Physikalisch-Technische Bundesanstalt
Braunschweig und Berlin

Assessing Time Transfer Methods for Accuracy and Reliability

Navigating the Time Transfer Trade-off Triangle

K. Teichel, T. Lehtonen and A. Wallin

Acknowledgement: The presented work is used in the project 17IND06 (FutureGrid II), which has received funding from the EMPIR programme co-financed by the Participating States and from the European Union's Horizon 2020 research and innovation programme.

Full Citation of the original article published by IEEE:

K. Teichel, T. Lehtonen and A. Wallin, "Assessing Time Transfer Methods for Accuracy and Reliability: Navigating the Time Transfer Trade-off Triangle," 2021 Joint Conference of the European Frequency and Time Forum and IEEE International Frequency Control Symposium (EFTF/IFCS), 2021, pp. 1-4,
DOI: 10.1109/EFTF/IFCS52194.2021.9604300

This is an author-created, un-copyedited version of an article accepted for publication in 2021 Joint Conference of the European Frequency and Time Forum and IEEE International Frequency Control Symposium (EFTF/IFCS), 2021, **DOI**: 10.1109/EFTF/IFCS52194.2021.9604300. The presented work is used in the project 17IND06 (FutureGrid II) which have received funding from the EMPIR programme co-financed by the Participating States and from the European Union's Horizon 2020 research and innovation programme.
This author-created, un-copyedited version of the article is available for open access, DOI: 10.7795/820.20211123K

Assessing Time Transfer Methods for Accuracy and Reliability

Navigating the Time Transfer Trade-off Triangle

Kristof Teichel
4.4 Time and Frequency
PTB
Braunschweig, Germany
kristof.teichel@ptb.de

Tapio Lehtonen, Anders Wallin
BA1703 Electrical metrology
VTT
Espoo, Finland

***Abstract*—We present a collected overview on how to assess both the accuracy and reliability levels and relate them to the required effort, for different digital methods of synchronizing clocks. The presented process is intended for end users who require time synchronization but are not certain about how to judge at least one of the aspects. It can not only be used on existing technologies but should also be transferable to many future approaches. We further relate this approach to several examples. We discuss in detail the approach of medium-range White Rabbit connections over dedicated fibers, a method that occupies an extreme corner in the evaluation, where the effort is exceedingly high, but also yields excellent accuracy and significant reliability.**

Keywords—time transfer; technological assessment; security; accuracy; effort; pre-deployment evaluation

I. Introduction

The presented work is directly motivated by a current EMPIR project [1] regarding the change from analog to digital instrumentation in the European power grid. Improving and cataloguing the availability of security, accuracy, and convenience of time transfer techniques is a stated goal in this. The project is, in turn, a continuation of another project with a similar scope [2]. Future endeavors in this vein are already being prepared as well. Overall, there is a significant demand in the energy sector for clarity about what is technologically feasible and how the different technologies relate to one another. The topic is, however, not just applicable in energy grid contexts, but has come up in other areas as well. Specifically, these areas have been the financial market, in particular the EU guideline MiFID II [3], as well as the telecommunication area and data center applications. There have also been recent efforts [4] to classify, assess and improve different synchronization techniques, especially those that require satellite support.

The first result we present is an informed but simplified procedure for numerical score-based assessment of time transfer technologies for the three categories accuracy, reliability, and effort. The second result we present concerns example evaluations of medium-range and long-range White Rabbit links, which are very accurate (so much so that they are visibly sensitive to changes in outdoor temperature in proximity to the fibre connection) and quite reliable but require large effort, and NTP connections secured with NTS, which are low-effort and very reliable, but relatively inaccurate.

Parts of the presented work are used in the project 17IND06 (FutureGrid II) which has received funding from the EMPIR programme co-financed by the Participating States and from the European Union's Horizon 2020 research and innovation programme.

II. Methods/Results

We present our method of answering a questionnaire and then evaluating an assigned scoring system, as well as our findings about trade-offs and some example evaluations.

