und der Konfiguration des Betriebssystems, Maßnahmen in der Anwendungssoftware und Maßnahmen in der Hardware müssen sich so ergänzen, dass die gesetzlichen Anforderungen erfüllt werden.

Bild 1 zeigt die typische Konfiguration eines Messgerätes mit einem integrierten Linux-Rechner. Genau genommen besteht das Messgerät nur aus wenigen zusätzlichen Bauelementen: dem Sensor, einem Display mit eventuell vorhandenen Bedienelementen und der Stromversorgung. Bei konventionellen Lösungen mit einem fest programmierten Mikrocontroller würde z. B. der WELMEC-Leitfaden 7.2 angewandt werden, um die gesetzlichen Anforderungen [MID [7], MEG [8], MEV[9]] zu erfüllen. Dieser Leitfaden enthält für Typ-U-Konfigurationen ebenfalls Anforderungen, welche bei integrierten universellen Computern angewandt werden sollen, jedoch ist der Bezug zu den komplexen Konfigurationsmöglichkeiten eines Universal-Betriebssystems wie Linux oder Windows kaum erkennbar; der Fokus des [W7.2] liegt auf der Anwendungssoftware eines Messgerätes.
AG 8.51 erarbeitet einen ergänzenden Leitfaden, der die spezifischen Anforderungen an universelle Betriebssysteme konkretisiert.

* Dr. Ulrich Grottker, ehemals Arbeitsgruppe 8.51 "Metrologische Software"

** Reinhard Meyer, Arbeitsgruppe 8.51 "Metrologische Software", E-Mail: reinhard.meyer@ptb.de

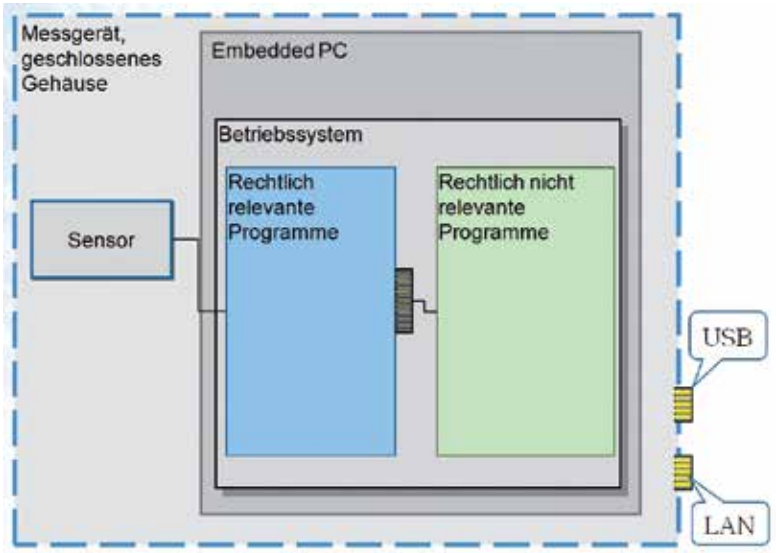

Bild1: Blockschaltbild eines typischen Messgerätes mit integriertem Universalrechner

Im Folgenden wird erläutert, wie die Eigenschaften eines Multiuser-Betriebssystems genutzt werden können, um einige von der Mess- und Eichverordnung [MEV] geforderten und in Leitfäden z. B. [W7.2] spezifizierten Schutzanforderungen zu realisieren.

2 Schutz eichrechtlich relevanter Software auf Plattformen mit Betriebssystem

2.1 Realisierung der Softwaretrennung mit Mitteln des Betriebssystems

In [MEV], Anlage 2 zu §7, Punkt 7.7 wird gefordert:

„Wenn ein Messgerät über zugehörige Software verfügt, die neben der Messfunktion weitere Funktionen erfüllt, muss die für die messtechnischen Merkmale entscheidende Software identifizierbar sein. Sie darf durch die zugehörige Software nicht in unzulässiger Weise beeinflusst werden.“

Werden entscheidende und zugehörige Softwareteile verschiedenen Benutzerkonten des Betriebssystems zugeordnet, so gewährleistet das Betriebssystem – bei richtiger Konfiguration – dass eine Beeinflussung der entscheidenden durch die zugehörige Software nicht möglich ist. Es ist nicht erforderlich, dass ein Verwender des Messsystems tatsächlich über eine Bedienoberfläche oder Kommandozeile Zugang zu diesen Benutzerkonten bekommt; es ist lediglich zu gewährleisten, dass der Schutz der Konten gemäß den Konfigurationsanforderungen (siehe 4.4) realisiert wird.

Befindet sich die entscheidende Software komplett und ausschließlich in der Domäne eines Benutzerkontos und die zugehörige Software in der Domäne eines anderen und sind die Benutzerkonten so konfiguriert, dass sie keine Schreibrechte auf Daten und Programme des jeweils anderen Nutzers haben, so erfüllt das System bezogen auf diese Softwareteile die Anforderung [W7.2] S1, bzw. [A50.7–3].

Die Kommunikation zwischen den Softwareteilen kann über vom Betriebssystem bereitgestellte Kanäle erfolgen (IPC – Interprozesskommunikation). In der eichrechtlich relevanten Anwendung befindet sich eine Softwareschnittstelle zum Kommunikationskanal des Betriebssystems. Wird die Rückwirkungsfreiheit dieser Schnittstelle in der Anwendung und auf Ebene der Betriebssystemressourcen nachgewiesen, so ist damit die Anforderung [W7.2] S3, bzw. [A50.7–3] erfüllt.

Neben den mindestens zwei Benutzerkonten für die entscheidenden und die zugehörigen Softwareteile sollte es ein weiteres Benutzerkonto für Systemfunktionen (z. B. das Administratorkonto) geben. Dieses Benutzerkonto beinhaltet die Schutzfunktionen und deren Konfigurationsparameter. Die Anforderungen in Abschnitt 4.4 sollen gewährleisten, dass die Schutzfunktionen nicht aus der Domäne des Benutzerkontos für die zugehörige Software beeinflusst werden kann und dass die Anwendungen in der Domäne der entscheidenden Software die Systemfunktionen nur in zulässiger Weise beeinflussen können.

Ist dieser Nachweis gelungen, so können Anwendungen in der Domäne der zugehörigen Software auch im Betrieb ausgetauscht werden, ohne dass die Messsicherheit dadurch beeinträchtigt werden kann. Die in 2.5 beschriebenen Anforderungen bezüglich der zugehörigen Software brauchen dann nicht beachtet zu werden.

2.2 Schutz von eichrechtlich relevanten Parametern

Das Betriebssystem stellt Mittel bereit, um eichrechtlich relevante Parameter zu speichern und gegen unerkennbare Änderung zu schützen. Der Zugriff sollte wieder mithilfe der Schutzmechanismen für die Datenbereiche von Benutzerkonten verhindert werden. Soll eine Parameteränderung im Betrieb ermöglicht werden, so kann ein Programm unter dem geschützten eichrechtlich relevanten Benutzerkonto diese Änderung durchführen, in einem dauerhaften Eichlog oder Ereigniszähler registrieren und dem Verwender durch eine Anzeige kenntlich machen („elektronisches“ Siegel).

2.3 Benutzerschnittstelle, Anzeige

Plattformen mit Betriebssystem bieten komfortable und ergonomische Realisierungsmöglichkeiten von Benutzerschnittstellen und Anzeigen. Als Anzeige eines Messgerätes muss sie bestimmte Anforderungen erfüllen, wie Unverwechselbarkeit mit anderen Anzeigen und nicht unterdrückbarer Präsenz während der Messung [W7.2], S2. Diese Einschränkungen lassen sich mit der richtigen Konfiguration des Betriebssystems umsetzen.

2.4 Rückwirkungsfreiheit von Schnittstellen

Plattformen mit Betriebssystem sind dadurch gekennzeichnet, dass sie mit einer Vielzahl von Schnittstellen ausgestattet sind, über die die Kommunikation mit unterschiedlichen Übertragungstechnologien erfolgt. Meist können mehrere voneinander unabhängige Kanäle gleichzeitig über eine Hardware-Schnittstelle betrieben werden. Es sind drei Fälle zu unterscheiden:

- Die Kommunikation über einen Übertragungskanal wird von einer eichrechtlich relevanten „entscheidenden" Anwendung kontrolliert.
- Die Kommunikation über einen Übertragungskanal wird von einer eichrechtlich nicht relevanten „zugehörigen" Anwendung kontrolliert.
- Die Kommunikation über einen Übertragungskanal wird von einem Programm kontrolliert, das Bestandteil des Betriebssystems ist (z. B. ein sogenannter „Dienst").

Gemäß [MID], Annex I, 8.1 und [MEV], Anl. 2, 8.1 dürfen die messtechnischen Merkmale durch das Anschließen eines anderen Gerätes an das Messgerät nicht in unzulässiger Weise beeinflusst werden. Dies gilt für alle oben genannten Fälle. In [W7.2] wird diese Anforderung berücksichtigt, bezieht sich aber primär auf die vom Messgerätehersteller bereitgestellten eichrechtlich relevanten Anwendungen. Mit den Anforderungen an die Konfiguration des Betriebssystems in Abschnitt 4 soll erreicht werden, dass die eichrechtlich relevanten Funktionen des Messgerätes auch nicht indirekt beeinflusst werden können und zwar weder mittels der Übertragungskanäle von eichrechtlich nicht relevanten Anwendungen, noch über Kanäle, die vom Betriebssystem verwaltet werden. Die eichrechtlich relevanten Anwendungen sollen mit Mitteln der Betriebssystemkonfiguration gekapselt werden. Die Maßnahmen ergänzen sich mit den in Abschnitt 2.1 beschriebenen Maßnahmen zum Schutz der Kommunikationskanäle zwischen Anwendungen.

2.5 Laden von Programmen im Betrieb

Mit dem neuen MessEG/EV wird erstmals für Deutschland geregelt, wie Software bei in Verwendung befindlichen Messgeräten erneuert werden kann, ohne dass ein Siegelbruch und damit eine Nacheichung erfolgen muss. Um ein Softwareupdate automatisch und aus der Ferne dem Gesetz entsprechend ausführen zu können, müssen nach [MEG, MEV] verschiedene Anforderungen erfüllt werden, die im Wesentlichen denjenigen in [W7.2], D1–D4 entsprechen. Im Einzelnen betreffen diese Anforderungen die Steuerung des Update-Vorgangs, die Authentizitäts- und Integritätsprüfung sowie Maßnahmen zur Nachvollziehbarkeit des Vorgangs für Kontrollzwecke als Ersatz für einen Siegelbruch. Mithilfe einer geeigneten Betriebssystemkonfiguration können diese Anforderungen sehr sicher und einfach erfüllt werden.

2.6 Verwendung einer Betriebssystemplattform in einem Messsystem ohne besondere Anforderungen an die Konfiguration des Betriebssystems

Eine besonders einfache technische Lösung für ein Messsystem mit Betriebssystemplattform kommt ohne die in Abschnitt 4 beschriebenen Anforderungen an die Konfiguration des Betriebssystems aus. Das Messsystem besteht in diesem Fall aus zwei Komponenten: einem Messwertaufnehmer mit Mikrocontroller und einem Rechner mit Betriebssystem. Es arbeitet mit verschlüsselter Übertragung zwischen dem Messwertaufnehmer und der eichrechtlich relevanten Anwendung / der eichrechtlich relevanten Anzeige. Eine genaue Beschreibung dieser technischen Lösung ist in [W7.2], U8 zu finden.

3 Prozess der Anforderungserhebung und -umsetzung

Aus den Ausführungen in 2.1–2.5 wird ersichtlich, dass zur Umsetzung dieser speziellen Schutzmaßnahmen eine Interpretation des Gesetzes und insbesondere der Anlage 2 der Mess- und Eichverordnung [MEV] für Hersteller und Prüfstellen notwendig ist. Das folgende Bild veranschaulicht den Prozess von der Identifizierung einer relevanten gesetzlichen Anforderung bis zur Erstellung von Prüfanweisungen und Beispielen von akzeptablen technischen Lösungen für einzelne Plattformen (Kombinationen aus Betriebssystem und Hardware-Architektur).

Im oberen Bereich des Bildes 2 sind die Anforderungen an eine mögliche Konfiguration des Betriebssystems dargestellt, die sich aus den gesetzlichen Regelungen ergeben [MID, MEV]. Diese sind aus der Sicht des Gesetzgebers und damit sehr generisch formuliert. Deshalb werden als weitere Referenzen bereits existierende technische Leitfäden auch aus benachbarten Bereichen herangezogen. Dazu gehören der WELMEC-Leitfaden 7.2 Software, aber auch in der BSI-Schriftenreihe zur Internet-Sicherheit (ISi)[1] und den NIST-Guidelines[2] veröffentlichte Anforderungen. Am Ende dieses Schrittes ergeben sich eine Anzahl grundlegender Anforderungen an die Betriebssystemkonfiguration für Messsysteme, die aber immer noch plattformübergreifend gelten.

[1] https://www.bsi.bund.de/DE/Themen/StandardsKriterien/ISi-Reihe/ISi-Reihe_node.html

[2] http://csrc.nist.gov/publications/Pubs-SPs.html

(Letzter Zugriff jeweils am 28.11.2016)

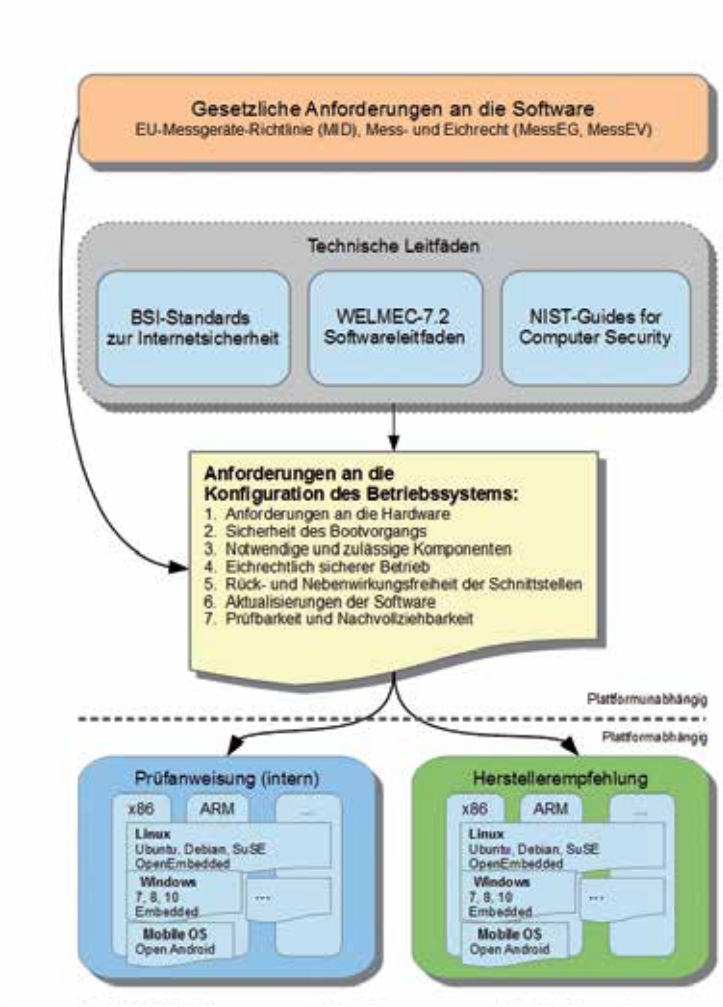

Bild 2: Ableitung von Anforderungen zur Betriebssystem-Konfiguration als Bestandteil des Messsystems

In der nächsten Entwicklungsstufe werden aus den Anforderungen prototypisch Konfigurationen für betriebsbewährte Plattformen erstellt und schrittweise verfeinert. Dadurch wird bereits bei einem großen Teil der Vorgänge die Konstruktion und Prüfung der betriebssystemgestützten Messgeräte erleichtert. Jedoch werden Hersteller und Prüfer bei anderen, experimentelleren Plattformen die Beispiele für den jeweiligen Bewertungsvorgang interpretieren müssen. Die dabei gesammelten Erfahrungen sollen systematisch beschrieben und in einer Datenbank (*Knowledge-Base*) gesammelt werden. Auf diese Weise wird die Konfiguration der Plattform und deren Prüfung kontinuierlich effizienter gestaltet werden können.

4 Anforderungen an die Eigenschaften der Betriebssystemplattform als Bestandteil des Messsystems

In Abschnitt 2 wurde erläutert, für welche eichrechtlich geforderten Funktionen und Eigenschaften eines Messsystems die Schutzmechanismen eines Multiuser-Betriebssystems verwendet werden können. In diesem Abschnitt werden die Anforderungen an die Konfiguration des Betriebssystems konkretisiert, die gewährleisten sollen, dass ein Messsystem mit Betriebssystem als Ganzes die grundlegenden eichrechtlichen Anforderungen [MEV] erfüllt.

4.1 Anforderungen an die Hardware

Neben den Anforderungen an die softwaretechnische Konfiguration des Betriebssystems sind zusätzlich Anforderungen an die Hardware, die zur Ausführung des Betriebssystems benötigt wird, zu befolgen. Dabei stellt die Hardware insbesondere Funktionalitäten bereit, um eine Vertrauenskette von einem hardwaretechnischen Sicherheitsanker bis hin zu der ausführbaren rechtlich relevanten Anwendung zu realisieren.

Es wird gefordert, dass Massenspeicher, die das Betriebssystem, eichrechtlich relevante Programme und/oder Parameter beinhalten oder von denen gebootet werden kann, physisch gegen Austausch geschützt werden. Auch offene Schnittstellen, über die Massenspeicher verbunden werden können, von denen gebootet werden kann, müssen mittels physischer Sicherung gegen Anschluss unzulässiger Medien geschützt werden.

4.2 Sicherheit des Bootvorgangs

Zur Fortsetzung der Vertrauenskette und um sicherzustellen, dass die richtigen Anwendungen in der richtigen Reihenfolge gestartet werden, sind Anforderungen an den Bootvorgang formuliert worden. Diese stellen auch sicher, dass kein weiteres, nicht durch die Konformitätsbewertung abgedecktes Betriebssystem gestartet wird.

Es muss gewährleistet sein, dass alle Funktionen des Betriebssystems, die für die eichrechtlich relevanten Funktionen und die Schutzmaßnahmen des Messsystems notwendig sind, bei jedem Bootvorgang gestartet werden. Es muss außerdem gewährleistet sein, dass Funktionen des Betriebssystems, die die eichrechtlich relevanten Funktionen oder Schutzmaßnahmen des Messsystems beeinträchtigen können, während des Bootvorgangs nicht gestartet werden.

Falls die Reihenfolge der Starts der Teilfunktionen des Betriebssystems und der Applikationen Einfluss auf die eichrechtlich relevanten Funktionen und die Schutzmaßnahmen des Messsystems haben kann, muss gewährleistet werden, dass bei jedem Bootvorgang die richtige Reihenfolge eingehalten wird.

4.3 Notwendige und zulässige Bestandteile und Funktionen des Betriebssystems

Die Funktionalität eines Multiuser-Betriebssystems im Rahmen einer Konformitätsbewertung zu validieren, ist unmöglich. Dies ist nicht ein spezielles Problem im gesetzlichen Messwesen. Selbst in

sicherheitsrelevanten Anwendungen wird in gewissen Fällen auf die Validierung gezwungenermaßen verzichtet. Nun werden Betriebssysteme in sehr großer Zahl verwendet und Fehler werden regelmäßig behoben. Nachdem ein Betriebssystem eine gewisse Zeit lang in unterschiedlichen Anwendungsumgebungen im Einsatz war und die Fehler vom Hersteller fortwährend behoben wurden, gilt das Betriebssystem als „betriebsbewährt". Darauf bauen die Anforderungen auf.

Es dürfen nur universelle betriebsbewährte Betriebssysteme zum Einsatz kommen. Sie dürfen nicht speziell für das Messgerät konzipiert worden sein. Nur in diesem Fall kann auf eine Prüfung des Betriebssystems verzichtet werden. Bei modularen Betriebssystemen und Kerneln muss der Hersteller eine betriebsbewährte Zusammenstellung von Modulen als Referenz angeben (z. B. von einer handelsüblichen Distribution). Abweichungen der Zusammenstellung oder eigene Veränderungen der Module müssen dokumentiert werden. Veränderte Module werden wie eichrechtlich relevante Applikationen behandelt.

Es dürfen nur Funktionen (Dienste) des Betriebssystems gestartet werden, die zum Betrieb des Betriebssystems gemäß Vorgaben des Betriebssystemherstellers und der eichrechtlich relevanten Applikationen notwendig sind. Werden andere Funktionen für andere Zwecke aktiviert, muss nachgewiesen werden, dass weder die sichere Konfiguration des Betriebssystems noch die eichrechtlich relevanten Applikationen unzulässig beeinflusst werden kann.

Aktivierte Funktionen (Dienste), die eine Kommunikation über die lokale Benutzerschnittstelle oder über eine Kommunikationsschnittstelle ermöglichen, müssen die Anforderungen der Rück- und Nebenwirkungsfreiheit (4.5.1) erfüllen.

4.4 Eichrechtlich sicherer Betrieb

Durch die Erfüllung der oben genannten Anforderungen gelangt das System in einen eichrechtlich sicheren Betriebszustand. Verschiedene weitere Maßnahmen sorgen dafür, dass die eichrechtlich relevanten Messgeräteeigenschaften im Betrieb erhalten bleiben. Dabei soll die Verwendung für eichrechtlich nicht relevante Zwecke ermöglicht werden, jedoch hat die Einhaltung der eichrechtlichen Anforderungen Vorrang.

Durch geeignete Konfiguration können die Zugriffsrechte auf Programme und Daten so eingestellt werden, dass eichrechtlich relevante „entscheidende" Software nicht durch andere unzulässig beeinflusst werden kann. Entsprechende konkrete Anforderungen befinden sich in Abschnitt 4.4.1. Hierzu gehört auch, dass durch Anforderungen geregelt werden muss, unter welchen Bedingungen ein Verwender des Messgeräts oder sonstige Rollenvertreter Zugang zu den Benutzerkonten erhalten, um bestimmte Aktionen und Bedienhandlungen an dem Messgerät durchführen zu können (Benutzer-Authentifizierung und -Autorisierung, siehe 4.4.4).

Eine indirekte Beeinflussung der eichrechtlich relevanten Funktionen ist möglich, falls eichrechtlich relevante und nicht relevante Software um gemeinsam genutzte Ressourcen konkurrieren müssen. In Abschnitt 4.4.2 werden Anforderungen genannt, die gewährleisten sollen, dass die eichrechtlich relevanten Funktionen immer Vorrang vor den übrigen Funktionen haben.

Sämtliche Funktionen und Konfigurationen, die aus den Anforderungen dieses Dokuments resultieren, sind als Programme, Skripte oder Konfigurationsdateien realisiert. Diese müssen selbst durch Schutzmaßnahmen vor unzulässigem Zugriff geschützt werden. Die entsprechenden Anforderungen werden in Abschnitt 4.4.3 genannt.

Für Benutzerauthentifizierung, Booten in einer *Trusted Chain*, Softwareupdates und Schutzmaßnahmen wird ein Sicherheitsanker benötigt. Die Anforderungen an den Sicherheitsanker werden in Abschnitt 4.4.4 genannt.

4.4.1 Schutz der rechtlich relevanten Daten- und Programmbereiche vor unzulässiger Veränderung

Ein Schutzmechanismus gegen unzulässige Zugriffe auf Programme, Daten und Parameter beruht darauf, dass ein Administrator den Benutzern des Systems die Berechtigungen für einen Zugriff auf jede einzelne Datei gibt oder versagt und dass er die Art des Zugriffs (mindestens Lesen, Schreiben und Ausführen – *Discretionary Access Control* (DAC)) festlegt. Auf der anderen Seite wird der Benutzer mit einem Namen dem System bekannt gemacht. Hat sich der Benutzer mithilfe eines Geheimnisses, das im System hinterlegt ist, authentifiziert, vergibt das System die zuvor festgelegten Zugriffsrechte. Werden die Zugriffsrechte entsprechend den Anforderungen gewählt, kann damit die Softwaretrennung nach [W7.2]/S1–S3 realisiert werden, da die Programm- und Datenbereiche des Benutzerkontos für die eichrechtlich relevanten Applikationen dadurch gegen Veränderung und Austausch geschützt werden.

Das Betriebssystem bietet für die Kommunikation zwischen Programmen die Interprozesskommunikation an. Diese lässt sich so konfigurieren, dass, bezogen auf das eichrechtlich relevante Programm, eine rückwirkungsfreie Softwareschnittstelle entsprechend [W7.2]/S3 entsteht. Alle eingehenden Befehle und Datenflüsse müssen dokumentiert werden. Auf nicht zulässige Befehle

darf die eichrechtlich relevante Applikation nicht reagieren und nicht zulässige Datenflüsse müssen blockiert werden.

Neben der Interprozesskommunikation zwischen eichrechtlich relevanten und nicht relevanten Applikationen gibt es auch Kommunikationskanäle von der Bedienoberfläche zur eichrechtlich relevanten Applikation und gegebenenfalls zu anderen eichrechtlich nicht relevanten Applikationen und zur Betriebssystem-Bedienschnittstelle. Mithilfe des Betriebssystems müssen diese Zugänge beschränkt oder gesperrt werden, damit für den Bediener keine unzulässigen Veränderungen an der Konfiguration und den eichrechtlich relevanten Funktionen und Daten möglich sind.

Häufig ist es am einfachsten, die Rückwirkungsfreiheit der Bedienschnittstelle nachzuweisen und zu prüfen, wenn dem Bediener überhaupt kein Zugang zur Benutzerschnittstelle des Betriebssystems gewährt wird. Die für den Benutzer sichtbare und bedienbare Oberfläche wird in diesem Fall von einer eichrechtlich relevanten Applikation gesteuert (Kiosk-Modus). Bei dieser Lösung wird gefordert, dass der Bootvorgang automatisch in den Start der Kiosk-Applikation mündet. Die Kiosk-Applikation darf bei beliebigen Bedienhandlungen, externen Ereignissen oder Fehlern nicht so reagieren, dass Betriebssystembefehle gegeben werden können oder die Bedienoberfläche des Betriebssystems erscheint.

4.4.2 Priorisierung der Plattform-Ressourcen für die eichrechtlich relevanten Funktionen

Bei der Verteilung der Ressourcen der Plattform wie Rechenleistung, Speicherplatz oder Übertragungsbandbreite müssen die eichrechtlich relevanten Anwendungen Vorrang vor anderen Anwendungen haben, wenn es für deren korrekte Funktion erforderlich ist. Die Konfiguration, durch die die Zuteilung festlegt wird, muss sich im geschützten Bereich des Systems (unter Schutzaccount) befinden.

4.4.3 Schutz der Systemkonfiguration durch ein besonders geschütztes Benutzerkonto

Bei Multiuser-Betriebssystemen ist immer mindestens ein Benutzerkonto vorhanden, das keinem normalen Benutzer sondern nur dem Administrator zugänglich ist. Dieses Konto hat volle Zugriffsrechte auf alle Systemressourcen. In einem eichpflichtigen System muss das Administratorkonto dazu verwendet werden, die eichrechtlich relevanten Funktionen sowie die Systemfunktionen und die Konfiguration des Betriebssystems zu schützen. Es wird als Schutzaccount bezeichnet. Die gesamte eichrechtlich relevante Betriebssystemkonfiguration in Form von Programmen, Skripten und Dateien muss sich im Programm- und Datenbereichen des Schutzaccounts befinden.

Die Programm- und Datenbereiche des Schutzaccounts müssen gegen Veränderung und Austausch geschützt werden. Hierzu müssen die Schutzmechanismen des Betriebssystems selbst benutzt werden. Das heißt, dass der Zugang zum Schutzaccount während der Verwendung des Messgerätes nur mit Siegelbruch möglich sein darf (siehe 4.4.4).

4.4.4 Eichrechtlicher Sicherheitsanker zur Realisierung von Zugangsbeschränkungen und des Schutzes der Konfiguration

An eichpflichtigen Messgeräten in der Verwendung dürfen keine Veränderungen vorgenommen werden können, die die Messgeräteeigenschaften unzulässig verändern, ohne dass diese Eingriffe für die zuständige Behörde erkennbar sind. Hierzu dienen physische Sicherungen in Form von Sicherungsmarken oder Plomben. Eine „elektronische“ Sicherung besteht aus Software, die die Eingriffe registriert und sichtbar macht, z. B. durch ein Kennzeichen in der Anzeige oder durch ein eichtechnisches Log, das zur Anzeige gebracht werden kann. Die elektronische Sicherung besteht aus Software, die selbst auch gegen unzulässige Veränderungen geschützt werden muss. Zur Sicherung dieser Software bleibt wiederum nur die eichtechnische physische Sicherung.

Eine Kette von aufeinander aufbauenden Software-Schutzmaßnahmen wird vertrauenswürdige Kette (*Trusted Chain*) genannt. Am Anfang dieser Kette befindet sich der Sicherheitsanker. Es gibt zwei Arten von eichrechtlichen Sicherheitsankern:

(a) Rollenfreier Sicherheitsanker: Um die Freigabe einer Funktion oder einer Information zu erhalten, muss der Bediener ein Geheimnis kennen und dieses dem Messgerät mitteilen.

(b) Rollengebundener Sicherheitsanker: Um die Freigabe einer Funktion oder einer Information zu erhalten, muss der Bediener dem Messgerät seine Identität zu erkennen geben und seine Vertrauenswürdigkeit beweisen.

Die Variante (b) beruht auf einem Rollensystem: Es wird festgelegt, welche Rollenvertreter Zugang zum Messgerät erhalten. Das Messgerät muss den zulässigen Freigabeumfang jeder Rolle kennen. Im gesetzlichen Messwesen kommt diese Art des Sicherheitsankers nur in Ausnahmefällen zur Anwendung. Nach dem MessEG/EV sind keine Rollen mit unterschiedlichen Rechten vorgesehen. Die Variante (a) beruht nicht auf Rollendefinitionen und ist deshalb die für das gesetzliche Messwesen am besten geeignete Lösung.

Der Sicherheitsanker besteht aus mehreren Komponenten.

