PhD by Portfolio

Module 3 Paper

Capstone Project

Niklaus H. König

Swiss School of Business Research

Author Correspondence

niklaus.konig@ssbr-edu.ch, koenig@sreng.ch, Tel. +47 412 61 209

An Advanced Process

for the

Design, Engineering and Development

of High-Assurance Systems

Photo credits: CRRC, BAE, Quora

Table of Contents

List of Figures

List of Tables

1. Introduction

This paper addresses the questions, themes and issues related to the Module 3 Capstone Project in the SSBR PhD by Portfolio programme.

In this paper, the **AIDED© Process** is presented in detail, a new, innovative process for the specification, development, implementation, and commissioning of high-assurance systems. (For the definition of a high-assurance system within the scope of this paper, see section 3.)

The Process has been developed exclusively by the author of this paper, based on over 30 years of experience in the development of complex high-assurance systems in the railway sector.[1]

Although the focus of this paper is the development of high-assurance systems for the railway industry, the AIDED© Process can be applied in any industry developing and delivering high-assurance systems.

In addition to the SSBR Capstone Project, this paper will also serve as a guideline for the implementation of the AIDED© Process in the two companies headed by the author, Swiss Railway Engineering SRE GmbH and SwissRapide AG, both based in Zurich, Switzerland, as well as for other innovative companies in the railway sector.

Extensive online research by the author has not shown any organisation that has publicly posted the application of a process similar to the AIDED© Process presented in this paper. Some of the steps and methods of the Process are used individually by some companies but not as a coherent, holistic process comparable to the AIDED© Process.

[1] All figures and tables in this paper not credited have been developed by the author.

2. Synopsis

Currently, the railway sector is plagued by the high costs, delays in the delivery as well as outdated processes and tools within the scope of the development of high-assurance systems in the industry.

The AIDED© Process addresses these deficiencies in the sector directly and provides a new, innovative approach to the development of high-assurance systems via the following the key elements:

- ✓ Definition and unification of the terms and abbreviations used in a project.
- ✓ Formal modelling of the system based on the international UML/SysML standards.
- ✓ Formal system requirements management linked directly to the formal system model.
- ✓ A complete simulation of the system functionality, driven by the formal system model and the system requirements, before any software code is developed.
- ✓ Automatic software code development based on Artificial Intelligence (AI) tools.
- ✓ Ongoing system validation by the client during the development process.
- ✓ Anchoring of the Process within an Agile Scrum Framework, including the supporting tool(s).

As proposed by Scott D. Anthony in his podcast "*To Reinvent Your Firm, Do Two Things at the Same Time*" (Anthony 2017), the management board of a company implementing the AIDED© Process will require the following key aspects:

- ➢ Courage
- ➢ Clarity
- ➢ Curiosity
- ➢ Conviction

With the implementation of AIDED© Process, companies have the opportunity to rectify the current shortcomings in the sector listed above and achieve a cutting edge for their systems in this highly competitive and lucrative industry.

3. Key Terms and Definitions

The following are key terms and their definitions pertaining to their application in this paper:

Term	Definition
(system) Acceptance	Approval by a National Safety Authority that a system has fulfilled the relevant standards for use in day-to-day operations.
ARTiSAN/KnowEnterprise toolset	ARTiSAN Real-time Studio software tool by PTC for formal system modelling based on UML with the KnowEnterprise add-on by KnowGravity Inc. for ARTiSAN
Capella	An open-source software tool for formal system modelling based on UML/SysML principles
Commissioning	The process of verifying that all systems and equipment in a project are installed and working as specified and can be taken into operation.
High-assurance system	"Critical systems which demand the highest level of quality in their software and hardware applications and components concerning Reliability, Availability, Maintainability, Safety (RAMS) and Security." High-assurance systems fall into the categories SIL 3 and SIL 4 as defined under the term "SIL" below in this table.
Maglev	Magnetic Levitation (trains and systems)
RAMS	Reliability, Availability, Maintainability and Safety Together with "Security", these are the key aspects in the definition of a high-assurance system.
SIL	Safety Integrity Level
Validation	The process of checking whether the system specification captures the customer's requirements. Validation includes activities such as requirements modelling, prototyping and user evaluation. (Arbour Group 2015)
Verification	The process of checking that the software meets the system specification. Verification includes all the activities associated with producing high quality software, i.e.: testing, inspection, design analysis, specification analysis, etc. (Arbour Group 2015)

Table 1. Key Terms and Definitions

4. International Standards for Railway High-Assurance Systems

The following are the key international standards from the railway sector which regulate the processes and methods for the design, specification, development, and commissioning of high-assurance systems:

1. CENELEC EN 50126-1:2017, Part 1: Generic RAMS Process (CENELEC EN 50126-1:2017)
    - Description of the RAMS process for the specifications, development and acceptance of electronic high-assurance systems for railway applications.
2. CENELEC EN 50126-2:2017, Part 2: Systems Approach to Safety (CENELEC EN 50126-2:2017)
    - Description of measures to ensure the required safety level within the context of the specifications, development, and acceptance of electronic high-assurance systems for railway applications.
3. CENELEC EN 50128:2011, Software for railway control and protection systems (CENELEC EN 50128:2011)
    - Description of processes and measures for the development of software within the context of the specifications, development, and acceptance of electronic high-assurance systems for railway applications.
4. CENELEC EN 50129:2018, Safety-related electronic systems for signalling (CENELEC EN 50129:2018)
    - Description of the requirements as well as the safety acceptance process for the specifications, development, and acceptance of electronic high-assurance signalling systems for railway applications.
5. CENELEC EN 50159:2010, Safety-related communication in transmission systems (CENELEC EN 50159:2010)
    - Description of the classification, threats, and requirements for defences for transmission systems within the context of railway applications.

Although these are European standards, they are generally applied for high-assurance systems in major railway projects around the globe.

One of the key parameters defined in the CENELEC EN 50126-1:2017 standard (CENELEC EN 50126-1:2017) is the Safety Integrity Level (SIL), which is illustrated in the following table:

Railway (CENELEC EN 50126-1:2017)	Failure Impact
SIL 4	Catastrophic (10 to hundreds of deaths)
SIL 3	Hazardous/Severe (1 to 10 deaths, severe damage to property)
SIL 2	Major (Major damage to property)
SIL 1	Minor (Minor damage to property)
SIL 0	Not applicable

Table 2. Safety Integrity Levels according to CENELEC EN 50126-1:2017

The determination of the Safety Integrity Level required by a system for operations is one of the key steps before starting the specification and development of the system. The SIL sets the requirements for which methods and processes will need to be applied during the development of the system in order to achieve system acceptance for operations.

Photo Credit: IVU Traffic Technologies

Figure 1. Advanced Railway Control Centre

5. High-Assurance Systems

For the purposes of this paper, high-assurance systems are defined as follows:

> "*Critical systems which demand the highest level of quality in their software and hardware applications and components concerning Reliability, Availability, Maintainability, Safety (RAMS) and Security.*"

In terms of the Safety Integrity Level (SIL) listed in section 4, systems evaluated to be developed based on SIL 3 or 4 are considered to be high-assurance systems.

The SwissRapide Maglev Train Management and Safety (MTMS) system (see (Koenig 2024)) required in all SwissRapide Maglev rail projects, such as the "Alberta Ultra-Highspeed Maglev Rail Project Calgary-Edmonton" (Koenig 2023), has the following major functions:

- Has a direct radio communication link with each Maglev train on the Maglev network.
- Controls the exact position of all Maglev trains on the Maglev network.
- Steers the path of where each train is to go based on the scheduling application within the MTMS.
- Controls the speed of each train.
- Ensures that trains do not collide with other trains or other vehicles on the Maglev guideway systems, for example, maintenance tractors.
- Handles conflicts in track occupation in case trains are delayed or defect.

Based on these critical functions, the SwissRapide MTMS is a SIL 4 system according to the CENELEC EN 50126-1:2017 standard (CENELEC EN 50126-1:2017) and thus is by definition a high-assurance system.

The following are some further examples of high-assurance systems:

- Avionics fly-by-wire and engine control systems
- Railway signalling and train control systems
- Nuclear power plant core control systems
- Chemical plant core control systems

Photo Credit: Daily Mail

Figure 2. Crashes of the Boeing 373 Max caused by a high-assurance system's defect.