A. The Questionnaire

Our informed but simplified procedure for numerical score-based assessment of time transfer technologies for the three categories accuracy, reliability, and effort consists of a tabular questionnaire and scoring system.

The questionnaire is divided into three parts. The first part concerns the transportation method used in the time transfer

TABLE I. Transportation Method Questionnaire

Question	Option	AR	RR	ER	Example Technology
Which transportation method is used?	Public Internet	1-4	1	0	NTP
	Closed Network	3-7	2	1	PTP
	Wireless Radio	4-8	3	0	GPS
	Dedicated Fibre (local)	8-12	10	3	WR
	Dedicated fibre (long-range)	7-11	5	10	PTP, WR
… and what is the message flow model?	One-way	-	-2	0	GPS
	Two-way	-	0	0	NTP

This is an author-created, un-copyedited version of an article accepted for publication in 2021 Joint Conference of the European Frequency and Time Forum and IEEE International Frequency Control Symposium (EFTF/IFCS), 2021, **DOI**: 10.1109/EFTF/IFCS52194.2021.9604300. The presented work is used in the project 17IND06 (FutureGrid II) which have received funding from the EMPIR programme co-financed by the Participating States and from the European Union's Horizon 2020 research and innovation programme.
This author-created, un-copyedited version of the article is available for open access, DOI: 10.7795/820.20211123K

method. Tab. I contains this part, dealing with both the question of the transportation medium and the message flow model. The second part concerns cryptographic methods used to protect the time transfer data. Tab. II displays this questionnaire part, treating both the question if any cryptography is used and, as importantly, how it is transported. The third part concerns the question of dedicated hardware required and used by the time transfer method. It is shown in Tab. III below.

B. *The Scoring System*

In this questionnaire, accuracy is scored by our estimation of the attainable offset level, and reliability and effort are scored via arbitrarily chosen additive scores.

The scores for the three criteria are calculated separately and differently. For accuracy rating, the score is calculated by determining the minimum value for both worst case (left value) and best case (right value). The two values then represent the worst and best case of the overall approach, respectively. The scores represent (very roughly) the order of magnitude of the resulting accuracy when used as a negative exponent to the power of 10 (e.g., a final score of 3-6 means: worst case 10^3

seconds, so millisecond level, best case 10^6 seconds, so microsecond level); thus, higher scores are better. For reliability rating, the final score is calculated simply by addition of all relevant values in the questionnaire. Higher scores are better. For the effort/inconvenience rating, the final score is also calculated by addition of all values in the questionnaire. Higher scores mean more effort, so lower scores are more desirable.

C. *The Time Transfer Trade-off Triangle*

In our experience with the time transfer technologies existing to date, there is no single technology that will achieve

TABLE III. CRYPTOGRAPHIC PROTECTION QUESTIONNAIRE

Question	Option	AR	RR	ER	Example Technology
Is there any cryptographic protection involved?	No	-	0	0	NTP, PTP
	Yes, weak source authentication	-	4	0	PTP with group key
	Yes, strong source authentication	-	10	0	NTS, Galileo OSNMA
… and if YES, then how is it communicated?	Separate message from the time data	-	-1	1	Secure PTP
	Same message as time data, without extra design effort	1-3	0	0	Roughtime (see [7])
	Same message as time data, with deliberate design	2-6	0	0	NTS

TABLE II. DEDICATED HARDWARE QUESTIONNAIRE

Question	Option	AR	RR	ER	Example Technology
To what extent is dedicated hardware used?	None, other than common multi-purpose hardware (PCs)	1-6	0	0	NTP
	Dedicated hardware for all end devices	3-8	2	1	DTM
	Dedicated hardware as both end devices and middleware	-	4	3	PTP, WR

even near the best scores in all three categories at once. In other words, the search for an "optimal" technology always involves a trade-off. A given technology (of the ones available, this does not seem to be an inherent immutable problem) reliably is either not very accurate, or not very reliable, or not very convenient in the sense that it requires high effort.

