TOWARDS METRICS FOR ASSURED TIME: A REPORT

Stefania Römisch, Bijunath Patla

NIST – Time and Frequency Division
Boulder, CO - USA

WSTS 2019 – San Jose, CA - USA

THE NEED

Reliable time has become an essential part of our critical infrastructure and thereby also effectively becoming one of its vulnerabilities.

The needs of different sectors of society are very expansive, spanning several orders of magnitude in terms of accuracy and quite diverse in terms of assuredness.

OVERARCHING GOAL

Ensure that civilian users are provided with ASSURED and ACCURATE TIME

Industry stakeholders
(timing equipment manufacturers, timing providers)

Provide products capable of satisfying diverse requirements for assuredness of time.

USERS
(energy, telecom, finance)

Identify commercial products providing the required level of assuredness of time

Assess time dependences and required level of assuredness of time for their systems.

Ensure minimal vulnerabilities in the US critical infrastructure

Government stakeholders

A CONFORMANCE FRAMEWORK

A Conformance Framework allows manufacturers to effectively compare the characteristics of their products among themselves and with respect to the needs of their customers, the users of time.

The users of time are now enabled to effectively compare the capabilities of the different products on the market without knowing the inner workings of the equipment they are acquiring.

OVERARCHING GOAL

Ensure that civilian users are provided with ASSURED and ACCURATE TIME

Industry stakeholders

(timing equipment manufacturers, timing providers)

Provide products capable of satisfying diverse requirements for assuredness of time.

CONFORMANCE FRAMEWORK

USERS

(energy, telecom, finance)

Identify commercial products providing the required level of assuredness of time

Assess time dependences and required level of assuredness of time for their systems.

Education campaign not addressed by Conformance Framework

Ensure minimal vulnerabilities in the US critical infrastructure

Government stakeholders

TERMINOLOGY

TIME

- time-of-day, including time and date information (local time and date, MJD, etc.)
- referenced to UTC realized by either UTC(NIST) or UTC(USNO) in the US.
- UTC, TAI and local time are considered equivalent (UTC-TAI = accumulated leap seconds, UTC-local time = integer number of hours depending on the time zones)
- Time-of-day is different from synchronization, which often simply refers to the capability of knowing (measuring) the time difference between two events or two locations.

ACCURACY:

How well do I know what time it is?

Accuracy is the uncertainty with which a quantity is known, with respect to a known standard.

ASSUREDNESS:

The state or quality of being assured.

Assured: characterized by certainty or security.

Merriam-Webster

RESILIENT:

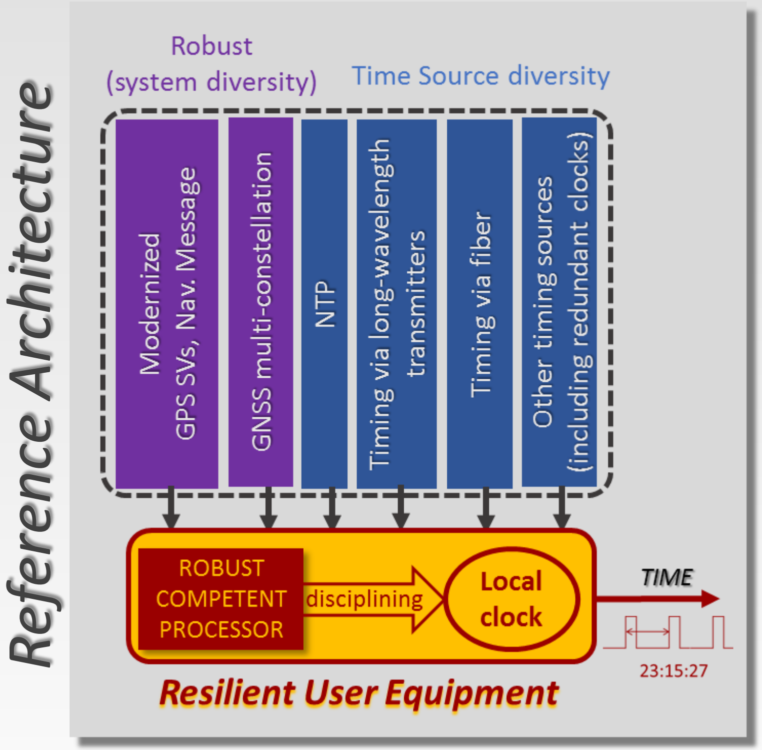
a. capable of withstanding shock without permanent deformation

b. tending to recover from or adjust easily to misfortune or change

RESILIENT systems provide **ASSURED** time

A PARADIGM SOLUTION

Because using a single delivery mechanism for time creates a timing infrastructure with a single point of failure, we identified a ***reference architecture*** where the ***user equipment*** uses multiple time sources and a ***Robust and Competent Processor***