Photo credit: AP/Vaggelis Kousioras

Figure 3. 2023 Train crash in Greece caused by bypassing a high-assurance system.

The following is a selection of major international companies who have the design and development of high-assurance systems at the core of their business:

Company	Sector
Airbus SE	Aerospace
Alstom SA	Railway
BASF	Chemical plants
Boeing Corporation	Aerospace
Bombardier	Aerospace
BP p.l.c.	Petrochemical plants
Dow Chemical Co	Chemical plants
Framatome, France	Nuclear power plants
GE Hitachi Nuclear Energy	Nuclear power plants
Hitachi Rail	Railway
Lockheed Martin Corporation	Aerospace
Shell	Petrochemical plants
Siemens	Railway
Thales	Aerospace
Toyo Engineering Corporation, Japan	Petrochemical plants
Union Carbide Corporation	Chemical plants
Westinghouse Electric Company	Nuclear power plants

Table 3. Selection of International Companies developing High-Assurance Systems

6. Conventional High-Assurance System Development Process

In order to better understand the benefits of the AIDED© process, the following is an overview of the conventional process for the development of high-assurance systems, including methods and tools currently used by railway organisations and supply companies in in the railway sector in Europe, based on the author's experience in the field.

Principally, the railway organisations and supply companies are obligated to follow the process prescribed in the standards listed in section 4. Of these, the key process is the system development based on the V-model from the (CENELEC EN 50126-1:2017) standard, shown below.

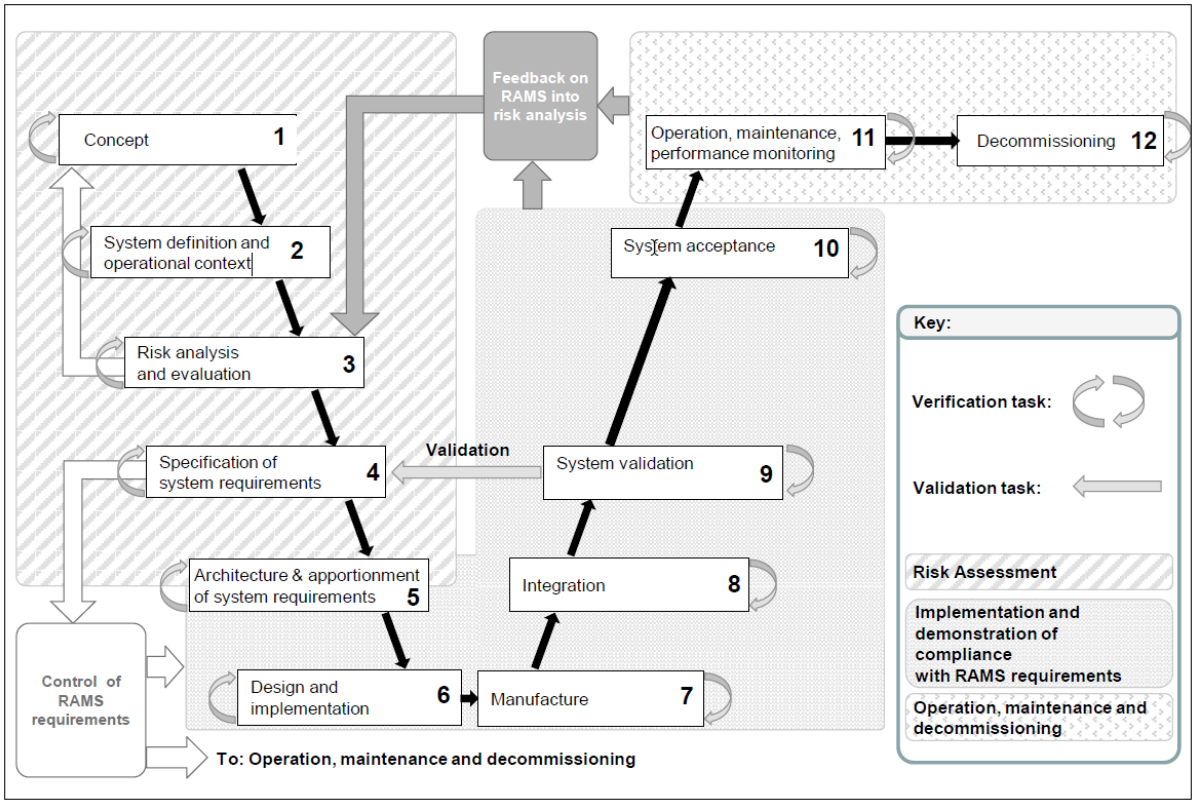


Figure 4. System development V-model from the (CENELEC EN 50126-1:2017) standard

Although the V-model and the corresponding requirement in the standards listed in section 4 are useable for high-assurance system development, in real life the overall process has a number of weaknesses and shortcomings:

- Although the standards suggest a number of methods to be used for high-assurance system development, it does not prescribe in detail how the methods are to be applied. This in turn leads to a great deal of ambiguity in the interpretation of the standards.
- Railway organisations often do not supply all of the documents required by the standards to the supply companies, thus making it difficult for the supply companies to follow the processes prescribed in the standards. The following are some examples:
    - When system requirements exist, they are often in the form of highly ambiguous textual requirements.
    - In some cases, the requirements are delivered in a Word-based, descriptive document rather than a clear set of formal requirements.
    - Some railway organisations still use Excel spreadsheets for the management of their high-assurance system's requirements.
    - Railway organisations often do not supply the operational rules and regulations pertaining the high-assurance system to be developed.
    - Railway organisations often do not deliver the Preliminary Hazard Analysis to the supply companies, as is prescribed as mandatory in the standards.
- Thus, system software development is often started without a precise and validated set of the client's respectively the end-user's requirements and without clear information concerning the operational rules and regulations pertaining to the system under development.
- Railway organisations and supply companies generally do not define a standardised glossary of terms and abbreviations within the scope of high-assurance systems development.
- The V-model foresees only one client validation step between process steps 9 and 4 in Figure 4 on the previous page. This means that the system development has been fully completed before the client can validate that the system actually meets the needs of the end-user.

- This in turn results in a significant number of software development iterations and releases are required in order to:
    - Fix the defects (bugs) in the software and system design.
    - Change or augment the system functionality until it satisfies the needs of the client respectively the end-users.
- Even after several years of operation, software bugs and functional deficiencies are still present in the system or application.
- Based on the author's experience as railway consultant, most railway supply companies developing high-assurance systems will use:
    - A software tool for managing textual requirements
    - A software tool for creating diagrams
    - A software tool for some simplified system modelling
    - A software tool for document management
    - A software tool for system software defect management
    - A software tool for project task management

  However, these tools are frequently used independently from one another, by different teams and without interfaces between the tools, and often without a clearly defined, coherent process in the system development life-cycle.
- The development time of high-assurance systems, from concept to system acceptance, ranges between 7 to 10 years.
- For each new client respectively for each new project, the system specification and development process is started from scratch, with little to no reuse from a previous project or system development.
- Cost overruns for the development of complex, high-assurance systems in the railway sector often range between 50% and up to 200%.
- There has been little progress in the field of software and system development, many of the supply companies still carry out the design and development of high-assurance systems in much the same manner as they did 20 to 30 years ago.

7. Overview of the AIDED© Process

In order to mitigate the many shortcomings of the conventional high-assurance systems development process, the innovative Advanced Integrated Design, Engineering and Development (AIDED©) process has been developed by the author of this paper. This new process is based on over 30 years of experience in the design, specification, development, commissioning, and acceptance of high-assurance systems in railway organisations and supply companies around the globe.

One of the key principles of the AIDED© process is:

"***Get it right the first time!***"

In a nutshell, this means that the high-assurance system is:

- Specified formally in detail, including all interface specifications.
- The formal system specification is validated by the client on an on-going basis.
- The system software code is developed via AI directly from the formal system specification.

The AIDED© process will be applied by SwissRapide AG for the development of the Maglev Train Management and Safety (MTMS) system.

Photo credit: Shanghai Maglev Transportation Development Co.,Ltd.

Figure 5. Shanghai Maglev Train Control Centre

The diagram of the following page provides an overview of the AIDED© process for the design, development, commissioning, and acceptance of high-assurance systems.