This can be expressed in a triangular graph, which is why we dub this phenomenon the Time Transfer Trade-off Triangle. A sketch of this can be seen in Fig. 1, which also outlines the corner cases and gives examples for each of them:

- Both GNSS and radio methods offer good accuracy and convenience, but they are inherently not very reliable.
- An NTS-Secured NTP connection is both very convenient and very reliable, but not very accurate.
- Protocols such as PTP and White Rabbit give very accurate time transfer with at least decent reliability (which can be improved with cryptography), but what they do not offer is good convenience.

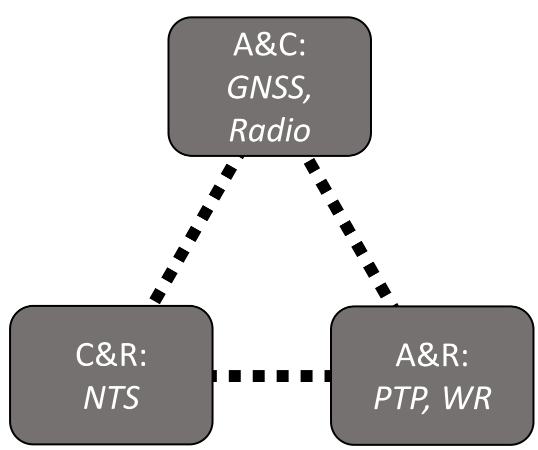


Fig. 1. The Time Transfer Trade-off Triangle, where A signifies "accurate", C signifies "convenient", and R signifies "reliable".

This is an author-created, un-copyedited version of an article accepted for publication in 2021 Joint Conference of the European Frequency and Time Forum and IEEE International Frequency Control Symposium (EFTF/IFCS), 2021, **DOI**: 10.1109/EFTF/IFCS52194.2021.9604300. The presented work is used in the project 17IND06 (FutureGrid II) which have received funding from the EMPIR programme co-financed by the Participating States and from the European Union's Horizon 2020 research and innovation programme.
This author-created, un-copyedited version of the article is available for open access, DOI: 10.7795/820.20211123K

D. *Exemplaric Evaluation*

One interesting corner case that presents itself is that of long-range White Rabbit connections. These offer great accuracy (often in the single nanosecond range), and very solid reliability, since the whole transportation network (both active electrical devices and fibre) are necessarily closely controlled. The effort of organizing a dedicated fibre connection plus the necessary White Rabbit hardware, however, is enormous. The evaluation of this corner case according to our assessment method as presented above can be seen in Tab. IV, with final scores of 7-11 for accuracy, 15 for reliability, but 13 for effort.

Another potentially interesting corner case is that of a simple NTP connection [8] secured measures according to the relatively new Network Time Security specification [5]. This offers about the highest reliability we could currently envision, and the effort is no more than having some kind of computer with an internet connection. The offered guaranteed accuracy is only in the millisecond range, however. This is visible in Tab. V, where this corner case is evaluated according to our approach.

TABLE IV. RESULTS FOR LONG-RANGE WHITE RABBIT

	Accuracy	**Reliability**	**Effort**
Dedicated fibre (long-range)	7-11	5	10
Two-way	-	0	0
No cryptography	-	0	0
Dedicated hardware both end and middle	0	10	3
Final Score	7-11	15	13

