Functional Distribution Framework

Xabier Artaetxebarria, CAF
Iñigo Odriozola, Ikerlan

CONNECTA has received funding from the European Union’s Horizon 2020 research and innovation programme under agreement No: 730539. Safe4RAIL has received funding from the Shift2Rail Joint Undertaking under grant agreement No: 730830. This Joint Undertaking receives support from the European Union’s Horizon 2020 research and innovation programme.
What is the FDF?

- A middleware to run software applications on top of it
- An abstraction layer from underlying hardware and communications
- A tool to facilitate the achievement of functional safety and application independence
What is the FDF?
What is the FDF?

- App 1 (no-safety)
- App 2 (SIL2)
- App 3 (SIL4)

FUNCTIONAL DISTRIBUTION FRAMEWORK

HARDWARE AND COMMUNICATIONS
## Why FDF?

<table>
<thead>
<tr>
<th>Today</th>
<th>With FDF</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device-based TCMS architecture</td>
<td>Function-based TCMS architecture</td>
</tr>
<tr>
<td>Heterogeneous software and hardware on board</td>
<td>Unified software and hardware on board</td>
</tr>
<tr>
<td>Multiple heterogeneous computing units</td>
<td>Few homogeneous computing units</td>
</tr>
<tr>
<td>Costly re-certification and re-commissioning after functions changes</td>
<td>Simplified re-certification and re-commissioning process</td>
</tr>
<tr>
<td>Complex obsolescence management</td>
<td>Simplified obsolescence management</td>
</tr>
</tbody>
</table>
FDF in detail

• Solutions in other domains
  – Automotive: AUTOSAR
  – Aviation: ARINC653

• Proposed solution for the railway domain
  – Safety
  – Security
  – Use example
  – Safe4RAIL implementations
Solutions in other domains

AUTOSAR
Enabling continuous innovations

- Time Management
- Execution Management
- Software Configuration Management
- Security Management
- Diagnostics
- Operating System
- Persistency
- Platform Health Management
- Logging and Tracing
- Hardware Acceleration
- Communication Management

(Virtual) Machine / Hardware
Solutions in other domains

ARINC 653

Safe4RAIL – SAFE architecture for Robust distributed Application Integration in rolling stock (730830)

CONNECTA – CONtributing to Shift2Rail's NExt generation of high Capable and safe TCMS and brAkes (730539)
Proposed solution
Proposed solution

Deployment Management

**Brief description**
Component that provides the ability to install and update application executables on the functional distribution framework partitions.

**Requirement specification**

<table>
<thead>
<tr>
<th>REQM</th>
<th>Name/Text</th>
<th>Safety-related</th>
</tr>
</thead>
<tbody>
<tr>
<td>CTA-D4.4-DM-1</td>
<td>Install executable on a partition (direct connection)</td>
<td>yes</td>
</tr>
<tr>
<td>CTA-D4.4-DM-2</td>
<td>Install executable on a partition (network connection)</td>
<td>yes</td>
</tr>
</tbody>
</table>

**Description**
- The FDF component "Deployment Management" shall provide the maintenance staff with the ability to install an executable on a partition via direct connection to the device.
- The FDF component "Deployment Management" shall provide the maintenance staff with the ability to install an executable on a partition via train network.

**Documentation**
- Rationale: [Requirement CTA-D4-1-128 CTA-D4-1-128]
- Satisfied by: [Block Deployment Management]
Safety

FDF Safety concept is defined by the set of safety measures coming from the FDF Hazard Analysis.

The FDF HA has been carried out in order to:

- identify any deviation
- assess the effects of hazardous deviations
- specify the measures

Safety measures include:

- **Countermeasures** - to be implemented by the FDF
- **Application conditions** - to be exported to users and/or external technical systems
- **Recommendations** - indications for the implementation of countermeasures
Countermeasures are classified according to the Technical Safety Report (EN 50129) sections:

- Assurance of functional operation
- Detection of faults
- Action following detection
- Independence of items
- Systematic and Random faults

RESULT

Countermeasures – FDF Requirements & FDF Requirements – FDF Components Traceability
Security

- **Risk analysis** for services provided by FDF by defining assets to be protected and threats.
- **Risk assessment** based on ISA/IEC 62443-3-3 “System security requirements and security levels”.

Target Security Level: SL3

RESULT

- 62443-3-3 Requirements – Countermeasures – **FDF Requirements** - **FDF software components** – **Security Objectives** traceability
Use example: Door control without FDF
Use example: Door control with FDF
Use example
Safe4RAIL implementations

- 3 Proof-of-concept demonstrators of FDF
- Bogie Monitoring System application
  - Read temperature sensors
  - Activate warm or hot alarm
Next station is

• CONNECTA-2 & OC
  – Higher TRL implementations of FDF
  – Development of applications on top of FDF
  – Maintenance of detailed specification and addition of interfaces (if required)
  – Handling technical issues not addressed by Safe4RAIL FDF implementations
Conclusions

• The FDF aims to have isolated but integrated applications instead of dedicated equipment (HW, SW, I/Os) for each train function.

• **Benefits:**
  – Reduce the number and complexity of **devices**
  – Reduce re-/certification complexity
  – **Interoperability**, reconfiguration, deterministic inter-partition communication
  – Hardware and communication **abstraction**