(a) Bestandteile des rollenfreien Sicherheitsankers:

- Ein kryptografisches Geheimnis (z. B. geheimer Schlüssel, Passwort),
- Maßnahmen zum Schutz gegen unberechtigte, unerkennbare Veränderung und Austausch des Geheimnisses,
- Maßnahmen zur Verhinderung des Lesens der geheimen Information ohne Spuren zu hinterlassen,
- kryptografische Hilfsfunktionen, die es ermöglichen, das Geheimnis kryptografisch einzusetzen, z. B. für einen Vergleich von Soll- und Ist-Wert eines Passwortes, ohne dabei das Geheimnis preiszugeben.

(b) Bestandteile des rollengebundenen Sicherheitsankers:

- Speicher für kryptografische Zertifikate vertrauenswürdiger Stellen,
- Referenztabellen mit den für die jeweiligen Rollen zulässigen Aktionen,
- Maßnahmen zum Schutz gegen unberechtigte unerkennbare Veränderung und Austausch der Zertifikate und Referenztabellen,
- Kryptografische Hilfsfunktionen, die es ermöglichen, die Vertrauenswürdigkeit eines Anmeldenden anhand der Zertifikate oder die Echtheit eines kryptografischen Zertifikats zu ermitteln.

An den rollenfreien Sicherheitsanker werden die folgenden Anforderungen gestellt:
Das kryptografische Geheimnis des Sicherheitsankers muss unter dem Schutzaccount liegen und / oder durch physische eichtechnische Sicherung oder Verwendung von spezieller kryptografischer Hardware gegen Veränderung, Austausch oder Ausspähen gesichert sein.

Soll-Werte der Passworte für den Schutzaccount und den Benutzeraccount der eichrechtlich relevanten Applikationen dürfen nicht im Klartext im Datenbereich des Schutzaccounts abgelegt werden.

Wenn der Zugang zum Schutzaccount durch ein Passwort geschützt ist, muss dieses verborgen, nicht lesbar im oder am Messsystem angebracht werden und durch ein Siegel fixiert werden. Das Passwort muss beim Inverkehrbringen erzeugt, bei jeder Eichung erneuert und mit Siegel gesichert werden können.

Die kryptografischen Hilfsfunktionen des Sicherheitsankers, wie der Vergleich eines eingegebenen Passwortes mit seinem gültigen Soll-Wert, müssen unter dem Schutzaccount liegen und/oder durch Verwendung spezieller kryptografischer Hardware-Bausteine gegen Veränderung und Austausch gesichert sein.

Ist das Messsystem in eine *Public Key Infrastructure* (PKI) eingebunden, wird ein rollengebundener Sicherheitsanker benötigt. Dieser muss die folgenden Anforderungen erfüllen:

Der Speicher für kryptografische Zertifikate muss alle im Betrieb benötigten Zertifikate speichern können. Diese Zertifikate müssen vom Hersteller vor dem Inverkehrbringen im Zertifikatsspeicher abgelegt werden. Der Speicher für die kryptografischen Zertifikate muss unter dem Schutzaccount liegen und/oder durch physische eichtechnische Sicherung oder Verwendung von spezieller kryptografischer Hardware gegen Veränderung und Austausch gesichert sein.

Die kryptografischen Hilfsfunktionen des Sicherheitsankers müssen unter dem Schutzaccount liegen und/oder durch Verwendung spezieller kryptografischer Hardware-Bausteine gegen Veränderung und Austausch gesichert sein.

4.5 Rück- und Nebenwirkungsfreiheit von Schnittstellen an Plattformen mit Betriebssystem

Bei Plattformen mit Betriebssystem bedeutet die Rück- und Nebenwirkungsfreiheit von Hardware-Schnittstellen an der zu untersuchenden Messsystemkomponente, dass sowohl die Kommunikation der Anwendungen als auch des Betriebssystems und der Dienste über die betreffende Schnittstelle betrachtet werden müssen. Bei diversen Schnittstellen sind diese Kommunikationsformen (quasi-)parallel möglich. Die hier betrachteten Plattformen sind serienmäßig mit Schnittstellen ganz unterschiedlicher Technologie ausgestattet, die unterschiedliche Formen der Kommunikation ermöglicht. Diese Vielfalt macht es erforderlich, dass die eichrechtliche Anforderung der Rückwirkungsfreiheit der Technologie entsprechend interpretiert und spezifiziert werden muss. Im Folgenden werden die heute bekannten und im Allgemeinen serienmäßig vorhandenen Schnittstellen der betrachteten Plattformen klassifiziert. Für die jeweilige Schnittstellenklasse wurde ein Satz von angepassten Anforderungen definiert.

Grundsätzlich gelten die Anforderungen nur für Schnittstellen, die im Betrieb zugänglich sind. Durch physische Maßnahmen verschlossene und gesicherte Schnittstellen müssen die Anforderungen nicht erfüllen.

4.5.1 *Anforderungen an Schnittstellen vom Typ A*

Charakterisierung

Sämtliche Kommunikationskanäle, die diese Schnittstelle benutzen, stehen unter der Kontrolle von Anwendungen, gegebenenfalls basierend auf externen „Treibern“ (in das Betriebssystem integrierten Softwaremodulen), die die niedrigen Schichten z. B. des OSI-Kommunikationsmodells [OSI] [10] realisieren. Das Betriebssystem selbst kann diese Schnittstelle nicht verwenden.

Hinsichtlich der Rück- und Nebenwirkungsfreiheit ist die Schicht 7 („Anwendungsebene“ im OSI-Kommunikationsmodell [OSI]) von besonderer Bedeutung. Diese Kommunikationsebene kann entweder in einer Anwendung realisiert sein, die eichrechtlich relevante Funktionen ausführt (z. B. Druckausgabe über RS232), oder in einer, die eichrechtlich nicht relevant ist (z. B. Fernbedienung von Messgerätefunktionen), oder diese Schnittstelle dient (quasi-)parallel bzw. sequenziell sowohl der Kommunikation mit eichrechtlich relevanten und nicht relevanten Anwendungen (typisch z. B. bei Feldbussen wie DSfG, CAN usw. und nicht vom Betriebssystem unterstützter funkbasierter Kommunikation wie „Wireless MBus“).

Spezifische Anforderungen

Die Rück- und Nebenwirkungsfreiheit wird bei diesem Schnittstellentyp allein auf der Anwendungsebene realisiert und es gelten die entsprechenden Anforderungen, z. B. [W7.2] oder [A50.7]. Dabei sind die dort genannten Anforderungen an Software-Treiber zur Kontrolle der Schnittstelle zu beachten. An das Betriebssystem werden hinsichtlich der Rück- und Nebenwirkungsfreiheit der betreffenden Schnittstelle keine zusätzlichen Anforderungen gestellt.

4.5.2 *Anforderungen an Schnittstellen vom Typ B*

Charakterisierung

Dieser Schnittstellentyp ist dadurch gekennzeichnet, dass prinzipiell beliebig viele Kommunikationskanäle (quasi-)parallel existieren (z. B. Ethernet). Diese Kanäle werden jeweils

- von in das Betriebssystem integrierten Anwendungen (Diensten),
- von eichrechtlich relevanten und
- von eichrechtlich nicht relevanten Anwendungen

aufgebaut und dann gleichzeitig nebeneinander genutzt. Das Betriebssystem realisiert die unteren Schichten des OSI-Kommunikationsmodells und bietet den Diensten und Anwendungen eine dokumentierte Schnittstelle zum Aufbau, Betrieb und Abbau eines Kommunikationskanals.

Für den hier behandelten Schnittstellentyp bieten Betriebssysteme optional eine Unterstützung zur Gewährleistung der Rück- und Nebenwirkungsfreiheit an (sogenannte *Firewall*).

Spezifische Anforderungen

Wenn eichrechtlich relevante Anwendungen über eine Schnittstelle dieses Typs kommunizieren, gelten bezüglich der Rück- und Nebenwirkungsfreiheit der Softwareschnittstellen dieser Anwendungen zunächst die einschlägigen Softwareanforderungen ([W7.2], [A50.7], [A50.8], [D31]). Zusätzlich gelten die folgenden Anforderungen, die die Rück- und Nebenwirkungsfreiheit der Schnittstelle bezüglich der Betriebssystemfunktionen gewährleisten sollen und damit verhindern, dass die eichrechtlich relevanten Funktionen des Messsystems indirekt über andere Kommunikationskanäle beeinträchtigt werden können.

Die Firewall muss immer aktiviert sein. Alle Kommunikationskanäle (*Ports*) müssen grundsätzlich geschlossen sein; nur diejenigen, die für eichpflichtige Zwecke benötigt werden oder von denen nachgewiesen wurde, dass über sie keine unzulässigen Nebenwirkungen auf die eichpflichtigen Funktionen erfolgen können, dürfen geöffnet werden. Dies gilt insbesondere für die in das Betriebssystem integrierten Applikationen (Dienste).

Die Konfigurationsdateien in denen die Firewall-Einstellungen festgelegt sind, müssen dem Schutzaccount zugeordnet und entsprechend gesichert sein.

In der Firewall-Konfiguration muss festgelegt werden, dass Verbindungen nur von innen nach außen (von der betrachteten eichrechtlich relevanten Komponente zu anderen) initiiert werden. Besteht der initiale Verbindungswunsch bei einer anderen Komponente, so darf die Firewall einen Rundruf von außen akzeptieren, die eichrechtlich relevante Komponente muss aber selbst anschließend für den Verbindungsaufbau sorgen.

4.5.3 *Anforderungen an Schnittstellen vom Typ C*

Charakterisierung

Dieser Schnittstellentyp ist dadurch gekennzeichnet, dass prinzipiell beliebig viele Kommunikationskanäle (quasi-)parallel existieren (z. B. USB, PCMCIA). Im Gegensatz zum Schnittstellentyp B wird die Kommunikation initiiert, sobald das System erkannt hat, dass

an der Schnittstelle ein Gerät angeschlossen wurde. Das Betriebssystem identifiziert daraufhin den Typ des Gerätes und wählt automatisch einen passenden Treiber, der genau auf die Eigenschaften des Gerätes abgestimmt ist (sogenannter *Plug&Play*-Mechanismus). Neben der Steuerung der Kommunikation realisiert der Treiber auch die unteren Schichten des OSI-Kommunikationsmodells und bietet den Diensten und Anwendungen eine dokumentierte Schnittstelle zum Aufbau, Betrieb und Abbau eines Kommunikationskanals.

Es können sehr viele Geräte an einer Schnittstelle in einer Baum-Topologie angeschlossen sein, wobei jedes Gerät zusätzlich noch mehrere Instanzen aufweisen kann, für die jeweils eigene Kommunikationskanäle aufgebaut und verwaltet werden. Die hier betrachtete Messsystemkomponente kann sich sowohl an der Wurzel der Baum-Topologie (Host) als auch an einem Blatt befinden (Client).

Die Kanäle können

- von eichrechtlich relevanten und
- von eichrechtlich nicht relevanten Anwendungen

zu beliebigen Instanzen auf beliebigen Geräten über die entsprechenden Treiber angefordert und dann gleichzeitig nebeneinander genutzt werden.

Spezifische Anforderungen

Die Kommunikation mit Geräten über die betreffende Schnittstelle muss unmittelbar nach der Erkennung durch den Plug&Play-Mechanismus grundsätzlich blockiert werden. Nur mit den Geräten, die für eichpflichtige Zwecke benötigt werden oder die die eichrechtlich relevanten Funktionen, Daten und Parameter nicht unzulässig beeinflussen können, darf die Kommunikation ermöglicht werden.

Die Konfigurationsdateien in denen die Parameter und Skripte für die korrekte Freigabe enthalten sind, sowie die Dateien, in denen der aktuelle Zustand des jeweiligen Gerätes gespeichert ist, müssen dem Schutzaccount zugeordnet sein und gemäß 4.4.3 gesichert werden.

Die mit dem Anschließen eines Gerätes automatisch geladenen Treiber dürfen die Rück- und Nebenwirkungsfreiheit der Schnittstelle nicht beeinträchtigen. In Betrieb dürfen nur die im Baumuster vorhandenen und dokumentierten Treiber geladen werden können – also Treiber, die entweder mit dem originalen Betriebssystem ausgeliefert oder von Herstellern bereitgestellt wurden, um an der Plug&Play-Schnittstelle weitere Geräte anzuschließen.

Treiber der Schnittstelle, die eichrechtlich relevante Funktionen realisieren, müssen wie eine Applikation gemäß [W7.2] behandelt werden.

4.5.4 Anforderungen an Schnittstellen vom Typ D

Charakterisierung

Hierbei handelt es sich um Funkschnittstellen. Sie sind nicht integraler Bestandteil der betrachteten Rechnerplattform. Es muss ein für die jeweilige Übertragungstechnik passender Hardware-Adapter über die vorhandenen plattformtypischen Schnittstellen wie SPI (bei „embedded“ Systemen), PCIe, USB oder Ethernet usw. angeschlossen werden. Der zugehörige Protokollstack wird im Allgemeinen als Treiber in das Betriebssystem integriert.

Handelt es sich um einen Kommunikationskanal, der von einer eichrechtlich relevanten Anwendung benutzt wird, so muss die Rück- und Nebenwirkungsfreiheit bezüglich dieser Anwendung gemäß [W7.2] nachgewiesen werden. Es können prinzipiell beliebig viele Kommunikationskanäle zu eichrechtlich relevanten und nicht relevanten Anwendungen aufgebaut werden, aber auch von Betriebssystemdiensten.

Die Anforderungen sollen gewährleisten, dass über die Funkkanäle weder das Betriebssystem noch dessen Konfiguration und damit indirekt die eichrechtlich relevanten Anwendungen unzulässig beeinflusst werden können.

Es sind verschiedene Funkverbindungstypen zu unterscheiden:

(a) Zentrale Verbindungsvermittlung, einkanalig

Die Funkverbindung wird über eine zentrale Vermittlungsstelle zwischen zwei Teilnehmern hergestellt. Es erfolgt eine Authentifizierung beim Verbindungsaufbau; weiteren Teilnehmern wird kein Zugang zu einer bestehenden Verbindung gewährt. Beispiele: GSM.

(b) Dezentrale Verbindungsvermittlung (Routing), keine Anpassung an die Funktionalität der Teilnehmer

Die Verbindung zwischen Kommunikationsendpunkten wird über Adressen hergestellt. Der Kommunikationskanal wird von Routern automatisch festgelegt.
Der in das Betriebssystem integrierte Protokollstack beinhaltet keine dynamische Anpassung der Datenübertragungsfunktionen an das jeweils angeschlossene Gerät (keine Profile). Beispiel: WLAN.

(c) Automatischer Verbindungsaufbau mit erreichbaren Teilnehmern, Anpassung an die Funktionalität des Teilnehmer

Bei dieser Funkkommunikation wird der Reihe nach eine Verbindung mit allen in Reichweite befindlichen möglichen Teilnehmern hergestellt. Daraufhin wird automatisch entschieden, ob es sich bei dem jeweils gefundenen Teilnehmer um den gesuchten handelt. Ansonsten wird automatisch weitergesucht. Wurde der Teilnehmer gefunden, erfolgt in den in das Betriebssystem der betrachteten Plattform integrierten Treibern eine automatische Anpassung der Funktionalität (Plug&Play) an den jeweiligen Teilnehmer. Beispiel: Bluetooth.

4.6 Aktualisierungen der Software

Das Aktualisieren von Software bei in Verwendung befindlichen Messgeräten ist im MessEG/EV §§37/40 geregelt. Es sind drei Fälle zu unterscheiden: Es kann sich um die Aktualisierung der eichrechtlich relevanten Anwendungen, der eichrechtlich nicht relevanten Anwendungen oder um Komponenten des Betriebssystems handeln.

Neben der softwaregesteuerten Aktualisierung besteht die Möglichkeit, das Siegel zu verletzen, die Software oder Teile der Software auszutauschen und das Messgerät anschließend eichen zu lassen (Instandsetzung).

4.6.1 Aktualisierung eichrechtlich relevanter Anwendungen

Das Betriebssystem bietet die technischen Voraussetzungen für die Erfüllung der Anforderungen bei Softwareupdates gemäß [W7.2], D1–D4. Das gesamte Download- und Update-Management besteht aus einer Kombination aus eichrechtlich relevanten Anwendungen und passender Betriebssystemkonfiguration.

Die Anwendungen, die die Anforderungen zur Authentizitätsprüfung (D2) und Integritätsprüfung (D3) ausführen, dürfen nur mit den Zugriffsrechten des Benutzerkontos der eichrechtlich relevanten Anwendungen oder denen des Schutzaccounts geändert oder gelöscht werden können. Dementsprechend müssen Maßnahmen getroffen werden, die verhindern, dass die Anwendung der Rückverfolgbarkeit (D4) oder das Eichlog verändert oder gelöscht werden kann.

4.6.2 Aktualisierung eichrechtlich nicht relevanter Anwendungen

Eichrechtlich nicht relevante Anwendungen, Daten oder Parameter dürfen in Betrieb ausgetauscht oder geladen werden, ohne im Eichlog registriert zu werden, wenn alle eichrechtlich relevanten Anwendungen, Parameter und Daten nur mit den Zugriffsrechten des eichrechtlich relevanten Benutzerkontos oder des Schutzaccounts geändert oder gelöscht werden können.

4.6.3 Aktualisierung des Betriebssystems

Das Betriebssystem und dessen Konfiguration liegt gemäß den zuvor genannten Anforderungen unter den Zugriffsrechten des Schutzaccounts. Bezüglich der Möglichkeit eines Betriebssystem-Updates muss das Konzept des eichrechtlichen Sicherheitsankers (siehe 4.4.4) beachtet werden.

Beruht der Schutz des Systems auf einem rollenfreien Sicherheitsanker, so kann das Betriebssystem und seine Konfiguration in Betrieb nicht ohne Siegelverletzung aktualisiert oder geändert werden. Es ist eine Instandsetzung erforderlich.

Beruht der Schutz des Systems dagegen auf einem rollengebundenen Sicherheitsanker, und existiert eine Rolle, der die Verantwortung für ein Betriebssystem-Update übertragen werden kann, so darf der Schutzaccount dieser Rolle zugewiesen werden. Damit ist ein vollständiges Update des gesamten Messsystems ohne Siegelbruch möglich. Die Anforderungen [W7.2], D1–D4 sind aber darauf nicht abgestimmt und können unter diesen Bedingungen nicht erfüllt werden.

4.7 Maßnahmen zur Gewährleistung der Prüfbarkeit und Nachvollziehbarkeit

Messgeräte müssen während der Verwendung auf die Konformität mit dem Mess- und Eichgesetz und Einhaltung der Anforderungen überprüft werden können. Über die Konfigurationsdateien des Betriebssystems, die die Einstellungen zum Schutz der eichrechtlich relevanten Funktionen und Eigenschaften des Messgerätes enthalten, muss eine Checksumme gebildet werden. Diese muss mit einfachen Mitteln im Betrieb angezeigt werden können.

5 Zusammenfassung

Softwareanforderungen an eichpflichtige Messgeräte existieren schon seit einigen Jahren sowohl im nationalen als auch europäischen und internationalen Rahmen. Mit der jüngsten technischen Entwicklung nahm die Komplexität der Software deutlich zu, vor allem durch die Verwendung von Betriebssystemen in den Messgeräten. Diese Technologie wird zwar in den existierenden Anforderungen des gesetzlichen Kontextes grundlegend berücksichtigt, es ist jedoch sowohl auf Seiten der Hersteller als auch der Prüfer ein Bedarf für eine weitergehende technische Spezifizierung zu erkennen. Hierzu sollte der vorliegende Aufsatz

einen Beitrag liefern. Die vorgestellten Anforderungen sind derzeit noch im Entwurfsstadium und müssen nach den geltenden Regeln entsprechend abgestimmt und vom Regelermittlungsausschuss verabschiedet werden.

Referenzen

[1] PTB-A 50.7 *Anforderungen an elektronische und softwaregesteuerte Messgeräte und Zusatzeinrichtungen für Elektrizität, Gas, Wasser und Wärme*, 2002

[2] PTB-A 50.8 *Smart Meter Gateway*, 2014

[3] *Guide for Examining Software* (Non-automatic Weighing Instruments), WELMEC 2.3, Issue 3, 2005

[4] *Guide for modular approach and testing of PCs and other digital peripheral devices* (Non-automatic Weighing Instruments), WELMEC 2.5 Software, Issue 2, 2000

[5] *Software Guide* (Measuring Instruments Directive 2014/32/EU), WELMEC 7.2, 2015

[6] *General requirements for software controlled measuring instruments*, OIML D31, 2008

[7] Measuring Instruments Directive 2014/32/EU, 26.02.2014

[8] *Gesetz über das Inverkehrbringen und die Bereitstellung von Messgeräten auf dem Markt, ihre Verwendung und Eichung sowie über Fertigpackungen* (Mess- und Eichgesetz – MessEG), 25.07.2013

[9] *Mess- und Eichverordnung Verordnung über das Inverkehrbringen und die Bereitstellung von Messgeräten auf dem Markt sowie über ihre Verwendung und Eichung* (Mess- und Eichverordnung – MessEV), 11.12.2014

[10] *Open Systems Interconnection Model*, ISO/IEC 7498-1:1994

Sichere Architekturen für eingebettete Systeme im gesetzlichen Messwesen

Daniel Peters*

Kurzfassung:

In vielen Einsatzgebieten muss Software stabil laufen und Angriffen standhalten. Durch den Trend des „Internet der Dinge“ häufen sich diese Angriffe in allen Bereichen, in denen Geräte über das offene Netzwerk verbunden sind. Mittlerweile betrifft das viele Alltagsgeräte, wie Smartphones, Tablets und einfache Messgeräte, die sich zu leistungsfähigen Universalgeräten mit offener Systemarchitektur entwickelt haben. Es ist festzustellen, dass IT-Systeme mit konventionellen Betriebssystemen kaum noch abzusichern sind. Neue Ansätze sind nötig, um der wachsenden Anzahl an Bedrohungen entgegenzuwirken. Mit dem Einsatz von Separationskernen wird das Ziel verfolgt, Teilkomponenten eines Softwaresystems nachweislich und mit hoher Verlässlichkeit sowohl räumlich wie auch zeitlich zu isolieren. Damit wird sichergestellt, dass die Fehlfunktion einer Komponente keine Auswirkung auf die Funktionsfähigkeit anderer Bereiche des Systems haben kann. Nur so kann das Risiko einer Fehlfunktion soweit abgesenkt werden, dass auch der Einsatz in kritischen Einsatzgebieten, wie in gesetzlich überwachten Messgeräten oder vernetzten Produktionsanlagen (Industrie 4.0), vertretbar wird. Dieser Artikel analysiert konkret die Anforderungen an gesetzlich geregelte Messsoftware und gibt Lösungen, wie eine Software-Systemarchitektur aussehen kann, die alle Anforderungen erfüllt und gleichzeitig der Marktüberwachung Mechanismen zur Verfügung stellt, um die Integrität von Messgerätesoftware im Umlauf zu überprüfen.

1 Einführung

Durch den starken Preisverfall bei Hard- und Software sind leistungsstarke Systeme so erschwinglich geworden, dass in den Industrie-Nationen selbst Kindern und Jugendlichen mehr Rechenleistung in Form ihrer Smartphones zur Verfügung steht, als es vor wenigen Jahren noch bei industriellen und kommerziellen Einrichtungen der Fall war. Auch im Bereich der Telefon- und Datentarife gab es einen ähnlich starken Preisverfall, sodass nun durch die Verfügbarkeit leistungsstarker Systeme und günstiger Verbindungen die Voraussetzungen für dauerhaft vernetzte, hochverfügbare Systeme gegeben ist: Die immer stärkere Mobilisierung und Individualisierung menschlicher Kommunikation und andererseits das Entstehen eines Internets der Dinge durch vernetzte Objekte sind unmittelbare und sichtbare Folgen dieser Entwicklung. Diese Entwicklung bietet unglaubliche Chancen: Durch die Verbindung von Kommunikations- mit Industrie-Automatisierungstechnologie verspricht man sich so starke Synergieeffekte, dass bereits von einer vierten industriellen Revolution gesprochen werden kann. Auch für die Energiewirtschaft, das Gesundheitswesen bis zum Smart Home kann diese Entwicklung zu revolutionären, positiven Veränderungen führen. Allerdings macht sich mittlerweile die Erkenntnis breit, dass das Selektionskriterium in der raschen Evolution der IT-Systeme Preis und Performanz und keine zugrunde liegenden Sicherheitsarchitekturen waren. Die ausgeprägte Komplexität moderner Systeme, gepaart mit klassischen Architekturmodellen und Systemarchitekturen, ermöglicht es Angreifern immer wieder, Programmierfehler, Lücken und Schwachstellen auszunutzen und Systeme erfolgreich anzugreifen. Der hohe Standardisierungsgrad in der IT und die weite Verbreitung einiger weniger Plattformen erlauben eine gute

* Daniel Peters, Arbeitsgruppe 8.52 "Metrologische IKT-Systeme", E-Mail: daniel.peters@ptb.de

Skalierbarkeit der Angriffe. Alle heute relevanten Systeme basieren auf Systemarchitekturen, deren Wurzeln mehrere Jahrzehnte zurückreichen und in deren Design viele Annahmen eingeflossen sind, die heute nur noch teilweise oder überhaupt keine Gültigkeit mehr haben. An erster Stelle steht hierbei der Mangel an Mechanismen, mit denen der Wirkungsbereich nicht vertrauenswürdiger Software strikt kontrolliert werden kann, was als Hauptgrund für die Bedrohung durch Schadsoftware anzusehen ist. Obwohl die Erweiterung bestehender Betriebssysteme mit zusätzlichen Sicherheitsfunktionen möglich ist, sind diesem Ansatz aus Rückwärtskompatibilitätsgründen oftmals Grenzen gesetzt. Ein Alternative besteht in Form von Virtualisierungstechnologien, deren potenzieller Einsatzbereich sich aufgrund der starken Leistungszunahme deutlich vergrößert hat. Aufgrund der speziellen Anforderungen, die sich aus den Einsatzgebieten von eingebetteten Systemen ergeben, sind Virtualisierungslösungen aus dem Desktop- und Serverbereich nicht ohne Weiteres einsetzbar.

Im Ausblick auf zukünftige Einsatzgebiete sind zwei Anforderungen zu erwarten, die von derzeitigen Systemen nicht erfüllt werden. Der parallele Betrieb von mehreren Gastsystemen stellt hinsichtlich von Echtzeitanforderungen, z. B. im industriellen Umfeld, neue Herausforderungen. Darüber hinaus wird den Isolationseigenschaften von virtuellen Maschinen bei der Sicherheitszertifizierung von Systemen eine wichtige Rolle zukommen. Nur wenn davon ausgegangen werden kann, dass eine Komponente unter keinen Umständen die Ausführung ihrer Umgebung beeinflussen kann, wird es möglich sein, die Teilzertifizierungen einzelner Komponenten mit geringem Aufwand zu einer Systemzertifizierung zusammenzufassen. Aus diesem Grund wird es einen Trend zu kleineren Kernen geben, deren Quelltextgröße die Schwelle unterschreitet, aber deren Sicherheitseigenschaften mit formalen Methoden bewiesen werden können.

Dieser Artikel ist wie folgt strukturiert: Kapitel 2 beschreibt die grundlegenden Technologien, die sich bei der Konstruktion sicherer Systeme in der Vergangenheit bewährt haben. In Kapitel 3 werden die Anforderungen an das gesetzliche Messwesen analysiert und hinsichtlich des Potenzials für den Einsatz von Separationskernen bewertet. Danach wird in Kapitel 4 ein Verfahren vorgestellt, mit dem sich die Dateisystemintegrität eines Messgerätes leicht überprüfen lässt. Kapitel 5 schließt den Artikel mit einer Zusammenfassung ab.

2 Allgemeine Anforderungen

Im folgenden Abschnitt werden allgemeine Anforderungen an Systeme in kritischen Einsatzgebieten diskutiert. Dabei werden verschiedene Ansätze beleuchtet und auch auf Arbeiten mit ähnlichen Anforderungen aus dem Bereich „funktionale Sicherheit“ verwiesen, um den Versuch zu unternehmen, sowohl Konzepte wie auch Terminologie auf das Gebiet der Datensicherheit zu übertragen.

2.1 Sicherheitskerne

Der Sicherheitskern (*security kernel*) eines Systems stellt sicher, dass Subjekte nur auf diejenigen Objekte Zugriff erhalten, die ihnen von einer *security policy* eingeräumt werden. Eine weit verbreitetet Art um diese Anforderungen auszudrücken, ist das Kürzel *NEAT*, welches die folgenden Kriterien an Sicherheitskerne definiert:

1. *Nonbypassable*: Das Sicherheitskonzept des Systems kann nicht umgangen werden. Komponenten können keine anderen Kommunikationspfade als die vorgegebenen verwenden, um das Sicherheitskonzept auszuhebeln.

2. *Evaluatable*: Die Sicherheitsarchitektur ist klein und hat eine geringe Komplexität. Damit wird eine formale Verifikation möglich. Komponenten müssen klein und modular aufgebaut sein, um die Verifikation zu erleichtern.

3. *Always-invoked*: Das Sicherheitskonzept ist immer aktiv. Jeder Zugriff und jede versendete Nachricht muss durch die Sicherheitsarchitektur geprüft und akzeptiert werden (die Sicherheitsarchitektur überprüft nur den ersten Zugriff und alle weiteren Zugriffe werden dann ohne eine erneute Überprüfung weitergeleitet.

4. *Tamper-proof*: Das System hat eine strikte Rechteverwaltung, speziell in Bezug auf das Modifizieren von Daten oder Codes. Die Sicherheitsarchitektur kontrolliert streng, welche Komponenten das System modifizieren können, um unautorisierte Änderungen am System zu verhindern.

Ein Sicherheitskern darf nicht mit einem Betriebssystemkern verwechselt oder gleichgesetzt werden. Vielmehr bezeichnet er diejenigen Komponenten, die innerhalb eines Betriebssytemkerns die Funktion eines *reference monitors* wahrnehmen. Ein bekanntes Beispiel für einen Sicherheitskern ist SELinux, eine Implementierung des *Flux Advanced Security Kernel* (FLASK) für Linux. SELinux ersetzt die normalerweise von Linux genutzte *discretionary access control* (DAC) durch die restriktivere Form der *mandatory access control* (MAC). Damit wird es

möglich, die Zugriffsrechte von Prozessen innerhalb eines Betriebssystemkerns auf die Funktion einer Ressource zu beschränken, die diese zur Erfüllung ihrer Aufgabe benötigt, eine Einschränkung die auch als *principle of least privilege* bekannt ist.