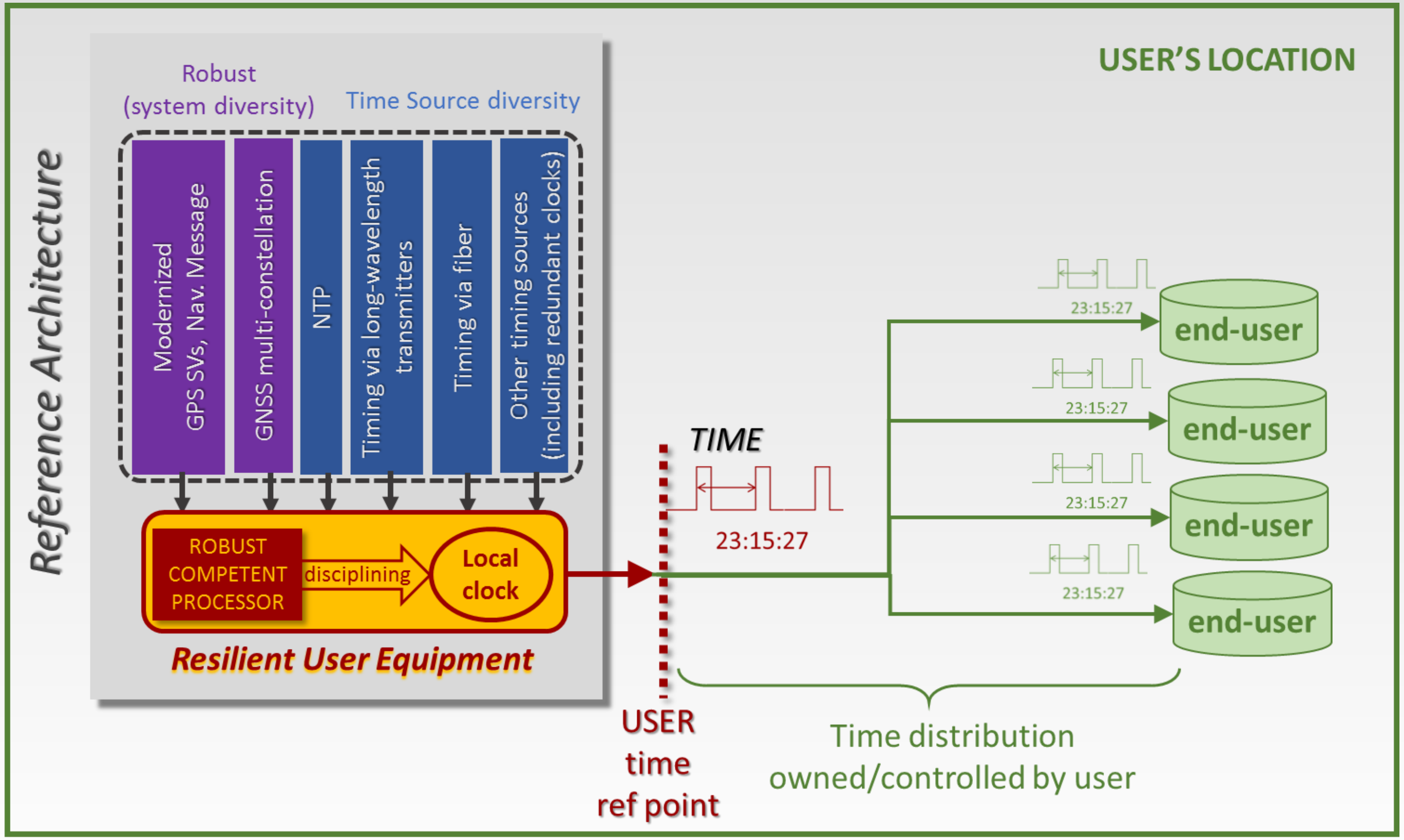
Resilient User Equipment

- Uses multiple and diverse time sources*
- It has a local clock that is disciplined by a **Robust and Competent processor (R&C processor)**
- It has a R&C processor that uses corollary information about the time signals (e.g. navigation message, antenna position for GPS time sources; health status for a redundant clock; encryption status for internet-based NTP time sources; etc.)