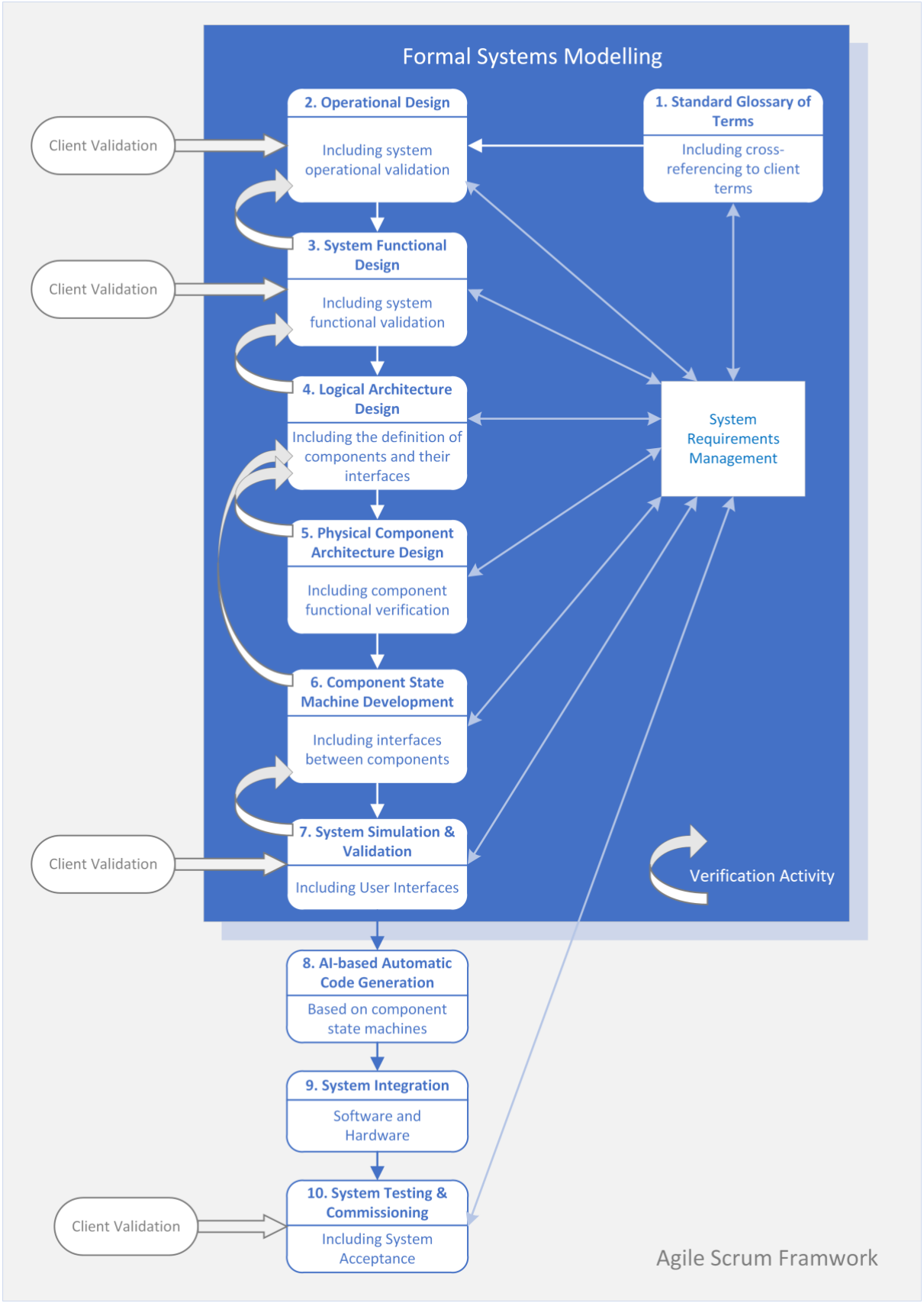


Figure 6. Overview of the AIDED© Process for High-Assurance Systems Development

The following are the key features of the AIDED© process:

- The operation of the system and its operational environment is defined by formal operational modelling and is validated by the client respectively the end-user.
- System functionality, based the operational modelling, is defined unambiguously in a formal system model and is validated by the client respectively the end-user.
- System respectively client requirements are linked to the formal system model, allowing automated verification of both the system model and the system requirements.
- Component and application functionality is defined unambiguously in a formal component/application model, based on the system model and the system requirements, and can be verified automatically within the model.
- A complete simulation of the overall system functionality is provided by the system simulation based on state diagrams developed in the model, which in turn are based on the formal component/application model and the system requirements.
- The overall system functionality is validated by the client respectively the end-user based on the system simulation before a single line of software code is developed.
- The software is developed automatically within hours via an AI-based system, based on the state diagrams in the model, which have been validated by the client via the system simulation.

  This eliminates human errors in the software and the addition of unnecessary functions by software developers in the software development process.
- No functional testing at component/application level is necessary.
- Only basic functional testing at system level is necessary in order to ensure that the software has been correctly integrated into its hardware and operational environment.
- System testing by the client within the commissioning process is highly simplified since the client has fully validated the system functionality at regular intervals in the AIDED© process (see Figure 6).

The following are some of the major advantages of the AIDED© process compared to the conventional high-assurance systems development processes:

- ✓ The development time of a high-assurance system, from concept to system acceptance, is reduced from 8-10 years to between 3 to 4 years.
- ✓ System development costs are significantly reduced by eliminating:
  - Corrections to the system specification after software development (a standard practice in the railway industry).
  - Repeated corrections to and releases of the system software for "bug" fixes as well as omitted or false system functions.
  - The costly effort for component and system re-testing, re-commissioning, and system re-acceptance activities.
- ✓ The client validation of the system specification and development is an ongoing process (see Figure 6), rather than a one-time step at the end of system development, as is the case in the conventional V-model for high-assurance system development (see Figure 4)
- ✓ System verification activities are automated in the model, thus reducing costs for manual verification.
- ✓ Reusability: The complete system model can be reused for other clients who have different functional needs (standard in the railway industry) by creating a copy of the model and adapting the functionality to the client's needs.
- ✓ Since project documents are generated automatically from the system model:
  - A high quality and consistency of the documents is guaranteed.
  - The high costs for document development typical in the development of high-assurance systems can be significantly reduced.
- ✓ The AIDED© process complies fully with the methods and processes prescribed in the international standards for railway high-assurance systems listed in section 4.
- ✓ The significant cost and time reductions achieved by the AIDED© process makes the company's high-assurance system product highly competitive in the market.

8. Formal System Modelling

In addition to the AIDED© Process principle "Get it right the first time" introduced in section 7, a further principle of the Process is:

"***The unification of methods and tools for the development of high-assurance systems***"