2.2 Separationskerne

Als Separationskern [41] wird eine kleine Softwarekomponente bezeichnet, die das System in Partitionen – alternativ auch Domänen genannt – unterteilt (Bild 1), wobei eine vollständige Trennung der Partitionen untereinander, sowohl zeitlich wie auch räumlich, sichergestellt wird. Partitionen können nur über streng kontrollierte Kanäle miteinander kommunizieren. Der Begriff Separationskern kommt aus dem Bereich der eingebetteten Systeme, wo Isolation einzelner Komponenten oftmals eine wichtige Rolle spielt. Dementsprechend sind die Anforderungen an Separationskerne sehr hoch. Die ARINC653 [36] Spezifikation definiert Anforderungen, die Betriebssysteme erfüllen müssen, um in Anwendungen, in denen funktionale Sicherheit garantiert werden muss, zugelassen zu werden. Dabei werden an diese Betriebssysteme vier Anforderungen gestellt, die von einem Separationskern erfüllt werden müssen:

1. Zeitliche Separation
2. Räumliche Separation
3. Kontrolle des Informationsflusses
4. Fehler-Isolation

Der Begriff Separationskern wird auch oft im Zusammenhang mit *Multiple Independent Levels of Security/Safety* (MILS) [7, 10] verwendet. Dabei stellt der Separationskern die unterste Schicht dieser Architektur dar. In den Partitionen läuft eine Middleware-Schicht als Verbindungsebene zu den Applikationen. Diese wird benötigt, da die vom Separationskern bereitgestellten Schnittstellen oft sehr rudimentär sind und nur ein Minimum an Funktionalität bereitstellen, um die Komplexität im Kern gering zu halten. Daher implementiert die Middleware fehlende Funktionalität, oft in Form von Bibliotheken, um Applikationen eine standardisierte Schnittstelle zu bieten (z. B. POSIX). Diese Bibliotheken umfassen verschiedenste Funktionen wie z. B. Speicherverwaltung, Threading oder mathematische Funktionen. Die Middleware kann allerdings auch eine Virtualisierungsschicht anbieten, womit die Möglichkeit besteht, in einer Partition auch Betriebssysteme mit einem größeren Funktionsumfang, z. B. Linux oder Windows, einzusetzen.

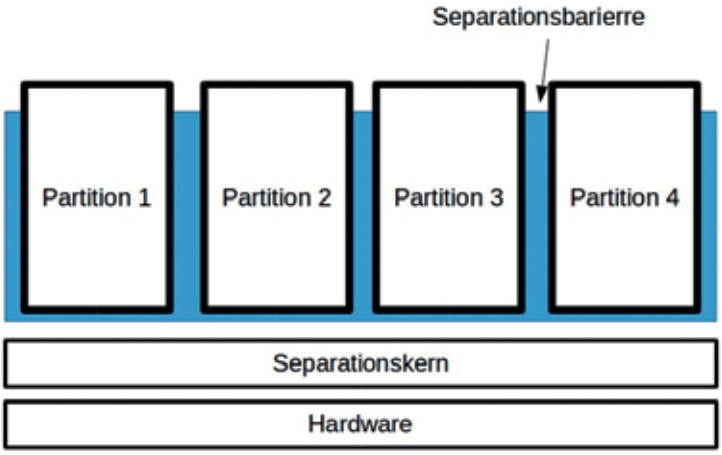

Bild 1: Architektur eines separierten Systems.

2.3 Virtualisierung

Unter einer virtuellen Maschine versteht man eine Softwareumgebung, die in ihren Eigenschaften physischer Hardware so ähnlich ist, dass in ihr Programme inklusive der dazugehörigen Betriebssysteme ausgeführt werden können[1]. An eine virtuelle Maschine werden folgende drei Forderungen gestellt, die erstmals von Popek und Goldberg formuliert wurden [34]:

1. Die von ihr bereitgestellte Umgebung ist im Wesentlichen identisch zu der, die die Software auf einer physischen Maschine vorfinden würde.
2. Programme, die in ihr ausgeführt werden, tun dies mit nahezu derselben Geschwindigkeit, wie sie dies auf der physischen Maschine ohne die virtuelle Maschine tun würden.
3. Das Gastsystem hat nur Zugriff auf Ressourcen, die ihm explizit zugewiesen wurden.

Ein *Hypervisor* oder *Virtual Machine Monitor* (VMM) [35] ist der Kern der Architektur. Dabei wird zwischen zwei Arten von Hypervisor unterschieden; Typ-I (Bild 2 links) und Typ-II (Bild 2 rechts). Der Typ-I-Hypervisor läuft direkt auf der Hardware (und wird daher auch *Baremetal Hypervisor* genannt). Bekannte Vertreter dafür sind Xen [9] (quelloffen), Hyper-V (proprietär) oder ESXi (proprietär). Der Typ-II-Hypervisor setzt ein vollständiges Betriebssystem voraus, in dessen Umfeld er als Applikation ausgeführt wird. Dabei setzt er auf die Hilfe des Betriebssystems in Form eines Systemtreibers, um über Ereignisse im Gast-System informiert zu werden. Bekannte Vertreter des Typ-II-Hypervisors sind VirtualBox (quelloffen) oder Parallels (proprietär).

Unabhängig ob ein Typ-I- oder ein Typ-II-Hypervisor zum Einsatz kommt, kann die Plattformvirtualisierung wiederum in zwei Arten

[1] Virtualisierung bezieht sich hier immer auf Plattformvirtualisierung. Andere Varianten wie OS Virtualisierung oder Prozessvirtualisierung spielen hier keine Rolle.

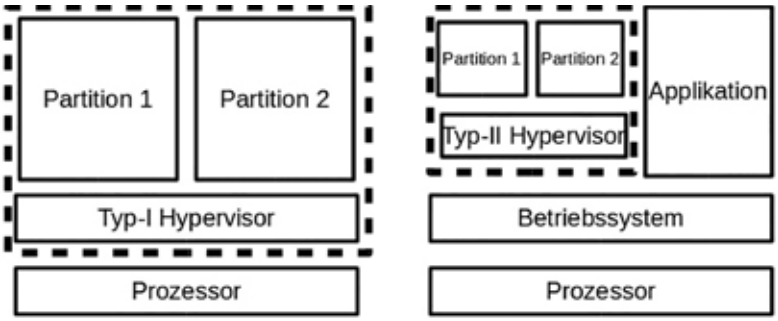

Bild 2: Hypervisor Architekturen

unterteilt werden: Para-Virtualisierung [3] und Vollvirtualisierung [3]. Para-Virtualisierung wird auf Plattformen verwendet, für die keine Hardware-Virtualisierungserweiterung (VE) zu Verfügung steht. Die Para-Virtualisierung spielt vor allem auf ARM[5]-basierten Systemen (*Smartdevices; Smartphones, Smart TVs, Smart Meters*, etc.) eine Rolle, weil diese meist noch keine VE haben. Die neueren Generation ARM-basierter Systeme; Der Cortex A7 [6] bzw. Cortex A15 [4] verfügt nun auch über eine VE. Allerdings dringen Geräte mit diesem Prozessortyp nur sehr langsam in den Markt, weshalb der Para-Virtualisierung noch eine wichtige Rolle zuzuordnen ist. Im Gegensatz dazu setzt die Vollvirtualisierung Hardware-Unterstützung voraus und erlaubt es, unveränderte Betriebssysteme auf einem Hypervisor laufen zu lassen. Diese Art der Virtualisierung ist im Desktop und Servermarkt bereits weit verbreitet, da die entsprechenden Prozessoren (x86) bereits seit 2006 [2, 1] über eine VE verfügen.

In Bezug auf MILS-Systeme hat Karger [20] bereits im Jahr 2005 den Einsatz von Virtualisierung diskutiert. Dabei ging es hauptsächlich darum, abzuwägen, welche Komponenten essenziell sind und welche nicht benötigt werden, um die Komplexität des Hypervisors gering zu halten. Das Konzept wurde später von Yang et al. [40] aufgegriffen, um auf den definierten Komponenten eine Virtualisierungslösung zu bauen.

Im Hinblick auf Separationskerne (Abschnitt 2.2) bzw. Sicherheitskerne (Abschnitt 2.1) wird die Entscheidung, entweder eine Virtualisierungslösung oder eine native Middleware-Schicht zu verwenden, von zwei Fragen getrieben. Diese beiden Fragen gehen auf die Arbeiten von Karger et al. [20] zurück und spielen nach wie vor eine entscheidende Rolle. Erstens soll die Kompatibilität mit bestehender Software möglichst hoch sein und zweitens sollen die Kosten für Entwicklung und Wartung neuer Software gering sein. Dabei liegt der Vorteil klar bei der Virtualisierung, da bestehende Betriebssysteme wie Linux (inklusive Android) und Windows bereits große Mengen an Applikationen bereitstellen und auch bestehende Entwicklungswerkzeuge weiter verwendet werden können. Während eine native Middleware mit einem hohen Wartungsaufwand verbunden ist.

3 Eine Systemarchitektur für das gesetzliche Messwesen

Im gesetzlichen Messwesen betrachtet man Messgeräte, die im kommerziellen, im Verwaltungs- oder im öffentlichen Interesse benutzt werden. In Deutschland sind mehr als 100 Millionen rechtlich relevante Messgeräte im Einsatz. Die meisten von ihnen werden für geschäftliche Zwecke verwendet, insbesondere sind es Haushaltszähler, die den Strom-, Gas-, Wasser- oder Wärmeverbrauch messen. Andere klassische Messgeräte, mit denen der Endanwender in Kontakt kommt, sind beispielsweise Zähler in Benzinpumpen oder Waagen im Lebensmittelbereich, aber auch Geschwindigkeits- oder Alkoholmessgeräte. Schätzungen zufolge werden etwa vier bis sechs Prozent des Bruttonationaleinkommens in Industrieländern von Messgeräten abgedeckt. In Deutschland allein entspricht dies einer Menge von 104 bis 157 Milliarden Euro pro Jahr [24]. Somit könnten Manipulationen an Messsoftware weitreichende finanzielle Folgen haben. Heutzutage bauen die meisten Hersteller von Messgeräten ihren Software-Stack bevorzugt auf Standard-Betriebssystemen, wie Linux und Windows, auf. Der Nachteil daran besteht darin, dass diese Systeme sehr groß, komplex und damit fehlerhaft sind. Ein so komplexer Code erhöht die Anfälligkeit dieser Systeme, weil eine einzige Schwachstelle dazu führen kann, dass ein Angreifer beliebigen Code auf dem Messgerät ausführen kann. Zusätzlich möchten Hersteller ihre Messgeräte in hohem Maße vernetzen, um Fernwartungsarbeiten durchzuführen oder auch um Messdaten in einer *Cloud* zu verwalten. Zum jetzigen Zeitpunkt werden Zulassungen für Messgeräte, die Softwaredownloads oder Wartungsarbeiten über das Internet durchführen möchten, selten oder überhaupt nicht erteilt, weil der Hersteller nicht glaubhaft sicherstellen kann, dass diese Funktionen genügend gegen Angriffe abgesichert sind. Die Aufgabe, sichere Systeme zu erstellen, ist somit für Hersteller sehr interessant, denn durch das neue Gesetz sind Software-Downloads (MessEV[2] §40 seit 01.01.2015 in Kraft getreten, sowie MessEG[2] §37 Absatz 6) und Remote-Diagnoseverfahren und Maintananceverfahren (MessEV §49 Absatz 3) über das Internet erlaubt, solange die Eignung der Software festgestellt wurde, d. h. die Sicherheit des Systems gewährleistet ist. Dieses Verfahren würde den Herstellern viel Zeit und Geld ersparen, weil sie bis jetzt meistens Wartungsarbeiten nur vor Ort durchführen können. Für die Harmonisierung von Vorschriften für Messgeräte über nationale Grenzen hinweg ist die Internationale Organisation für das gesetzliche Messwesen (OIML) zuständig. Software-Anforderungen für diesen Zweck sind indem OIML-D-31-Dokument [29] formuliert. Speziell für Europa

[2] http://www.gesetze-im-internet.de/messev/ (Letzter Zugriff am 28.11.2016)

hat der WELMEC-Ausschuss diese Aufgabe. Dabei bietet der WELMEC 7.2 Software-Guide [39] eine Anleitung für Hersteller und Prüfer, um sichere Software für Messinstrumente zu bauen und zu prüfen, die die Forderungen des MessEV und MessEG und besonders der *Directive 2014/32/EU of the European Parliament and of the Council*[3] – die Anforderungen für Software in Europa regelt – umsetzt.

3.1 Die Systemarchitektur

Laut WELMEC 7.2 Software-Guide sind alle Module rechtlich relevant, die Messergebnisse erstellen oder beeinflussen. Diese Module ermöglichen Funktionen wie das Anzeigen von Daten, den Schutz von Daten, das Speichern von Daten, die Identifizierung der Software, das Ausführen von Downloads, die Übertragung von Daten und die Überprüfung der empfangenen oder gespeicherten Daten. Zusätzlich soll Software, die rechtlich relevante Aufgaben durchführt, von rechtlich nicht relevanter getrennt werden.

Durch diesen modularen Ansatz, den der Guide fordert, wird deutlich, dass eine Systemarchitektur auf Basis eines Separationskerns sehr geeignet ist. Unsere vorgeschlagene Systemarchitektur nimmt die Forderungen des WELMEC 7.2 Software-Guides wörtlich und stellt für jede rechtlich relevante Aufgabe ein Modul zur Verfügung, wie in Bild 4 gezeigt. Die Zuordnung der Funktionen zu den Modulen ist wie folgt:

- *Secure GUI*: Anzeige von Daten (Einteilen der Benutzeroberfläche in rechtlich relevant und nicht rechtlich relevant)
- *Key & Signature Manager*: Schutz von Daten (Verwaltung von Schlüsseln und *Hashes*)
- *Storage Manager*: Speichern von Daten (verschlüsselt), Aufzeichnen von Änderungen (*Audit Trail*)
- *Download Manager*: Ausführen von Downloads (Überprüfen der Authentizität)
- *Connection Manager*: Übertragen von Daten über das Netzwerk (Vertraulichkeit, Integrität, Authentizität)
- *Communication Monitor*: Umleiten von Anfragen von und zu den E-/A-Geräte, wie z. B. Sensoren, Tastatur und Bildschirm

Es wird ein „öffentlicher Bereich“ und ein „privater Bereich“ eingerichtet. In diesem Fall sind es die rechtlich relevante virtuelle Maschine

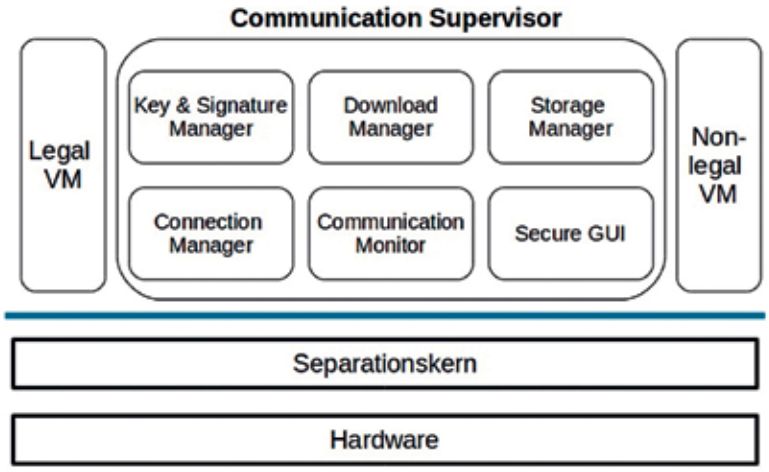

Bild 3:
Metrologisches Rahmenwerk

(L VM) und die nicht rechtlich relevante VM (N VM). In der L VM werden alle Berechnungen durchgeführt, die für das Messverfahren benötigt werden, beispielsweise Bildverarbeitung in einem Verkehrsmessgerät. Die N VM darf nur Software ausführen, welche keinen Messzweck hat, z. B. das Öffnen der Bedienungsanleitung oder die Anzeige eines Taschenrechners.

Diese Module können in eine unterschiedliche Anzahl von virtuellen Maschinen zusammengefasst werden, oder auch eigenständige native Prozesse sein. Eine vollkommene, einheitliche Modularisierung wird erreicht, wenn alle Module unterschiedliche virtuelle Maschinen sind. Virtualisierung ermöglicht es, die umfangreiche Funktionalität von Standard-Betriebssystemen zu nutzen, wie die große Verfügbarkeit von Treibern und Applikationen, und stellt trotzdem Sicherheit durch Kapselung her. Zudem kann durch die Aufteilung der Funktionen in einzelne Module individuell auf jedes Messgerät eingegangen werden. Falls ein Messgerät beispielsweise keinen Download-Mechanismus benötigt, kann der Download-Manager entfernt werden, oder wenn

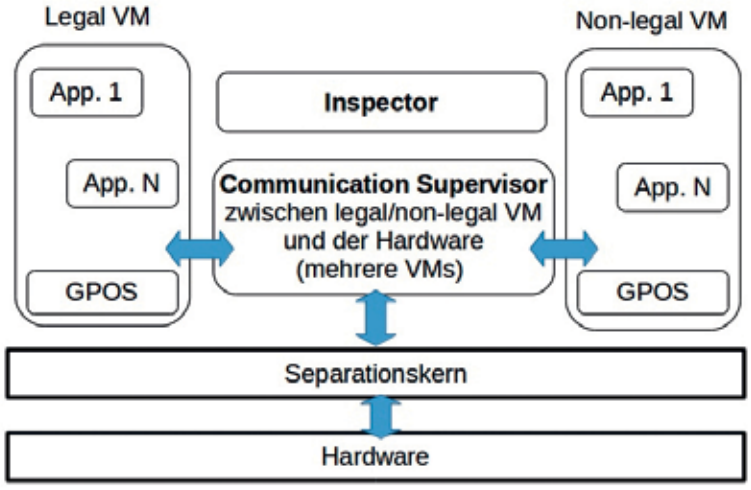

Bild 4:
Kommunikation und Integritätsprüfung durch den Inspector

[3] Directive 2014/32/EU [19] muss von den Europäischen Mitgliedstaaten bis Mitte 2016 umgesetzt werden und basiert auf der jetzigen Directive 2004/22/EC [18], bekannt als die Measuring Instruments Directive (MID)

kein Netzwerkzugriff benötigt wird, der Connection Manager. Neben der L VM sind die Module, die jedes Messgerät braucht, der Key & Signature Manager, der Storage Manager, der Communication Monitor und der Inspector (s. u.).

Bild 4 zeigt, wie die Kommunikation mit der Hardware über die Module stattfindet. Da nur der Communication Supervisor direkten Hardware-Zugriff hat, leiten sowohl N VM wie auch L VM alle ihre Anfragen über die Module im Communication Supervisor. Falls alle Module durch virtuelle Maschinen abgebildet sind, geschieht dies mithilfe eines virtualisierten Netzwerkes. Jede VM besitzt dabei eine virtuelle Netzwerkkarte und kann über das virtuelle Netzwerk Daten an die anderen VMs schicken. Andernfalls werden die Anfragen über virtuelle Gerätetreiber an das entsprechende Modul weitergeleitet.

4 System-Integritätsprüfung

Software von Geräten, die für amtliche Zwecke im gewerblichen Gebrauch oder im öffentlichen Interesse zum Einsatz kommen (MessEG, MID), müssen in festgelegten Abständen auf Integrität bzgl. ihrer Software geprüft werden. Bei gesetzlich geregelten Messgeräten, beispielsweise Verkehrsmessgeräten, Waagen, etc., geschieht dies durch benannte Stellen und die Marktüberwachung (Landeseichbehörden). Die benannte Stelle überprüft die Software vor dem Inverkehrbringen und die Marktüberwachung überprüft zyklisch, ob sich auf den Geräten noch dieselbe Software befindet, die von einer Konformitätsbewertungsstelle, z. B. der PTB, zugelassen wurde. Dies ist insbesondere für alle Geräte in kritischen Infrastrukturen nötig, um Manipulationen und Fehlverhalten rechtzeitig zu erkennen.

In Messgeräten zeigen heutige Verfahren in den meisten Fällen auf Anfrage eine kurze Checksumme auf dem Display an. Die Berechnung dieser Checksumme ist in den wenigsten Fällen vertrauenswürdig und kann das Auffinden von Veränderungen an Dateien nicht garantieren, weil sie oft nur auf unsicheren und leicht „knackbaren“ Checksummen-Algorithmen basiert, z. B. CRC-16.

Eines der Hauptprobleme jetziger Systeme ist zudem, dass die Überprüfung der Dateien auf dem gleichen System stattfindet, welches die Dateien auch verwaltet. Dabei wird einem System vertraut, von dem man die Vertrauenswürdigkeit abfragt – das System prüft sich also selbst! Dies birgt insofern Risiken, weil intelligente Schadsoftware die Eigenschaft besitzt, sich während der Checksummen-Berechnung zu verstecken und Änderungen an Dateien zu kaschieren. Außerdem sind Checksummen-Algorithmen nicht zum Auffinden von Manipulationen geeignet und es sollten geeignetere Algorithmen verwendet werden, z. B. Hash-basierte Algorithmen.

Eine bessere Alternative ist ebenfalls in Bild 4 abgebildet, die Inspector VM, die für die Identifizierung und Integritätsprüfung der Software zuständig ist. Ein Messgerät ist so auszulegen, dass die Marktüberwachung (Eichbehörden) die Integrität der Software überprüfen können muss, auch nachdem das Messgerät in Verkehr gebracht und in Betrieb genommen wurde. Der Inspector ist eine Überwachungs-VM, die auf Anfrage eine eindeutige ID des Geräts anzeigen kann. Der Inspector selbst prüft das System automatisch nach einem festgelegten Zeitintervall und nach dem Auftreten von wichtigen Ereignissen. Der Inspector kann auch den Storage Manager beauftragen, das Datei-System und die einzelnen Messungen auf Integrität zu überprüfen. Um den verwendeten Arbeitsspeicher zu überprüfen, erhält der Inspector einen *Snapshot* der Speicherbereiche vom Separationskern, welche von den einzelnen VMs benutzt werden. Zusätzlich kann der Inspector eine VM neu starten, falls sie nicht reagiert.

Da die Zuverlässigkeit des Systems immer noch von den Gast-Betriebssystemen und ihren Applikationen abhängt, müssen die VMs als Ganzes auf Integrität geprüft werden. Darüber hinaus muss ein vertrauenswürdiger Pfad hergestellt werden, um sicherzustellen, dass man nicht mit einer manipulierten VM kommuniziert. Dieser Pfad fängt bei der Firmware an und endet bei den Applikationen in den einzelnen VMs. Die Firmware sollte von einem manipulationssicheren Chip überprüft werden, der vom Hersteller signierte kryptografische Schlüssel enthält. Im gesetzlichen Messwesen gilt dabei ein Chip schon als manipulationssicher, sobald er versiegelt wird, denn wenn das Siegel gebrochen wurde, ist das Gerät auch nicht mehr geeicht. Dieser Chip überprüft die Integrität der Firmware, die dies ihrerseits für den *Bootloader* tut. Danach überprüft der Bootloader den Separationskern, welcher seine VMs überprüft. Die Anwendungen erhalten ihre Zertifikate durch Erzeugung eines privaten / öffentlichen Schlüsselpaares und dann durch einen besonderen Aufruf an den Separationskern, um den öffentlichen Schlüssel zu übergeben. Der Separationskern generiert und signiert das Zertifikat, das einen Hash über die Anwendungen und deren öffentliche Schlüssel mit weiteren Anwendungsdaten enthält. Dieses Zertifikat bindet den öffentlichen Schlüssel an die Anwendung, deren Hash in der Bescheinigung angegeben wird.

Für Laufzeitintegritätsmessungen muss zudem die Kontinuität der Integrität über die Messzeit hinweg gewährleistet werden. Ein Angreifer könnte beispielsweise ein Programm ändern, nachdem es gemessen wurde, aber bevor es ausgeführt wird. Dieses Problem ist als *time-of-check-to time-of-use*(TOCTTOU)-Konsistenz bekannt und sollte durch Abfangen von kritischen System-

aufrufen und Überwachung vom Gast-Speicher gelöst werden. Um Systemaufrufe, Interrupts und Ausnahmen abzufangen, benötigt der Separationskern Messfunktionen zur Integritätsprüfung, die den Hashwert des betroffenen Speicherbereiches berechnen. Dieser Hash wird mit seiner ID, zum Beispiel in Verbindung mit dem Dateinamen und der zugehörigen VM, an die Inspector VM übertragen. Der Inspector überwacht das Speicherlayout aller Prozesse in seiner VM und den Hash von jeder Seite des gemessenen Speicherbereiches. Mit diesen Informationen kann der Inspector die richtigen Hashwerte in seiner Datenbank mit denen, die in den Speicher geladen sind, vergleichen. Wenn sie nicht übereinstimmen, kann davon ausgegangen werden, dass der Prozess nicht vertrauenswürdig ist. Bis der Inspector diesen Vergleich beendet hat, wird der geprüften VM nicht erlaubt, den Speicherbereich auszuführen oder zu modifizieren, um TOCTTOU-Konsistenz zu gewährleisten. Dies kann durch Hardware-Unterstützung erreicht werden, wie beispielsweise dem NX-Bit Flag, welches auf den meisten Hardware-Plattformen verfügbar ist. Das Ausführen eines Befehls von einer Seite, die durch das NX-Flag geschützt ist, verursacht eine Ausnahme, die der Separationskern abfängt. Nachdem eine Seite vom Inspector überprüft wurde, markiert der Separationskern diese Seite als ausführbar, aber nicht beschreibbar.

4.1 Dateisystemstrukturprüfung

Ein weiteres bzw. zusätzliches Verfahren ist die einfache Überprüfung des Dateisystems. Falls die Dateien und die Dateisystemstruktur auf dem Messgerät sich nicht verändert haben, kann man davon ausgehen, dass noch dieselbe Software auf dem Gerät läuft, die auch zugelassen wurde.

Das hier vorgestellte Verfahren konzentriert sich auf eine effiziente und platzsparende Prüfung der Dateisystemintegrität, um auch für eingebettete, ressourcenarme Geräte einsetzbar zu sein. Dabei werden folgende Punkte erfüllt bzw. ermöglicht:

- Einhaltung der gesetzlichen Vorgaben des Messwesens
- Nachvollziehbares Verfahren bis zur Hashberechnung
- Auslagerung der Dateien und des Dateisystems auf andere Geräte (z. B. bei Cloud-Anbindung)
- Hash-Überprüfung über offene Netzwerke aus der Ferne, um die Vorort-Prüfung zu ersetzen
- Effiziente Berechnung der Dateisystemstruktur mit geringem Platzverbrauch

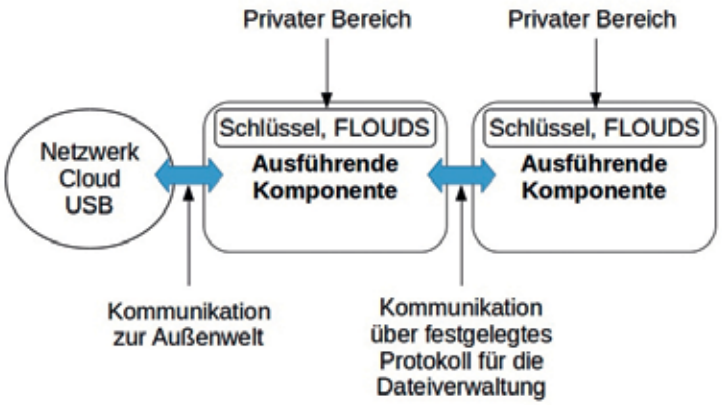

Bild 5: Trennung der Datei-Verwaltung vom restlichen System. Die Datenstruktur (FLOUDS) wird im weiteren Text erklärt.

4.1.1 Grundstruktur

Um eine sichere Überprüfung des Dateisystems zu ermöglichen, muss die Dateisystem-Verwaltung von dem eigentlichen System getrennt werden, wie in Bild 5 gezeigt.

Diese Dateiverwaltungs-Komponente kann sich auf dedizierter Hardware, oder auch gekapselt über Virtualisierung auf einem Separationskern (Hypervisor) in einer virtuellen Maschine, befinden. Durch die Separation wird sichergestellt, dass die ausführende Komponente keine Veränderungen an dem Dateisystem durchführen kann, ohne vorher mit der Dateiverwaltungs-Komponente zu kommunizieren. Die Kommunikationsschnittstelle darf dabei nur Befehle verarbeiten, welche folgende Aufgaben erfüllen:

- Einlesen von Dateien/Ordnern
- Senden der Dateisystemstruktur
- Senden des berechneten Hashwertes
- Schreiben von Dateien/Ordnern
- Umbenennen von Dateien/Ordnern
- Löschen von Dateien/Ordnern
- Erstellen von Dateien/Ordnern

Die Dateiverwaltungs-Komponente sollte zudem keine anderen Anfragen annehmen bzw. keine anderen Aufgaben erfüllen, welche nicht für die Dateiverwaltung benötigt werden. Das Verwenden eines Dateisystemprotokolls wie NFS, wobei alle anderen Ports geschlossen werden, ist beispielsweise eine zulässige Lösung. Somit kann die Dateiverwaltung auf ein dediziertes Gerät ausgelagert werden, welches über das Netzwerk angeschlossen ist. Falls eine Implementierung der gesamten Software auf nur einem Gerät gewünscht wird, kann dies bei Virtualisierung über die Emulation eines virtuellen Netzwerkes geschehen, in dem der Hypervisor einen *shared Buffer* aufbaut und die virtuellen Maschinen über virtuelle Netzwerkarten miteinander verbindet.

4.1.2 Einlesen von Dateien / Ordnern

Um Dateien zu lesen, sendet die Dateiverwaltungs-Komponente, die Datei bzw. einen angefragten Teil der Datei, an eine berechtigte Komponente. Falls die Komponente auf der gleichen Hardware, bzw. über eine fest verdrahtete Verbindung angeschlossen ist, ist keine Authentifizierung notwendig. Jedoch sollten Hardware-Manipulationen ersichtlich werden, wie es beispielsweise bei Messgeräten im gesetzlichen Messwesen, durch das Anbringen von Siegeln am Gehäuse, ermöglicht wird.