*these may include *redundant local clocks*, which are in addition to the disciplined local clock in the figure.

A PARADIGM SOLUTION

The output of the user equipment is the time reference point at the user's location
The user time reference point is a privileged place where time is defined in relation to UTC.



ASSURED ACCESS TO ACCURATE TIME - I

Q: *How do we* ***describe*** *the accuracy and assuredness of the time at the user's reference point?*

Q: *How do we* ***describe*** *the resilience of user equipment (with its R&C processor) that provides assured and accurate time?*

ASSURED ACCESS TO ACCURATE TIME - I

We identified a number of attributes of TIME:

- Accuracy: uncertainty in the calibration with respect to UTC
  - Expressed using standard statistics (1-sigma, etc.) and/or "not-to-exceed" matrics
  - Requires a calibration.

  Example: GPSDO sent to NIST

- Stability:
  - Describes the noise processes affecting the time signal and therefore indicates how often the calibration needs to be repeated to maintain stated accuracy.

  Example: that GPSDO calibrated on January 31st 2019 may need to be re-calibrated after a year.

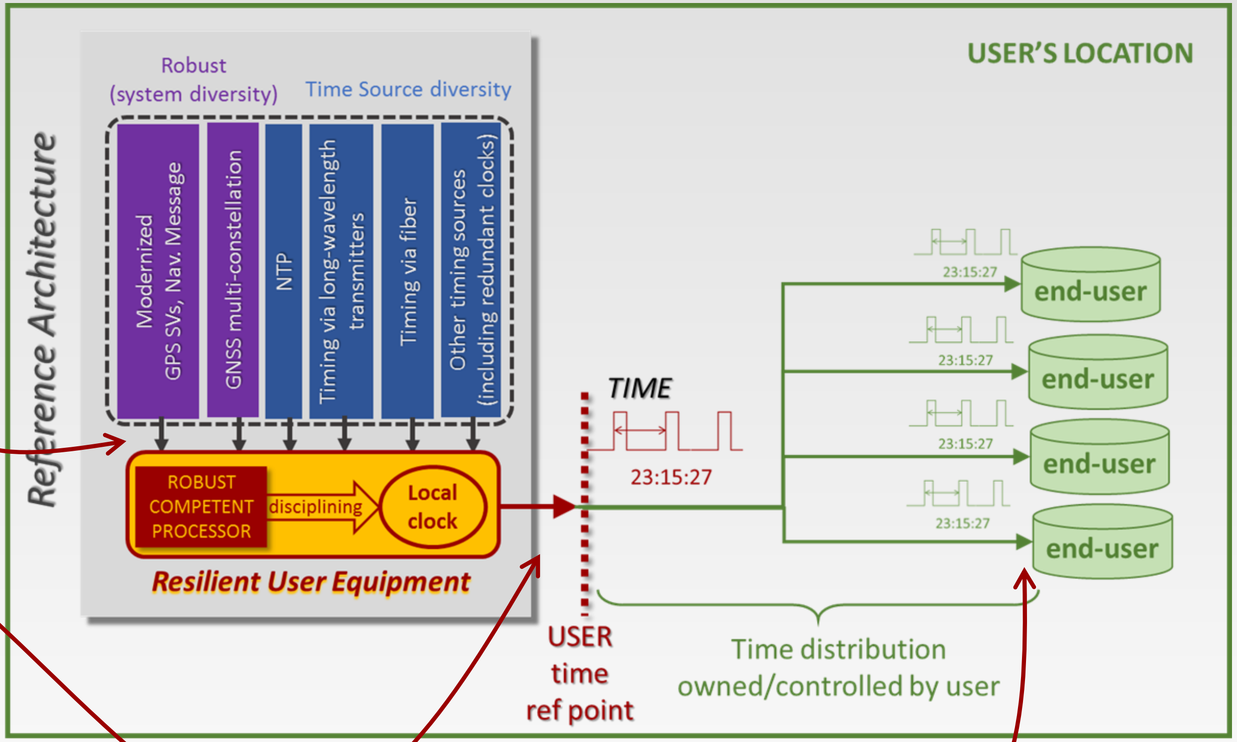
- Assuredness: confidence that the delivered time fits one or more stated models
  - Measurable deviation from a predicted behavior
  - Assessment of change in noise type
  - Detection of signal anomalies

- Availability: when assuredness is compromised, or a not-to-exceed accuracy value is violated, the signal may be denied, or flagged as unhealthy.

