Suitability and Reliability Assessment of TELEPERM XS Digital Safety I&C

A Qualitative and Quantitative Evaluation

Steffen RICHTER,
Christian HESSLER
AREVA NP
Moscow, 2017-06-21
Outline

1. Generic and application specific evidences for licensing of TELEPERM XS systems
2. Evolution of requirements for equipment qualification
3. Update of platform and evidences for TELEPERM XS
4. Qualitative reliability assessment: Approved by 3rd party accredited body
5. Quantitative reliability assessment: Data for the TELEPERM XS system software
Suitability and Reliability of TXS – ICT/SRi, CHe – 2017-06-21

The information in this document is AREVA NP property and is intended solely for the addressees. Reproduction and distribution are prohibited.
Evolution of IEC Codes & Standards

IEC 61513 (2001): General requirements for systems
IEC 60880 Ed 2 (2006): Update + integration of 60880-2 (CCF, software tools, ...)
IEC 62340 (2007): Requirements to cope with common-cause failure (CCF)
IEC 60987 Ed 2 (2007): Hardware requirements
IEC 62003 (2009): EMC testing
IEC 62566 (2012): HDL circuits for systems performing cat. A functions

TELEPERM XS generic evidences have been updated and made explicit to address:
- Explicit requirements on application-oriented languages & code generation
- Explicit requirements on firmware, configware, complex electronic components
- Traceability of requirements
- Explicit requirements to cope with CCF
- Cyber Security

TELEPERM XS platform and qualification is continuously maintained,
and proven by successfully licensed applications in 17 countries
Suitability and Reliability of TXS – ICT/SRI,CHe – 2017-06-21

TELEPERM XS
New Build / Completion Projects

- **FINLAND**
  - Olkiluoto 3

- **RUSSIA**
  - Novovoronesh II 1&2
  - Leningrad II 1&2

- **UNITED KINGDOM**
  - Hinkley Point C

- **FRANCE**
  - Flamanville 3

- **SLOVAKIA**
  - Mochovce 3&4

- **CHINA**
  - Taishan 1&2
  - Tianwan 3&4
  - Fuqing 5&6

- **BRASIL**
  - Angra 3
Evolution of I&C Platform and Qualification Evidences
Reliable basis for licensing international I&C projects

**TELEPERM XS Safety I&C (by AREVA NP)**
- TXS platform qualification includes Type Approval according to Finnish YVL 5.5 accepted by STUK
- Design update of Input / Output modules – Enhanced self-monitoring capabilities, accuracy, EMC (IEC 62003)
- Cyber Security Plans - based on latest requirements by standards – developed on platform level and for safety I&C projects
- Advanced tool suite for engineering and maintenance
- Platform selected for plant modernization projects by Belgian utility and well accepted by Belgian safety authority in 2016

**SPPA T-2000 Operational I&C (by partner SIEMENS AG)**
- Continuously developed with respect to recent requirements by international codes & standards including Cyber Security
- Interfaces between TXS and T-2000 such as gateway and priority module well proven to support comprehensive I&C solutions for NPP
- T-2000 platform and system designs accepted for EPRs in Flamanville 3 and Olkiluoto 3
Measures to Cope with CCF on Platform Level
- summarized as ‘TXS System Properties’

1. Definition of I&C functionality by application software
2. Defined operating modes and transitions of TXS Computers
3. Cyclic operation mode of TXS Computers
4. Deterministic system response time
5. Independent operation of TXS Computers
6. Independent operation of separated I&C functions
7. Fault detection by TXS Computers
8. Signal acquisition, processing and output considering status information
9. Fail-safe behavior
10. Reliable and secured data exchange via network
11. Monitoring & Service Interface (MSI) constitutes IT security barrier

Reflects the features necessary for safety demonstration
Easy to maintain despite evolution of requirements
Generic Qualification Evidences - on platform level