Bei Komponenten, die über offene Schnittstellen (beispielsweise auch über das Internet) auf die Dateiverwaltungs-Komponente zugreifen, sollte die Kommunikation über kryptografische Methoden abgesichert werden. Ein mögliches Szenario wäre ein virtuelles privates Netzwerk (VPN) über das Transport Layer Security (TLS) Protokoll zu erstellen, oder manuell bei jeder Anfrage eine Challenge beizufügen, die nachher bei der Antwort verschlüsselt mit der Signatur der Datei (auch verschlüsselt) zurückgegeben wird. Hierbei wird ein asymmetrisches Verschlüsselungsverfahren benutzt. Die anfragende Komponente sendet ihre Signatur und die Challenge verschlüsselt durch ihren privaten Schlüssel an die Dateiverwaltungs-Komponente. Diese überprüft die Signatur nach dem Entschlüsseln mit dem öffentlichen Schlüssel der Komponente. Falls diese Komponente nun befugt ist, wird die Anfrage ausgeführt und die Antwort mit der Signatur und der Challenge (beide mit dem privaten Schlüssel verschlüsselt) zurückgesendet. So können sich beide Komponenten gegenseitig authentifizieren. Falls gewünscht kann bei größeren Systemen eine Public Key Infrastructure (PKI) benutzt werden, um die Zertifikate und öffentlichen Schlüssel zu verwalten.

Falls Dateien aufgeteilt auf mehreren Servern, z. B. in einer Cloud, verwaltet werden, sollte zudem der Hashwert der angefragten Datei von dem Server mit zugesendet werden, damit die ausführende Komponente überprüfen kann, ob es sich um die Datei handelt, die auch angefragt wurde. Dabei muss die ausführende Komponente die Hashwerte der benötigten Dateien intern abspeichern.

Alle Anfragen über das Netzwerk, wie der Dateiliste zum Prüfen der Integrität, können über die ausführende Komponente (s. Bild 5) laufen, solange diese die privaten Schlüssel des Anfragenden und der Dateiverwaltungskomponente nicht kennt, denn sie kann die Dateiliste nicht unbemerkt verändern.

4.1.3 Erstellen der Dateisystemstruktur

Um dem Anfragenden den Hashwert zu schicken, oder der ausführenden Komponente die Dateisystemstruktur, muss diese erstellt werden. Am geeignetsten ist es, sich an bekannten, platzsparenden Datenstrukturen für Bäume zu orientieren, wie der *level order unary degree sequence* (LOUDS) [19], der *balanced parantheses* (BP) [26] oder der *depth first unary degree sequence* (DFUDS) [11]. Diese sind in Bild 6 dargestellt.

Die LOUDS wird gebildet, indem eine Breitensuche durch den Baum durchgeführt wird, angefangen bei einem *Super-root,* der mit dem echten Wurzelknoten verbunden ist. Für jeden durchlaufenen Knoten wird dann 1...10 angefügt, wobei die Anzahl von 1en der Anzahl seiner Kinder entspricht.

Die BP und DFUDS verwenden die Tiefensuche. Bei der BP wird für jeden Sprung zu einem Abwärtsknoten eine offene Klammer notiert, und für jede Abarbeitung eines Teilbaumes eine geschlossene Klammer. Die DFUDS kombiniert die BP und die LOUDS, indem für die Anzahl der Kinder jedes Knotens offene Klammern notiert werden. Dabei wird anfangs eine offene Klammer eingefügt, ähnlich des Super-Roots in der LOUDS. Für jede Abarbeitung eines Knotens wird eine geschlossene Klammer notiert.

Um Funktionen, wie das Ausgeben des Vaters oder der Kinder eines bestimmten Knotens zu ermöglichen, werden folgende Hilfsfunktionen benötigt:

Für ein String S der Länge |S| = n gilt:

- rank_a(S,p): Mit p <= n, gibt sie Anzahl von Zeichen a bis Position p in S aus.
- select_a(S,n): Gibt die Position des n-ten Zeichens a in S aus.
- Sei nun der String S ein Bitvektor (bestehend aus den beiden Zeichen ‚(, und ‚)')
- enclose(S,p): Findet das Klammernpaar, welches die offene Klammer an Position p am engsten einschließt und gibt die Position der offenen Klammer des Klammernpaares zurück.
- findclose(S,p): Gibt die Position der geschlossenen Klammer zu der offenen Klammer an Position p zurück

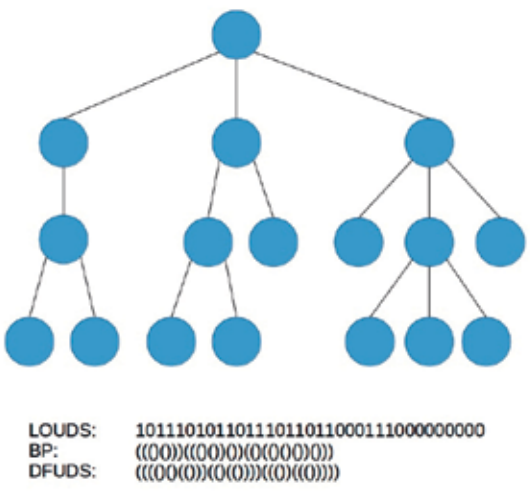

Bild 6: Vergleich von LOUDS, BP und DFUDS

- findopen(S,p): Gibt die Position der offenen Klammer zu der geschlossenen Klammer an Position p zurück

Alle Funktionen können für einen Bitvektor in O(1) Zugriffszeit realisiert werden, mit geringem Platzverbrauch von o(n).

Ein Verfahren, das baumartige Graphen, wie es Dateisysteme mit Links sind, darstellt, ist in [15, 16] erklärt. Dieses Verfahren wurde primär für die Darstellung von phylogenetischen Netzwerken entwickelt und setzt auf der LOUDS auf. In der ursprünglichen Version wird eine Trit-Variante vorgeschlagen, die aber für Dateisysteme eher nicht geeignet ist, weil man meistens zwischen mehr Dateitypen als Links und regulären Dateien differenzieren will. In diesem Dokument wird eine neue angepasste Variante namens FLOUDS (*Filesystem Level Order Unary Degree Sequence*) beschrieben (s. Bild 7), die auch auf der LOUDS aufsetzt. Die LOUDS als Basis ist im Vergleich zu den anderen beiden Verfahren (BP und DFUDS) vorteilhaft, denn es müssen nur die Funktionen *select* und *rank* erstellt werden, um ein Traversieren zu ermöglichen. Dies führt zu einem einfacheren, schnelleren und sogar platzeffizienteren Aufbau.

Für eine detailliertere Darstellung von Dateitypen sollten die Dateien nicht nur in Links und normale Dateien eingeteilt werden, sondern wie beispielsweise in Linux in unterschiedliche Typen:

1. Reguläre Dateien
2. Verzeichnisse
3. Links (hard-, soft)
4. Blockorientierte Geräte
5. Zeichenorientierte Geräte

Diese Liste lässt sich beliebig erweitern (Sockets, Pipes, MIME-Typen) oder kürzen.

Die FLOUDS wird nun wie folgt erstellt: Durchführen einer Breitensuche durch den Dateisystembaum, wobei die vordefinierte Nummer des Dateityps an den Platz der Knotennummer in S geschrieben wird. Falls der Knoten der erste Knoten von einem Vater ist, wird in B an die Stelle eine 1 notiert, sonst eine 0. Das *Array S* kann direkt als *Wavelet-Tree* [17] erstellt werden, wenn man die Anzahl der Dateitypen t von Anfang an kennt, oder später nach dem kompletten Durchlauf. Ein Wavelet-Tree ermöglicht rank und select in O(lg t) Zeit auf einem Alphabet der Größe t und ist zudem platzeffizient.

Zusätzlich werden die Datei- / Ordnernamen in N hintereinandergeschrieben, wobei Bn durch 1en markiert, wo der Name eines neuen Knotens anfängt/endet. Nach einem kompletten Durchlauf ist dann S, B, N und Bn erstellt und man kennt die Anzahl der Knoten n und die Anzahl der Links l.

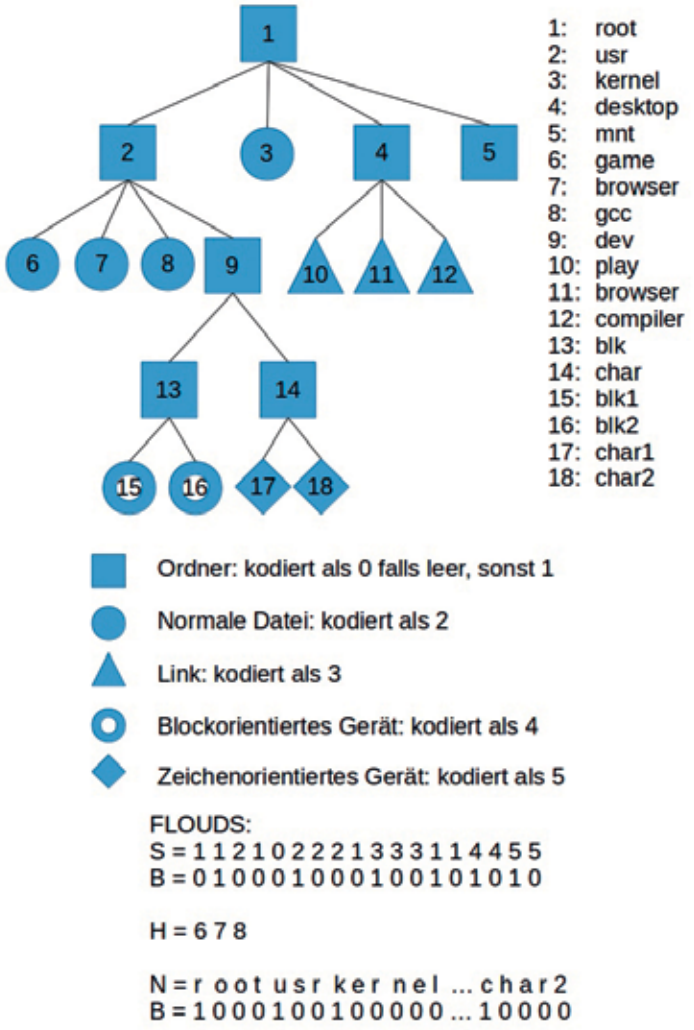

Bild 7: Neue Datenstruktur FLOUDS bestehend aus S, B, H, N und Bn. Dateinamen (oben rechts) werden separat gespeichert

Mit dieser Information kann dann auch das Array H erstellt werden, welches benutzt wird, um die Linkadresse auf den echten Knoten zu speichern. Dieses benötigt l*lg(n) Platz und speichert in der Reihenfolge in denen die Links in S vorkommen deren Nummer zu dem Originalknoten. Dafür wird von jedem Link der Dateipfad ermittelt (s. Abschnitt Traversieren der FLOUDS) und dann der Pfad zu der Datei, auf die er zeigt, ausgelesen. Über diesen kann wiederum die FLOUDS-Nummer der Datei ermittelt werden, welche in H abgelegt wird. H sollte zum Schluss auch in ein Wavelet-Tree umgewandelt werden, um rank und select effizient zu ermöglichen.

Die FLOUDS wird vor der Inbetriebnahme des Gerätes erstellt und in die privaten Bereiche der Komponenten übertragen (s. Bild 6). Auf die privaten Bereiche hat nur die jeweilige Komponente Zugriff.

4.1.4 Traversieren der FLOUDS

Über S und B aus Bild 7 kann man zu jedem Knoten traversieren, ähnlich wie es in der LOUDS

gemacht wird. Funktionen parent und child sind wie folgt:

- child (n, i) = select_1(B; rank_1(S; n)) + i – 1, falls S[n] = 1
- parent(n)=select_1(S; rank_1(B; n))

Über H kann auch noch abgefragt werden, ob ein Knoten ein Link ist (S[n] = 3), bzw. weitere Links besitzt und welche Knotennummer diese haben (über den Wavelet Tree von H):

- get_link(n, i) = select_3(S; select_n(H; i))
- get_orig(n) = H[rank_3(S; n)], falls S[n] = 3

Zusätzlich können über die rank und select Funktionen folgende Operationen direkt ausgeführt werden:

- Bestimmung der Anzahl von Knoten eines Ordners und deren Auflistung
- Bestimmung der Anzahl bestimmter Dateitypen in einem Ordner und deren Auflistung
- Bestimmung der Anzahl bestimmter Dateitypen im gesamten Dateisystem und deren Auflistung

4.1.5 Dateisystemintegritätsprüfung

Es gibt mehrere Varianten die Dateisystemintegrität zu überprüfen:

1. Die FLOUDS wird bei Anfrage einfach mit den Dateinamen signiert übermittelt;
2. Die FLOUDS wird neu erstellt und beim Traversieren der Dateisystemstruktur wird von jeder Datei auch ein Hashwert berechnet. Dieser wird in ein Hash-Array der Größe n an die richtige Stelle geschrieben;
3. Um Platz bei der Übertragung zu sparen, können die Dateinamen ausgelassen werden und in die Hashwerte von Punkt 2 einfließen;
4. Es wird nur von einer kleinen Anzahl von vordefinierten Dateien der Hash gebildet, um noch mehr Platz zu sparen. Der Dateiverwaltungskomponente wird dabei vorher eine Liste der Dateinummern übergeben. Diese gibt dann die FLOUDS und die Hashwerte für genau diese Dateinummern wieder;
5. Es wird nur ein einziger Hashwert über die gesamte Struktur gebildet.

Die fünfte Methode benötigt den geringsten Platz, weil nur ein Hashwert übertragen werden muss. Dieser kann beispielsweise bei Anfrage, auf dem Display des Gerätes dargestellt werden. Falls er nicht mit dem erwarteten Wert übereinstimmt, kann man eine der anderen Methoden aufrufen, um sich die genaue Dateisystemstruktur zuschicken zu lassen. Dabei wird ersichtlich, welche Dateien genau verändert wurden.

Der benutzte Hash-Algorithmus sollte so kollisionsfrei wie möglich sein. Er kann aber je nach Performance, Platzgründen oder Sicherheitsnachfrage beispielsweise von einfachen Checksummen wie CRC16 bis hin zu sicheren Hasch-Algorithmen wie SHA-2 reichen.

4.1.6 Verändern von Dateien

Bei Aufrufen, welche die Struktur des Dateisystems verändern, beispielsweise durch das Löschen und Erstellen von Ordnern/Dateien, muss immer überprüft werden, ob dies erlaubt ist, wie im Abschnitt zum Einlesen von Dateien beschrieben, beispielsweise über Signaturen. Nachher können diese Zugriffe *lazy* oder *eager* übernommen werden, also direkt nach dem Aufruf, oder erst einmal intern auf der Komponente und später sobald genügend Änderungen vorhanden sind, auf der Dateiverwaltungs-Komponente.

Änderungen an der Dateisystemstruktur sollten generell nur selten passieren und sind bei Geräten im amtlichen und gewerblichen Interesse auch oft nicht zulässig (nur nach Überprüfung und erneuter Zulassung). Falls Änderungen jedoch vorgenommen werden sollen, muss die Dateisystemstruktur neu erstellt werden. Bei der einfachen Namensdarstellung, wie in Bild 8 zu sehen über N und Bn, können Änderungen leichter übernommen werden. Werden jedoch andere Verfahren zum Abspeichern der Dateinamen verwendet (s. nächsten Abschnitt), müssen die Strukturen der Dateinamen oft komplett neu aufgebaut werden, was zeitaufwendig sein kann.

4.1.7 Auffinden von Dateinamen

Eine einfache Methode Dateien schneller zu finden, wird erreicht, indem man die Ordnereinträge alphabetisch sortiert, wodurch man über die binäre Suche in O(lg(k)) Zeit einen Ordner nach einem Präfix durchsuchen kann, wobei k die Anzahl der Ordnereinträge ist. Insgesamt bräuchte man somit O(f*lg(k)) Zeitaufwand, um alle Ordner nach einem Präfix zu durchsuchen, wobei f die Anzahl der Ordner darstellt.

Eine effizientere Suche eines Teilstrings in den Dateinamen kann durch das Anwenden von *2-Way Dictionaries* erreicht werden. Ein Beispiel wäre über die *Burrows-Wheeler Transformation* (BWT) [12] mit Lauflängenkodierung auf N von Bild 8. Genauer wird das Vorgehen in [14] beschrieben. Hierbei können Teilstrings effizient gefunden und auf deren FLOUDS-Nummern abgebildet werden, oder über die FLOUDS-Nummer, der Dateiname ausgelesen werden. Zusätzlich werden die Dateinamen auch komprimiert.

Ein weiteres Verfahren ist in [8] beschrieben. Dabei wird der Lempel-Ziv 78 Algorithmus so verändert, dass das Auffinden von Präfixen ermöglicht wird. In dem konkreten Fall würde man für jeden Knoten den gesamten Pfad der Dateisystemstruktur speichern (für Knoten 5 aus Bild 8 wäre das beispielsweise „root/mnt“). Nun kann aus der Pfadeingabe über die Struktur die FLOUDS-Nummer bestimmt werden. Zusätzlich wird jeder Datei- bzw. Ordnername auch noch extra in die Struktur aufgenommen (für Knoten 5: „mnt“). Dies ermöglicht die Präfixsuche nach Datei/Ordnernamen. Das Verfahren eignet sich so gut für die Integritätsprüfung von Dateisystemstrukturen, weil man ein Auffinden von Dateinamen über Teilstrings nicht benötigt, sondern den genauen Dateinamen eingeben würde. Für eine effiziente Auflistung aller Dateien, die einen bestimmten Teilstring enthalten, wie z. B. in Linux über den „locate“ Befehl, eignet sich die erste Variante aus [14] jedoch besser.

4.1.7 Mögliche Einsatzfelder

Wie anfangs erwähnt, sind die Messgeräte des gesetzlichen Messwesens (ca. 130 Mio. Geräte in Deutschland in ca. 150 Messgerätetypen, Teilgeräten und Zusatzeinrichtungen) ein großes Einsatzgebiet für diese Struktur. Ansonsten kann diese Struktur gut für Geräte verwendet werden, die über Cloud-Anbindung verfügen. Die Dateien sind hierbei in der Cloud gespeichert, das Gerät besitzt aber die Dateiliste mit der es die Dateien auf unterschiedlichen Servern ansprechen kann. Durch die Netzwerkanbindung brauchen Geräte ohne Speichermedium, bzw. mit kleinem Speicherplatz anfangs nur die Dateilisten abzuspeichern. Außerdem ermöglicht die Datenstruktur ein schnelles Auffinden von Dateien und eignet sich sehr gut für die Grundlage eines komprimierten read-only Dateisystems.

Das Verfahren ist auch für Technologiefelder wie Industrie 4.0, die intensiv auf sichere Cloud-Anwendungen setzen, interessant.

5 Zusammenfassung

Die hier vorgestellte Systemarchitektur für Messgeräte wurde durch die Analyse der Anforderungen des gesetzlichen Messwesens zusammen mit Methoden und Konzepten aus Hochsicherheits-Softwaresystemen konstruiert. Der Ansatz der Systemarchitektur lässt sich in drei Schritten zusammenfassen:

1. Die rechtlich relevanten Teile werden von den nicht rechtlich relevanten getrennt, indem sie in verschiedenen virtuellen Maschinen isoliert werden.
2. Ihre virtuellen Maschinen haben keinen direkten Zugriff auf Eingabe- oder Ausgabe-Geräte.
3. Durch ein sicheres Rahmenwerk, welches wieder selber aus getrennten virtuellen Maschine besteht, und das den Informationsfluss überwacht und Anfragen an E/A-Geräte delegiert, werden Verifikationsbehörden bei der Prüfung der Systemintegrität unterstützt.

Um Gerätetreiber und Netzwerkstapel von Standard-Betriebssystemen zu nutzen, wird Virtualisierung über einen Separationskern angewandt, wodurch Sicherheit mit Benutzerfreundlichkeit kombiniert wird. Über den Separationskern wird die Softwaresicherheit erhöht, welche in vielen Messgeräten aufgrund der Anbindung an das Internet über Standard-Betriebssysteme häufig gar nicht gewährleistet werden kann. Zusätzlich ist die Verifikation der Software im Feld für Messgeräte sehr wichtig, weshalb in diesem Artikel auch eine Methode vorgestellt wurde, mit der die Dateisystemintegrität leicht und korrekt überprüft werden kann. Dabei wird es dem Hersteller erleichtert, konkrete Testsoftware zu erstellen, um der Marktüberwachung zu ermöglichen, die Integrität der Software zu überprüfen, so wie gesetzlich gefordert (s. MID Annex I 7.6, Annex I 8.2, Annex I 8.3).

Referenzen

[1] *AMD64 Virtualization Codenamed „Pacifica“ Technology Secure Virtual Machine Architecture Reference Manual*, Whitepaper, May 2005

[2] *Intel Virtualization Technology and Intel Active Management Technology in Retail Infrastructure*, Whitepaper, December 2006

[3] *Understanding Full Virtualization, Paravirtualization, and Hardware Assist*, Whitepaper, September 2007

[4] *Cortex-A15 Technical Reference Manual*, Whitepaper, September 2011

[5] *ARM Architecture Reference Manual*, ARMv7-A and ARMv7-R edition, Whitepaper, July 2012

[6] *Cortex-A7 Technical Reference Manual*, Whitepaper, May 2012.

[7] J. Alves-Foss, W. Scott Harrison, P. Oman und Carol Taylor: *The mils architecture for high-assurance embedded systems*, Journal of Embedded Systems, 2:239–247, 2006, International

[8] J. Arz und J. Fischer: *LZ-Compressed String Dictionaries*, Data Compression Conference (DCC), 322–331, 2014

[9] Paul Barham, Boris Dragovic, Keir Fraser, Steven Hand, Tim Harris, Alex Ho, Rolf Neugebauer, Ian Pratt und Andrew Wareld: *Xen and the art of virtualization*, SIGOPS Oper. Syst. Rev., 37(5), 164–177, October 2003

[10] R. Beckwith, W. Mark Vanfleet und Lee MacLaren: *High assurance security/safety for deeply embedded, real-time systems*, Systems Conference, Citeseer, 2004

[11] D. Benoit, E.D. Demaine, J.I. Munro, R. Raman, V. Raman und S.S. Rao: *Representing trees of higher degree*, Algorithmica 43 (4), 275–292, 2005

[12] M. Burrows und D. Wheeler: *A block sorting lossless data compression algorithm*, Technical Report 124, Digital Equipment Corporation, 1994

[13] Kevin Elphinstone und Gernot Heiser: *In Embedded From l3 to sel4 what have we have learnt in 20 years of l4 microkernels*? In Proceedings of the Twenty-Fourth ACM Symposium on Operating Systems Principles, 133–150, ACM, 2013

[14] P. Ferragina und R. Venturini: *The compressed permuterm index*, ACM Trans. Algorithms 7, 1, Article 10, 21 pages, 2010

[15] J. Fischer und D. Peters: *GLOUDS: Representing tree-like graphs*, Journal of Discrete Algorithms 11/2015; DOI:10.1016/j.jda.2015.10.004

[16] J. Fischer und D. Peters: *A Practical Succinct Data Structure for Tree-Like Graphs*, WALCOM: Algorithms and Computation, Dhaka, Bangladesh, 02/2015

[17] R. Grossi, A. Gupta und J. S. Vitter: *High-order entropy-compressed text indexes*, Proceedings of the 14th Annual SIAM/ACM Symposium on Discrete Algorithms (SODA), 841–850, 2003

[18] Hermann Härtig, Michael Hohmuth, Jochen Liedtke, Jean Wolter und Sebastian Schönberg: *The performance of µ-kernel-based systems*, In Proceedings of the Sixteenth ACM Symposium on Operating Systems Principles, SOSP '97, 66–77, New York, NY, USA, ACM, 1997

[19] G. Jacobson: *Space-efficient static trees and graphs*, In Proceedings of the 30th Annual Symposium on Foundations of Computer Science (SFCS '89), IEEE Computer Society, Washington, DC, USA, 549–554, 1989

[20] Paul A. Karger: *Multi-level security requirements for hypervisors*, Computer Security Applications Conference, 21st Annual, 9–pp. IEEE, 2005

[21] Paul A. Karger, Mary Ellen Zurko, Douglas W. Bonin, Andrew H. Mason und Cliord E. Kahn: *kernel. A retrospective on the vax vmm security,* IEEE Trans. Softw. Eng., 17(11), 1147–1165, November 1991

[22] Gerwin Klein, Kevin Elphinstone, Gernot Heiser, June Andronick, David Cock, Philip Derrin, Dhammika Elkaduwe, Kai Engelhardt, Rafal Kolanski, Michael Norrish, Thomas Sewell, Harvey Tuch und Simon Winwood: Proceedings of the ACM SIGOPS 22nd Symposium on Operating Systems Principles. sel4: *Formal verication of an os kernel*, In SOSP '09, 207–220, New York, NY, USA, ACM, 2009

[23] Adam Lackorzynski, Alexander Warg und Michael Peter: *Virtual processors as kernel interface*, In Proceedings of the Twelfth Real-Time Linux Workshop, Nairobi, Proceedings of the Twelfth Real-Time, 2010

[24] N. Leer und F. Thiel: *Im Geschäftsverkehr das richtige Maß*, In Schlaglichter der Wirtschaftspolitik, Monatsbericht, November 2013

[25] *Jochen Liedtke*: On µ–kernel construction. In System Principles, ACM, 1995

[26] J.I. Munro und V. Raman: *Succinct representation of balanced parentheses and static trees*, SIAM J. Computing, 31, 762–776, 2001

[27] Official Journal of the European Union, Directive 2004/22/EC of the European Parliament and of the Council, March 2004

[28] Official Journal of the European Union, Directive 2014/32/EU of the European Parliament and of the Council, February 2014

[29] OIML D 31, General requirements for software controlled measuring instruments, 2008

[30] Michael Peter, Jan Nordholz, Matthias Petschick, Janis Danisevskis, Julian Vetter und Jean-Pierre Seifert: *Undermining isolation through covert channels in the Fiasco.oc microkernel*

[31] D. Peters, F. Thiel, M. Peter und J.-P. Seifert: *A Secure Software Framework for Measuring Instruments in Legal Metrology*, Instrumentation and Measurement Technology Conference (I2MTC), 2015 IEEE International, Pisa, 05/2015

[32] D. Peters, U. Grottker, F. Thiel, M. Peter und J.-P. Seifert: *Achieving software security for measuring instruments under legal control*, Federated Conference on Computer Science and Information Systems, ISBN 978-83-60810-57-6 (online), Warsaw, ISSN 3300–5963, 09/2014

[33] D. Peters, M. Peter, J.-P. Seifert und F. Thiel: *A Secure System Architecture for Measuring Instruments in Legal Metrology*, 4(7), 61–86, 03/2015; DOI:10.3390/computers4020061

[34] Gerald J. Popek und Robert P. Goldberg: *Formal requirements for virtualizable third generation architectures*, Commun. ACM, 17(7), 412–421, July 1974

[35] Reiner Sailer, Trent Jaeger, John Linwood Grin, Stefan Berger, Leendert van Doorn, Ronald Perez und Enriquillo Valdez: *Building a general-purpose secure virtual machine monitor*, RC23537 (W0502–132), 2005

[36] Slawomir Samolej: *Arinc specification 653 based real-time software engineering*, E-Informatica, 5(1), 39–49, 2011

[37] Michael von Tessin: *The clustered multikernel: An approach to formal verication of multiprocessor OS kernels*. In Proceedings of the 2nd Workshop on Systems for Future Multi-core Architectures, Bern, Switzerland, 2012

[38] F. Thiel, M. Esche, D. Peters und U. Grottker: *Cloud Computing in Legal Metrology*, 17th International Congress of Metrology, EDP Sciences 2015, Paris, 09/2015

[39] WELMEC European cooperation in legal metrology, WELMEC 7.2 Issue 5 Software Guide, March 2012

[40] Xia Yang, Xiangyu Zhao, Jian Lei und Guangze Xiong: *A trusted architecture for escs with mls,* In Embedded Software and Systems Symposia, 2008 ICESS Symposia'08. International Conference on, pages 44-49. IEEE, 2008

[41] Yongwang ZHAO, MA Dianfu und YANG Zhibin: *A survey on formal specification and verification of separation kernels*, Technical report, Tech. rep., National Key Laboratory of Software Development Environment (NLSDE), Beihang Univerisity, 2014

Referenzarchitektur für das Cloud-Computing im gesetzlichen Messwesen

Alexander Oppermann*

1 Einleitung

In den vergangenen Jahren hat sich die *Cloud-Computing*-Technologie ständig weiterentwickelt und ist an verschiedenen Herausforderungen gewachsen, im Besonderen in den Bereichen Sicherheit, Stabilität und Zuverlässigkeit. Daher stellt sich nun die Frage, ob Cloud-Computing reif genug ist, um den Anforderungen, Erwartungen und Herausforderungen des gesetzlichen Messwesens zu genügen.

Gartners Hypecycle aus dem Jahr 2015 zufolge [9] hat sich Cloud-Computing als aufstrebende Technologie gerade etabliert, denn Unternehmen setzen Cloud-Lösungen zunehmend in industriellen Anwendungen ein.

Im gesetzlichen Messwesen nehmen die Anfragen von Messgeräteherstellern und Marktaufsichtsbehörden zu, die sich für rechtskonforme Umsetzungen der Cloud-Technologien interessieren. Erste vielversprechende Ansätze, Cloud-Computing in bestehende Geschäftskonzepte einzubinden oder in Produkte zu integrieren, werden an die Zulassungsbehörden herangetragen. Dabei zielt man insbesondere auf die Vorteile der Virtualisierung ab, Infrastruktur einfach und schnell den Anforderungen entsprechend skalieren und auf die Industrieprozesse ausdehnen zu können, sodass kosteneffiziente und moderne Lösungen entstehen können. Indem man Daten zentral speichert und verwaltet, oder auch komplette Softwareprozesse externalisiert, also in die Cloud verlagert, wird es möglich, Verwaltungs-, Wartungs- und Unterhaltskosten erheblich zu senken.

