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.

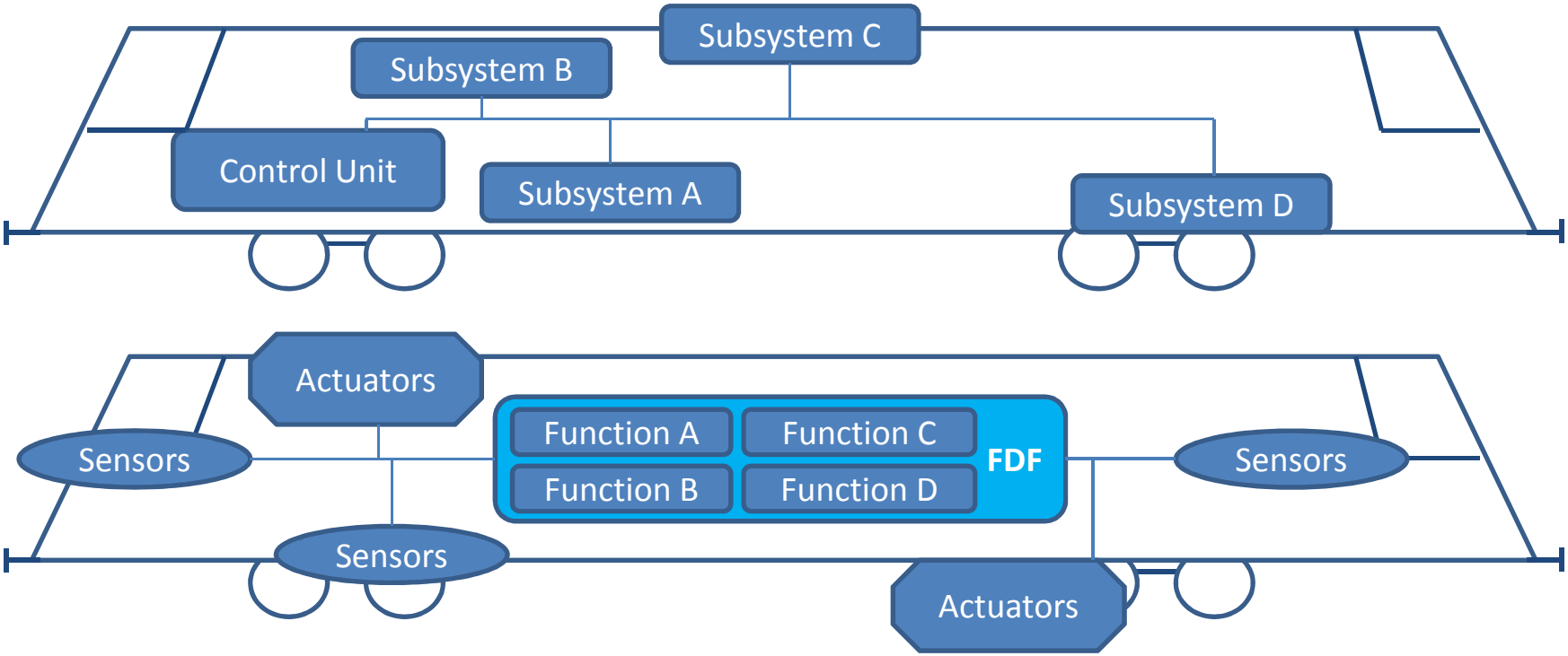
Safe4RAIL – SAFE architecture for Robust distributed Application Integration in roLling stock (730830)

