CONNECTA-2

CONtributing to Shift2Rail's
NExt generation of high
Capable and safe TCMS.
Phase 2

Safe4RAIL2

SAFE architecture for
Robust distributed
Application Integration
in roLling Stock 2

Lessons learned and way forward

Igor Lopez (CAF), Thomas Waschulzik (Siemens), Gernot Hans (ALSTOM)

The projects CONNECTA-2 and Safe4RAIL-2 have received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 826098 (CONNECTA-2) and No. 826073 (Safe4RAIL-2) respectively. The information and views set out in this document are those of the author(s) and do not necessarily reflect the official opinion of Shift2Rail Joint Undertaking. The JU does not guarantee the accuracy of the data included in this article. Neither the JU nor any person acting on the JU's behalf may be held responsible for the use which may be made of the information contained therein.

Lessons learned building the demonstrators (I)

✓Correct approach of incorporating existing knowledge from other industries instead of reinventing the wheel

- ➢Potential reduction of costs by incorporating products/technologies with larger market scale.
- ➢Learn from other critical industries with similar problems/challenges.

✓Correct assumptions in the definition of standardized interfaces:

- ➢Application Profiles for the interfaces to the subsystems.
- ➢Functional Open Coupling for the interfaces between CCUs of coupled consists from different manufacturers.
- ➢SysML models usage:
  - ➢Alignment between standardized interfaces and internal development possible
  - ➢Tool integration supports the direct reusability of CONNECTA-2 work by industry members
- ➢Successful definition and use of modelling guidelines

Lessons learned building the demonstrators (II)

× Standards neither fully defined nor mature for application:

- ➢Some important standards of TSN are still being defined, delaying the final specification which slows down their adoption in the market ➔ Configuration tools not available (e.g. IEEE 802.QBV IEEE 802.1CB)
- ➢The progress of the standardization of AUTOSAR Adaptive Platform especially towards the deterministic execution and safety were not as fast as expected ➔ perspective unclear
- ➢Ambiguity in IEC 61375-2-5 and IEC 61375-2-3 led to incompatible first development between MOXA-Westermo and MOXA-CAF, as well as in ambiguity in the ECSC interface between ETBN and CCU.

Lessons learned building the demonstrators (III)

×We underestimated complexity of adopting some technologies:

Time synchronization (and its configuration) inside a consist and when coupling these

➢Comparing to other critical industries, railway onboard networks are dynamic when units are coupled which is not covered by the TSN standard.

➢TCMS integrators already have well established configuration workflows which must be adapted for TSN, which implies to have standard interfaces with network management tools to avoid vendor locking.

Integration of communication stacks into AUTOSAR Adaptive Platform

➢The integration of new communication protocols (OPC UA / TRDP) is much more complex than expected

➢Insufficient extensibility of AUTOSAR Adaptive communication architecture might harm the integration of new features in CONNECTA3

➢Up to now it seems complex to add additional features in the actual specification of the AUTOSAR Adaptive Platform for instance security OPC UA

Integrity-based FDF implementation current limitations

➢No possibility of effective cross-compilation (need of Integrity license to compile the third party code)

➢No clear safe instruction in Integrity to synchronize execution time partitions with network timing

➢Lack of service-oriented support, not clear path to make it deterministic

Lessons learned building the demonstrators (IV)

×We underestimated integration timing specially in COVID-19 times:

All the tests have to be executed using ad-hoc solutions which interconnect different sites using L2 VPNs.

Most of deliveries from Safe4Rail-2 came to CONNECTA-2 in the last months of the project

- ➢TRL5 solutions are far from be Plug&Play.
- ➢Most of the bugs were detected in the last 6 months of both projects which created a high work overloaded in both project.
- ➢The bug fixing, implementation, validation process was slower remotely than traditionally with physical workshops.

We shall not repeat same problems in future projects:

- ➢Continuous Integration processes shall be established
- ➢Prototypes shall be integrated in demonstrators from an early stage of the project
- ➢Using collaborative platforms (e.g. GIT and SVN) continuous feature improvement can be directly tested in target demonstrators

What did change during the CONNECTA2 project that might be or will be game changers in the future? (I)