Darüber hinaus werden durch die Virtualisierung und Externalisierung Messgeräte erheblich in ihrer Größe reduziert und damit kostengünstiger. Folgerichtig gehen die Prognosen für den zukünftigen Entwurf eines Messgerätes von einer gekoppelten, rudimentären Sensor- und Kommunikationseinheit für die Internetverbindung im Feld aus (vgl. [1]). Der metrologische „Rest", z. B. Datenverarbeitung und -speicherung, wird sich in die Cloud verlagern und so die bisherigen Lösungen stärker zentralisieren.

Mit Einführung von Cloud-Computing im gesetzlichen Messwesen wird sich das Zusammenspiel aller Marktteilnehmer (Hersteller, Verwender, benannte Stellen und Marktüberwachung) verändern. Darüber hinaus entstehen neue Rollen (z. B. Cloud-Service-Betreiber), deren Pflichten und Aufgaben bestimmt und in das bestehende Rahmenwerk des gesetzlichen Messwesens integriert werden müssen.

In Europa werden alle Messgeräte, die dem gesetzlichen Messwesen unterliegen, durch benannte Stellen konformitätsbewertet, um sicherzustellen, dass die grundlegenden Anforderungen der europäischen Messgeräterichtlinie (*Measuring Instrument Directive* 2014/32/EU (MID)) [2] erfüllt werden. National wird die MID durch das Mess- und Eichgesetz abgebildet und stellt Anforderungen an national geregelte Messgeräte. Zusätzlich zur MID gibt es weitere Dokumente, wie den WELMEC-Softwareleitfaden [3] oder den OIML-Leitfaden [4], die technische Hilfestellungen für softwaregestützte Messgeräte auf Basis grundlegender Anforderungen der Rechtsnorm anbieten. Die Entwicklung neuer Standards, Validierungen und Empfehlungen für Cloud-Computing im gesetzlichen Messwesen ist Teil weiterer Forschung und wird in die Überarbeitung der Handlungsempfehlungen der genannten Dokumente einfließen, um sie auf dem Stand der Technik zu halten (vgl. [1]).

Als vorläufiges Forschungsergebnis soll hier eine Referenzarchitektur vorgestellt werden, die die wesentlichen Anforderungen der europäischen Norm auf höchstem Sicherheitsniveau erfüllt. Diese Architektur kann an die instrumentenspezifischen Anforderungen angepasst und auf das jeweilige Sicherheitsniveau skaliert werden.

* Alexander Oppermann, Arbeitsgruppe 8.52 „Metrologische IKT-Systeme", E-Mail: Alexander.Oppermann@ptb.de

Durch den Einsatz der Cloud-Technologie entstehen neue Rollen. Diese sollen hier beschrieben und in das Rechtsgebäude eingefügt werden.

2 Gesetzliches Messwesen

Die Aufgabe des gesetzlichen Messwesens ist die Sicherstellung des richtigen Messens und damit die Erhaltung des Vertrauens in Messgeräte. Das gesetzliche Messwesen ist einer der Grundpfeiler unseres ökonomischen Systems und garantiert einen fairen Handel, wobei das Hauptaugenmerk auf dem Schutz des Endverbrauchers liegt.

Das gesetzliche Messwesen umfasst ein weites Spektrum und reicht von kommerziell bis hin zu amtlich eingesetzten Messgeräten. Über 100 Millionen eichpflichtige Messgeräte sind in Deutschland im Einsatz. Davon wird der Großteil für geschäftliche Zwecke eingesetzt. Besonders hervorzuheben sind hier Verbrauchsmessgeräte im Bereich Elektrizität, Gas, Wasser und Wärme (vgl. [10]), aber auch Zähler in Kraftstoffzapfsäulen und Waagen, bspw. in Supermärkten.

Die Vertrauenskette, bestehend aus der Konformitätsbewertung, die den Produktentwurf und die darauffolgende Produktion bewertet, und der nachfolgenden Markt- und Verwendungsüberwachung dieser Geräte im Feld, bildet die Grundlage für die Marktakzeptanz der Messgeräte und neuer Technologien beim Verwender und Endverbraucher.

3 Die Rolle des Cloud-Service-Betreibers

Die am häufigsten wiederkehrende Fragestellung zum Thema Cloud-Computing konzentriert sich auf den Aspekt der Bereitstellung der Cloud und deren Dienste. Diese Rolle wird vom Cloud-Service-Betreiber übernommen und soll im Folgenden näher im Rechtsgefüge des Mess- und Eichgesetzes (MessEG) beleuchtet werden.

Im gesetzlichen Messwesen gibt es vier etablierte Hauptakteure. Dies sind die Konformitätsbewertungsstelle (benannte Stelle), der Hersteller, der Verwender und die Markt- und Verwendungsüberwachung. Durch das Cloud-Computing wird, wie bereits erwähnt, eine zusätzliche Cloud-Service-Betreiberrolle (siehe Bild 1) eingeführt. Diese Rolle ist im gesetzlichen Messwesen nicht definiert. Ihre Rechte und Pflichten in Bezug zu den anderen Marktteilnehmern ist zudem insbesondere unzureichend geklärt, wenn keiner der etablierten Marktteilnehmer diese Rolle übernimmt. Die Anforderungen für Cloud-Service-Betreiber müssen daher festgelegt und geregelt werden, damit sich diese in das bisherige rechtliche Rahmenwerk einfügen können. Diese rechtlichen Fragestellungen werden aktuell national und auf EU-Ebene geklärt. Klar ist jedoch, dass keiner der im MessEG bekannten wirtschaftlichen Akteure seine Rechte und Pflichten an einen Dritten abgeben kann. Es können privatrechtliche Verträge mit Partnern ausgehandelt werden, die deren Aufgaben, als Cloud-Service-Betreiber, übernehmen. Die Verantwortlichkeiten verbleiben jedoch beim Auftraggeber. Bisher existieren vier absehbare Szenarien für Cloud-Service-Betreiber:

1. Die Rolle des Cloud-Service-Betreibers wird vom Hersteller ausgefüllt, sodass dieser die Cloud im eigenen Unternehmen aufbaut und betreut (*On-Premise*-Lösung). Dies wird Teil des Produktentwurfs und im Zuge der Modul-B-Prüfung durch die Konformitätsbewertungsstelle bewertet.

2. Der Verwender übernimmt die Verantwortung für die Cloud und implementiert die On-Premise-Lösung. Damit übernimmt dieser im Rahmen der Verwenderpflichten die Verantwortung dafür (§23 MessEV).

3. Die Cloud-Service-Lösung wird vom Hersteller ausgelagert und an Unterauftragsnehmer vergeben (*Off-Premise*-Lösung).

4. Der Verwender vergibt an einen Unterauftragsnehmer die Bereitstellung der Cloud-Dienste (Off-Premise-Lösung).

Bei der Off-Premise-Lösung sind die privatrechtlichen Vertragsbedingungen, sogenannte *Service-Level-Agreements* (SLAs), entscheidend, da damit insbesondere die Verfügbarkeit, das Sicherheitsniveau und die Notfallkonzepte geregelt werden. Für die jeweilige Cloud-Lösung kann dies z. B. über beizubringende Zertifikate oder einzuhaltende Standards (z. B. ISO 27001/2, BSI-Standard 100-4) reglementiert werden.

Bild 1 stellt den Cloud-Service-Betreiber als frei schwebende Rolle zwischen den Akteuren und zusätzlich deren Wechselbeziehung dar. Die Rolle kann, wie bereits beschrieben, vom Hersteller oder Verwender ausgefüllt werden.

4 Sicherheitsaspekte für Cloud-Computing im gesetzlichen Messwesen

Im gesetzlichen Messwesen gelten drei besondere Grundsätze für die Messgeräte, diese sind:

- Messsicherheit,
- Messbeständigkeit und
- Prüfbarkeit.

Durch Einhaltung der wesentlichen Anforderungen der Rechtsnorm wird dies erfüllt. Zusätzlich

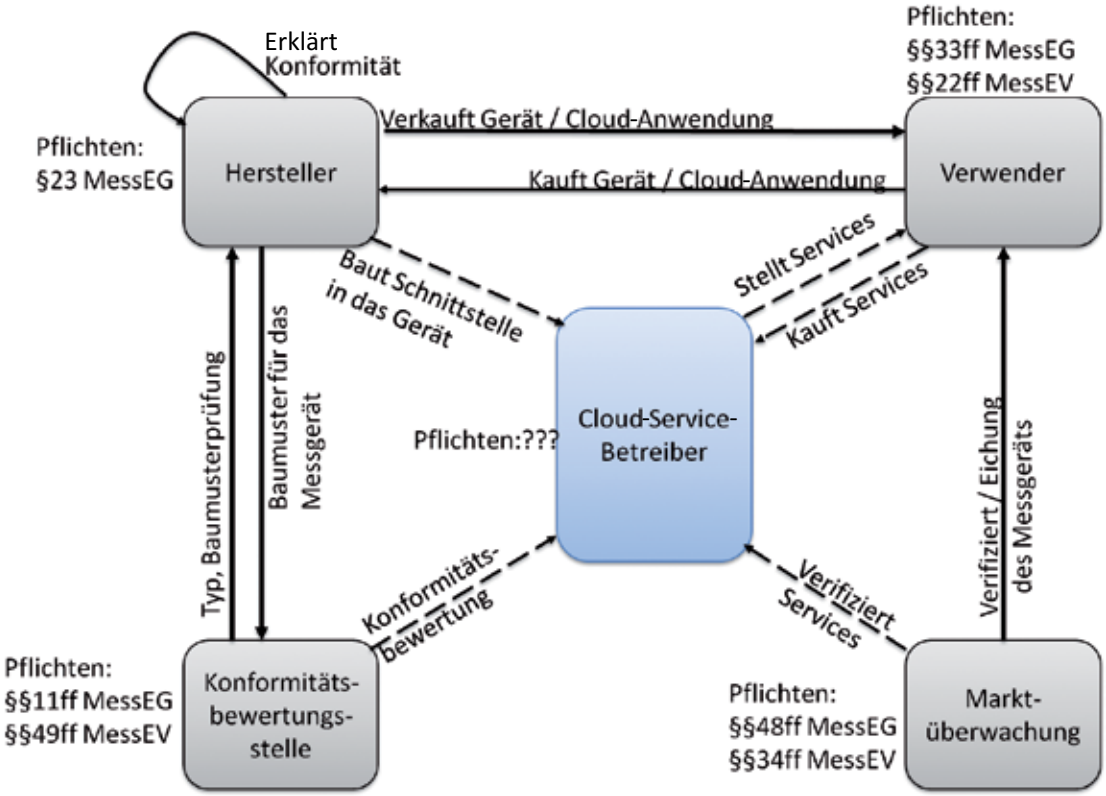

Bild 1: Überblick über die Akteure im gesetzlichen Messwesen. Die Rolle des Cloud-Service-Betreibers muss noch bestimmt werden.

werden die Integrität, die Authentizität sowie die Nicht-Bestreitbarkeit der Messdaten und Messergebnisse gewährleistet. Technische Interpretationen dieser wesentlichen Anforderungen für Softwarelösungen liegen in Form eines europäisch harmonisierten Guides (WELMEC [3]) vor.

Darüber hinaus können verschiedene Cloud-Lösungen und Anbieter mithilfe von Zertifikaten vergleichbarer und transparenter für Hersteller, Verwender und Endverbraucher werden.

Weiterhin kann durch harmonisierte Normen und Regularien für Cloud-Service-Betreiber die Sicherheit implizit erhöht werden, da man sich auf einen einheitlichen und grundsätzlichen Standard für adäquate Sicherheit beziehen kann. Die ENISA (*European Union Agency for Network and Information Security*) hat mit der europäischen Cloud-Strategie (vgl. [17]) bereits viele offene Fragestellungen benannt und Antworten erarbeitet. ENISA gibt außerdem einen Überblick über die bereits vorhandenen Zertifikate (vgl. [16]).

4.1 Verifikation der Cloud im Markt

Die Sicherheit der Cloud und deren Dienste müssen auch im Feld durch die Marktüberwachungsbehörden verifizierbar sein. Dafür ist es für die Prüfung im Feld günstig, dass die Verifikation komplexer Technologien auf einfache Weise möglich wird. Die Überprüfungsroutinen für Software, Architektur und Daten sollen ein unzweideutiges Ergebnis liefern, das wiederum den einfachen Vergleich mit dem ausgestellten Zertifikat erlaubt. Der Hersteller muss solche Testroutinen bereitstellen und beschreiben (vgl. MID Annex I 7.6). Weiterhin muss jeder Versuch einer Einflussnahme (erlaubt oder unerlaubt) in einem geschützten Logbuch überprüfbar verzeichnet werden (vgl. MID Annex I 8.2). Für die Marktüberwachung muss die Identifikation der verwendeten Software leicht feststellbar sein. Bisher werden die Maßnahmen der Marktüberwachung vor Ort überprüft. Durch die Verwendung von Cloud-Technologien ist es zukünftig denkbar, solche Überprüfungen aus der Ferne am System direkt durchzuführen, bzw. teilweise zu automatisieren, indem man z. B. Logbucheinträge bei kritischen Ereignissen, wie bspw. einer Softwareaktualisierung, direkt an die Marktüberwachungsbehörde schickt.

4.2 Bekannte Angriffe auf die Cloud-Infrastruktur und Risikoanalyse

Angriffe und Bedrohungen auf Cloud-Infrastrukturen sind bekannt. Diese werden regelmäßig auf europäischer Ebene – durch die ENISA – analysiert und veröffentlicht. Daraus sind die relevanten Angriffe für das gesetzliche Messwesen zu identifizieren, die etwa durch neue Rollen oder die gewählte Architektur entstehen.

Ein geeignetes Hilfsmittel zur Bewertung ist die Risikoanalyse [18]. In der MID (2014/32/EU) und dem MessEG sind Risikoanalyse und Risikobewertung – u. a. bei der Modul-B-Prüfung – verpflichtend angelegt für den Hersteller von Messgeräten.

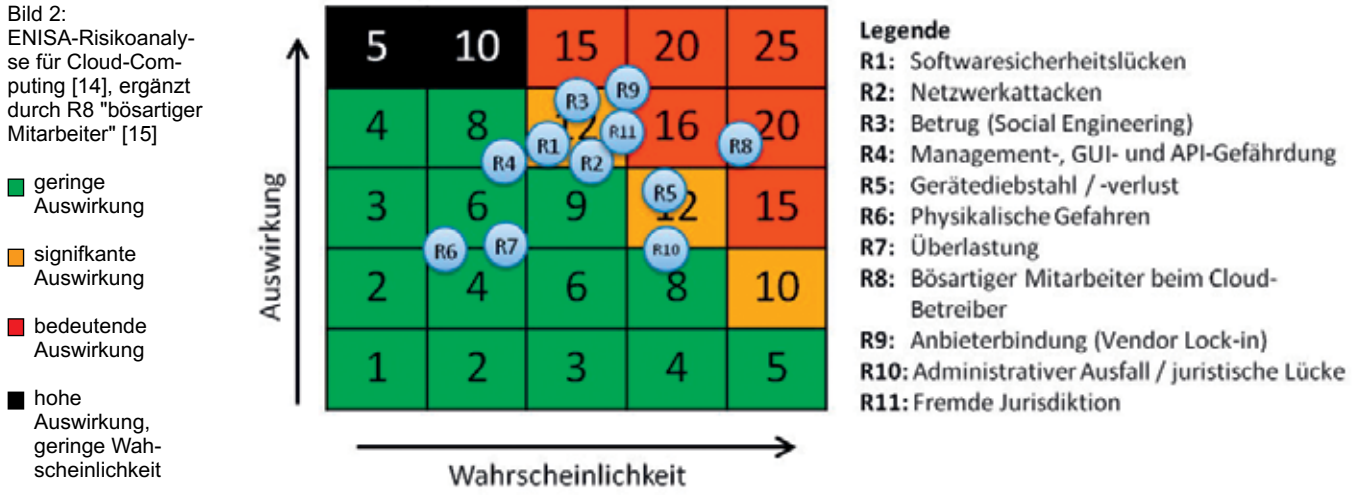

Bild 2: ENISA-Risikoanalyse für Cloud-Computing [14], ergänzt durch R8 "bösartiger Mitarbeiter" [15]

Metrologische Sicherheit ist dabei abzugrenzen von der IT-Sicherheit, obgleich deren Methoden im gesetzlichen Messwesen zum Einsatz kommen und die Überschneidungen groß sind. Aufgrund der rechtlichen Rahmenbedingungen ist die Herangehensweise jedoch unterschiedlich.

Ein großer Teil der Risikoanalyse und -bewertung – im Hinblick auf Bedrohungen des metrologischen Kerns – wird durch die Prüfung der softwareseitigen Implementierung der Messgeräte bestimmt. Sie wird sich an internationalen Industrie-Standards zur Bewertung der Sicherheit von IKT-Komponenten orientieren müssen. Nur auf diese Weise entstehen objektive Vorgehensweisen zur Bewertung neuester Risiken für Messgeräte [18].

Konformitätsbewertungsstellen begründen ihre Entscheidungen auf dem Stand der Technik. Daher ist es eine immerwährende Aufgabe für sie, das Wissen um Bedrohungen der in Messgeräten implementierten IT-Maßnahmen zur Sicherung der gesetzlichen Anforderungen aktuell zu halten.

Die Idee der Risikoanalyse ist, das vorhandene Risiko bestimmter Angriffe zu quantifizieren und damit eine Handlungsempfehlung zur Anpassung der Sicherheit von Produkten zu erhalten. Dabei werden die Auftrittswahrscheinlichkeit einer Bedrohung und die zu erwartende Wirkung (Schaden) abgewogen. Das daraus resultierende quantifizierte Risiko wird dann auf einer Risikomatrix eingetragen und auf dieser Basis bewertet (vgl. Bild 2). Dabei kann der Hersteller außerdem auf vorhandenes Wissen seiner Produktreihen zurückgreifen, um einen einfachen Einstieg zu finden.

Bild 2 zeigt, wie solch eine Risikoanalyse-Matrix aussehen kann. Hierbei wurden die wahrscheinlichsten Angriffsvektoren für Cloud-Computing bei kleinen und mittleren Unternehmen (KMU) von der ENISA evaluiert. Im Entwurf der Referenzarchitektur für Cloud-Computing wird dem Risiko des nicht vertrauenswürdigen Systemadministrators (R8 – *Malicious Insider*) und der manipulierten virtuellen Maschine (VM) (R1 – *Software Security Vulnerability*) bzw. dem Durchgriff von einer VM zur nächsten besondere Bedeutung beigemessen.

Durch Verhinderung dieser beiden Angriffe (R1, R8) werden der Zugriff und die Manipulation von Messdaten in der Cloud durch einen lokalen Administrator oder einen aus der Ferne agierenden Angreifer (Manipulation der VMs) unterbunden. Dies wird in den nächsten Kapiteln näher erläutert. Damit sind grundsätzlich die Angriffe mit dem größten Schadensrisiko für kleine und mittlere Unternehmen berücksichtigt.

5 Anforderungen an eine sichere Cloud-Referenzarchitektur

Eine Architektur für Messgeräte muss Messsicherheit, Messbeständigkeit und Prüfbarkeit der Daten bzw. der Plattform gewährleisten. Die flexible Anpassung der Plattform an instrumentenspezifische Eigenschaften, also die Skalierbarkeit der Architektur, sind zusätzliche Anforderungen. Detailliert sind die technischen Anforderungen im WELMEC-Leitfaden 7.2 Software, in seiner neuesten Fassung von 2015, beschrieben. Diese Anforderungen sollen durch die Referenzarchitektur mindestens abgedeckt werden.

Im Zuge dieses Projektes soll eine sichere Cloud-Referenzarchitektur entwickelt werden, die grundlegend die Sicherheit durch Separierung des Gesamtsystems erzielt. Dazu werden metrologisch relevante Teile in verschiedene, voneinander informationstechnisch isolierte Kompartimente, sogenannte virtuelle Maschinen (VM), aufgeteilt. Damit wird z. B. das Risiko eines Ausfalls des Gesamtsystems bei einer Attacke auf eine Systemkomponente vermindert (hohe Resilienz) und die Systemwartung ohne längere Ausfallzeiten ermöglicht. Die PTB hat dieses Prinzip bereits erfolgreich bei eingebetteten Systemen mithilfe

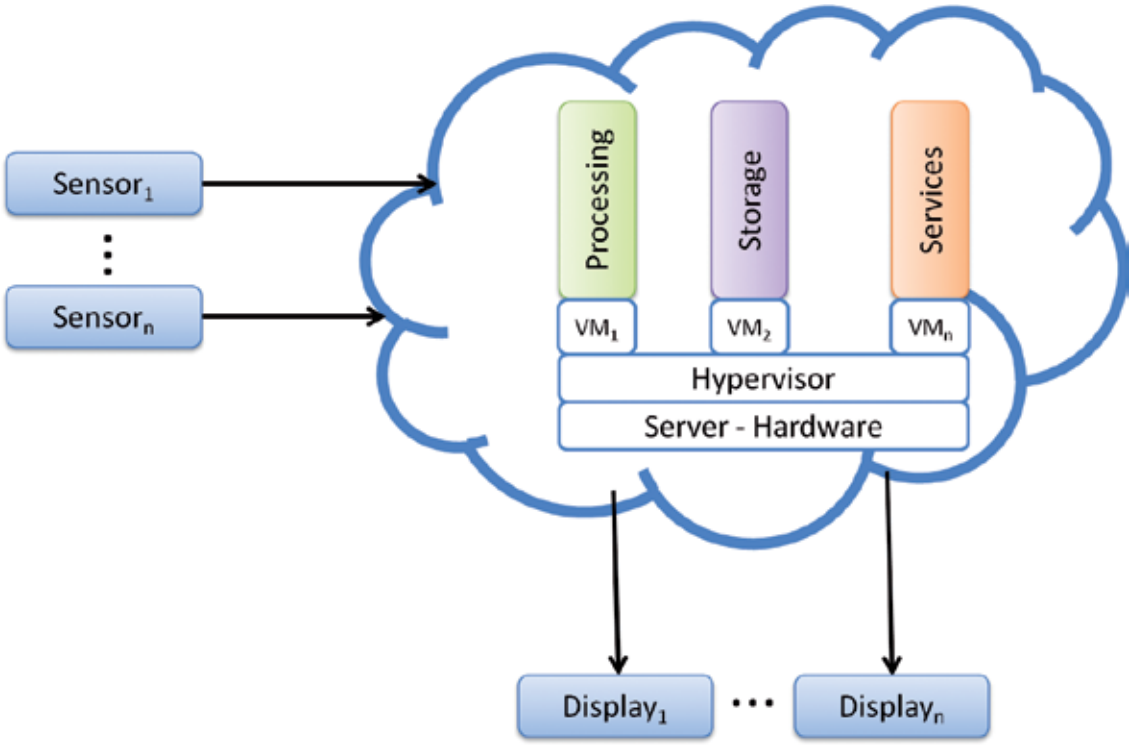

Bild 3: Cloud-Referenzarchitektur mit Software- und Prozessseparierung, sowie physikalischen Sensor(en) und Display(s)

eines Mikrokernels angewendet [5]. Der Nachweis, dass die wesentlichen Anforderungen in Bezug auf die Softwaresicherheit sichergestellt sind, wurde experimentell erbracht (vgl. [6],[7]).

Durch den Einsatz von Cloud-Computing-Technologien ist ein Paradigmenwechsel bzgl. der Überprüfung von Messgeräten absehbar. So könnte die Marktaufsichtsbehörde in Zukunft durch einen Fernwartungszugang Zutritt zum System erhalten und die Plattform, mit geeigneten Testdaten, von einer Zentrale aus prüfen. Darüber hinaus ist es denkbar, dass alle systeminternen Ereignisse und durchgeführten Systemänderungen (Events und Change-Logs) der Marktüberwachung mithilfe eines Push-Verfahrens zur Fernüberprüfung auf einfache Weise bereitgestellt werden.

Um Vertrauen und Akzeptanz in eine neue Technologie zu fördern, braucht es Mechanismen, die eine zuverlässige Prüfung der korrekten Funktionstüchtigkeit und die Integrität der eingesetzten Technologie bzw. Daten im Feld bestätigen. Referenzarchitekturen beinhalten daher immer eine Verifikationsmethode für die Überprüfung der Messgeräte in der Verwendung. Diese sollen, auch wenn auf komplexen Verfahren beruhend, einfach zu prüfende Ergebnisse liefern, damit eine zügige Bewertung der Konformität im Feld ohne Spezialkenntnisse möglich wird.

Solche Referenzarchitekturen vereinfachen den Konformitätsbewertungsprozess, die Verifikation im Feld für die Markt- und Verwendungsüberwachung und die Wartung solcher Messgeräte für den Hersteller.

In Bild 3 wird der Entwurf der sicheren Referenzarchitektur schematisch dargestellt. Es wird hier das Fernziel eines vollständig virtualisierten Messgerätes angestrebt. In der physikalischen Welt verbleiben lediglich die Sensoren zur Messwertaufnahme und die Anzeige. Alle verbleibenden Funktionen werden virtualisiert auf einer zentralen Plattform angeboten. Sogar die Anzeige könnte, wenn die rechtlich relevanten Informationen gesichert an einer geeigneten Schnittstelle bereitgestellt werden, als gesicherte Anzeige-Applikation in einem gängigen Web-Browser ausgeführt werden.

Die Sensoren stellen ihre Messwerte der Cloud-Architektur gesichert zur Verfügung. Die Messergebnisse werden in der Cloud berechnet und gespeichert. Dabei wird gefordert, dass der Sensor und die messwertverarbeitende Software in der Cloud ein „verkettetes Paar“ bilden. Als Vorbild dient hier die kryptografisch gesicherte Pairing-Lösung (*Secure Simple Pairing* – SSP) aus dem Bereich der Funktechnik, um bspw. eine *Man-in-the-Middle*-Attacke oder den autorisierten Ersatz baugleicher Sensoren abzuwehren.

Das Secure Simple Pairing sichert die Kommunikation zwischen Endgeräten ab. Es bietet verschiedene kryptografische und Authentifizierungsmechanismen an. Es wird eine Pin zwischen 6 und 16 Stellen ausgetauscht und bei erfolgreicher Authentifizierung gespeichert, um sich in Zukunft der Identität des Gegenübers zu versichern. Danach wird die Verbindung via *Elliptic Curve Diffie Hellmann* verschlüsselt.

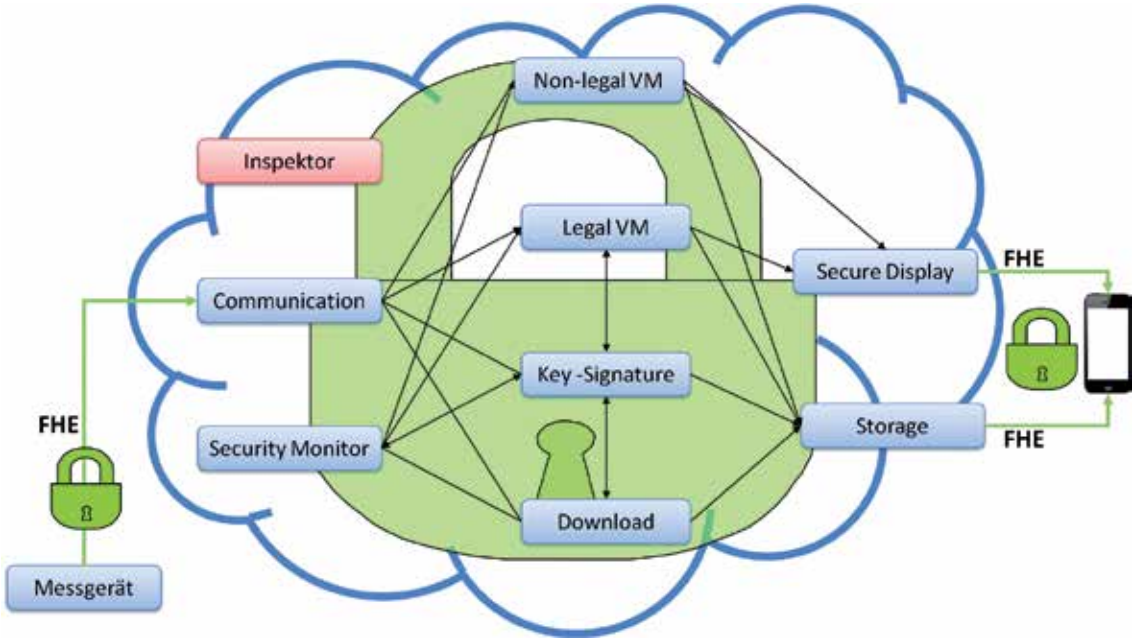

Bild 4: Referenzarchitektur in Detailansicht mit den verschiedenen geforderten Sicherheitseigenschaften des gesetzlichen Messwesens. Zusätzlich abgesichert via TLS (*Transport Layer Security*) und Homomorpher Verschlüsselung (FHE).

In der Cloud können der Hersteller oder der Verwender die Messdaten durch zusätzliche Dienste (*Services*) aufbereiten. Diese Dienste werden gemäß der Rechtsnorm als „zusätzliche Software" eingestuft (MID Annex I, 7.6), die nicht als gesetzlich relevant betrachtet wird, und deshalb den metrologischen Teil nicht beeinflussen darf. Diese Anforderung wird durch den grundlegenden Separierungsansatz mithilfe virtueller Maschinen (VM) unterstützt, sodass der metrologische Teil in einem gesondert abgetrennten Kompartiment läuft und von unerlaubter Einflussnahme abgeschirmt wird.

Eine Aktualisierung im rechtlich nicht relevanten Bereich führt daher nicht zum Erlöschen der Konformität. Der Hypervisor unterstützt diesen architektonischen Aufbau durch die Bereitstellung verschiedener Werkzeuge für eine kontrollierte Kommunikation zwischen den VMs.

Die Kommunikation zwischen den unterschiedlichen Kompartimenten wird durch einen *Watchdog*-Prozess (Inspektor) sichergestellt, der unerlaubte Zugriffe und Veränderungen unterbindet. Damit wird die Unveränderbarkeit, also Beständigkeit, der Messdaten sichergestellt. Die Messdaten werden in einer separaten VM bereitgestellt, die nur für die Speicherung der Messergebnisse zuständig ist. Der Zugriff auf diese Daten wird von anderen Prozessen nur lesend vorgenommen und dies wird vom Inspektor überwacht. In Bild 4 wird die Detailansicht der Referenzarchitektur bezüglich des Kommunikationsnetzwerkes zwischen den virtuellen Maschinen veranschaulicht.

