Software design patterns with safety properties for safer railway applications

Christophe Gransart
Univ Lille Nord de France, F-59000 Lille, France
IFSTTAR, LEOST, F-59650 Villeneuve d'Ascq, France
christophe.gransart@ifsttar.fr

1. The reason for the research

Railways systems must exchange more and more information due to the increase of interactions between a large set of actors. This need is pushed by the automation of operation and the telematics applications deployed for transportation systems. As they are involving safety and non safety related functions, requirement allocated to data exchange must be compliant with safety constraints (SIL). Due to these safety constraints, the current systems are generally developed using proprietary solutions as their compliance with the safety requirements is easier to check. The main problem is that these proprietary solutions are expensive to develop and can limit the evolution of the system during its life cycle. Figure 1 presents an example of a typical distributed application with different levels of SIL. The application needs to exchange information with several ground applications using SIL0 to SIL 4 levels.

![Fig 1: Example of a safety application in the railway domain](image)

The SIRSEC project aims to use middleware commercial based solutions for the distribution of information ensuring the required safety level and to structure by design patterns all the information that will be used to deliver the certification of the solution. This research work wants to bring some answer to the challenge “For an even safer and more secure railway”. The partners in this project are Alstom Transportation, Thalès Rail Signaling Solutions, Geensoft, Prismtech, Serma ingénierie, CEA, IRIT and IFSTTAR (ex INRETS).

Figure 2 presents the scope of the project: It is mainly on middleware layer with data distribution functionalities and common services to offer a common safety API to the applications.
Challenge H: For an even safer and more secure railway

Figure 2: Scope of SIRSEC

This communication layer should transport the messages between the applications according to a quality of service required by the SIL level of the application. As this code is qualified of non functional code, it should be reused between various developments.

2. The methodology

From an information exchange analysis done at system level including SIL 4 requirements, we propose to analyze the design patterns coming from the software engineering and to add to them the safety properties and relationships required.

The work is based on Model Driven Engineering philosophy. The goal of MDE is to improve the development process and the quality of the software produced, MDE is characterised by keywords like modelling, reuse, capitalisation, management of complexity, and the models shared between the development teams can be used to generate automatically programming code. The runtime system is based on software components.

2.1 Study of the development cycle

In classical development, the “V” development cycle is used (Fig 3): from the analysis step, followed by design, implementation, test and validation. There is another “V” cycle (in red on the picture) dedicated to safety aspects of the software. This cycle defines the following steps: safety requirements, safety principles, verification and finally certification [6]. All these steps take a long time and are very costly.
Challenge H: For an even safer and more secure railway

The alternative to this cycle that we are studying is the “Y” cycle where COTS communication and middleware layer should be reused from one project to another one (see Figure 4). The vertical part of the green “Y” is the code reused. We are now studying if we can also reuse some part of the safety cycle (in red). The main goal is to verify and (pre)certify the lowest part once and then reuse it. The code reused is defined as a catalogue of design patterns and runtime communication middleware layer.

Figure 3: “V” development cycle

Figure 4: “Y” development cycle
2.2 Design Patterns

Design patterns [4] are commonly used to simplify the development and coding and reuse of applications. In the project, we are studying such patterns like client/server, publish/subscribe, voting pattern to extend them by adding safety properties and requirements.

The properties that we want to study are for instance: real-time constraints, bandwidth requirements, network architecture or liveness, freshness of data.

2.3 Model Driven Engineering

Our work is based on a MDE (Model Driven Engineering) approach. From an abstract model, we are enriching it by information more and more precise in point of view of the design, implementation, target hardware platform and we transform it through model transformation tools. At the end of the process, we obtain the code for a specific target platform.

Figure 5 illustrates the process for our project. From the software model, we are applying some design patterns to obtain a model with safety patterns constraints. Next, we are fixing the details for the target platform so that at the end, we obtain the code for a specific platform.

3. Communication middleware

For communication COTS, we are reusing a middleware based on the Data Distribution Specification made by the OMG; the middleware is called OpenSplice and made by Prismtech[5]. We think that this kind of middleware is well suited for periodic communications in the railway domain. A solution based on DDS was already tested during the InteGRail project [7].

The DDS (Data Distribution Service) is a specification of a publish/subscribe middleware taking into account QoS properties[1]. This specification has been defined by the OMG during 2004.
The DDS General Architecture

This new service is suitable for a new class of applications that require real-time Quality of service. The DDS features include[2]:

- A vendor-neutral API
- Support for typed interfaces
- Applications developers deal only with native types on each platform
- Provide a strict separation of publisher and subscriber roles
- Optimal efficiency and predictability
- Minimized dynamic resource allocation
- The avoidance of unbounded or hard-to-predict resources
- Minimize data copying
- Control of service behaviour through QoS properties
- Characterize what the system must do, and not how it does it
- Being a service that is complementary to the existing CORBA services
- Suitable for use in Real-Time Systems and other applications that need high volume, robust, fault-tolerant data distribution

The main idea of the DDS specification is that a ‘Global’ Data Store is accessible by applications to read and write data (see Fig 6, 7).

Figure 6: DDS global data store (from[3])

DDS provides flexibility, power and modular structure by decoupling:

- **Application location** through anonymous publish/subscribe
- **Redundancy**. A system can have any number of readers and writers
- **Quality of service**: asynchronous, disconnected, time sensitive, scalable and reliable data distribution
- **Platform and protocols**. Decoupling platform and protocols permits to add more easily existing transport protocols.
4. Conclusion and expected results

We have presented the main ideas of the SIRSEC project: using and reusing communication COTS and middleware, applying a MDE process for the development of safety related applications using generation tool chain from the design to the implementation and developing a catalogue of precertifiable design patterns including safety properties.

From a first deployment in the safety related railway systems, future implementation in other domains related to embedded systems (like automotive) is possible. Development tools proposing specific libraries of safety related Design Patterns would also be available.

Finally, we think that the effort associated to safety activities will be reduced by the automation in the production of the evidences. Quality of the system will be improved due the larger reuse of software components. We propose to use commercial based solutions for the distribution of information ensuring the same safety level and to structure by design pattern all the information (documents, test results, requirements...) that will be used to deliver the certification of the solution. The dossier that will be elaborated from the model will provide all the evidences necessary for the Safety Case. This research work wants to bring some answer to the challenge “For an even safer and more secure railway”.

Acknowledgments

This work is partially sponsored by FUI 7, DGCIS, i-Trans and Systematic competitiveness clusters.

Bibliography

Challenge H: For an even safer and more secure railway


Biography

Christophe GRANSART is full time researcher at IFSTTAR-LEOST. His research interest is on communicating mobile objects: design of middleware solutions dedicated to transportation systems using wireless communications.