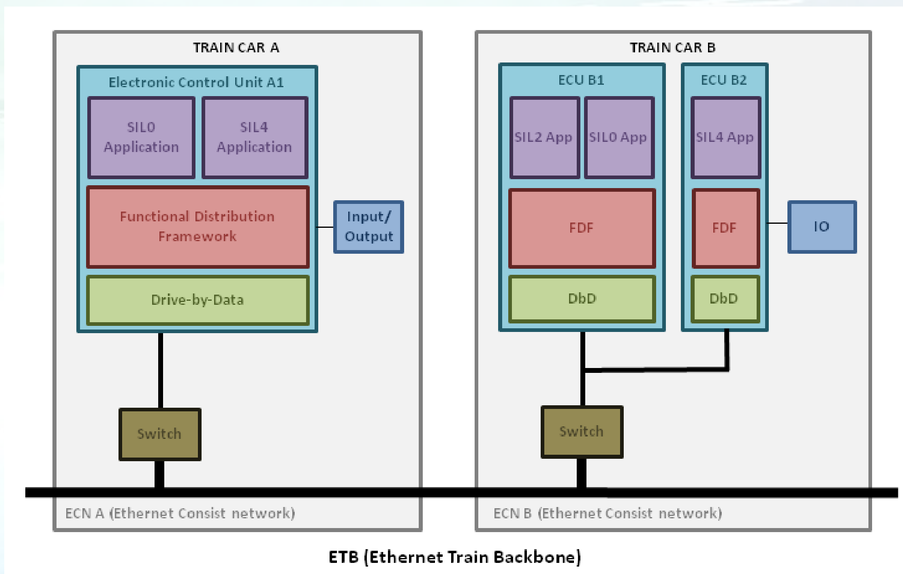
# Motivation

- Complexity: Nowadays' railway systems consist of a complex architecture of many separate subsystems of different SIL which perform a specified functionality within the train.
- Diversity: Typically each of these functions uses own concrete equipment, controllers, wires and connectors which results in a maintenance and recommissioning nightmare and high lifecycle costs.
- Interoperability: Train cars of different manufacturers cannot communicate with each other when being coupled, an issue that entails a big constraint for the railway domain.

In order to overcome these issues, there is the need of a "Functional Distribution" Architecture (FDA) concept for a mixed-criticality embedded Framework, that enables creating an execution environment to:

- Host multiple TCMS application functions
- Ensure strict time/space partitioning
- Provide abstraction from location, underlying network protocols and hardware

# FDA Concept




The Framework, by the use of the "Functional Distribution" Architecture concept, allows executing and monitoring distributed TCMS safe and secure applications and act as an **Abstraction Layer** from:

- Synchronization.
- Communication.
- IO managing.

In order to achieve these goals, it must provide the following **services**:

- Initialization.
- Global clock synchronization.
- Scheduled execution of applications.
- Execution of applications of different SIL.
- Safe local data distribution.
- Safe and secure remote data distribution.
- Transparent IO reading and writing.
- Health-monitoring.
- Remote monitoring.
- Maintenance.

For this mission, Drive-by-Data technology will provide the global time and manage deterministic and best-effort data traffic. This architecture will include a standardized interface (API) supporting a broad set of functions.

# Safe4RAIL

# Functional Distribution Framework

## FDA Framework

### Conceptual view

The FDA Framework or Functional Distribution Framework (FDF) offers its services by the use of a set of logical and physical elements.

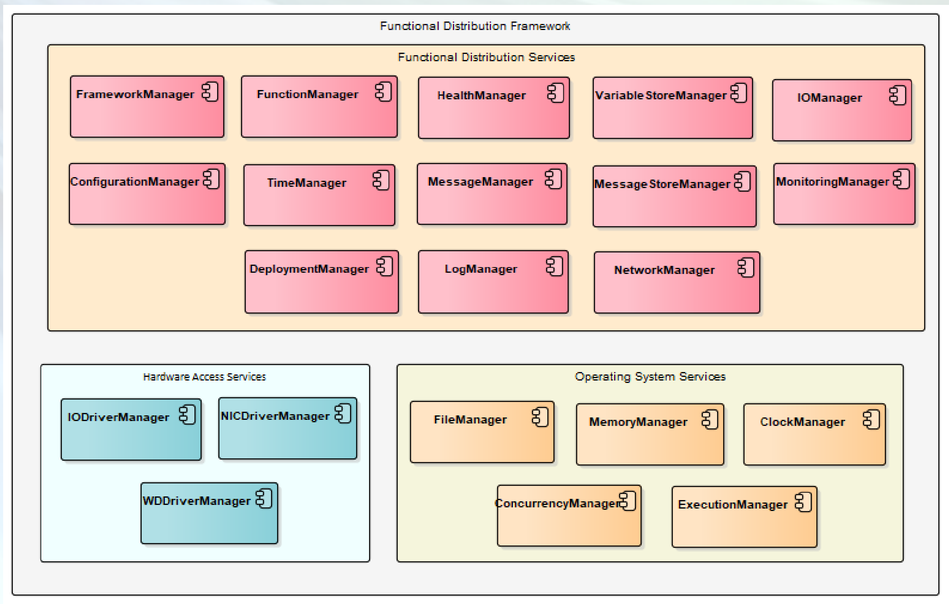
There are three main **logical** elements:

- Function: Schedulable software to execute some logic. It can be a generic FDF service or a concrete app logic provided by the user.
- Variable: Data structure to share information between Functions.
- Message: Data structure to share Variables between remote Functions (Not in same ECU).

On the other side, the **physical** elements are:

- Process: Thread or group of threads with an isolated memory address space (Spatial separation). Functions are executed here.
- Partition: Execution environment with an isolated memory address space and limited execution time (spatial and temporal separation). Processes are executed here.
- Shared Memory: Memory that may be simultaneously accessed by multiple processes. Variables and Messages are stored here.

### Portable architecture




The FDF Functionalities are distributed in three groups of components which facilitate the portability to different solutions. Some components may have different versions for different SILs, which implement the safety mechanisms for that SIL.

- **FDF Services**: The code of these components is portable across different Platforms/OS because the Hardware Access Service and OS Service layers provide well-defined interfaces.
- **OS Services**: These components have the same interface but different implementations for each Platform/OS. They provide either a complete implementation of the services or an adapter to the services provided by the underlying OS.
- **HW Access Services**: These components have the same interface but different implementations for each IO and NIC Hardware. They provide either a complete implementation of the services or an adapter to the services provided by the underlying Drivers.

**Project Coordinator:**
Arjan Geven
TTTech Computertechnik AG
Schönbrunner Straße 7
1040 Vienna
Austria
Tel.: +43 158 5343 4942
Email: arjan.geven@tttech.com

**Contact person for WP2:**
Iñigo Odriozola
IK4-Ikerlan
Pº J. M. Arizmendiarrieta 2
20500 Arrasate-Mondragón
Spain
Tel.: +34 943 71 24 00
Email: iodriozola@ikerlan.es

**Project start:** 1st of October, 2016
**Project duration:** 2 years

This project 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 and Austria, Spain, Germany, Czech Republic, Italy, France. The content of this document reflects only the author's view—the Joint Undertaking is not responsible for any use that may be made of the information it contains.