5.1 Prozessierung metrologischer Daten in der Cloud

Beim Entwurf der Architektur werden neue Ansätze untersucht, um insbesondere Angriffe durch einen internen Angreifer (R8) oder eine manipulierte VM beim Cloud-Computing zu verhindern. Es wurde im Text schon auf die Unterschiede zwischen IT-Sicherheit und metrologischer Sicherheit hingewiesen. Dies wird besonders bei der Rolle des Administrators deutlich. Im gesetzlichen Messwesen ist die Rolle eines „gutmütigen" oder „wohlwollenden" Systemadministrators unbekannt. Wenn man dem Systemadministrator und Cloud-Service-Betreiber misstraut, laufen klassische Sicherheitskonzepte ins Leere, um die Authentizität, Integrität und Sicherheit der Daten sicherzustellen.

Möchte man die Daten vor dem Zugriff des Systemadministrators schützen, so liegt die Verwendung herkömmlicher Verschlüsselungsverfahren nahe. Ohne Entschlüsselung sind die Daten, allerdings auch für den Benutzer, weder einsehbar noch prozesszierbar. Daraus folgt zwangsweise, dass eine Cloud-Lösung, die auf zentralisierte Datenverarbeitung setzt, nicht mehr anwendbar ist. Aus dem Blickwinkel der Sicherheitsforschung führt dies zu den Herausforderungen, die Skalierbarkeit, Flexibilität und Kosteneffizienz der Cloud zu erhalten und dennoch die Integrität und Sicherheit der Daten zu gewährleisten. Zur Lösung dieses Dilemmas werden homomorphe Verschlüsselungsverfahren eingesetzt.

Im Jahr 1978 haben Rivest, Shamir und Adleman das asymmetrische Verschlüsselungsverfahren RSA vorgestellt [11] und später, in leicht veränderter Konstellation (Rivest, Adleman, Dertouzos), die Möglichkeit der homomorphen Verschlüsselung angedeutet [12]. Allerdings war RSA nur in der Lage, die homomorphen Eigenschaften für die Multiplikation zu erhalten. Um ein System vollständig homomorph

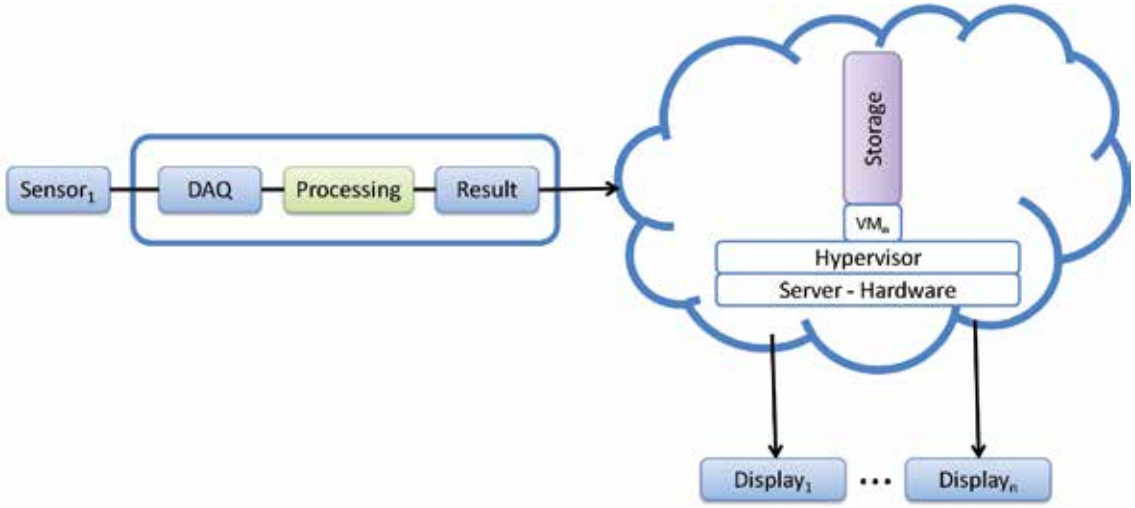

Bild 5: Herkömmliches Messgerät mit Anbindung an eine Cloud als Speicherlösung für Messergebnisse

zu nennen, müssen die Operationen der Addition und der Multiplikation vollständig erhalten bleiben. Im Jahr 2009 stellte Gentry ein vollständig homomorphes Verschlüsselungssystem (*Fully Homomorphic Encryption* (FHE)) vor [8, 13], dass beide Operationen erhält. Homomorphe Verschlüsselung erlaubt es Operationen, Addition und Multiplikation, direkt auf verschlüsselten Daten auszuführen, ohne die Daten vorher entschlüsseln zu müssen. Damit können die zuvor genannten Herausforderungen bewältigt werden.

In Bild 4 wird die Detailansicht des Kommunikationsnetzwerkes der virtuellen Maschinen der Referenzarchitektur unter Verwendung der vollständigen homomorphen Verschlüsselung (FHE) veranschaulicht. Das Messgerät generiert zuerst einen öffentlichen und einen privaten Schlüssel. Der öffentliche Schlüssel dient zum Verschlüsseln und der private zum Entschlüsseln. Nun wird der private Schlüssel dem Empfänger der Messergebnisse auf einem sicheren Weg mitgeteilt, sodass nur dieser in der Lage ist, die Daten zu sehen. Dieser Schlüsselaustausch ist auf der Abbildung nicht enthalten.

Danach werden die Messdaten vor dem Versenden via FHE verschlüsselt und an die Cloud geschickt. Dort werden die Daten vom *Communication Manager* in Empfang genommen und, nachdem der Inspektor die Daten überprüft hat, an die jeweilige Virtuelle Maschine weitergeleitet. In unserem Fall sind es Messdaten, die an die metrologische Instanz (*Legal VM*) weitergeschickt und dort z. B. zu abgeleiteten Messergebnissen prozessiert werden. Danach werden die Daten in dem Speicher (*Storage*) abgelegt. Die Daten können direkt dem sicheren Anzeige-Dienst (*Secure Display*) zur Verfügung gestellt werden, damit diese vom Endgerät direkt abgefragt werden können. Möchte der Nutzer ältere Messergebnisse nachprüfen, so muss er eine Anfrage an den Speicherdienst (Storage) stellen.

Das Besondere an der Architektur ist, dass alle Daten in der Cloud verschlüsselt sind. Somit kann weder ein interner Angreifer Zugriff auf den Klartext der Daten erhalten, noch können die Daten manipuliert werden, ohne dass dies erkannt wird. Sollte eine Virtuelle Maschine kompromittiert werden und versuchen, eine andere Virtuelle Maschine auszuspionieren, ist der Informationsgewinn aufgrund der Verschlüsselung irrelevant. Am Ende ist nur das rechtmäßige Endgerät, das den privaten Schlüssel erhalten hat, in der Lage, die Daten im Klartext zu lesen. Die PTB arbeitet an der Weiterführung des Ansatzes, damit nicht nur alle arithmetischen Funktionen, sondern auch komplexe Operationen auf verschlüsselten Daten möglich werden. So können dann einfache Programme in der Cloud ablaufen. Damit wird ein neuer Weg eröffnet, Teile der Messgerätesoftware gesichert in einer virtuellen Umgebung anzubieten.

5.2 Abgeleitete Beispielanwendungen

Die Referenzarchitektur stellt eine umfassende Virtualisierungslösung dar, die sich am höchsten Sicherheitsniveau im gesetzlichen Messwesen orientiert. Daraus lassen sich Architekturen für Anwendungen herauslösen, die nur Teilaspekte benötigen. Die Referenzarchitektur ist also skalierbar im Umfang und im anzustrebenden Sicherheitsniveau.

An dieser Stelle werden Lösungen vorgestellt, die bereits heute als gesetzeskonform eingestuft werden. So wird in Bild 5 eine Cloud-Lösung dargestellt, die als externe Speicherlösung fungiert. Dabei verbleibt der metrologische Kern im geeichten Messgerät und nur die (kryptografisch) gesicherten Messergebnisse werden in die Cloud verschoben. Von dort aus können diese von einem externen Display sicher abgerufen werden. Die Möglichkeit eines externen Displays ist heutzutage noch eine Herausforderung für das gesetzli-

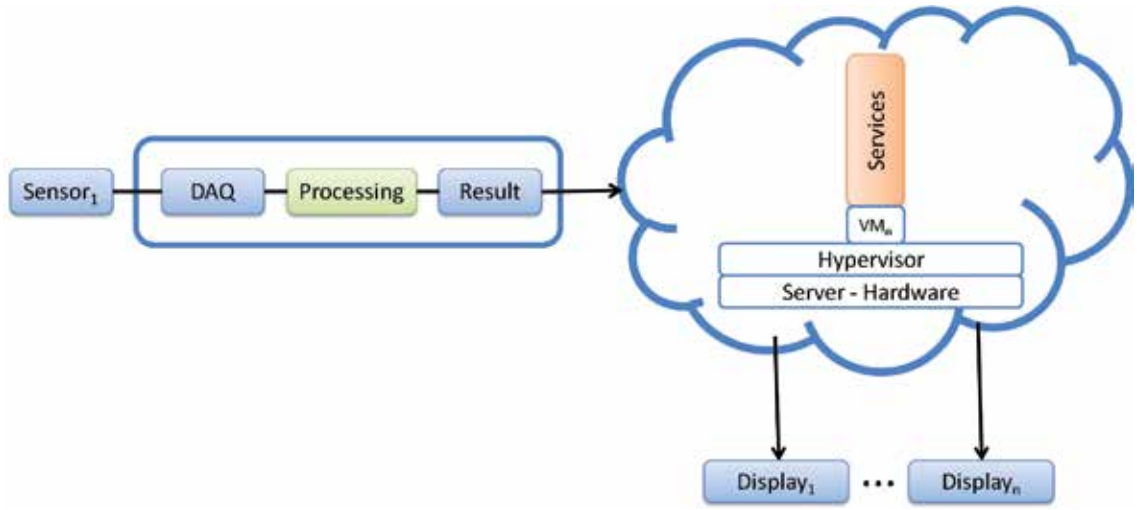

Bild 6:
Herkömmliches geeichtes Messgerät mit Anbindung an eine Cloud für rechtlich nicht relevante Applikationen/ Dienste.

che Messwesen, die aber aufgrund des erhöhten Marktdrucks durch die große Verbreitung vernetzter Endgeräte gelöst werden muss.

In Bild 6 wird ein Messgerät zugrunde gelegt, das seine Messergebnisse auch in die Cloud verschiebt. Die Messergebnisse verweilen jedoch zusätzlich dauerhaft im Speicher des Messgeräts (Messwertwiederholung). Die gesendeten Messergebnisse sind also kryptografisch gesicherte Kopien in der Cloud, die mit rechtlich relevanten Diensten des Herstellers oder Verwenders aufbereitet bzw. verknüpft werden, um einen Mehrwert zu schaffen.

Die Cloud kann als zentrale Instanz nicht nur Daten aufnehmen, sondern auch Daten an die angebundenen Geräte ausgeben. So können Updates, Zertifikate, Produktinformationen etc. an die Klienten ausgeliefert werden. Messgeräte zentral verwalten zu können, man spricht hier von *Managed Hardware*, bietet dem Hersteller u. a. die Möglichkeit, Wartungsdienste und -aufgaben für den Verwender zu übernehmen. Der Hersteller schafft so einen Mehrwert für den Kunden und kann Probleme und Sicherheitslücken schnell beheben. Das Konzept der Managed Hardware gibt dem Hersteller zusätzlich Rückmeldung, in welcher Umgebung die Messgeräte eingesetzt und verwendet werden. Diese Daten können zur Produktoptimierung eingesetzt werden.

Aus Kostengründen lagern Hersteller ihre interne Produktion an externe Subunternehmer aus. Damit geht die Gefahr der Produktpiraterie und billiger Konkurrenz einher, da diese nicht die hohen Investitionskosten für Forschung und Entwicklung der Innovation tragen müssen.

Bild 7 zeigt die Möglichkeit mittels einer Cloud-Lösung, trotz ausgelagerter Produktion der Messgeräte, das geistige Eigentum zu schützen. Ansatzpunkt des Verfahrens ist, dass sich das Messgerät erst im Augenblick der Verwendung beim Hersteller authentifiziert. Erkennt der Hersteller dieses Gerät als aus eigener Produktion stammend an, so gibt er notwendige Parameter oder Algorithmen frei und lässt diese herunterladen. Das Messgerät ist erst dann in der Lage, die notwendige Berechnung lokal auszuführen.

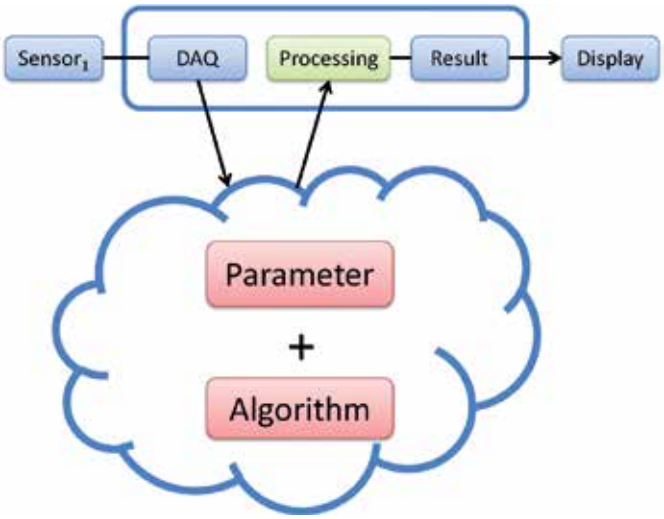

Bild 7:
Managed Hardware – Cloud als Lösung gegen Produktpiraterie. Das Messgerät authentifiziert sich bei der Cloud und bekommt die notwendigen Algorithmen zur lokalen Berechnung zur Verfügung gestellt.

6 Zusammenfassung

Cloud-Computing hat sich in den vergangenen Jahren zu einer ausgereiften Technologie entwickelt. Es erscheint nun möglich, die Anforderungen des gesetzlichen Messwesens zu erfüllen. Im Rahmen dieses Artikels wird ein sicherer und modularer Ansatz für Cloud-Infrastrukturen verfolgt, der mit der europäischen Messgeräterichtlinie (MID) im Einklang steht. Dabei werden die Sicherheitsanforderungen des gesetzlichen Messwesens berücksichtigt, ohne die Vorteile des Cloud-Computing einzuschränken. Die entworfene Cloud-Computing-Architektur wird entsprechende Verifikationsmethoden für die Markt- und Verwendungsüberwachung bereitstellen, die eine leichte Überprüfung der Konformität ermöglicht.

Der gesetzeskonforme, sichere und geschützte Datenverkehr ist dabei eine entscheidende Herausforderung, die durch den Einsatz von homomorpher Verschlüsselung entsprechend bewältigt werden soll. Dieses Verfahren verhindert zusätzlich die Hauptbedrohungen des Cloud-Computings, die von europäischen Sicherheitsbehörden (ENISA) identifiziert wurden.

Die PTB arbeitet an der Weiterführung des Ansatzes der homomorphen Verschlüsselung, damit nicht nur arithmetische Funktionen, sondern auch komplexe Operationen auf verschlüsselten Daten möglich werden.

Als nächster Schritt werden Leistungstests auf der Architektur vorgenommen, um die Effizienz der homomorphen Verschlüsselung und deren Effektivität gegen ausgewählte Angriffsvektoren zu spezifizieren. Abschließend wird das Gesamtsystem einer Risikoanalyse unterzogen, um eventuelle Schwachstellen identifizieren und angemessen schließen zu können. Ziel ist es, diese Referenzarchitektur im Rahmen des Technologietransfers kleinen und mittleren Unternehmen zur Verfügung zu stellen.

Referenzen

[1] F. Thiel, M. Esche, D. Peters und U. Grottker: *Cloud-Computing in Legal Metrology*, 17th International Congress of Metrology, EDP Sciences, 2015

[2] *Directive 2014/32/EU of the European Parliament and of the Council from 26 February 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of measuring instruments* (2014). Available for download from: http://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX:32014L0032 (Letzter Zugriff 15.12.2016)

[3] WELMEC Guide 7.2: Software Guide (Measuring Instruments Directive 2004/22/EC), available for download at: www.welmec.org.

[4] Organisation Internationale de Métrologie Légale (OIML), *General requirements for software controlled measuring instruments*, OIML D-31, 2008

[5] D. Peters, M. Peter, J.-P. Seifert und F. Thiel: *A Secure System Architecture for Measuring Instruments in Legal Metrology*, In MDPI Computers, 4(2), 61–86, 2015

[6] F. Thiel, U. Grottker und D. Richter: *The Challenge for legal metrology of Operating Systems Embedded in Measuring Instruments*, OIML BULLETIN, 52 (LII), 7–16, ISSN 0473–2812, 2011

[7] F. Thiel, U. Grottker, V. Hartmann und D. Richter: *IT Security standards and legal metrology – a Validation*, EPJ Web of Conferences, Vol. 77, 00001, 1–6, ISSN 2100-014X, 2014; DOI 10.1051/epjconf/20147700001

[8] C. Gentry: *A fully homomorphic encryption scheme*, Diss. Stanford University, 2009

[9] J. Rivera und R. Van der Meulen: *Gartner's 2015 Hype Cycle for Emerging Technologies Maps the Journey to Digital Business,* Retrieved March, 2015

[10] N. Leffler und F. Thiel: *Im Geschäftsverkehr das richtige Maß – Das neue Mess- und Eichgesetz, Schlaglichter der Wirtschaftspolitik*, Monatsbericht, Bundesministerium für Wirtschaft und Technologie (BMWi), 2013

[11] R. L. Rivest, A. Shamir und L. Adleman: *A method for obtaining digital signatures and public key cryptosystems*, Communications of the ACM, 21(2), 120–126, 1978

[12] R. L. Rivest, L. Adleman und M. L. Dertouzos: *On data banks and privacy homomorphisms*; Foundations of secure computation, 4(11),169–180, 1978

[13] C. Gentry et al.: *Fully homomorphic encryption using ideal lattices*, In STOC, volume 9, 169–178, 2009

[14] M.A.C. Dekker und D. Liveri: *Cloud Security Guide for SMEs – Cloud-Computing security risks and opportunities for SMEs*, In European Union Agency for Network and Information Security (ENISA), 2015; DOI 10.2824/508412

[15] L. Dupré und T. Haeberlen: *Cloud-Computing: benefits, risks and recommendations for information security*. In European Union Agency for Network and Information Security (ENISA), 2012

[16] *Cloud Computing Certification – CCSL and CCSM*. In European Union Agency for Network and Information Security (ENISA); https://resilience.enisa.europa.eu/cloud-computing-certification (Letzter Zugriff 3.6.2016)

[17] Communication from the commission to the European parliament, the Council, the European economic and social committee and the committee of the regions, European Commission – Brussels, 2012

[18] M. Esche und F. Thiel: *Software risk assessment for measuring instruments in legal metrology*, In Computer Science and Information Systems (FedCSIS), 2015 Federated Conference on, 1113–1123, IEEE

Risikoanalyse für Software im Rahmen der Modul-B-Konformitätsbewertung

Marko Esche*

1 Einleitung

Für Messgeräte, die dem Mess- und Eichgesetz (MessEG) [1] unterliegen und der Konformitätsbewertungsstelle (KBS) der PTB zur Konformitätsbewertung im Rahmen von Modul B vorgelegt werden, muss gemäß Anlage 1 § 10 der Mess- und Eichverordnung (MessEV) [2] vom Hersteller des Geräts eine „geeignete Risikoanalyse und -bewertung des Messgeräts im Hinblick auf die Einhaltung der wesentlichen Anforderungen" der MessEV erstellt werden. Diese Forderung folgt direkt aus der Umsetzung der europäischen Messgeräterichtlinie (MID) [3] in nationales Recht. Im europäischen Recht ergibt sich die Forderung nach einer Risikoanalyse hinsichtlich der Erfüllung der wesentlichen Anforderungen aus der Umsetzung der Entscheidung 768/2008/EC [4] des EU-Parlaments und der EU-Kommission durch die MID. Während die nationale Forderung nach einer Risikoanalyse bereits seit dem 1.1.2015 in Kraft ist, besitzt die europäische Vorgabe erst seit dem 16.4.2016 Gültigkeit.

Da in beiden Rechtsrahmen die zugrundeliegenden wesentlichen Anforderungen (siehe Anhang I der MID bzw. Anlage 2 zur MessEV) gleichlautend sind, hat der Fachbereich 8.5 „Metrologische Informationstechnik" im Jahr 2014 damit begonnen, ein Risikoanalyseverfahren speziell für die Software von Messgeräten im gesetzlichen Messwesen zu entwickeln. Dieses Verfahren, das ursprünglich in [5] publiziert und später durch [6] ergänzt wurde, soll dem Hersteller ein einheitliches Werkzeug bieten, um eine Risikoanalyse strukturiert durchführen zu können. Gleichzeitig kann dadurch der Aufwand seitens der PTB bei der Bewertung einer vorgelegten Risikoanalyse minimiert werden. Das Verfahren wird auf Wunsch der Hersteller seit Juli 2015 testweise in der PTB für national geregelte Messgeräte angewendet, ein entsprechendes Merkblatt ist als Handlungshilfe verfügbar. Eine Datenbank über bereits durchgeführte und bewertete Risikoanalysen befindet sich gerade im Aufbau.

In diesem Artikel soll zunächst ein Überblick über bestehende Verfahren zur Risikoanalyse gegeben werden. Darauf aufbauend wird dann die grundsätzliche methodische Vorgehensweise des in der PTB verwendeten Verfahrens dargestellt. Diese wird im Anschluss anhand eines Beispiels näher erläutert. Den Abschluss des Artikels bilden eine Zusammenfassung sowie ein Ausblick.

2 Überblick über alternative Verfahren

2.1 WELMEC Guide 5.3

Die *European Cooperation in Legal Metrology* (WELMEC) ist eine Kooperation verschiedener europäischer Konformitätsbewertungs- und Marktaufsichtsbehörden, die im Bereich des gesetzlichen Messwesens tätig sind. Die Arbeitsgruppe 5 der WELMEC *Market Surveillance* hat unter anderem einen Leitfaden zur Risikoanalyse (WELMEC Guide 5.3 *Risk Assessment Guide for Market Surveillance: Weigh and Measuring Instruments*) [7] veröffentlicht. Dieser beschäftigt sich mit der Risikoanalyse von Messgeräten aus Sicht der Marktaufsicht (siehe Verordnung 765/2008 [8] Artikel 19/20). Dabei liegt der Fokus allerdings weniger auf der Wahrscheinlichkeit einer Verletzung der wesentlichen Anforderungen durch ein Messgerät, als auf dem Risiko, das aus einem bereits im Markt befindlichen, nicht konformen Messgerät resultiert. Einen Schwerpunkt stellt weiterhin die Priorisierung von einzuleitenden Marktüberwachungsmaßnahmen dar. Um dies zu erreichen, werden verschiedene Bewertungskriterien, wie Zielgruppenverhalten und Rechtskenntnisse der Zielgruppe, herangezogen. Da der Leitfaden damit weniger die technischen Eigenschaften

* Dr. Marko Esche, Arbeitsgruppe 8.51 "Metrologische Software", E-Mail: marko.esche@ptb.de

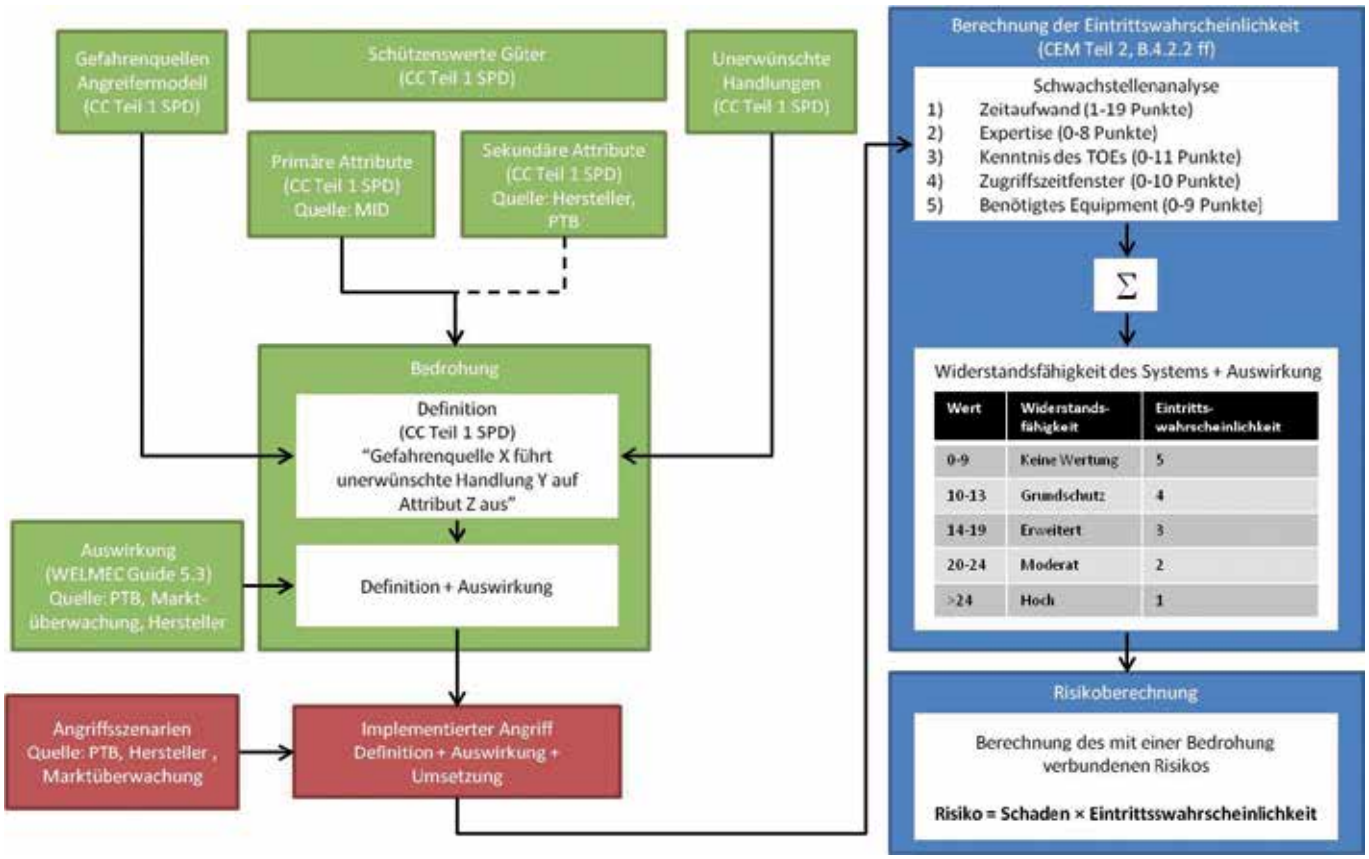

Bild 1: Visualisierung des vollständigen Risikoanalyseverfahrens bestehend aus der Ableitung schützenswerter Güter (grün), der Identifikation von Angriffsvektoren (rot) und der Berechnung der Eintrittswahrscheinlichkeit (blau)

eines Geräts betrachtet und zeitgleich versucht, das vollständige Gesamtgerät abzudecken, ist er nur unzureichend für die Modul-B-Konformitätsbewertung und Risikoanalyse von Software in einem Messgerät geeignet.

2.2 *ETSI TISPAN*

Ein weiteres Alternativverfahren zur Risikobewertung, das im Telekommunikationssektor Anwendung findet, wurde vom *European Telecommunications Standards Institute* (ETSI) veröffentlicht. Diese internationale Organisation hat sich zum Ziel gesetzt, Standards für die Telekommunikation auf europäischer Ebene zu etablieren. Der Standard ETSI TS 102 165-1 „*Telecommunications and Internet converged Services and Protocols for Advanced Networking*" beinhaltet im Teil 1 „*Method and proforma for Threat, Risk, Vulnerability Analysis*". Dieses Verfahren umfasst mehrere Schritte, in denen zunächst das zu untersuchende Objekt (*target of evaluation* (TOE)) definiert wird. Anschließend werden aus dieser Definition schützenswerte Güter abgeleitet, die unter Ausnutzung sogenannter Angriffsschnittstellen (*attack interfaces*) verändert oder manipuliert werden können. Die schützenswerten Güter sind dabei auf die Bereiche Equipment, menschliche Ressourcen und gespeicherte Information beschränkt. Zusätzlich ist die vorgegebene Liste an möglichen Angriffen sehr stark eingeschränkt, was allerdings auch die Intention des Standards ist. Beide Umstände führen dazu, dass der Standard zwar ein gutes Anwendungsbeispiel für eine Risikoanalyse liefert, aber nicht zur Risikobewertung von Software im Allgemeinen anwendbar ist. Im letzten Teil des Standards wird die Eintrittswahrscheinlichkeit einer realisierten Bedrohung mithilfe der AVA_VAN-Klasse der ISO/IEC 18045 [9] unter der Verwendung der technischen Spezifikationen bestimmt. Dieser Schritt wird im hier vorgestellten Verfahren (siehe Abschnitt 3) ebenfalls verwendet werden.