ASSURED ACCESS TO ACCURATE TIME - I

The same attributes are used to describe TIME at all relevant locations

- At the origin (UTC(NIST)
- At the inputs of the reference architecture
- At the output of the user equipment (user reference point)
- Eventually at each end-user, if relevant



ASSURED ACCESS TO ACCURATE TIME - I

We also identified a number of attributes of resilient user equipment (in the reference architecture) that may describe its capability to deliver assured time:

- Number of timing inputs: minimum number depends on specifics of each source;
- Degree of diversity between inputs: see vulnerability space of each source;
- Health self-assessment: knowledge of the status of the Robust and Competent processor is critical;
- Use of corollary information: critical when <3 independent timing sources are available. For GNSS, as an example:
  - Accurately surveyed fixed antenna helps with spoofing detection
  - Checking of sub-frames in navigation message helps in the verification of SV's orbits
  - Etc…
- Graceful degradation: in presence of compromised inputs, the processor should be still capable of providing time with inferior assuredness or accuracy;
- Recoverability: the processor needs to be capable of returning to a known state after a degradation or denial of time.

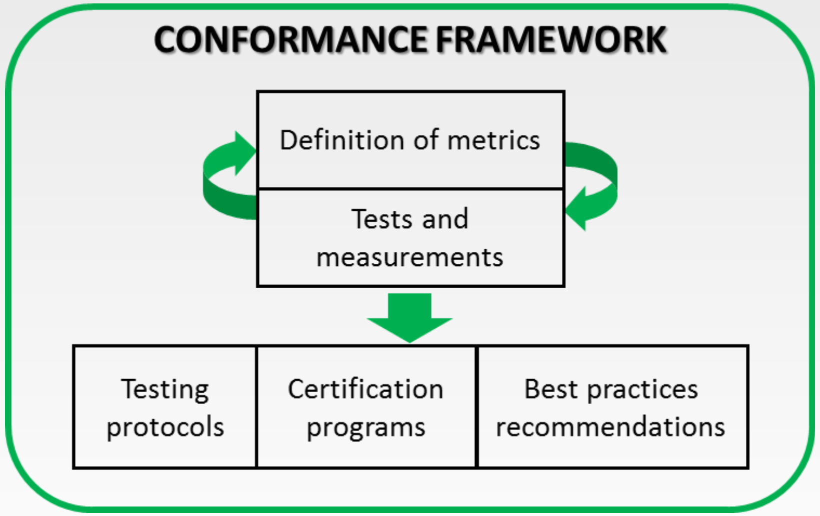
TOWARDS A CONFORMANCE FRAMEWORK

1. Identify metrics defining the resilience of the User Equipment and the assuredness and accuracy for time, both at the inputs of the User Equipment and at its output (user reference point)