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

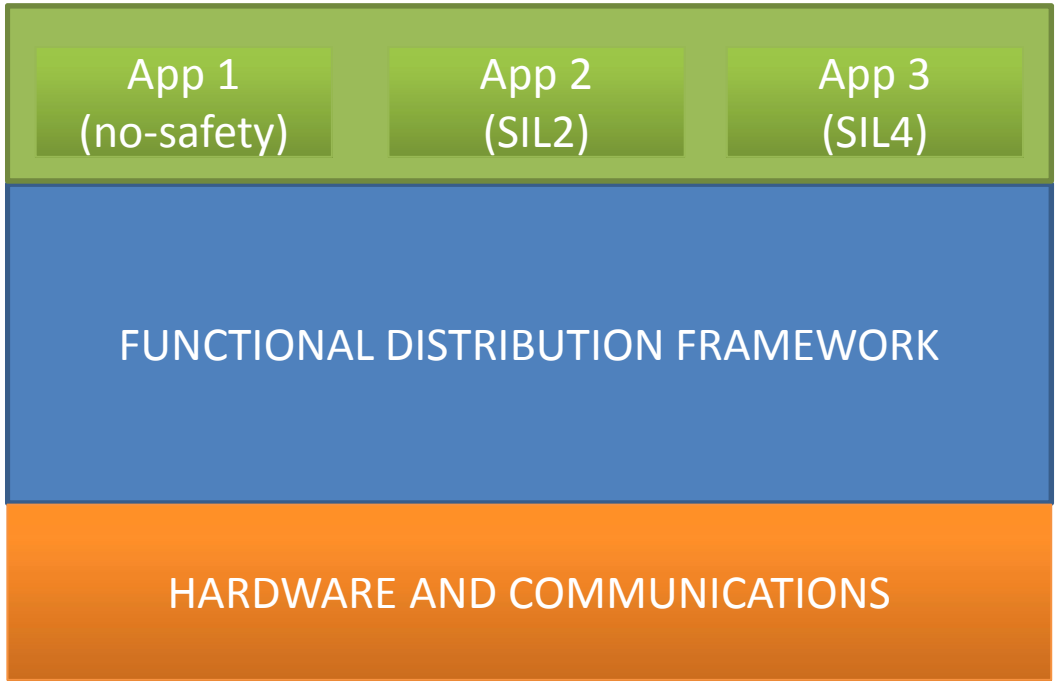
What is the FDF?

- 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?



Why FDF?

Today	With FDF
Device-based TCMS architecture	Function-based TCMS architecture
Heterogeneous software and hardware on board	Unified software and hardware on board
Multiple heterogeneous computing units	Few homogeneous computing units
Costly re-certification and re-commissioning after functions changes	Simplified re-certification and re-commissioning process
Complex obsolescence management	Simplified obsolescence management

FDF in detail

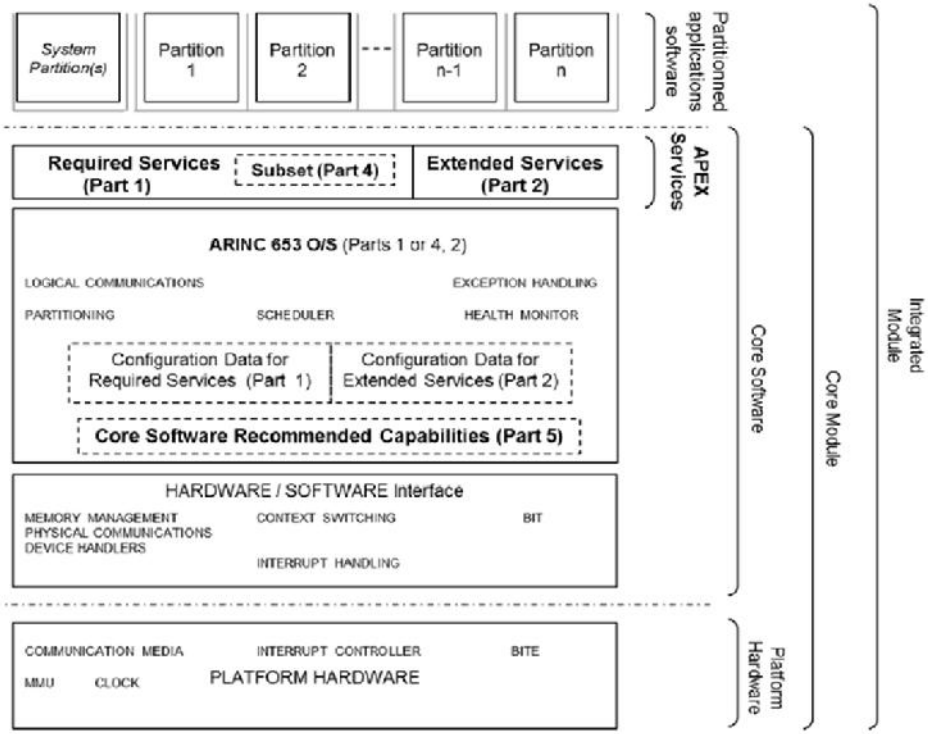
- Solutions in other domains
  - Automotive: AUTOSAR
  - Aviation: ARINC653
- Proposed solution for the railway domain
  - Safety
  - Security
  - Use example
  - Safe4RAIL implementations