**TXS System Properties: „Main features of the platform“**

- Summary of technical features as a basis for licensing
- Supplemented by high-level descriptions:
  - „Operating principles“, „Fail-safe characteristics“ …
- Mapped to technical features of HW or SW components
- Mapped to test and analysis documentation
- „Standard compliance analyses“ of design and QA with requirements from codes & standards
- “Design rules” specify constraints for the application design

| 1 | Definition of I&C functionality by application software |
| 2 | Defined operating modes and transitions of TXS Computers |
| 3 | Cyclic operation mode of TXS Computers |
| 4 | Deterministic system response time |
| 5 | Independent operation of TXS Computers |
| 6 | Independent operation of separated I&C functions |
| 7 | Fault detection by TXS Computers |
| 8 | Signal acquisition, processing and output considering status information |
| 9 | Fail-safe behavior |
| 10 | Reliable and secured data exchange via network |
| 11 | MSI constitutes IT security barrier |

Generic qualification files on equipment and platform level have been approved by 3rd party accredited body through Type Approval

**Complementary documentation**

- Generic, qualitative CCF analyses → Basis for system-level CCF analyses
- Operating Experience analysis → Evaluation of robustness and availability
Analysis of Operating Experience
Looking backwards…

TELEPERM XS has undergone several modifications since “t₀“

<table>
<thead>
<tr>
<th>These address</th>
<th>Found „bugs“ handled as „non-conformances“ (NCRs)</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Improvements of maintainability</td>
<td>• All were analyzed and communicated</td>
</tr>
<tr>
<td>• Replacement of obsolete hardware</td>
<td>• The platform concepts were never affected</td>
</tr>
<tr>
<td>• Minor bug fixes</td>
<td>• No functional consequences for operating installations</td>
</tr>
<tr>
<td></td>
<td>• Changes were limited to hardware upgrades</td>
</tr>
</tbody>
</table>

Quantitative evaluation of the operating experience used to estimate CCF probability of TXS systems
Estimate of CCF Probability for TXS Systems based on Operating Experience - Basis

- Evaluation of all events linked to underlying causes with systematic nature
  - Non-conformance database, maintained since 2000
  - Covers all events and near-misses signaled from design, test field, commissioning, plant operation
  - Last full analysis in 2016
  - 111 individual, separated I&C systems / applications

Type A
Failures triggered by time-based long-term effects / saturation

Type B
Failures triggered by fault-propagation via networks

Reference group: whole I&C systems
Relevant operating time: 8.3 Mio h

Type C
Failures triggered by particular signal values / internal states

Type D
Ageing, wear & tear of computerized equipment

Reference group: set of 4 processing units
Relevant operating time: 79.7 Mio h

Note:
Type E – “faults in the application” are not considered: not platform-related, expected to be consistent with traditional I&C technology
## TXS Platform Contribution to CCF Probability – Conservative estimate of system unavailability

### Type A
Failures triggered by time-based long-term effects / saturation

- 0 coincident failures observed
- 0 events assigned

### Type B
Failures triggered by fault-propagation via networks

- 2 events with coincident malfunctions, triggered by maintenance errors
  - Conservatively evaluated as “complete loss” and assigned to the platform. Unavailability of some functions for ~1/4 h
  - Unavailability of one system < 1.9 * 10^-7

### Type C
Failures triggered by particular signal values / internal states

- 0 coincident failures
- Assumed conservatively 1 coincident failure
  - Unavailability < 3.8 * 10^-9

### Type D
Ageing, wear & tear of equipment

- 0 events assigned

Conservative evaluation shows very low platform contribution to CCF, clearly dominated by maintenance errors but not by digital technology.
Throughout the operational life of the I&C systems they behaved in the predetermined way.

The controls for failure handling have been effective.

The operating experience confirms the adequacy of the TXS system properties and their correct implementation.

TELEPERM XS provides generic qualification files successfully utilized for licensing of safety I&C in more than 80 international projects.

It includes all characteristics for the minimization of risk of CCF, recommended by IEC 62340.
Thank you for your attention!
Editor and Copyright 2017: AREVA GmbH – Paul-Gossen-Straße 100 – 91052 Erlangen, Germany. It is prohibited to reproduce the present publication in its entirety or partially in whatever form without prior written consent. Legal action may be taken against any infringer and/or any person breaching the aforementioned prohibitions.

Subject to change without notice, errors excepted. Illustrations may differ from the original. The statements and information in this brochure are for advertising purposes only and do not constitute an offer of contract. They shall neither be construed as a guarantee of quality or durability, nor as warranties of merchantability or fitness for a particular purpose. These statements, even if they are future-orientated, are based on information that was available to us at the date of publication. Only the terms of individual contracts shall be authoritative for type, scope and characteristics of our products and services.