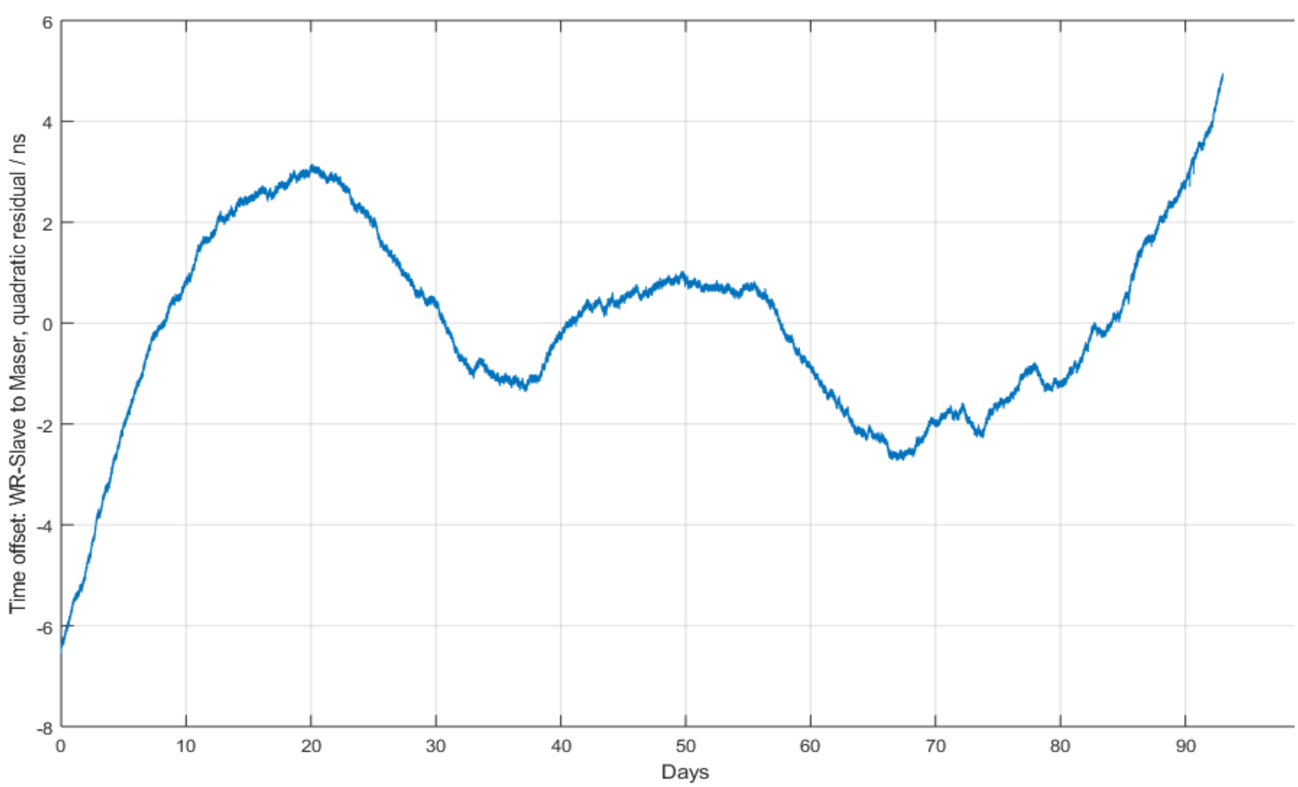
III. DISCUSSION/INTERPRETATION

We have designed this evaluation method with the philosophy in mind that a reduction to small numeric values has been found to be the most useful in decision making processes [6]. We aimed to make it just granular enough so that it abstracts away as much information as possible while still remaining useful.

We have found that, somewhat regrettably, the three aspects of accuracy, reliability and (in)convenience must be evaluated separately, as merging them into a single aggregate score loses information that is essential in many cases. This is due to the fact that there are often very strict and separate constraints on the parameters.

The kind of long-range White Rabbit connection presented as an example above has become ever more relevant over the

Fig. 2. Time offset between a slave WR-switch and a remote hydrogen maser.



This is an author-created, un-copyedited version of an article accepted for publication in 2021 Joint Conference of the European Frequency and Time Forum and IEEE International Frequency Control Symposium (EFTF/IFCS), 2021, **DOI**: 10.1109/EFTF/IFCS52194.2021.9604300. The presented work is used in the project 17IND06 (FutureGrid II) which have received funding from the EMPIR programme co-financed by the Participating States and from the European Union's Horizon 2020 research and innovation programme.
This author-created, un-copyedited version of the article is available for open access, DOI: 10.7795/820.20211123K