Solutions in other domains

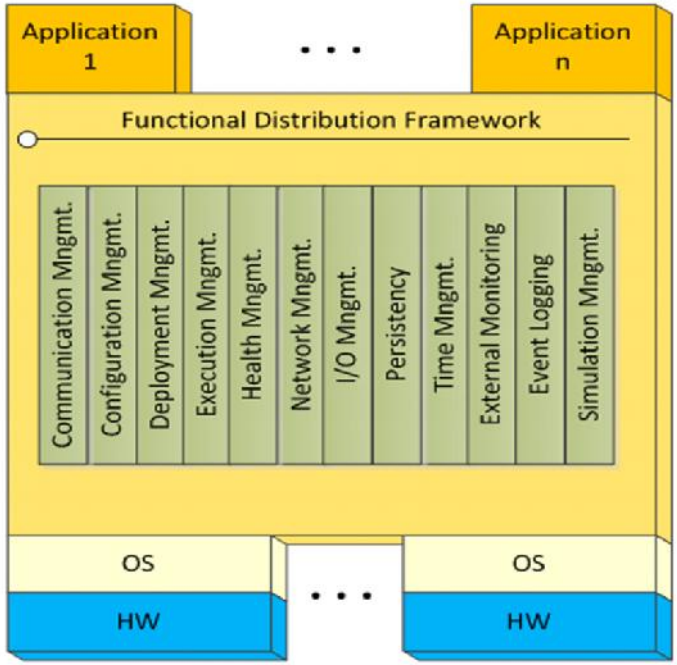
AUTOSAR
Enabling continuous innovations

Solutions in other domains

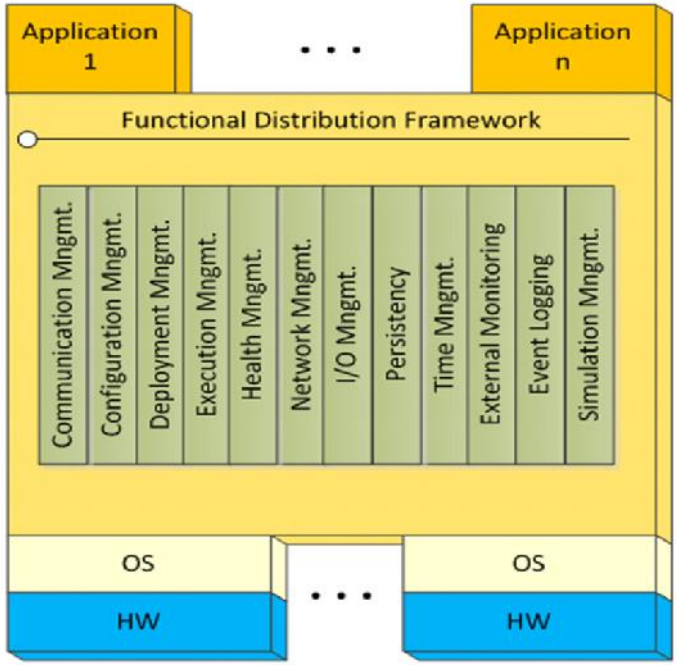
ARINC 653



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

REQ Id	Name/Text	Safety-related
CTA-D4.4-DM-1	**Install executable on a partition (direct connection)** 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. Documentation: Rationale: Derived from: Requirement CTA-D4.1-128 CTA-D4.1-128 Satisfied by: Block Deployment Management	yes
CTA-D4.4-DM-2	**Install executable on a partition (network connection)** 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: Derived from: Requirement CTA-D4.1-128 CTA-D4.1-128 Satisfied by: Block Deployment Management	yes