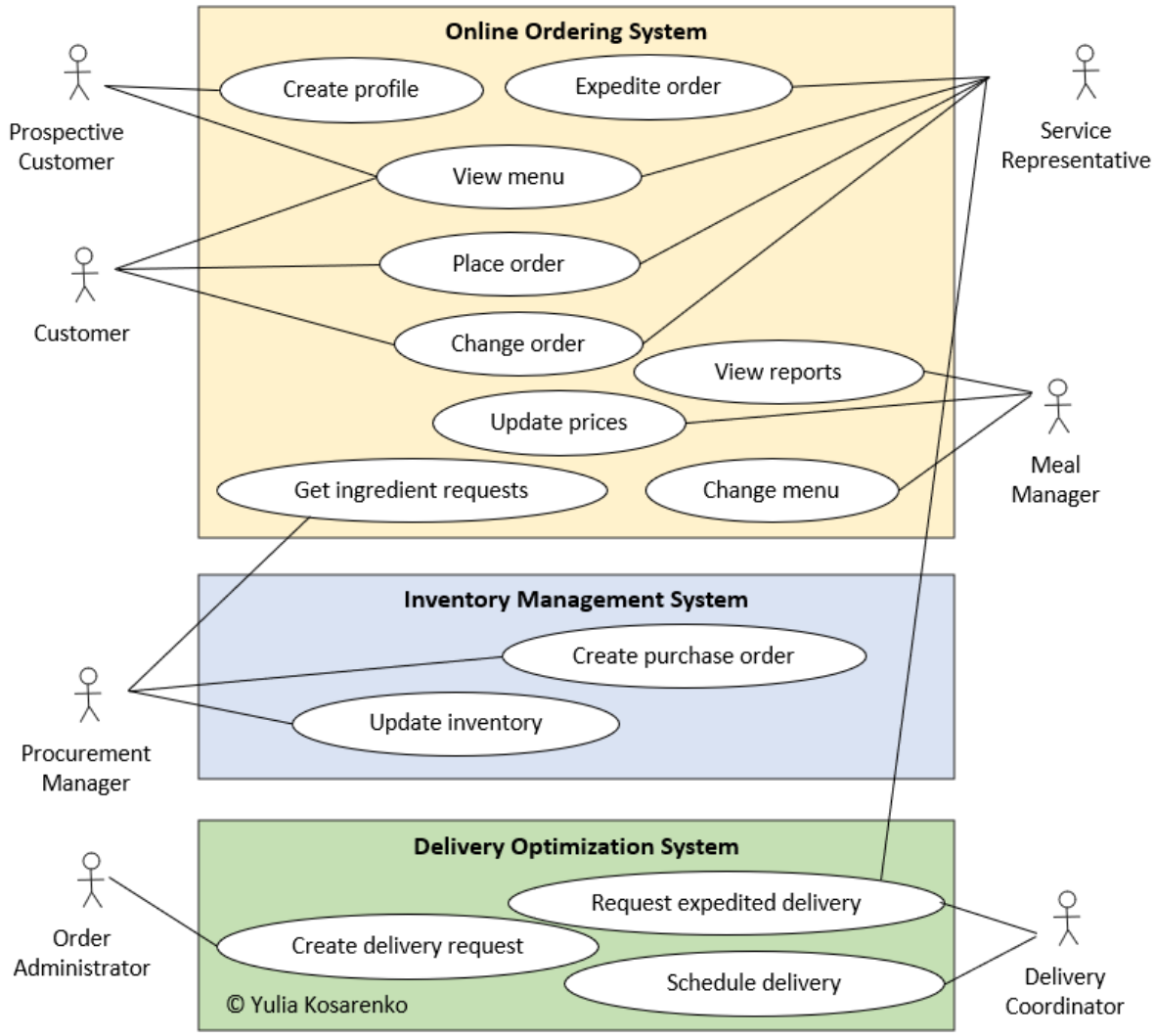
This is primarily to be achieved by applying **formal system modelling**, based on Model-based System Engineering (MBSE) principles, in steps 1 to 7 illustrated in Figure 6 (including System Requirements Management). The methods are based on the international Unified Modelling Language (UML) and the Systems Modelling Language (SysML) standards, and all modelling and requirements management is carried out in a **single software tool**.

The advantages of applying formal systems modelling in the AIDED© Process has the following advantages (based on (MSc-IT Study Material 2011)):

- The models developed provide a precise pictorial representation of the operations and functionality of the system, thereby providing the basis for detailed communication between the systems developers and the client concerning how the system will perform.
- In addition to visualising individual functions and their interdependencies, each object in the model can be enriched with a myriad of information related to the object, the relationship to other objects or functions.
- Any given object can be reused in any number of modelling diagrams. Any change, improvement, or addition of information to an object is automatically updated in all diagrams where the object is used. This provides a high level of consistency throughout the model, a key factor for highly complex systems.
- Any individual model manages complexity through abstraction, individual functions can be modelled in detail by concentrating on one aspect of the system, leaving other aspects of the system to be modelled separately.
- Models impose formal structure on the information, providing a clear and concise representation of functions and their interrelationships.
- The techniques by which models are constructed assist in highlighting areas where the specification or analysis of a function may be incomplete, incorrect or inconsistent.
- The specified system functionality can be validated by the client in detail on an on-going basis based on the model diagrams.

- The state diagrams developed within the model can be used directly for the automatic AI software code generation for the system.

The following is an example of a UML Use Case Diagram, illustrating an end-to-end online ordering process involving three systems and the corresponding actors in the process:



Credit: Why Change Consulting/Yulia Kosarenko

Figure 7. Example of a Use Case Diagram in UML

For the specification of the high-assurance systems required within the scope of the company's Maglev rail projects, it is foreseen by SwissRapide AG that the formal modelling within the scope of the AIDED© Process will be realised by the implementation of the following UML-based toolset:

- ARTiSAN Real-time Studio by PTC
- KnowEnterprise add-on for ARTiSAN by KnowGravity Inc.

The ARTiSAN/KnowEnterprise toolset for formal systems modelling has the following features:

- All **project terms and abbreviations** are managed within the system model.
- All **system requirements** are managed within the system model.
- All **document text elements and diagrams external to the model** are managed as objects within the system model.
- All **project documents** are generated automatically out of the system model, i.e. no project documents are written by hand. The generated documents include but are not limited to:
    - A title page
    - A document approvals section
    - A history of the document
    - A table of contents, including hyperlinks to each section in the document
    - A list of figures, including hyperlinks to each figure in the document
    - A list of tables, including hyperlinks to each table in the document
    - A glossary of all terms and abbreviations used in the document.
    - All terms and abbreviations are highlighted and hyperlinked to the glossary of terms and abbreviations.
    - A listing of all reference documents
    - An index with all terms and abbreviations used in the document.

Based on the author's experience, a 40-page, perfectly formatted document with the aforementioned content can be developed from scratch within 3 to 4 hours. The automatic document generation time for a 40-page document is about 10 minutes.

An example of this is the "*SwISS-S V1.2 Spezifikation Layer 1-5*" document in Annex 3. All text elements, chapter sections, diagrams, tables, terms and abbreviations, reference documents, etc. are contained in the SwISS model in the ARTiSAN/ KnowEnterprise toolset.

This means that any of these elements only needs to be developed once within the model and then can be reused by any other project document requiring that element. Any update to an element (e.g. a version update of a reference document) is automatically updated in all documents using the reference.

9. Details of the AIDED© Process

The following sections provide details of the AIDED© Process and how this unification will be accomplished. The following sections correspond to the individual steps in the AIDED© Process as illustrated in Figure 6.

9.1. Standard Glossary of Terms and Abbreviations

One of the most important steps in the AIDED© Process is the development of a standard glossary of terms and abbreviations at the start of a project.

The Project Management Institute's report on "The Essential Role of Communications" in projects (Project Management Institute 2013) revealed that companies risk approximately $135M for every $1 billion spent on a project. A startling $75M of that $135 million (which translates to approximately 56%) is at risk due to ineffective communications. As an example, a company that the author has consulted for uses over 300 abbreviations in the development of their high-assurance systems, without providing a standardised glossary for the definition of the abbreviations.

Accordingly, communication has the power to spell either the success or failure of a project.

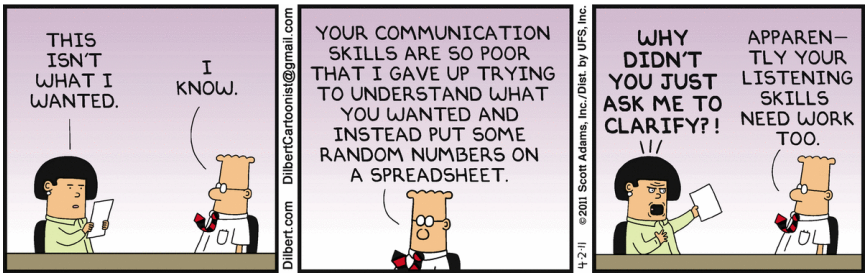


Figure 8. Communications Skills: Dilbert 2011

With the scope of high-assurance systems development, the importance of having a standardised glossary of terms and abbreviations cannot be overstated.

A good example of this was the SwISS project that the author led under contract with the Swiss Federal Railways (SBB). For 10 years, a team at SBB had been trying to specify a standardised, IT-based (FAP) interface between high-assurance systems, without success.

The author's company, Swiss Railway Engineering SRE GmbH, together with a partner company was then contracted by the SBB to carry out the specification work. In the initial phase of the project, it was revealed that SBB employees used the key term "FAP" with no less than 12 different meanings. Owing to the development of a standardised glossary of

terms (among others), the contracted group was able to deliver the specifications for two different high-assurance system's interfaces within three years of project start.