TABLE V. RESULTS FOR NTS-SECURED NTP

	Accuracy	Reliability	Effort
Public Internet	1-4	1	0
Two-way	-	0	0
Strong source authentication	-	10	0
Same message as time data, with deliberate design	2-6	0	0
No dedicated hardware, other than common multi-purpose hardware (PCs)	1-6	0	0
Final Score	2-4	11	0

last years, and between White Rabbit and PTP, this trend seems to continue. Long-range White Rabbit connections are in operation between Scandinavian NMIs (data from one such link can be seen in Fig. 2). They are also evolving in numerous countries from NMIs to end users such as financial institutions, who now often must implement new and strict requirements from regulatory documents such as the MiFID II directive [3]. This lends extra relevancy to this example case. Our presented evaluation might also help to highlight that this technological approach is helpful in cases where accuracy and reliability requirements simply outweigh the need for convenience to a large degree.

The other presented corner case of NTS-secured NTP will likely become ever more prevalent over the coming years, simply because it is very convenient, which is in our opinion the most likely facilitator of widespread adoption. As described, it is also highly reliable, and even its relatively low accuracy is still much better then one-second level, which makes it relevant for lots of use cases.

IV. CONCLUSIONS

We have presented a reasonably concise way to navigate the Time Transfer Trade-off Triangle before the deployment of any technology. We have also shown two corner-cases in it that future users might find useful.

The next steps in refining our approach could consist of documenting a common metrological consensus on the accuracy score (which currently represents our own prognosis) and researching a more concrete quantifying approach for reliability and effort scores. It is hard to quantify reliability, though, and even though it might be tempting to measure effort in monetary values or units such as person months, we feel that prognoses in this area carry a greater inherent risk of error, and thereby of misleading users into decisions that later may turn out to be wrong.

We believe that the coming years will bring increased need for users from all kinds of fields to select dedicated time transfer technologies for their applications, and that there will be no one-size-fits-all solution that is in some way ideal for everyone. We hope that our work can help clarify for individual entities how they should approach the search for their own personal best solution and navigate the Time Transfer Trade-off Triangle without fear of getting lost.

V. REFERENCES

[1] 1 “Metrology for the next-generation digital substation instrumentation”, Short Name: FutureGrid II, Project Number: 17IND06. https://projectsites.vtt.fi/sites/FutureGrid2/

[2] “Non-conventional voltage and current sensors for future power grids”, Short Name: FutureGrid, Project Number: ENG61. http://futuregrid.emrp.eu/

[3] “DIRECTIVE 2014/65/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU”, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014L0065&from=EN

[4] M. Weiss, P. Diamond and D.A. Goward, “A Resilient National Timing Architecture Securing Today’s Systems, Enabling Tomorrow’s,” Proceedings of the 52nd Annual Precise Time and Time Interval Systems and Applications Meeting, p. 411-436, January 2021. https://doi.org/10.33012/2021.17795.

[5] D. Franke, D. Sibold, K. Teichel, M. Dansarie and R. Sundblad, “Network Time Security for the Network Time Protocol”, RFC 8915, DOI 10.17487/RFC8915, September 2020, https://www.rfc-editor.org/info/rfc8915.

[6] D. Kahneman, (2011). Thinking, fast and slow. Farrar, Straus and Giroux.

[7] A. Malhotra, A. Langley, W. Ladd, M. Dansarie, “Roughtime”, Internet Draft. https://datatracker.ietf.org/doc/html/draft-ietf-ntp-roughtime

[8] Mills, D., Martin, J., Ed., Burbank, J., and W. Kasch, “Network Time Protocol Version 4: Protocol and Algorithms Specification”, RFC 5905, DOI 10.17487/RFC5905, June 2010, https://www.rfc-editor.org/info/rfc5905.

This is an author-created, un-copyedited version of an article accepted for publication in 2021 Joint Conference of the European Frequency and Time Forum and IEEE International Frequency Control Symposium (EFTF/IFCS), 2021, **DOI**: 10.1109/EFTF/IFCS52194.2021.9604300. The presented work is used in the project 17IND06 (FutureGrid II) which have received funding from the EMPIR programme co-financed by the Participating States and from the European Union’s Horizon 2020 research and innovation programme.
This author-created, un-copyedited version of the article is available for open access, DOI: 10.7795/820.20211123K