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

Safety

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

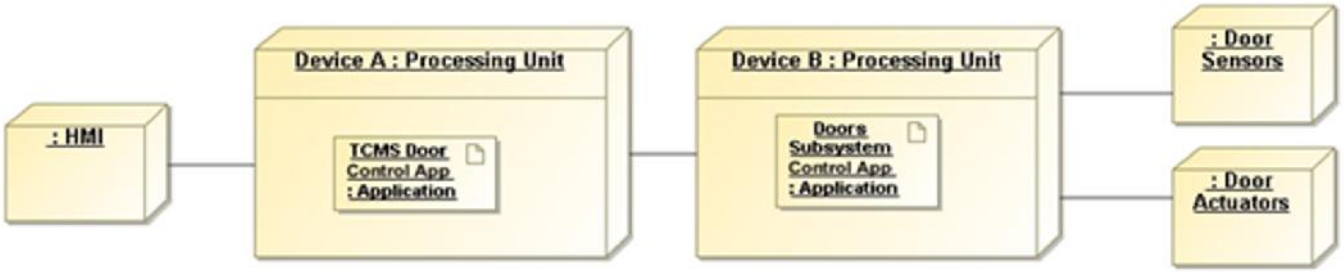
Cybersecurity		Attack Potential (worst case)					Damage Potential (worst case)			Cybersecurity Risk Estimation				
Security Objective	Attack	Elapsed Time	Expertise	Information about the target	Access to Target	Equipment	Personal Damage	Operative Damage	Financial Damage	Attack Potential		Damage Potential		Risk Value
SO.1 Authorized use of FDF	Session hijacking	Months	Multiple Experts	Critical	Difficult	Specialized	Severe and life-threatening injuries (survival possible	Maintenance required	< 100.000 euros	Beyond High-Rate	43	Catastrophic	1020	Undesirable
	FDF manipulation	Months	Expert	Critical	Difficult	Multiple Bespoke	Severe and life-threatening injuries (survival possible	Unusable	< 1.000.000 euros	Beyond High-Rate	46	Catastrophic	1200	Undesirable
	Authorization/Privileges modification	Months	Expert	Critical	Difficult	Specialized	Severe and life-threatening injuries (survival possible	Maintenance required	< 100.000 euros	Beyond High-Rate	41	Catastrophic	1020	Undesirable
	Password hack	Months	Proficient	Restricted	Moderate	Standard	Severe and life-threatening injuries (survival possible	Comfort affected	< 100.000 euros	High	20	Catastrophic	1011	Undesirable
	Power failure	Hours	Layman	Public	Difficult	Standard	No effect	Maintenance required	< 10.000 euros	Enhanced-Basic	11	Medium	10	Undesirable
	Hard drive failure	Hours	Expert	Public	Difficult	Standard	No effect	Unusable	< 10.000 euros	Moderate	17	Critical	100	Undesirable
	User supplantation	Weeks	Proficient	Restricted	Moderate	Standard	No effect	Comfort affected	< 100.000 euros	Moderate	14	Medium	11	Undesirable
SO.2 Restricted access to ECU instructions	CPU manipulation	Months	Expert	Critical	Difficult	Multiple Bespoke	Severe and life-threatening injuries (survival possible	Unusable	< 1.000.000 euros	Beyond High-Rate	46	Catastrophic	1200	Undesirable
	Data injection/deletion	Months	Expert	Critical	Difficult	Multiple Bespoke	Severe and life-threatening injuries (survival possible	Unusable	< 100.000 euros	Beyond High-Rate	46	Catastrophic	1100	Undesirable
SO.3 Application isolation	Data corruption	Months	Proficient	Restricted	Difficult	Multiple Bespoke	Severe and life-threatening injuries (survival possible	Maintenance required	< 100.000 euros	Beyond High-Rate	35	Catastrophic	1020	Undesirable
	Network flooding	Years	Expert	Sensitive	Moderate	Multiple Bespoke	Severe and life-threatening injuries (survival possible	Maintenance required	< 100.000 euros	Beyond High-Rate	16	Catastrophic	1020	Undesirable
SO.4 Data authentication and encryption	Breach of cryptography	Years	Multiple Experts	Critical	Difficult	Specialized	Severe and life-threatening injuries (survival possible	Maintenance required	< 100.000 euros	Beyond High-Rate	53	Catastrophic	1020	Undesirable
	Collect sensitive information (keys, logs)	Months	Expert	Critical	Difficult	Specialized	Severe and life-threatening injuries (survival possible	Maintenance required	< 100.000 euros	Beyond High-Rate	41	Catastrophic	1020	Undesirable
SO.5 Trusted message exchange	Message injection	Months	Expert	Critical	Difficult	Multiple Bespoke	Severe and life-threatening injuries (survival possible	Comfort affected	< 100.000 euros	Beyond High-Rate	46	Catastrophic	1011	Undesirable
	Man-in-the-Middle	Months	Multiple Experts	Sensitive	Moderate	Multiple Bespoke	Severe and life-threatening injuries (survival possible	Comfort affected	< 10.000 euros	Beyond High-Rate	30	Catastrophic	1001	Undesirable
SO.6 Trusted input/output devices	Peripheral device supplantation	Months	Multiple Experts	Public	Difficult	Bespoke	Severe and life-threatening injuries (survival possible	Maintenance required	< 10.000 euros	Beyond High-Rate	35	Catastrophic	1001	Undesirable
	Port tampering	Hours	Expert	Public	Difficult	Bespoke	No effect	Maintenance required	< 10.000 euros	High	24	Medium	10	Tolerable
	Ethernet tampering	Hours	Expert	Public	Difficult	Bespoke	No effect	Maintenance required	< 10.000 euros	High	24	Medium	10	Tolerable
	Repudiation	Hours	Expert	Public	Difficult	Bespoke	No effect	Maintenance required	< 10.000 euros	High	24	Medium	10	Tolerable