3 Methodenbeschreibung

Das hier beschriebene Verfahren nutzt als Basis die ISO/IEC 27005 [10], in der die Grundlagen der Risikoanalyse und -bewertung für Informationssicherheitsmanagementsysteme (ISMS) definiert werden. Den Kern der Risikoanalyse bildet dabei die Definition des Risikos als eine Kombination des Schadens, der aus einem unerwünschten Ereignis (Bedrohung) resultiert, und der Eintrittswahrscheinlichkeit der Bedrohung. Da die ISO/IEC 27005 auch explizit die Verwendung numerischer Größen zur Beschreibung von Schaden und Eintrittswahrscheinlichkeit erlaubt, kann auch die folgende Formel zur Darstellung des Risikos verwendet werden:

Die ISO/IEC 27005 definiert den Risikoanalysevorgang ferner als einen dreistufigen Prozess bestehend aus Risikoidentifikation, Risikoberechnung und Risikobewertung. Während der Iden-

Tabelle 1:
Auflistung der aus der Messgeräterichtlinie 2014/32/EU abgeleiteten schätzenswerten Güter

Softwarebezogene wesentliche Anforderung im Anhang I der MID bzw. in Anlage 2 zur MessEV	**Attribut (Objekt-ID)**	**Sicherheitseigenschaft**
7.6 Wenn ein Messgerät über zugehörige zusätzliche Software verfügt, die neben der Messfunktion weitere Funktionen erfüllt, muss die für die messtechnischen Merkmale entscheidende Software identifizierbar sein; sie darf durch die zugehörige zusätzliche Software nicht in unzulässiger Weise beeinflusst werden.	Identifikation der rechtlich relevanten Software (O9)	Verfügbarkeit, Integrität
	unzulässige Beeinflussung der rechtlich relevanten Software (O5) durch andere Software	Nichtverfügbarkeit[1]
8.1 Die messtechnischen Merkmale eines Messgeräts dürfen durch das Anschließen eines anderen Geräts, durch die Merkmale des angeschlossenen Geräts oder die Merkmale eines abgetrennten Geräts, das mit dem Messgerät in Kommunikationsverbindung steht, nicht in unzulässiger Weise beeinflusst werden.	unzulässige Beeinflussung der rechtlich relevanten Software (O5) über Kommunikationsschnittstellen	Nichtverfügbarkeit
8.3 Software, die für die messtechnischen Merkmale entscheidend ist, ist entsprechend zu kennzeichnen und zu sichern. Die Identifikation der Software muss auf einfache Weise vom Messgerät zur Verfügung gestellt werden. Eventuelle Eingriffe müssen über einen angemessenen Zeitraum nachweisbar sein.	Anzeige der Softwareidentifikation (O10)	Verfügbarkeit
	Nachweis eines Eingriffes (O2)	Verfügbarkeit, Integrität
8.2 Eine für die messtechnischen Merkmale entscheidende Baueinheit ist so auszulegen, dass sie gesichert werden kann. Die vorgesehenen Sicherungsmaßnahmen müssen den Nachweis eventueller Eingriffe ermöglichen. 8.4 Messdaten, Software, die für die messtechnischen Merkmale entscheidend ist, und messtechnisch wichtige Parameter, die gespeichert oder übertragen werden, sind angemessen gegen versehentliche oder vorsätzliche Verfälschung zu schützen.	Messergebnisse (O3)	Integrität, Authentizität
	rechtlich relevante Software, die für den Messzweck entscheidend ist (O1)	Integrität, Authentizität
	messtechnisch wichtige Parameter (O4)	Integrität, Authentizität
10.1 Die Anzeige des Ergebnisses erfolgt in Form einer Sichtanzeige oder eines Papierausdrucks.	Anzeige des Messergebnisses (O6)	Verfügbarkeit, Integrität
10.2 Die Anzeige des Ergebnisses muss klar und eindeutig sowie mit den nötigen Markierungen und Aufschriften versehen sein, um dem Benutzer die Bedeutung des Ergebnisses zu verdeutlichen. Unter normalen Einsatzbedingungen muss ein problemloses Ablesen des dargestellten Ergebnisses gewährleistet sein.	Klare und eindeutige Anzeige des Ergebnisses, Markierungen und Aufschriften (O7), die ein Messergebnis begleiten	Verfügbarkeit, Integrität
11.1 Ein Messgerät, das nicht der Messung von Versorgungsleistungen dient, muss das Messergebnis und die zur Bestimmung eines bestimmten Geschäftsvorgangs erforderlichen Angaben dauerhaft aufzeichnen, wenn a) die Messung nicht wiederholbar ist und b) das Messgerät normalerweise dazu bestimmt ist, in Abwesenheit einer der Parteien benutzt zu werden. 11.2 Darüber hinaus muss bei Abschluss der Messung auf Anfrage ein dauerhafter Nachweis des Messergebnisses und der zur Bestimmung eines bestimmten Geschäftsvorgangs erforderlichen Angaben zur Verfügung stehen.	dauerhaft gespeichertes Messergebnis und zusätzlich erforderliche Angaben (O8)	Verfügbarkeit

[1] Der Begriff „Nichtverfügbarkeit“ muss hier wie folgt verstanden werden:
„Es darf keine unzulässige Beeinflussung der rechtlich relevanten Software vorhanden sein.“

tifikationsphase müssen dabei zunächst die oben bereits angesprochenen schützenswerten Güter definiert werden. Hier können diese schützenswerten Güter direkt aus dem Gesetzestext abgeleitet werden (siehe nachfolgenden Abschnitt). Im Anschluss daran erfolgt die Berechnung des Risikos. Dazu werden anhand der technischen Beschreibung des Messgeräts eine Anzahl von Angriffsvektoren identifiziert, die verwendet werden können, um Eigenschaften der schützenswerten Güter zu manipulieren. Angriffsvektoren können dabei als explizite technische Schritte zur Umsetzung einer Bedrohung verstanden werden. Das hier beschriebene Verfahren ermöglicht es weiterhin, einer jeden durch einen Angriffsvektor realisierten Bedrohung einen numerischen Risikowert zuzuordnen. Indem dabei auf Module der ISO/IEC 18045 [9] zurückgegriffen wird, soll sichergestellt werden, dass die Ergebnisse objektiv und reproduzierbar sind. Abschließend wird während der Risikobewertung entschieden, welche Konsequenzen sich aus dem berechneten Risiko ergeben. Einen Überblick über das gesamte Verfahren bietet Bild 1.

3.1 Ableitung schützenswerter Güter

Grundlage einer jeden Risikoidentifikation ist eine Liste schützenswerter Güter. Diese ermöglicht es dann, auf ihnen basierende Bedrohungen in Form von Verletzungen sogenannter Sicherheitseigenschaften zu formulieren. Beispielhaft sei hier die wesentliche Anforderung 8.3 aus der MID genannt:

„*Software, die für die messtechnischen Merkmale entscheidend ist, ist entsprechend zu kennzeichnen und zu sichern. Die Identifikation der Software muss auf einfache Weise vom Messgerät zur Verfügung gestellt werden. Eventuelle Eingriffe müssen über einen angemessenen Zeitraum nachweisbar sein.*“ Aus der Formulierung lassen sich zumindest zwei Attribute ableiten. Zum einen ist dies die Anzeige der Softwareidentifikation, die stets wenigstens auf Befehl verfügbar sein muss. Hinzu kommt der Nachweis eines Eingriffs, der für einen bestimmten Zeitraum verfügbar sein muss und nicht gelöscht oder verändert werden können darf.

Tabelle 2:
Abbildung der berechneten Punktsumme auf das Eintrittswahrscheinlichkeitsmaß.

Punktsumme	Widerstandsfähigkeit des TOEs	Eintrittswahrscheinlichkeitsmaß
0–9	keine Wertung	5
10–13	Grundlegend	4
14–19	Erweitert	3
20–24	Moderat	2
>24	Hoch	1

3.2 Bestimmung der Eintrittswahrscheinlichkeit

Zur Abschätzung eines Maßes für die Eintrittswahrscheinlichkeit einer Bedrohung wird auf die Schwachstellenanalyse aus der sogenannten *Common Evaluation Methodology* ISO/IEC 18045 (CEM) [9] zurückgegriffen. Die CEM bildet zusammen mit den *Common Criteria* ISO/IEC 15408 (CC) einen Baukasten zum Beschreiben, Implementieren und Prüfen von Sicherheitsfunktionalitäten in IT-Produkten. Die Common Criteria existieren in ihrer jetzigen Form seit 1999 und sind weltweit etabliert.

Sobald ein Angriffsvektor zur Realisierung einer Bedrohung für das untersuchte Messgerät identifiziert worden ist, wird der Angriff bezüglich der folgenden fünf Bewertungskategorien untersucht:

1. Benötigte Zeit
2. Expertise
3. Detailkenntnis des Messgeräts
4. Zugriffszeitfenster
5. Equipment

In jeder der Kategorien wird eine Punktzahl zwischen 0 und maximal 19 vergeben. Für die benötigte Zeit bspw. bedeutet eine Punktzahl von 0, dass ein Angriff innerhalb eines einzigen Tages umgesetzt werden kann. Eine Punktzahl von 19 hingegen gibt an, dass ein Angriff länger als ein halbes Jahr dauert. Nachdem in jeder Kategorie eine Punktzahl vergeben worden ist, werden alle Werte aufaddiert und eine Punktsumme gebildet. Diese Punktsumme wird dann abschließend anhand der folgenden Tabelle in ein Maß für die Eintrittswahrscheinlichkeit überführt.

3.3 Korrektur der Eintrittswahrscheinlichkeit anhand eines Angreifermotivationsmaßes

Nach der initialen Bewertung der Eintrittswahrscheinlichkeit werden die Punktewerte in den einzelnen Bewertungskategorien gemäß der in [6] beschriebenen Methode angepasst. Dabei wird zunächst die geschätzte Motivation des Angreifers entsprechend Tabelle 2 in einen numerischen Wert umgewandelt.

Dieser Punktewert wird dann als Mindestwert für die Kategorien Expertise und Equipment verwendet: Sollte die entsprechende Punktewertung

niedriger als der Motivationswert sein, so wird sie durch den Motivationswert ersetzt. Dies reflektiert die Annahme, dass bei niedriger Motivation kein Interesse an der Aufwendung umfangreicher Ressourcen besteht. Gleichzeitig führt diese Anpassung der Punktewertungen zu einer niedrigeren Eintrittswahrscheinlichkeit im Falle einer geringen Angreifermotivation. Das ursprüngliche Bewertungsmaß entsprechend der Anleitung aus [9] übernimmt damit die Rolle einer Obergrenze an die Eintrittswahrscheinlichkeit, die nur im Falle eines überdurchschnittlich hoch motivierten Angreifers realisiert wird. Theoretisch kann durch die Berücksichtigung der Motivation das numerische Risiko von 5 auf bis zu 1 reduziert werden, wenn ein Angriff nur sehr begrenzte Ressourcen und Kenntnisse benötigt, damit leicht umsetzbar ist, gleichzeitig aber auch keine nennenswerte Angreifermotivation vorliegt. Die Einflussfaktoren zur Bestimmung der Angreifermotivation sind dabei individuell von der Messgeräteklasse und der Verwendung des Einzelgeräts abhängig.

3.4 Berechnung des Risikos

Gemäß der eingangs genannten Formel, kann das mit der Software eines Messgeräts verbundene Risiko hinsichtlich der Verletzung der wesentlichen Anforderungen durch einfache Multiplikation des vermuteten Schadenswertes mit der Eintrittswahrscheinlichkeit bestimmt werden. Da als Maß für die Eintrittswahrscheinlichkeit hier Werte zwischen 1 und 5 verwendet werden und die Schadenswerte stets kleiner gleich 1 sind, nimmt das Risiko ebenfalls Werte zwischen 1 und 5 an. Im Allgemeinen wird einem Messgerätehersteller schon ab einem berechneten Risiko mit Wert 3 oder größer eine Nachbesserung am Entwurf des Geräts bzw. an der Nutzerdokumentation empfohlen. Im folgenden Abschnitt soll das Gesamtverfahren noch einmal anhand eines ausführlichen Beispiels erläutert werden.

4 Beispiel

Betrachtet werde ein Beispielgerät auf Basis eines Universalcomputers (PC), das über einen eichpflichtigen Messwertspeicher verfügt. Dieser Speicher sei in Form einer Textdatei realisiert, auf die nur die rechtlich relevante Applikation sowohl lesend als auch schreibend zugreifen darf. Die Zugriffskontrolle werde mit Betriebssystemmitteln realisiert und sei über ein geheimes Administratorpasswort (hier: 4 Ziffern) gesichert. Ein möglicher Angriff auf die Verfügbarkeit der gespeicherten Messergebnisse (O8) besteht folglich darin, dass ein Angreifer durch Ausprobieren das richtige Passwort errät und dann die entsprechende Textdatei löscht. Das Messgerät sei für den Verwender uneingeschränkt verfügbar. In diesem Beispiel ist das schützenswerte Attribut ein gespeichertes Messergebnis (O8). Die dazugehörige Sicherheitseigenschaft ist Verfügbarkeit.

Motivation	**Punktwert**
keine Motivation	9
Niedrig	6
Moderat	3
Hoch	0

Tabelle 3: Punkteskala zur Berücksichtigung der Angreifermotivation

4.1 Bedrohung

Die in diesem Beispiel betrachtete Bedrohung lässt sich wie folgt formalisieren: „Der Verwender mit gewöhnlichen Nutzerrechten verletzt die Verfügbarkeit der gespeicherten Messergebnisse (O8).“

4.2 Angriffsszenario

Ein mögliches, zu der Bedrohung passendes Angriffsszenario ist das Erraten des Administratorpassworts. Formal lautet das Angriffsszenario dann: „Der Verwender errät das Administratorpasswort durch Ausprobieren beliebiger vierstelliger Zahlenkombinationen und löscht anschließend die Textdatei, die die gespeicherten Messergebnisse enthält.“

4.3 Bewertung

- **Benötigte Zeit:** Es gibt $10^4 = 10.000$ verschiedene mögliche vierziffrige Passwörter. Wenn angenommen wird, dass man zur Eingabe eines vierziffrigen Passworts inklusive Passwortüberprüfung durch das Gerät maximal 10 Sekunden benötigt, lassen sich alle 10.000 Kombinationen in 100.000 Sekunden = 27,78 Stunden = 1,15 Tage ausprobieren. Selbst wenn der Angreifer täglich nur 4 Stunden lang nach der richtigen Kombination sucht, benötigt er dafür maximal $1{,}15 \cdot 24/4 = 6{,}9$ Tage. Im statistischen Mittel wird die richtige Kombination schon nach der Hälfte der durchprobierten Passwörter, also nach 3,5 Tagen, gefunden werden. In jedem Fall dauert die Suche nicht länger als eine Woche. Die zu vergebende Punktzahl ist also 1.

Tabelle 4:
Beispielbewertung eines Angriffszenarios

Bedrohung	Angriffsszenario	Benötigte Zeit	Expertise	Detailkenntnisse des Messsystems	Erforderliches Zugriffszeitfenster	Equipment	Summe	Wahrscheinlichkeitsscore	Schaden	Risiko
Der Verwender mit gewöhnlichen Nutzerrechten verletzt die Verfügbarkeit der gespeicherten Messergebnisse (O8).	Der Verwender errät das Administratorpasswort durch Ausprobieren beliebiger vierstelliger Zahlenkombinationen und löscht anschließend die Textdatei.	1	0	3	0	0	4	5	1	5

- **Benötigte Expertise:** Zum Erraten einer Ziffernkombination und zum Löschen einer Datei sind keinerlei Spezialkenntnisse notwendig. Dementsprechend kommt ein Laie als potenzieller Angreifer in Frage und es werden 0 Punkte für Expertise vergeben.

- **Benötigte Detailkenntnisse des Messsystems:** Zunächst muss der Angreifer in Erfahrung bringen, wo auf dem System die Messwerte gespeichert werden und feststellen, dass sie nur unter Eingabe des Administratorpassworts verändert werden können. Bei den meisten Betriebssystemen genügt allerdings das Auffinden der Datei, da dann beim Öffnen der Datei automatisch das Administratorpasswort abgefragt werden würde. Es sind also allenfalls eingeschränkt verfügbare Detailkenntnisse notwendig. Die zu vergebende Punktzahl ist also 3.

- **Erforderliches Zugriffszeitfenster:** Da der Verwender bei diesem Gerät als Angreifer in Frage kommt, hat er unbegrenzt Zugriff auf das System und läuft dabei nicht Gefahr entdeckt zu werden. Entsprechend sind hierfür 0 Punkte zu vergeben.

- **Benötigtes Equipment:** Es wird kein Equipment benötigt (0 Punkte).

Da die beschriebene Bedrohung Konsequenzen für alle vorhergehenden Messungen haben kann und der Schaden somit 1 ist, ist hier nach der Multiplikation von Wahrscheinlichkeitsscore und Schaden das ermittelte Risiko identisch mit dem berechneten Wahrscheinlichkeitsscore.

4.4 Berücksichtigung der Angreifermotivation

Aufgrund des fiktiven Verwendungsszenarios des Messgeräts werde eine moderate Angreifermotivation (Punktwert 3 gemäß Tabelle 3) angenommen. Dementsprechend sind die Punktewerte in Tabelle 4 in den Kategorien Expertise und Equipment auf 3 zu erhöhen. Die veränderte Beispielbewertung ist nachfolgend angegeben.

4.5 Konsequenzen

Im Regelfall müssen alle Bedrohungen mit einem Risiko von 4 oder 5 durch technische oder organisatorische Maßnahmen abgemildert werden, bis nach einer neuerlichen Bewertung das Risiko im Bereich 1 bis 3 liegt. Im genannten Beispiel würde eine Anpassung der Passwortlänge auf 6 Zeichen (100-mal mehr Kombinationen als für 4 Zeichen) dafür sorgen, dass für die benötigte Zeit (3,5 Tage · 100 = 350 Tage) 19 Punkte vergeben werden müssten. Damit ließe sich die Bedrohung mittels Erratens der richtigen Passwortkombination nahezu ausschließen.

5 Zusammenfassung und Ausblick

In diesem Artikel wurde das an der PTB entwickelte Risikoanalyseverfahren für Software im gesetzlichen Messwesen detailliert beschrieben. Das Verfahren wird seit Januar 2015 für innerstaatlich geregelte Geräte testweise verwendet. Auch wenn der Hersteller eines solchen Messgeräts auch beliebige andere Vorgehensweisen nutzen kann, so bietet das Verfahren den großen Vorteil, dass es aufgrund der Verwendung etablierter Standards reproduzierbare, objektive und

Tabelle 5:
Beispielbewertung nach der Berücksichtigung der Angreifermotivation

Bedrohung	Angriffsszenario	Benötigte Zeit	Expertise	Detailkenntnisse des Messsystems	Erforderliches Zugriffszeitfenster	Equipment	Summe	Wahrscheinlichkeitsscore	Schaden	Risiko
Der Verwender mit gewöhnlichen Nutzerrechten verletzt die Verfügbarkeit der gespeicherten Messergebnisse (O8).	Der Verwender errät das Administratorpasswort durch Ausprobieren beliebiger vierstelliger Zahlenkombinationen und löscht anschließend die Textdatei.	1	3	3	0	3	10	4	1	4

vergleichbare Ergebnisse liefert. Darüber hinaus bietet sich das Verfahren dazu an, in einer objektiven Form die „Angemessenheit" von Sicherungsmaßnahmen zu identifizieren, wie es in der MID im Anhang I 8.4 gefordert wird. Derzeit wird das Verfahren zusammen mit verschiedenen europäischen Partnern im Rahmen eines Projekts der WELMEC-Arbeitsgruppe 7 weiter getestet sowie gegebenenfalls angepasst und verbessert. Im Zuge dessen sollen insbesondere Mechanismen untersucht werden, die eine Anpassung der Risikobewertung in Abhängigkeit von Daten der Marktüberwachung aus dem Feld ermöglichen. Denkbar ist dabei eine Verwendung von Informationen aus den nationalen (SAM) und EU-weiten Datenbanken (ICSMS) der Marktaufsichtsbehörden. Weiterhin ist der Hersteller gemäß §8 der MID Absatz 4 und 8 ohnehin verpflichtet, selbstständig Auffälligkeiten auf dem Markt zu beobachten, ggf. Korrekturmaßnahmen einzuleiten und die zuständigen Behörden zu informieren. Auch diese Daten könnten zukünftig nicht nur zur Validierung der Risikoanalyse, sondern ggf. auch zu ihrer Korrektur Verwendung finden.

Referenzen

[1] *Gesetz über das Inverkehrbringen und die Bereitstellung von Messgeräten auf dem Markt, ihre Verwendung und Eichung sowie über Fertigpackungen*, Bundesgesetzblatt, 25. Juli 2013

[2] *Verordnung über das Inverkehrbringen und die Bereitstellung von Messgeräten auf dem Markt, ihre Verwendung und Eichung sowie über Fertigpackungen*, Bundesgesetzblatt, Bd. 1, Nr. 58, 2014

[3] *Directive 2014/32/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of measuring instruments, Official Journal of the European Union, 26. Februar 2014*

[4] *Decision No 768/2008/EC of the European Parliament and of the Council of 9 July 2008 on a common framework for the marketing of products, and repeqling Council Decision 94/465/EEC*, Official Journal of the European Union, 9. Juli 2008

[5] M. Esche und F. Thiel: *Software Risk Assessment for Meausring Instruments in Legal Metrology*, Federated Conference on Computer Science and Information Systems (FedCSIS), 1113–1123, September 2015

[6] M. Esche und F. Thiel: *Incorporating a Measure for Attacker Motivation into Software Risk Assessment for Measuring Instruments in Legal Metrology*, 18. GMA/ITG-Fachtagung Sensoren und Messsysteme, 2016

[7] *WELMEC 5.3 Risk Assessment Guide for Market Surveillance: Weigh and Measuring Instruments*, European cooperation in legal metrology, WELMEC Secretariat, Mai 2011

[8] *Decision No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the reuqirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93*," Official Journal of the European Union, Juli 2008

[9] *ISO/IEC 18045:2008 Information technology – Security techniques – Methodology for IT security evaluation*, International Organisation for Standardization, August 2008

[10] *ISO/IEC 27005:2011(e) Information technology – Security techniques – Information security risk management*, International organization for Standardization, 2011

IT-Sicherheitsstandards für die Digitalisierung der Energiewende

Dennis Laupichler*

Einleitung

Angesichts knapper werdender Rohstoffe und der damit zunehmenden Bedeutung erneuerbarer Energien ist die Energieversorgung in Deutschland sowie in Europa insgesamt im Wandel. Ressourcen wie Sonne und Windkraft lassen sich nicht planen oder steuern wie Kohle- oder Kernkraftwerke. Darüber hinaus führt die zunehmende Zahl dezentraler Erzeuger, wie zum Beispiel Photovoltaik-Anlagen, zu schwer vorhersehbaren Schwankungen und erheblichen Herausforderungen für die Stabilität im Stromnetz. Da elektrische Energie nur begrenzt gespeichert werden kann, steht die Energieversorgung vor einem Paradigmenwechsel: War es bisher üblich, genau so viel Strom zu erzeugen wie verbraucht wurde, so soll zukünftig möglichst dann Energie konsumiert werden, wenn diese zur Verfügung steht.

Die Energiewende erfordert daher die Digitalisierung der Energieversorgung durch ein intelligentes Netz, das Energieerzeugungsanlagen, Speicher- und Verbrauchseinrichtungen und andere digitale Systemlösungen effizient verknüpft und ausbalanciert. Damit der Aufbau eines intelligenten Netzes gelingt, müssen eingebettete Systemkomponenten zu intelligenten Systemen verbunden und eine sichere, nachvollziehbare Erfassung und der Austausch von Informationen zur digitalen Verarbeitung für verschiedene Anwendungsfälle ermöglicht werden.

Datenschutz und Datensicherheit

Grundvoraussetzungen für den Aufbau eines intelligenten Stromnetzes der Zukunft sind zum einen die Schaffung einer standardisierten, sicheren und digitalen Infrastruktur und zum anderen verbindliche Regelungen zum Umgang mit Daten unter Berücksichtigung von Vorgaben zum Datenschutz und zur Datensicherheit.

Das Gesetz zur Digitalisierung der Energiewende [1] trägt diesen Kernanforderungen Rechnung und schafft deshalb entscheidende Voraussetzungen für den Aufbau einer intelligenten Infrastruktur für die Energiewende. Gegenstand des neuen Stammgesetzes über den Messstellenbetrieb und die Datenkommunikation in intelligenten Energienetzen (Messstellenbetriebsgesetz – MsbG) in Artikel 1 ist u. a. die Festlegung hoher technischer Standards in Form von Schutzprofilen (*Protection Profiles*, PP) und Technischen Richtlinien (TR) des Bundesamtes für Sicherheit in der Informationstechnik (BSI) [2] zur Gewährleistung von Datenschutz und Datensicherheit, welche die stufenweise Einführung und den Betrieb von nachweislich sicheren, intelligenten Systemkomponenten wie das Smart Meter Gateway für die Digitalisierung des Energienetzes regeln.

Sichere Kommunikationsplattform für das intelligente Netz

Intelligente Messsysteme sind wichtige Systemlösungen der modernen Mess-, Steuerungs- und Kommunikationsinfrastruktur des intelligenten Netzes. Auf der einen Seite sorgen intelligente Messsysteme für eine aktuelle Verbrauchstransparenz, auf der anderen Seite für eine sichere Übermittlung von Mess-, Steuerungs- und Netzführungsdaten sowie Energiemanagement- und Mehrwertdienst-Daten. Mit der zusätzlichen Fähigkeit, eine Plattform für die Steuerung von elektronischen Verbrauchsgeräten und Erzeugungsanlagen zu bieten, verbessern intelligente Messsysteme zukünftig das Last- und Erzeugungsmanagement im Verteilnetz, da auch diese Anwendungsfälle über die sichere und standardisierte Plattform abgewickelt werden können.

* Dennis Laupichler, Bundesamt für Sicherheit in der Informationstechnik (BSI), Referat D 11 – Cyber-Sicherheit in der Digitalisierung, E-Mail: dennis.laupichler@bsi.bund.de

Smart Meter Gateway: Dreh- und Angelpunkt des intelligenten Messsystems

Zentrale Komponente eines intelligenten Messsystems ist das Smart Meter Gateway als Kommunikationseinheit, welches die elektronischen Messeinrichtungen im Lokalen Metrologischen Netz (*Local Metrological Network*, LMN) mit den verschiedenen Systemen der Marktteilnehmer (u. a. Messstellenbetreiber, Verteilnetzbetreiber, Energielieferanten) im Weitverkehrsnetz (*Wide Area Network*, WAN) und den Aktor- und Steuerungseinheiten des lokalen Heimnetzes (*Home Area Network*, HAN) verbindet.

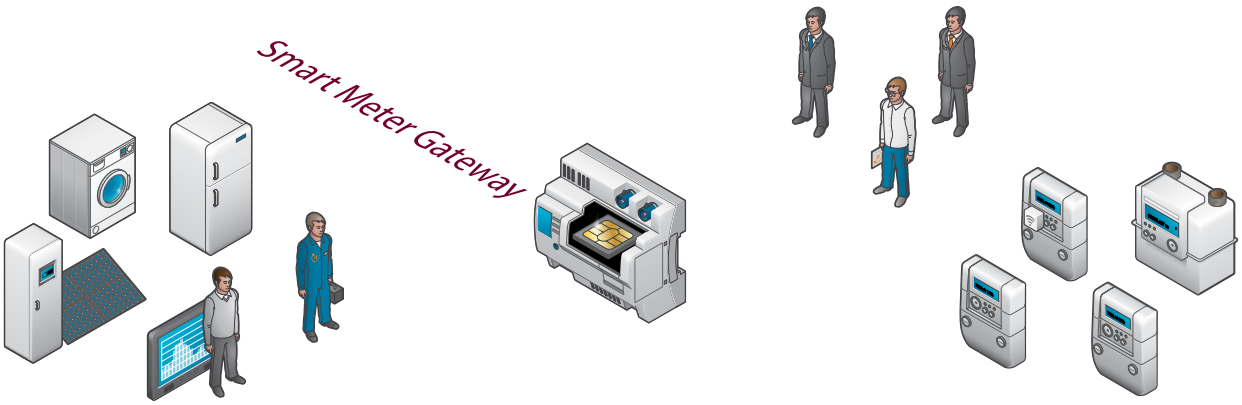

Bild 1: Smart Meter Gateway – Systemarchitektur

Das Smart Meter Gateway hat in diesem Gefüge dafür Sorge zu tragen, dass alle Kommunikationsverbindungen verschlüsselt werden und dass nur bekannten Teilnehmern und Geräten vertraut wird. Zusammen mit dem integriertem Sicherheitsmodul stellt das Smart Meter Gateway eine Basissystemarchitektur zur Etablierung eines intelligenten Netzes mit einheitlichem Sicherheitsniveau bereit. Da es beim Aufbau und der Nutzung eines intelligenten Netzes nicht zuletzt auch um die Verarbeitung personenbezogener Daten geht, sind die Sicherheit und der Schutz eben jener Daten eine zentrale Voraussetzung für Vertrauen und Akzeptanz der Bürgerinnen und Bürger in die neue Technik.

Bund und Wirtschaft erarbeiten Sicherheitsstandards gemeinsam

Durch die Digitalisierung und Vernetzung von zentralen und dezentralen Anlagen werden die Kommunikationsinfrastrukturen komplexer, die zu verarbeitenden Datenmengen vervielfachen sich. Dadurch vergrößert sich grundsätzlich die potenzielle Angriffsfläche. Im Auftrag des Bundesministeriums für Wirtschaft und Energie entwickelt das BSI daher bereits seit 2010 Anforderungen an vertrauenswürdige Produktkomponenten (Smart Meter Gateway mit integriertem Sicherheitsmodul), an die Informationssicherheit bei Administration und Betrieb sowie an die vertrauenswürdige Kommunikationsinfrastruktur (*Smart-Metering-Public-Key-Infrastruktur*).

Sicherheitsstandards können nur dann erfolgreich sein, wenn sie bereits in der Innovationsphase mitgestaltet werden (*Security & Privacy by Design*) sowie auf breite Akzeptanz bei Herstellern und Anwendern stoßen. Daher hat das BSI diese von Anfang an in die Erstellung und Weiterentwicklung der Schutzprofile und der Technischen Richtlinien eingebunden.

Eingebunden in die Entwicklung wurden verschiedene Verbände aus den Bereichen Telekommunikation, Informationstechnik, Energie, Wohnungswirtschaft und Verbraucherschutz sowie die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI), die Bundesnetzagentur (BNetzA) sowie die Physikalisch-Technische Bundesanstalt (PTB) und die Landeseichbehörden. Das BSI setzt die Datenschutzanforderungen der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) im Rahmen der BSI-Vorgaben um.