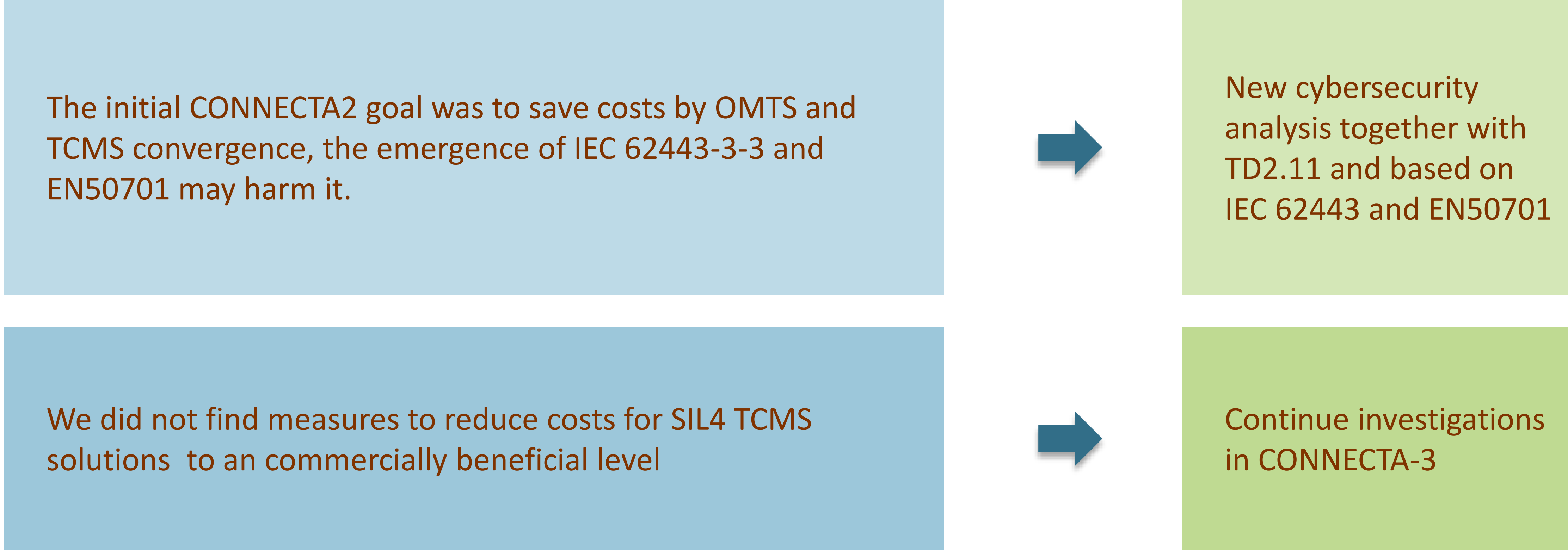
- ➢FRMCS and CCS requirements have to be included in the communication system specification
- ➢ Security became one of the driving features of the communication infrastructure including the handling of the private key infrastructure

→ Broadened scope for drive by data

Digitalization is driving the dynamics even in safety and real time systems

→ New level of Agility brought in by the CCS and TWG-ARCHI activities

What did change during the CONNECTA2 project that might be or will be game changers in the future? (II)



The initial CONNECTA2 goal was to save costs by OMTS and TCMS convergence, the emergence of IEC 62443-3-3 and EN50701 may harm it.

New cybersecurity analysis together with TD2.11 and based on IEC 62443 and EN50701

We did not find measures to reduce costs for SIL4 TCMS solutions to an commercially beneficial level

Continue investigations in CONNECTA-3

Conclusions taken for the way forward (I)

Drive by data

1

1. Use new set of requirements defined for TCMS, CCS, FRMCS and OMTS to find a consistent solution that also enables the convergence of subsystems wherever possible.
2. Evaluate the TSN alternatives to scheduled traffic on the ETB (Ethernet Train Backbone) such as frame preemption (IEEE 802.1Qbu) and strict priority (IEEE 802.1Q)
3. Identify and implement better configuration and integration solutions for the TSN features

Conclusions taken for the way forward (II)

2

Replacement of the train lines

1. Up to now no cost efficient solution for SIL4 FDF is available with high TRL
2. Hardware will not be available in SILx capability in CONNECTA3
   a. ETBN (SIL2)
   b. Computing architecture for SIL4 (CCU+ Safety-Architecture)
3. No middleware available supporting mixed criticality up to SIL4 including time and data determinism with service oriented communication real market expectations go up to SIL2
4. Further research in CONNECTA3 required

Conclusions taken for the way forward (III)

3

Middleware

1. A stable and long lasting decision on the middleware is not possible at the moment
   a. None of the candidates fulfills the major requirements for our domain with SIL4
   b. Good evolvability additionally is required to support the rapid changes in our domain for digitalization and decarbonization
   c. Even the Automotive for the ADAS domain tried now for more than 5 years without success to define a suitable solution and fast movers use successfully alternative solutions

→ standardization of the middle ware is not feasible at the moment

Conclusions taken for the way forward (IV)

3

2. Interoperability and evolvability are better achieved by SysML based Application Profiles
   a. already represent a considerably engineering cost improvement.
   b. Supports direct integration of the standardization in the development tool chain
   c. Leaves required degrees of freedom for innovation and standardization
3. Binary interoperability is not suitable due to different
   a. Operating Systems (OS),
   b. Hardware
   c. Serialization of Communication protocols
4. APIs from application to the FDF is usually implementation dependent and requires code generation to avoid user failures in safety critical systems

Technological feasibility

CONNECTA2 taught us a lot about technological feasibility and gives a clear direction for CONNECTA3.

Defined features

The features defined in the CONNECTA2 scope for FDF and drive by data are correct, but the achievable TRL or/and SIL are not aligned with the market evolution pace.

CONNECTA3

CONNECTA3 should honestly build upon the findings of CONNECTA2 and the concepts