9.2. Operational Design

Another innovation and a key in the AIDED© Process is the development of a **formal model for the operational environment** in which the high-assurance systems under development is to be operated.

The following is an example of some of the operational environment modelling in UML/SysML for a railway Traffic Management System (TMS):

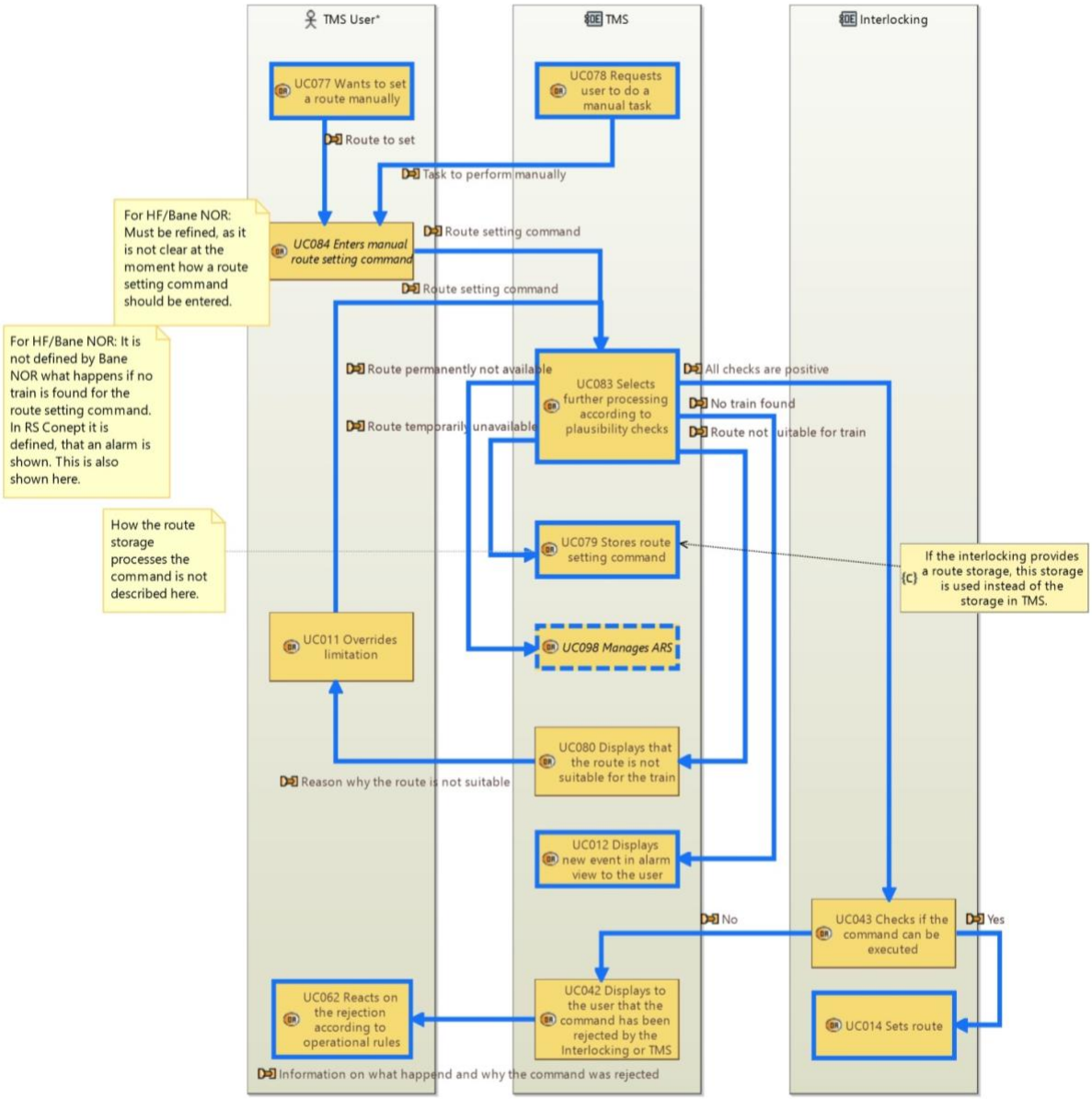


Figure 9. Example of Operational System Modelling in UML/SysML

The following are some of the key advantages of operational system modelling:

- The operational environment and the interfaced systems are defined formal system model before work on the functional design is started.
- The roles and actions of all actors related to the system are defined.
- Since the AIDED© Process also prescribes that the operational system modelling be validated by the client (see Figure 6), the operational scope and interfaces are then fully collaborated with the client before starting the development of the system functional design.

An example of what happens when the operational environment of a high-assurance system is not defined is the development of the European Train Control System (ETCS). The intention of ETCS was to provide the European railways with a new, standardised signalling and train control system, with the aim to:

- Ensure interoperable train operation across national borders, and
- Significantly reduce costs for new train signalling systems.

However, the International Union of Railways (UIC), who lead and financed the development of the ETCS specification, never specified the operational rules and regulations or the operational environment for the system. As a result:

- Each railway ordered the system with a different, unique set of operating rules, thus requiring that supply companies develop a different ETCS functionality for each railway ordering the system.
- In some cases, such as at the SBB in Switzerland, even different ETCS projects within the country defined different operating rules.
- The true interoperability of trains between borders is not given since train drivers must be exchanged at the border, e.g., since Swiss train drivers are not familiar with the German or Italian ETCS operating rules.
- The ETCS on-board equipment and the corresponding infrastructure systems (e.g., the Radio Block Centre controlling train movements) are not standardised.
- Only two of the over 20 interfaces in the system are standardised.
- The factors above have led to soaring costs to the railways when procuring the new ETCS systems.

9.3. System Functional Design

In the next step of the AIDED© Process, the overall system functionality is defined via the development of a **formal functional model** of the system.

The aims of the formal functional model are to:

- Define the overall white-box functionality of the system under development and model this in the formal system model.
- Define the functionality and exchange of information at the interfaces to the external systems.
- Validate the overall system functionality and interfaces with the client.

The following is a definition of the **white-box functional model** of a system:

> "White-box models are the type of models which one can clearly explain how they [the systems] behave, how they produce predictions and what the influencing variables are." (Tannam 2019)

The development of the formal system functional model is based on two key inputs:

1. The formal modelling of the operational environment completed in step 2 of the AIDED© Process.
2. The formal system requirements, either
    - supplied by the client in the Customer Requirement Specification (CRS), or
    - developed within the model based on the formal model of the operational environment completed in step 2 of the AIDED© Process and augmented with the development of additional requirements based on the formal system functional model.

In the AIDED© Process, the formal system requirements are then linked directly with the formal functional model of the system, a novum for the railway sector, and an invaluable advancement for the validation of the system functional model by the client.

The following is an excerpt from the formal functional model in UML/SysML of a high-assurance system, including the linking of the system requirements (on the right) with the system functions (in green):

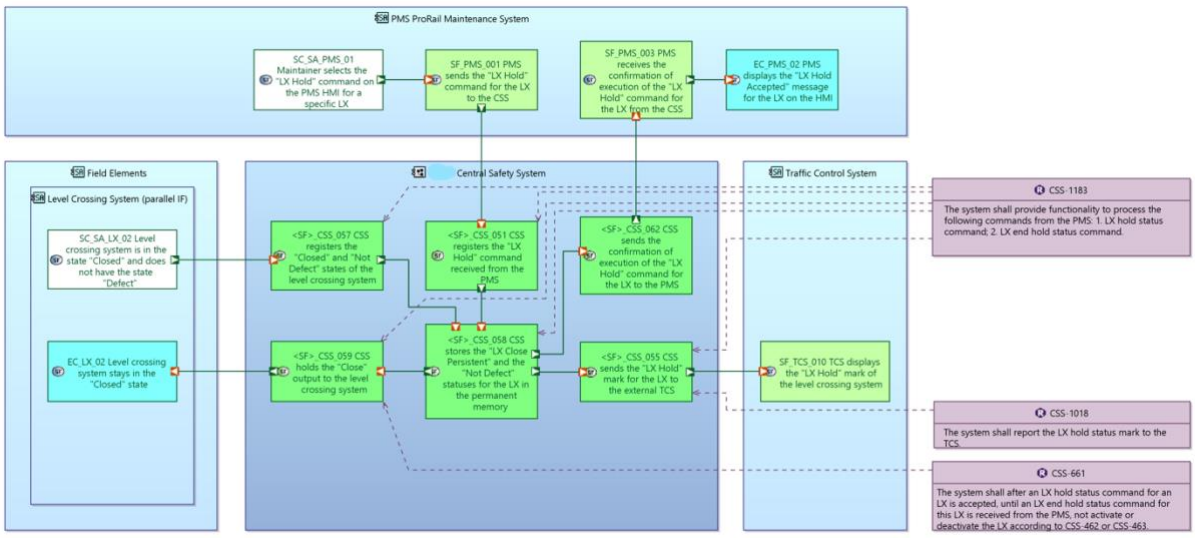


Figure 10. Formal System Functional Model in UML/SysML with Requirements Linking

It is important to note that the detailed formal functional modelling of a system in the AIDED© Process is an innovation for the railway sector, as well as in other sectors implementing high-assurance systems. Based on the author's experience as an expert in this field, most system functional modelling has been carried out as an academic exercise on systems **already existing**, but not in defining a **new system** to be developed.