Counter-measures

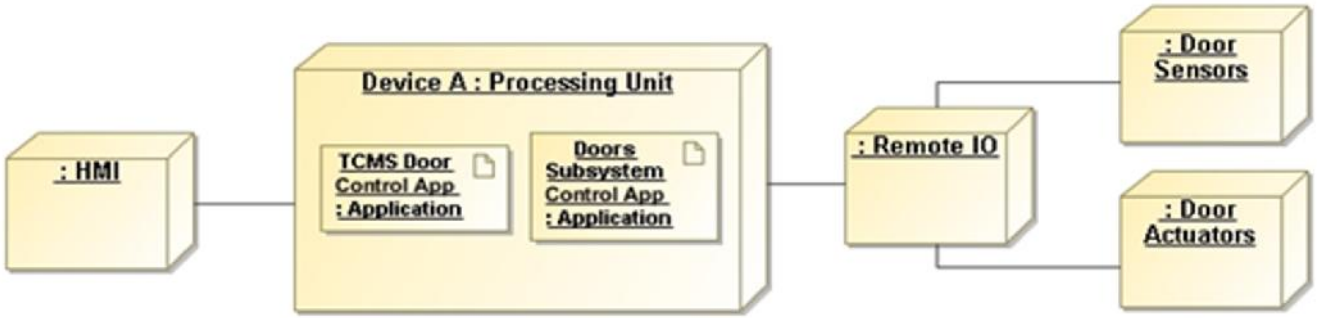
RESULT

- *62443-3-3 Requirements – **Countermeasures – FDF Requirements** - FDF software components – Security Objectives* traceability