Die BSI-Vorgaben decken bereits einige eichrechtliche Aspekte der Physikalisch-Technischen Bundesanstalt (PTB) und der Landeseichbehörden ab. Alle eichrechtlichen Anforderungen werden in der PTB-Anforderung PTB A50.8 [3] zusammengefasst, wobei jeweils auf bereits durch die BSI-Zertifizierung erfüllte eichrechtliche Anforderungen verwiesen wird. Dadurch werden Prüf- und Zertifizierungsaufwände vereinfacht und Synergieeffekte für Anwender und Hersteller gehoben. Die bewährte Zusammenarbeit zwischen BSI und PTB bei der Erarbeitung von Schutzprofilen und Technischen Richtlinien wurde nun im Gesetz zur Digitalisierung der Energiewende [1] entsprechend regulativ

verstetigt, u. a. durch einen vom BMWi geleiteten Ausschuss zur Gateway-Standardisierung.

Einheitlicher und interoperabler Sicherheitsstandard

Die Schutzprofile und die Technischen Richtlinien des BSI als wesentlicher Bestandteil des Gesetzes zur Digitalisierung der Energiewende gewährleisten damit ein hohes Maß an Datenschutz und Datensicherheit und sorgen für einen einheitlichen und interoperablen Sicherheitsstandard im künftigen Energieversorgungssystem. Um Bedrohungen (z. B. Manipulation und Ausspähen von Daten, Manipulation von Firmware-Updates, unberechtigte Zugriffe auf Geräteeinstellungen oder auf die Infrastruktur des Betreibers) wirksam zu begegnen, definieren die organisatorischen und technischen Vorgaben des BSI eine Reihe von Sicherheitszielen, die von Smart Meter Gateways, den angeschlossenen Komponenten und deren Betreibern erfüllt werden müssen.

Beispiele für Sicherheitsanforderungen sind u. a.:

- Verschlüsselter und beidseitig authentifizierter Kommunikationskanal zwischen Sender und Empfänger
- Inhaltsdatenverschlüsselung, Integritätssicherung und Signierung
- Verwendung standardisierter Protokolle
- Funktionalität zur sicheren Software-/Firmware-Aktualisierung
- Verwendung von Zufallszahlengeneratoren mit hinreichender Entropie sowie kryptografisch sicher
- Überprüfung der korrekten Implementierung des Smart Meter Gateways (inkl. Prüfung des Sourcecodes)
- Öffentliche Schlüssel der Nutzer stammen in Form von Zertifikaten aus einer vertrauenswürdigen Public-Key-Infrastruktur (PKI)
- Anforderungen an den sicheren IT-Betrieb beim Administrator / regelmäßige Auditierung des Administrators und Zertifizierung gemäß IT-Grundschutz oder ISO/IEC 27001

Datenschutzkonzept des intelligenten Messsystems

Das im Smart-Meter-Gateway-Schutzprofil und in der Technischen Richtlinie TR-03109-1 beschriebene und im Gesetz verankerte Datenschutzkonzept des intelligenten Messsystems nach § 60 MsbG regelt, dass die Messwerterfassung, Verarbeitung (inklusive Plausibilisierung und Ersatzwertbildung) und Speicherung vor Ort im Gateway erfolgt (Datenhoheit). Dabei werden Messdaten anonymisiert, pseudonymisiert und aggregiert im Gateway aufbereitet (Datensparsamkeit) und sternförmig direkt an berechtigte Stellen verschlüsselt durch das Gateway versendet (Zweckbindung). Letztverbraucher wie z. B. Haushalts- und Gewerbekunden haben damit volle Transparenz über die im Smart Meter Gateway verarbeiteten Daten und können Kommunikations- und Verarbeitungsschritte nachvollziehen (im Logbuch). Durch die Dokumentation im Logbuch würde zudem jeder Datenmissbrauch erkennbar und nachweisbar, was die Durchsetzung von Verbraucherrechten erheblich erleichtert. Die gesicherte, korrekte Verarbeitung der Daten durch das Gateway wird durch die Prüfung und Zertifizierung des Gateways beim BSI nachgewiesen.

Bis zu einem Jahresverbrauch von 10.000 Kilowattstunden sieht das Gesetz nach § 60 MsbG standardmäßig nur eine Übermittlung von jährlichen Jahresarbeitswerten an Berechtigte vor. Der Durchschnittshaushalt in Deutschland verbraucht ca. 3.500 Kilowattstunden Strom im Jahr. Nur wenn der Letztverbraucher selbst einen Tarif oder einen Mehrwertdienst wählt, der eine häufigere Datenübermittlung erfordert, werden diese zweckgebunden auch an Netzbetreiber und Lieferanten oder weitere berechtigte Marktteilnehmer versendet.

Das BSI gewährleistet damit die technische Umsetzung der Datenschutzanforderungen des BfDI im Schutzprofil sowie in der Technischen Richtlinie und stellt nachweislich sicher, dass die Gesamtheit der detaillierten Verbrauchsdaten lediglich in der Obhut der Letztverbraucher ist, und nur aufbereitete Daten durch das Gateway, soweit dies erforderlich ist, verschlüsselt an berechtigte Dritte übermittelt werden.

Zertifizierung und Einbaupflicht des Smart Meter Gateways

Systemkomponenten wie das Smart Meter Gateway, die die Einhaltung der Vorgaben von Schutzprofilen und Technischen Richtlinien nachweislich belegen müssen, werden durch anerkannte Prüfstellen des BSI überprüft und durch abschließende Zertifikate des BSI belegt. Aktuell haben acht Smart-Meter-Gateway-Hersteller das Zertifizerungsverfahren begonnen und befinden sich mit ihren Produkten in der Evaluierungsphase.

Die Pflicht zum Einbau eines Smart Meter Gateways wird nach § 30 MsbG jeweils erst dann

aktuell, wenn für den konkreten Anwendungsfall die technische Möglichkeit des Einbaus und dessen sicheren Betriebs besteht. Erforderlich hierfür ist nach § 30 MsbG eine am Einsatzbereich des Smart Meter Gateways durchgeführte Prüfung des BSI. Erst wenn das BSI eine Freigabe erteilt hat, kann die technische Möglichkeit zum Einbau vorliegen und folglich die Einbauverpflichtung für den konkreten Anwendungsfall greifen. Systeme, die diese Anforderungen nicht erfüllen, sind nur übergangsweise und unter besonderen Umständen zulässig (vgl. § 19 Abs. 5 MsbG).

Das Konzept der am Einsatzbereich orientierten Weiterentwicklung von Schutzprofilen und Technischen Richtlinien des BSI stellt in § 30 MsbG sicher, dass für den Beginn des Rollouts von Smart Meter Gateways der Nachweis der geleisteten Sicherheitsfunktionalität für die verordneten Anwendungsbereiche im Vordergrund steht. Daher ist der Nachweis zur Erfüllung der sicherheitstechnischen Anforderungen im Rahmen des Zertifizierungsverfahrens nach Common Criteria (CC) durch das BSI entscheidend. Der Zeitpunkt der Nachweispflicht zur Interoperabilität wird durch das BSI noch festgelegt und in dem dafür vorgesehenen Verfahren bekannt gemacht werden. Hersteller von Smart Meter Gateways haben erst zu diesem Zeitpunkt das Zertifikat zur Konformität nach der Technischen Richtlinie dem Smart-Meter-Gateway-Administrator vorzulegen.

Zertifizierung des Smart-Meter-Gateway-Administrators

Neben den CC-zertifizierten Smart Meter Gateways müssen auch die Messstellenbetreiber (MSB) in der technischen Funktion des Administrators entsprechende Mindestanforderungen zur Durchsetzung der Informationssicherheit nachweisen.

Die entsprechenden Mindestanforderungen an die Informationssicherheit sind in § 25 MsbG verankert und legen verbindlich fest, dass der Administrator neben dem obligatorischen und der hierfür notwendigen Sicherheitskonzeption auch die in der TR-03109-6 beschriebenen Mindestanforderungen angemessen berücksichtigen muss.

Der Nachweis der Umsetzung der definierten Mindestanforderungen beim Smart-Meter-Gateway-Administrator kann nach § 25 MsbG entweder durch eine ISO-27001-Zertifizierung auf Basis von IT-Grundschutz (beim BSI) oder alternativ durch eine Zertifizierung gemäß ISO / IEC 27001 bei der Deutschen Akkreditierungsstelle (DakkS) erbracht werden.

Der MSB kann den technischen Adminbetrieb des intelligenten Messsystems teilweise oder ganz an einen Dritten outsourcen. Nicht alle der ca. 900 MSB werden die Smart-Meter-Gateway-Administration technisch selbst aufbauen und durchführen, sondern diese Dienstleistung über Outsourcing oder Kooperationen mit anderen Marktteilnehmern in Anspruch nehmen, um Skaleneffekte zu erzielen. Derzeit befinden sich bereits 11 Unternehmen beim BSI in Beratung. Nach Einschätzung des BSI werden ca. 20 technische Dienstleister in der Rolle des Administrators erwartet.

Vertrauenswürdige Smart-Metering-Public-Key-Infrastruktur (PKI)

Ebenso wird im Gesetz festgelegt, dass der Austausch von personenbezogenen Daten, Stammdaten und Netzzustandsdaten nur über die Smart-Metering-PKI-gestützte Kommunikation mit den berechtigten Teilnehmern erfolgen darf.

Um den Schutz der von den Haushalten übermittelten Messdaten zu gewährleisten, ist für die Verbindung des Smart Meter Gateways zu einem berechtigten Teilnehmer im Weitverkehrsnetz daher eine gegenseitige Authentisierung der Kommunikationspartner erforderlich. Die Kommunikation erfolgt dabei stets über einen verschlüsselten, integritätsgesicherten Kommunikationskanal. Zudem werden zu sendende Daten vom Smart Meter Gateway zusätzlich auf Inhaltsebene für den Endempfänger verschlüsselt und signiert. Für die gegenseitige Authentisierung der Teilnehmer und zur Etablierung eines verschlüsselten, integritätsgesicherten Kommunikationskanals, als auch für die Verschlüsselung und Signatur von Daten werden Zertifikate bereitgestellt.

Die vertrauenswürdige und sichere WAN-Kommunikation in der Smart-Metering-Infrastruktur basiert technisch auf einer Public-Key-Infrastruktur (PKI), der Smart-Metering-PKI (SM-PKI). Hierzu hat das BSI Vorgaben der TR-03109-4 an die Architektur der SM-PKI entwickelt, mit der die Authentizität der bei dieser Kommunikation eingesetzten öffentlichen Schlüssel der Kommunikationspartner auf WAN-Ebene sichergestellt wird. Das BSI ist nach § 28 MsbG für den Betrieb der *Smart Metering Root Certificate Authority* (SM-Root-CA) verantwortlich, welche die Wurzelinstanz (*Root*) der SM-PKI bildet. Der Betrieb der Root wird seit dem 1. März 2015 unter der Aufsicht des BSI von einem Zertifizierungsdiensteanbieter durchgeführt.

Für die sichere Kommunikation der Teilnehmer der Smart-Metering-Infrastruktur werden Zertifikate eingesetzt, welche von unterschiedlichen kommerziellen Anbietern unterhalb der im Auftrag des BSI betriebenen SM-Root-CA ausgestellt werden. Um die Entwicklung von Komponenten und Systemen zu unterstützen bzw. Funktionstests durchführen zu können, werden zusätzliche Public-Key-Infrastrukturen als Entwicklungs- und Testumgebungen durch das BSI bereitgestellt.

Die SM-Test-PKI dient hier insbesondere zur Entwicklung und Erprobung von Prototypen von Smart Meter Gateways und zugehöriger Infrastrukturkomponenten unter funktionalen Echtbedingungen. Dabei ist das Sicherheitsniveau der SM-Test-PKI niedriger als dass der SM-PKI, die für den produktiven Einsatz vorgesehen ist. Ein Übergang aus der SM-Test-PKI in die SM-PKI ist daher nicht möglich.

Hinsichtlich der SM-Test-PKI muss zwischen der PKI an sich und der vom BSI bereitgestellten SM-Test-BSI-Sub-CA unterschieden werden. Die SM-Test-PKI bildet die gesamte Testumgebung bzw. Testinfrastruktur, während die SM-Test-BSI-Sub-CA nur ein Test-System bzw. eine Test-Instanz in der Testumgebung darstellt.

Die zugehörige Zertifizierungsrichtlinie nach § 28 MsbG wird durch das BSI vorgegeben und regelt die Teilnahmebedingungen an der Smart-Metering-PKI für jeden berechtigten Teilnehmer des intelligenten Netzes. Das MsbG regelt somit alle Vorgaben für einen sicheren Datenaustausch zwischen autorisierten Teilnehmern und den intelligenten Systemkomponenten und setzt somit einen einheitlichen Sicherheitsstandard für die sichere Kommunikation zwischen den Systemen des intelligenten Netzes durch.

Um vollumfänglich die Anwendungsfälle des intelligenten Messsystems umsetzen zu können, müssen entsprechende Prozesse der Marktkommunikation durch die Bundesnetzagentur noch im Festlegungsverfahren angepasst und durch die Anwender auch umgesetzt werden.

Somit regelt der Rechtsrahmen nicht nur die Entwicklung von einheitlichen und hohen technischen Standards, sondern setzt auch eine hohe Vertrauenswürdigkeit für die jeweiligen Systemkomponenten und deren sicheren Betrieb in Form von Evaluierungs- und Auditnachweisen und der erfolgreichen Zertifizierung durch.

Weiterentwicklung der technischen Vorgaben

Das Gesetz zur Digitalisierung der Energiewende ermöglicht den kontinuierlichen stufenweisen Ausbau der intelligenten Messsysteme und anderer Komponenten um weitere Anwendungsfälle wie z. B. das netzdienlichen Einspeise- und Lastmanagement von Erzeugern und Verbrauchern sowie die Integration von weiteren Sparten (Wärme, Wasser). Überlappungen zu Zukunftsthemen wie Industrie 4.0 und der Ladesäuleninfrastruktur im Bereich der Elektromobilität sind bereits jetzt absehbar. Mit dem Inkrafttreten des Gesetzes wird das BSI eine Roadmap zur Weiterentwicklungsstrategie der technischen Vorgaben in Form von Schutzprofilen und Technischen Richtlinien für weitere Anwendungsfälle veröffentlichen. Hierzu gehören auch die Anwendungsfälle zur Steuerung der Erzeugungsanlagen über die Smart-Meter- Gateway-Infrastruktur.

Zur Weiterentwicklung der technischen Vorgaben wird weiterhin die intensive Mitarbeit von technischen Fachexperten aus allen betroffenen Interessengruppen benötigt, um eine innovative, sichere und eichrechtskonforme Systemarchitektur auf Basis der adressierten Anwendungsfälle weiterzuentwickeln.

Eingebunden in die Entwicklung der Standards wurden und werden weiterhin sämtliche betroffenen Verbände aus den Bereichen Telekommunikation, Informationstechnik, Energie, Wohnungswirtschaft und Verbraucherschutz sowie die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, die Bundesnetzagentur sowie die Physikalisch-Technische Bundesanstalt und die Landeseichbehörden.

Zusammenfassung

Intelligente Messsysteme sind wichtige Bausteine im intelligenten Netz und benötigen *Security & Privacy by Design* in dieser kritischen Infrastruktur. Das Smart Meter Gateway ermöglicht als sichere Kommunikationsplattform die digitale Sektorkopplung und wird zum Treiber für Innovationen der Digitalisierung.

Die Schutzprofile und die Technischen Richtlinien des BSI als wesentlicher Bestandteil des Gesetzes zur Digitalisierung der Energiewende gewährleisten ein hohes Maß an Datenschutz und Datensicherheit und sorgen für einen einheitlichen und interoperablen Sicherheitsstandard im künftigen Energieversorgungssystem.

Das Datenschutzkonzept des intelligenten Messsystems berücksichtigt eine zweckgebundene, eichrechtskonforme Datenverarbeitung und sternförmige Datenversendung des Gateways.

Dadurch wird sowohl eine Nachvollziehbarkeit als auch eine Transparenz für den Letztverbraucher gewährleistet und der Umgang der Daten im Sinne der Datensouveränität technisch auch durchgesetzt.

Für die Nachweise zur Einhaltung der Schutzprofile und der Technischen Richtlinien werden entsprechende Prüfungen bei anerkannten Prüfstellen mit abschließender Zertifizierung durch das BSI durchgeführt.

Das Gesetz zur Digitalisierung der Energiewende ermöglicht den ersten wichtigen Schritt zur digitalen Transformation der Infrastruktur zu einer innovativen, digitalen Infrastruktur des intelligenten Netzes. Mit dem Rechtsrahmen wird zusätzlich die Grundlage geschaffen, um eine stufenweise Fortentwicklung der Sicherheitsvorgaben des BSI sowohl für intelligente Messsysteme als auch für weitere wichtige Systemkomponenten des

intelligenten Energienetzes über eine Roadmap zur Digitalisierung umzusetzen.

In Zusammenhang mit den technischen Standards des BSI schafft das Gesetz die notwendige Rechtssicherheit und setzt das im Koalitionsvertrag verfolgte Ziel um, verbindliche Rahmenbedingungen für den sicheren und datenschutzkonformen Einsatz von intelligenten Messsystemen für vielfältigste Anwendungsfälle im intelligenten Netz zu regeln.

Referenzen

[1] *Gesetz zur Digitalisierung der Energiewende*, 2. September 2016

[2] *Übersicht über die Schutzprofile und Technischen Richtlinien des BSI nach § 22 Abs. 2 Satz 1 MsbG,* https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/SmartMeter/UebersichtSP-TR/uebersicht_node.html (Letzter Zugriff: 6.12.2016)

[3] PTB-A 50.8 „Smart Meter Gateway“, Physikalisch-Technische Bundesanstalt, Dezember 2014

Aktuelles aus der OIML

Bericht über die 15. Internationale Konferenz der OIML und die 51. Sitzung des CIML in Straßburg

Roman Schwartz*

Die 15. Konferenz der Internationalen Organisation für das gesetzliche Messwesen (OIML) und die 51. Sitzung des Internationalen Komitees für das gesetzliche Messwesen (CIML) fanden vom 17. bis 21. Oktober 2016 in Straßburg, Frankreich, statt. Insgesamt nahmen 174 Delegierte und Beobachter aus 51 Mitgliedstaaten, 16 korrespondierenden Mitgliedstaaten sowie mehreren internationalen Organisationen teil.

Die Internationale Konferenz findet im vierjährlichen Turnus statt; ihr obliegt die Entscheidung über Grundsatzfragen und das Budget der OIML.

Das CIML tagt jährlich, wählt den Präsidenten und die beiden Vizepräsidenten, genehmigt den Strategie-, Prioritäten- und Aktionsplan, überwacht die technischen Arbeiten und das Internationale Büro für das gesetzliche Messwesen (BIML).

Zur deutschen Delegation gehörten neben dem Autor die Herren Johann Fischer, Direktor des Landesamtes für Mess- und Eichwesen Berlin-Brandenburg und Vertreter der Bundesländer, sowie Dr. Peter Ulbig, Leiter der PTB-Abteilung „Wissenschaftlich-technische Querschnittsaufgaben“ und Vizepräsident von COOMET [1]. Darüber hinaus nahm Prof. Manfred Kochsiek als OIML-Ehrenmitglied und ehemaliger CIML-Präsident an den Sitzungen teil.

Die wichtigsten Entscheidungen und Entwicklungen werden nachfolgend vorgestellt.

Alle Resolutionen der 15. OIML-Konferenz und der 51. CIML-Sitzung finden sich unter [2].

1. OIML-Mitgliedstaaten

Die OIML hat zurzeit 62 Mitgliedstaaten. Kolumbien ist seit 2016 neues OIML-Mitglied; wieder beigetreten ist Sambia. Die Zahl der korrespondierenden Mitgliedstaaten hat sich durch den Beitritt von Angola auf 64 erhöht.

Aufgrund der in den letzten Jahren stetig gestiegenen Mitgliederzahlen bleiben die OIML-Mitgliedsbeiträge in den nächsten vier Jahren stabil, nachdem sie 2012 erstmals in der Geschichte der OIML sogar leicht abgesenkt werden konnten.

* Dir. u. Prof. Dr. Roman Schwartz, Vizepräsident der PTB, deutsches Mitglied im Internationalen Komitee für das Gesetzliche Messwesen (CIML) und CIML-Vizepräsident, E-Mail: roman.schwartz@ptb.de

Bild 1: Teilnehmer der 51. Sitzung des Internationalen Komitees für Gesetzliches Messwesen (CIML) in Straßburg, Frankreich

2. Zusammenarbeit mit anderen Organisationen

In seinem Bericht hob der OIML-Präsident, Peter Mason (UK), die guten Arbeitskontakte zum BIPM und den regelmäßigen Austausch zwischen den Direktoren beider Organisationen, Dr. Martin Milton (BIPM) und Stephen Patoray (BIML), hervor.

Gute Kontakte bestehen auch zu den internationalen Organisationen für Normung, ISO und IEC, für Akkreditierung, ILAC und IAF, zu den europäischen Herstellerverbänden für Waagen (CECIP) und Kraftstoffmess- und -verteilanlagen (CECOD) sowie zu den regionalen Organisationen für gesetzliches Messwesen (RLMO). Am „*RLMO-Roundtable*“ nahm neben Vertretern von AFRIMETS, APLMF, COOMET, SIM und WELMEC erstmals auch ein Vertreter von GULFMET (*Gulf Association for Metrology*) teil.

Eine Beratergruppe unter der Leitung des CIML-Präsidenten, Peter Mason, und des früheren AQSIQ-Vizeministers, Pu Changcheng (Volksrepublik China), wurde damit beauftragt, die Zusammenarbeit der OIML mit „*Countries and Economies with Emerging Metrology Systems* (CEEMS)” zu konkretisieren und bis zur nächsten CIML-Sitzung ein entsprechendes B-Dokument (*Basis Publication*) zu erarbeiten.

3. Revision der technischen Richtlinien der OIML

Wichtigste Arbeitsgrundlage für alle technischen Aktivitäten in den Technischen Komitees (TCs) und Subkomitees (SCs) der OIML ist das Dokument B 6 „*Directives for OIML technical work*“ mit den Teilen 1 „*Structures and procedures for the development of OIML publications*“ und 2 „*Guide to the drafting and presentation of OIML publications*“.

Dieses Dokument wurde 2011 in erheblich überarbeiteter Form verabschiedet und seitdem noch zweimal revidiert; die aktuelle Fassung von 2013 steht auf den OIML-Webseiten zur Verfügung [3].

Eine Projektgruppe arbeitet zurzeit an Vorschlägen für weitere Verbesserungen mit dem Ziel, den Entwicklungsprozess für neue und zu revidierende OIML-Publikationen weiter zu beschleunigen.

4. Neues OIML-Zertifizierungssystem

In früheren CIML-Sitzungen war beschlossen worden, die beiden parallel existierenden OIML-Zertifizierungssysteme, das *Basis-* und das *Mutual-Acceptance-Arrangement*(MAA)-Zertifizierungssystem, substanziell zu überarbeiten und zu einem einzigen Zertifizierungssystem zusammenzuführen. Eine CIML-Projektgruppe (*Certification System Project Group* = CSPG) war damit beauftragt worden, die notwendigen Dokumente und Prozeduren auf der Basis der OIML-Publikationen B 3:2011 [4] und B 10:2012 [5] zu erarbeiten. Die Arbeit war überschattet vom unerwarteten Tod des stellvertretenden BIML-Direktors Willem Kool, der von Anfang an maßgeblich beteiligt war. Dennoch konnte die Projektgruppe einen Entwurf für ein neues Rahmendokument vorlegen, das bei der 51. CIML-Sitzung als „*Basic Publication*“ B 18 *Framework for the OIML Certification System* (OIML-CS) fast einstimmig verabschiedet wurde [6].

Das neue OIML-CS sieht ein „*Management Committee*“ als zentrales Steuer-, Lenkungs- und Koordinierungsgremium unter dem Vorsitz des ersten CIML-Vizepräsidenten vor, sowie ein „*Advisory Panel*“ als Pool von technischen Experten, die für Begutachtungen von OIML-Prüflaboratorien und für fachliche Empfehlungen an das *Management Committee* zur Verfügung stehen, weiterhin ein „*Test Lab Forum*“ als Online-Plattform für den fachlichen Austausch der Personen in den Prüflaboratorien, die für die Prüfung von Messgeräten nach bestimmten OIML-Empfehlungen verantwortlich sind.

Die entsprechenden Management-Dokumente, sogenannte „*operational and procedural documents*“, sollen im Jahr 2017 von einem „*provisional Management Committee*“ (prMC) erarbeitet und verabschiedet werden, sodass das neue OIML-CS zum 1. Januar 2018 starten kann. Die erste Sitzung des prMC ist für den 14.–16. Februar 2017 im Institut Berlin der PTB geplant.

Die für das OIML-CS wichtigsten Messgerätekategorien sind nichtselbsttätige Waagen (R 76), Wägezellen (R 60), Wasserzähler (R 49), selbsttätige Kontrollwaagen (R 51), E-Zähler (R 46), Messgeräte für Flüssigkeiten außer Wasser (R 117) und Gaszähler (R 137). Um zukünftig OIML-CS-Zertifikate für diese Messgerätearten ausstellen zu können, müssen „*Issuing Authorities*“, wie die PTB, ihre Kompetenz auf der Basis der ISO/IEC 17025 im Rahmen einer Akkreditierung oder eines „*Peer Assessments*“ nachweisen.

Die bisherigen OIML-Basis- und MAA-Zertifikate sollen ihre Gültigkeit behalten; die am OIML-CS teilnehmenden Länder können jedoch ihre Akzeptanz hinsichtlich Messgeräteart und Zeitpunkt der Ausstellung von OIML-Zertifikaten einschränken.

5. OIML-Publikationen

Folgende OIML-Publikationen wurden verabschiedet:

- *New Recommendation* (R xxx): *Protein measuring instruments for cereal grains and oilseeds.*
- New Recommendation (R xxx): *Standard black body radiator for the temperature range from –50 °C to 2500 °C*
- Revidierte R 59 *Moisture meters for cereal grains and oilseeds.*
- Revidierte R 87 *Quantity of product in prepackages.*

Alle OIML-Publikationen stehen im Internet frei zur Verfügung [7].

6. Neue und laufende Projekte

Folgende neue Projekte wurden beschlossen:

- TC 5/SC 2 *Software*:
  Revision von D 31:2008 *General requirements for software controlled measuring instruments* (Vorsitz: PTB/Deutschland)
- TC 8/SC 1 *Static volume and mass measurement*
  Revision der R 125:1998 *Measuring systems for the mass of liquids in tanks*
  (Vorsitz: USA und Niederlande)
- TC 8/SC 7 *Gas metering*
  Revision der R 139:2014 *Compressed gaseous fuel measuring systems for vehicles*
  (Vorsitz: Niederlande)
- TC 9/SC 1 *Non-automatic weighing instruments*
  Revision der R 76:2006 *Non-automatic weighing instruments* (Vorsitz: PTB/Deutschland und Frankreich); die Projektgruppe wird insbesondere auch um Vorschläge gebeten, wie Fragen der Eichung und Inspektion zukünftig noch konkreter in der R 76 adressiert werden können
- TC 9/SC 2 *Automatic weighing instruments*
  Ausarbeitung einer neuen Empfehlung für *"Continuous totalizing automatic weighing instruments of the arched chute type"*
  (Vorsitz: UK)
- TC 12 *Instruments for measuring electrical quantities*
  Revision der R 46:2012 *Active electrical energy meters* (Vorsitz: Australien)
- TC 17/SC 2 *Saccharimetry*
  Ausarbeitung einer neuen Empfehlung für *"Near infrared instruments"*
  (Vorsitz: Russland)

Für die folgenden, laufenden Projekte wurde der Vorsitz dem BIML übertragen:

- TC 3/SC 5/p 5: Neue Publikation *Guide for the application of ISO/IEC 17065 to assessment of certification bodies in legal metrology,*
- TC 3/SC 5/p 12: Revision von D 30 *Guide for the application of ISO/IEC 17025 to the assessment of Testing Laboratories involved in legal metrology.*

Die Sekretariate von TCs und SCs sowie Vorsitzenden von Projektgruppen, die für OIML-Empfehlungen für Verbrauchsmessgeräte verantwortlich sind, werden gebeten, bei neuen Empfehlungen oder Revisionen von Empfehlungen für diese Messgeräte darauf zu achten, dass die Anforderung aufgenommen wird, dass solche Messgeräte die Fehlergrenzen nicht einseitig und systematisch zu Lasten einer Partei ausnutzen dürfen.

7. Personalien und Ehrungen

Dr. Roman Schwartz wurde als 1. Vizepräsident des CIML für eine weitere Amtszeit wiedergewählt.

Willem Kool, dem im Februar 2016 verstorbenen stellvertretenden BIML-Direktor, wurde posthum die OIML-Medaille für seine besonderen Verdienste um das internationale gesetzliche Messwesen verliehen.

Die OIML-Auszeichnung für „exzellente Beiträge von Entwicklungsländern zum gesetzlichen Messwesen" wurde dieses Jahr an das „*Institute of Trade and Standards Administration*" (Kenia) verliehen.

8. Termine

Die 52. CIML-Sitzung wird 2017 in Cartagena (Kolumbien) stattfinden, die 53. CIML-Sitzung im Oktober 2018 in Hamburg (Deutschland). Weitere OIML-Veranstaltungen und Termine finden sich unter [8].

Referenzen

[1] www.coomet.org (Letzter Zugriff am 6.12.2016)
[2] https://www.oiml.org/en/structure/conference/pdf/15-conf-resolutions-english.pdf und https://www.oiml.org/en/structure/ciml/pdf/51-ciml-resolutions-english.pdf (Letzter Zugriff am 6.12.2016)
[3] Teil 1: https://www.oiml.org/en/files/pdf_b/b006-1-e13.pdf , Teil 2: https://www.oiml.org/en/files/pdf_b/b006-2-e12.pdf (Letzter Zugriff am 6.12.2016)
[4] https://www.oiml.org/en/files/pdf_b/b003-e11.pdf (Letzter Zugriff am 6.12.2016)
[5] https://www.oiml.org/en/files/pdf_b/b010-amended-2012-e11.pdf (Letzter Zugriff am 6.12.2016)
[6] https://www.oiml.org/en/files/pdf_b/b018-e16.pdf (Letzter Zugriff am 6.12.2016)
[7] https://www.oiml.org/en/publications/introduction (Letzter Zugriff am 6.12.2016)
[8] https://www.oiml.org/en/events/calendar (Letzter Zugriff am 6.12.2016)