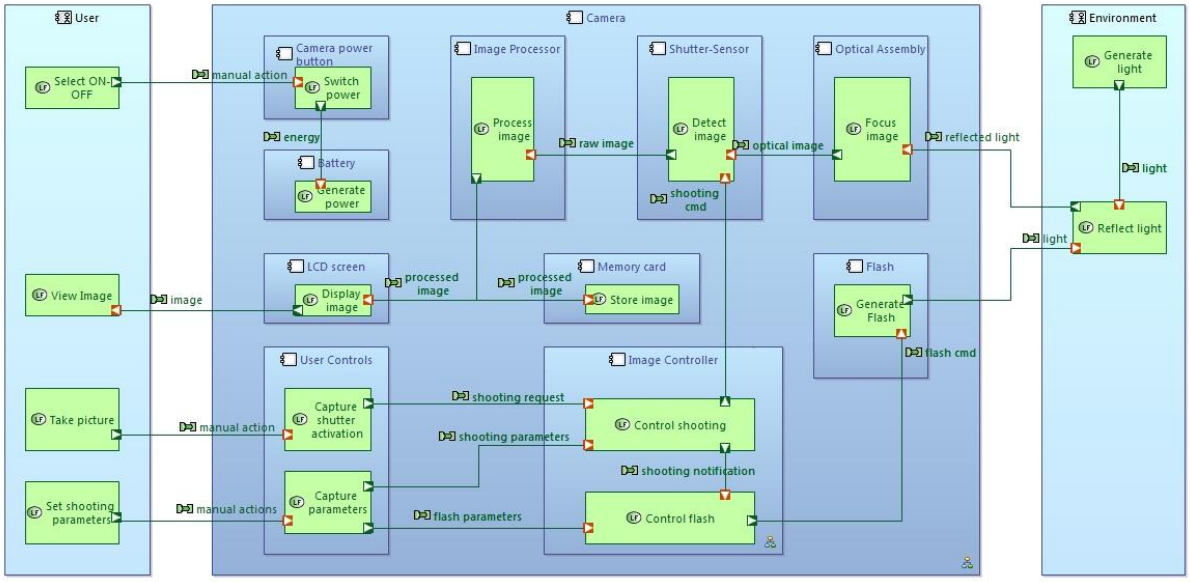
9.4. Logical Architecture Design

The main aims of step 4 “Logical Architecture Design” in the AIDED© Process are to:

- Define the internal logical (functional) architecture for the logical components within the system in the formal system model.
- Define the detailed functionality of each logical components as well as each interface between logical components in the formal system model.
- Allocate the formal system requirements from step 3 to the logical components respectively to the appropriate functional objects in the subsystems of the formal system model.
- Develop detailed System/Subsystem Specification (SSS) requirements for each logical components based on the functionality modelled.

The following is a (simplified) example of the logical architecture model of a digital camera, including:

- The internal logical components (e.g., “Image Processor”)
- External systems and actors (e.g., “User” and “Environment”) and their interfaces to the system (Camera)
- The functions respectively functional objects of each logical component (in green)
- The functional interfaces between the logical components (e.g., “raw image”)



Credit: mbse-capella.org

Figure 11. Example of a Formal Logical Architecture Model in Capella

In addition, the SSS requirements are then linked to the functional objects within the logical components in the formal logical architecture model of the system. The following is an example of the requirements linking, with the appropriate requirements listed on the right side of the diagram:

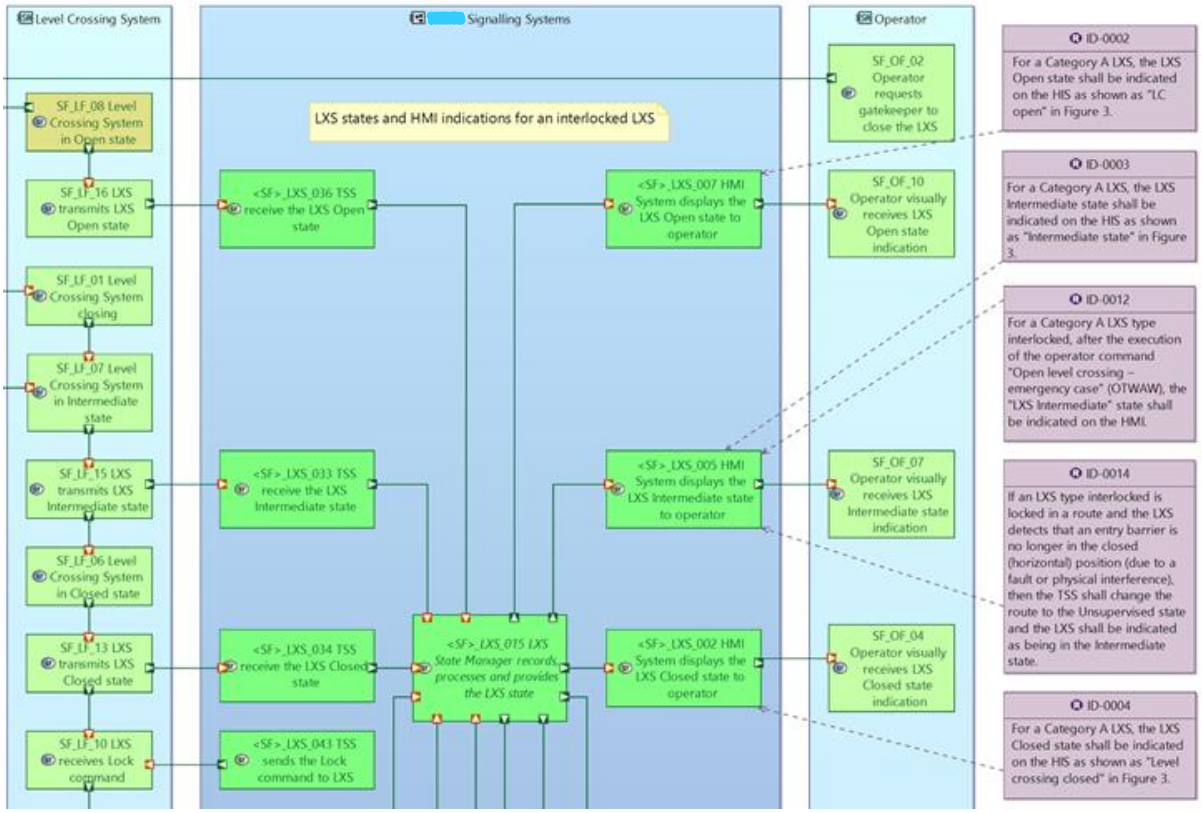


Figure 12. Example of linking SSS Requirements with Functional Objects in the Model

The **verification** of the formal logical architecture model (as per Figure 6) can be carried out **automatically** (instead of manually) by the UML/SysML tool used, since the system requirements from step 3 of the AIDED© Process are linked directly to the logical components respectively the functional objects of the logical architectural model in step 4.

Based on this, the UML/SysML tool can automatically verify that all system requirements have been covered by at least one function in the logical architecture model.

9.5. Physical Component Architecture Design

The main aims of step 5 “Physical Component Architecture Design” in the AIDED© Process are to:

- Define the structure of the **physical components of the system** in the formal system model.
- Where relevant, define the specific **software applications** required within the system components in the formal system model.