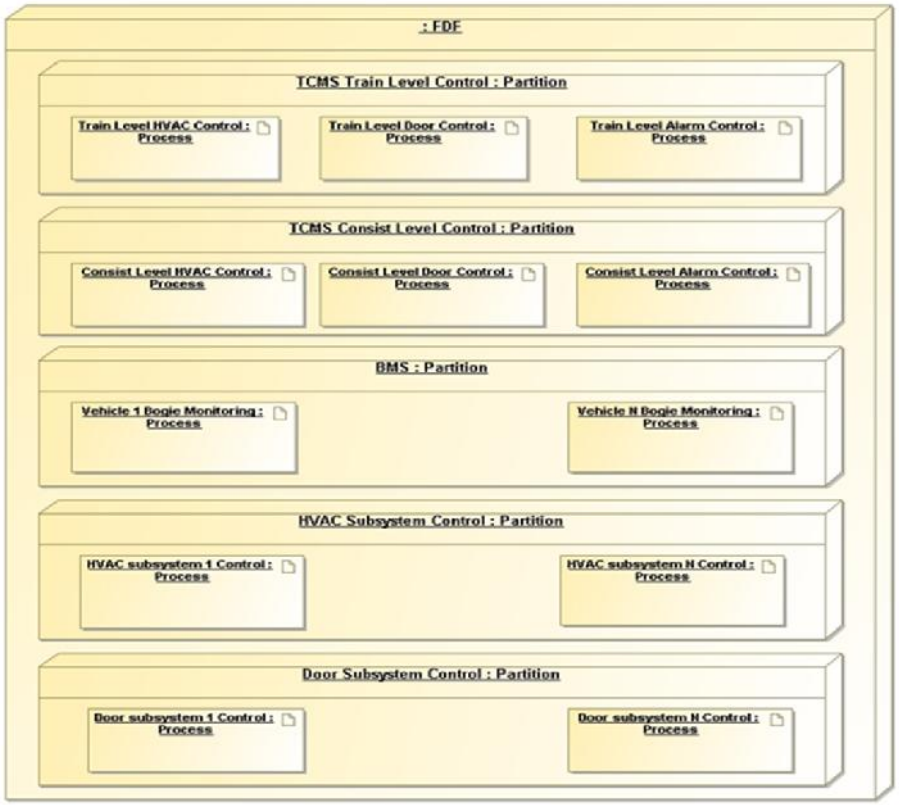
Use example: Door control without FDF



Use example: Door control with FDF

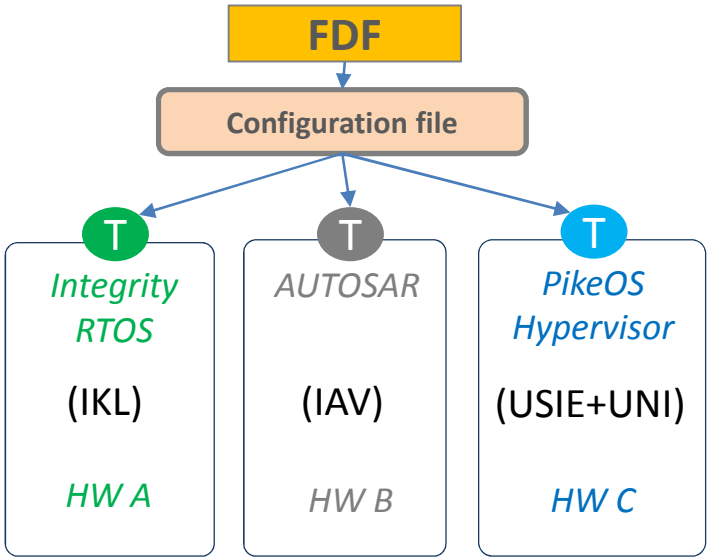


Use example


: FDF
TCMS Train Level Control : Partition
Train Level HVAC Control : Process
Train Level Door Control : Process
Train Level Alarm Control : Process
TCMS Consist Level Control : Partition
Consist Level HVAC Control : Process
Consist Level Door Control : Process
Consist Level Alarm Control : Process
BMS : Partition
Vehicle 1 Bogie Monitoring : Process
Vehicle N Bogie Monitoring : Process
HVAC Subsystem Control : Partition
HVAC subsystem 1 Control : Process
HVAC subsystem N Control : Process
Door Subsystem Control : Partition
Door subsystem 1 Control : Process
Door subsystem N Control : Process

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