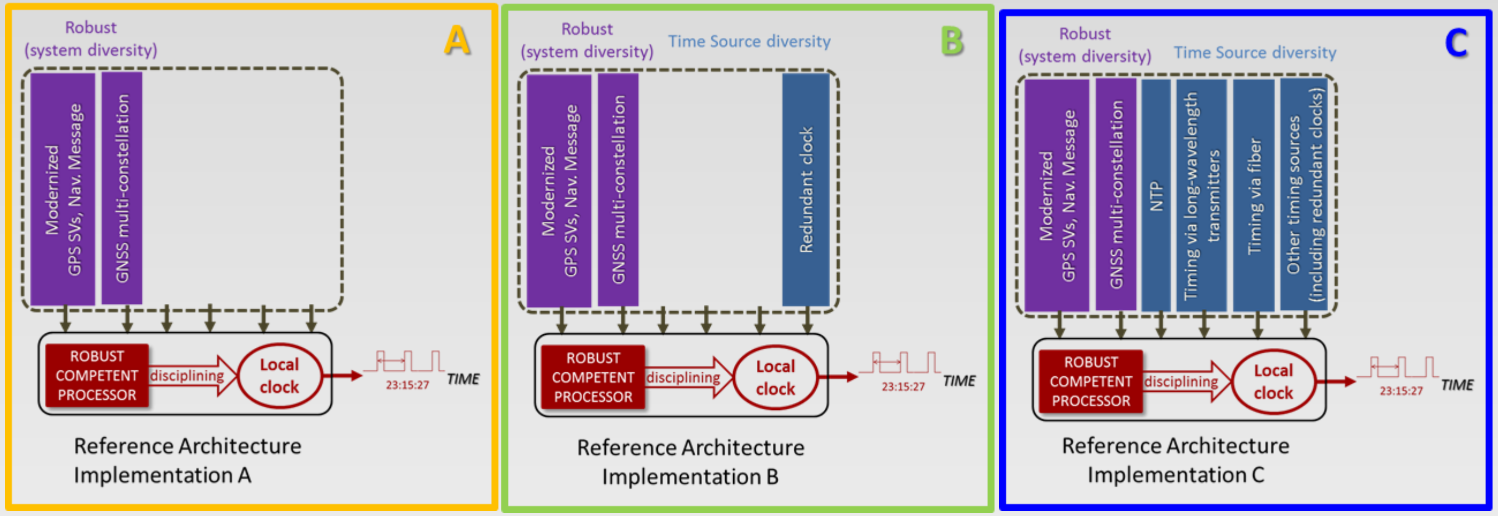
2. Investigate and identify measurement techniques, test procedures to characterize delivered time and the user equipment.

3. Use the experience gleaned from 2. to inform 1. creating an evolving set of metrics that are closely coupled with the available technologies.

- Implementations of the Reference Architecture
- Categorization of the vulnerability space
- Categorization of user requirements



ASSURED ACCESS TO ACCURATE TIME - II



RESILIENT REFERENCE ARCHITECTURE	Level 0	Level 1	Level 2	Level 3	Level 4
Number of time inputs	1	1	≥ 2	≥ 3	≥ 4
Inputs' degree of diversity	N/A	N/A	Y*	Y*	
Assessment of input's assuredness	N	Y	Y	Y	
R&C Processor self-assessment	N/A	Y	Y	Y	
Use of corollary information	N	Y	Y	Y	
Graceful degradation	N	N	Y	Y	
Recoverability	N	N	Y	Y	
Holdover (capability in absence of any time inputs)	N	Y	Y	Y	
Cybersecurity	N	basic	Y	Y	

* To be quantified

Implementations

- Three implementations of the reference architecture with increasing levels of complexity
- Allows draft of Conformance Framework in stages
- Allows different focus on simple, but widespread implementation vs complex less common one

ASSURED ACCESS TO ACCURATE TIME - II

Vulnerabilities

- *Vulnerability* is a better word than *threat*
- Three proposed categorizations:
  - Typology
  - Geographical impact
  - Timing impact
- Different timing sources have different vulnerability spaces, which must be clearly understood before choosing what implementation is the best choice
- Categorization of vulnerabilities is a crucial step in determining testing procedures

Timing source	Threat/vulnerability Categorization		
	By typology	**By geographical impact**	**By timing impact**
GNSS	Scheduled events (e.g. rollover)	Global	Large step
	Unscheduled system anomalies (e.g. 26 Jan)	Global	Large step
	Jamming	Local	Step
	Measurement Spoofing	Local	drift
	Data spoofing	Local	drift
	Cyberattacks		
NTP	…		
	…		
PTP over fiber	…		
	…		
….	…		

ASSURED ACCESS TO ACCURATE TIME - II

Users

criticality

Small end-users
(simple GPS-only timing sources, no internal timing expertise, remote location)

- implementation A,
- vulnerability space is GNSS

Medium users
(modernized GNSS timing source with holdover, minimal timing expertise, serving limited number of end-users, e.g. within a few buildings)

- implementation B
- vulnerability space is GNSS plus local clock

Large users – system integrators
(multi-source timing in few privileged locations, owns and manage timing distribution to large number of end-users, has internal timing expertise and testing capabilities, designs user timing equipment)

- Implementations A and C, depending on location in the timing hierarchy
- Complex vulnerability space

FUTURE WORK

- Three working groups to produce a report in the next 6-9 months about implementations, vulnerabilities and user requirements;
- Merging of findings from working groups to start initial identification of methods, needs and venues for testing programs
- Assured access to Accurate Time III in 2020 to discuss implementation of initial testing programs

THANK YOU!