  Id est, in the past in the railway sector, each logical component (step 4 of the AIDED© Process) was implemented on its dedicated hardware. In recent years, the move has been to run a number of the logical components as software applications on a server platform (see Figure 13 below).
- Allot the logical components from step 4 of the AIDED© Process to the physical components of the system respectively to the specific software applications in the formal system model.

  With this, the detailed system functions developed in step 4 are **automatically allocated** to the logical components respectively to the specific software applications in the formal system model.

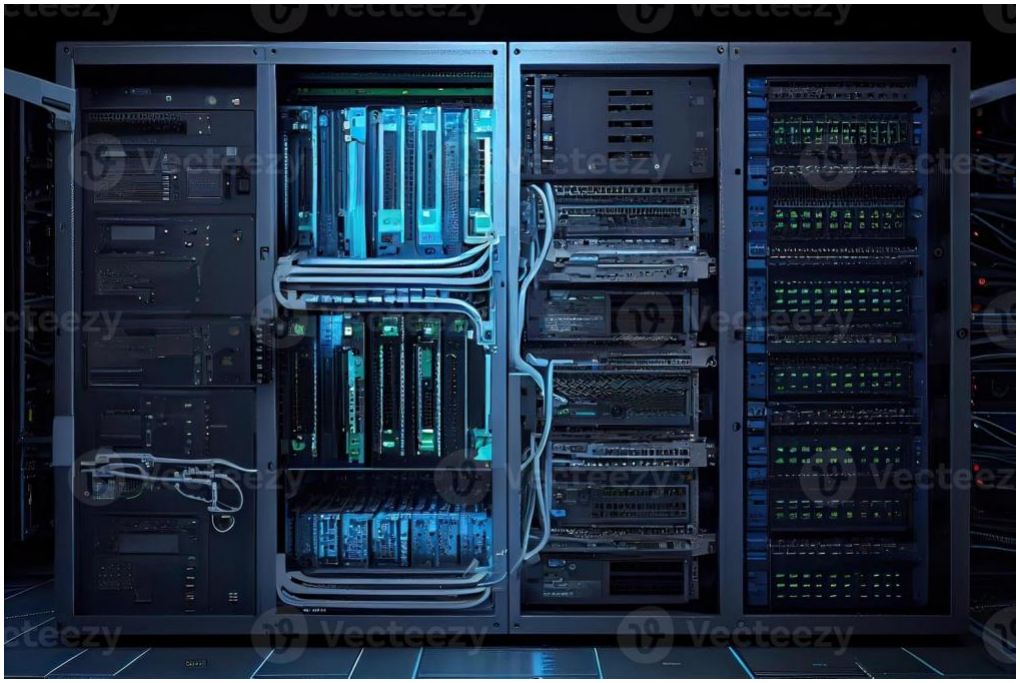
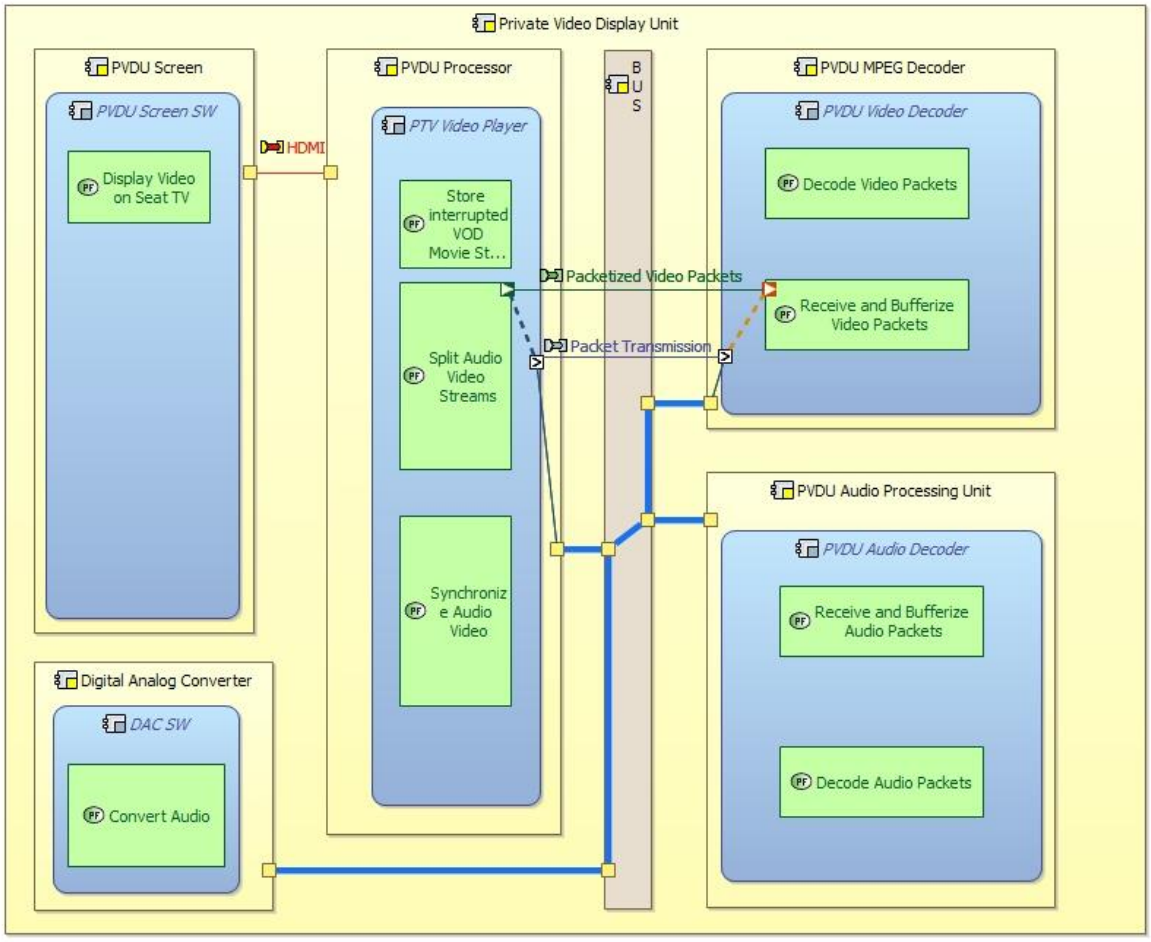


Photo credit: Vecteezy

Figure 13. Example of a Server Array Running a Number of Software Applications

The following is a (simplified) example of the physical component architecture model of a video display unit, including:

- The internal physical components (in this case, microchips) in yellow (e.g., “PVDU Processor”)
- The logical components (in blue), allotted to the appropriate physical components.
- The functions respectively functional objects of each logical component (in green), implemented in the appropriate physical component.
- The physical interfaces between the physical components (e.g., “Packetized Video Packets” via the bus)



Credit: mbse-capella.org

Figure 14. Example of Physical Component Architecture Design in a System Model

The **verification** of the physical component architecture model (as per Figure 6) can be carried out **automatically** (instead of manually) by the UML/SysML tool used, since the logical components respectively the functional objects from step 4 of the AIDED© Process are linked directly to the physical components in step 5.

9.6. Component State Machine Development

Based on the physical component architecture modelling in step 5 of the AIDED© Process, in step 6 the state machines (also known as "state diagrams") are developed:

- For each component and its functions
- For the interfaces between components
- For the interfaces to external systems and actors

The state machines in step 6 are the basis for the following:

- ➢ The system simulation in step 7 of the AIDED© Process.
- ➢ The component software is developed automatically via an appropriate AI tool directly from the state machines in the system model.

The following is an example of a state machine from the SwISS system model in the ARTiSAN/ KnowEnterprise toolset (see Annex 4).

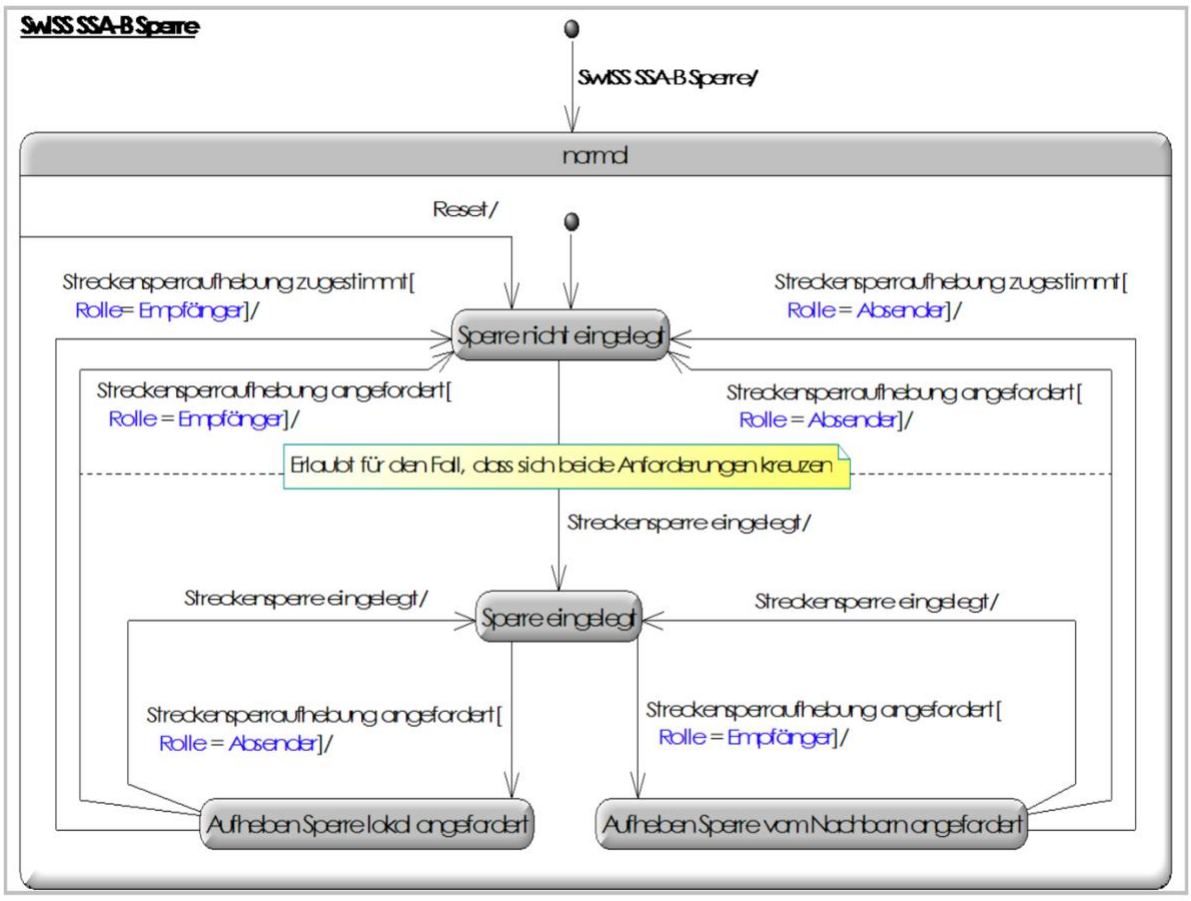


Figure 15. Example of a State Machine from the SwISS System Model

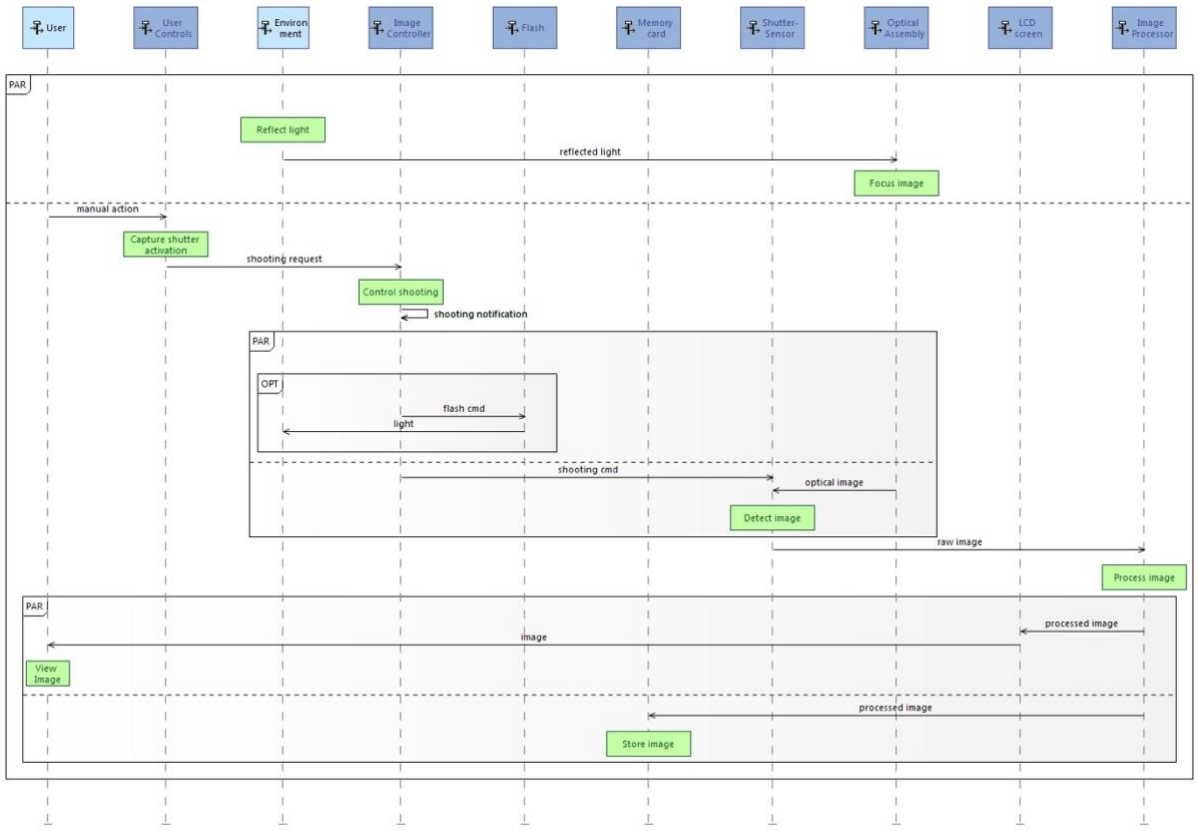
A key factor of the AIDED© Process is that the **detailed system functions** developed in step 4 “Logical Architecture Design” of the Process are **linked directly** to the state machine implementing the function.

Based on this, the UML/SysML tool can **automatically verify** that all system functions listed in the logical architecture model have been implemented by one or more state machines in the system model. The automatic verification contributes to significantly reduce the manual work required in for verification (reducing development time and costs) and also simplifies the system acceptance process.

If **timing constraints** are an issue in the development of a high-assurance system, sequence diagrams can be developed in the system model parallel to the development of the state machines in step 6 of the AIDED© Process.

Sequence diagrams enable both the visualisation of timing constraints as well as support in the detection of timing constraints not previously considered.

The following is an example of a sequence diagram in the system model of a digital camera, including considerations coming from the external environment and actors.



Credit: mbse-capella.org

Figure 16. Example of a Sequence Diagram in the System Model of a Digital Camera

9.7. System Simulation & Validation

Step 7 of the AIDED© Process is the simulation of the overall system and its interfaces to external systems and actors.

The system simulation is linked directly to and run from the state machines developed in the system model in step 6 of the process. As far as possible, the user interface (UI) for the simulation should reflect the system once it is implemented and in operation.

The system simulation has two major objectives:

- To **verify** that the detailed system functions developed in step 4 of the AIDED© Process have been correctly implemented in the state machines from step 6.
- To enable the client respectively the user to **validate** the system functionality (see Figure 6) in detail before any software code is developed or hardware is implemented.

The system simulation in the AIDED© Process is a type of Digital Prototyping (see (Wikipedia Digital Prototyping 2023)), enabling companies to visualise and validate the final high-assurance system before any software code for the system is developed.

With the ARTiSAN/ KnowEnterprise toolset, the simulation is implemented directly in the toolset and is run from the state machines in the system model. The following is an example of the GENERIS system simulation of a complex high-assurance train control system in the ARTiSAN/ KnowEnterprise toolset from the European Euro-Interlocking Project, founded and managed by the author (see Annex 5).

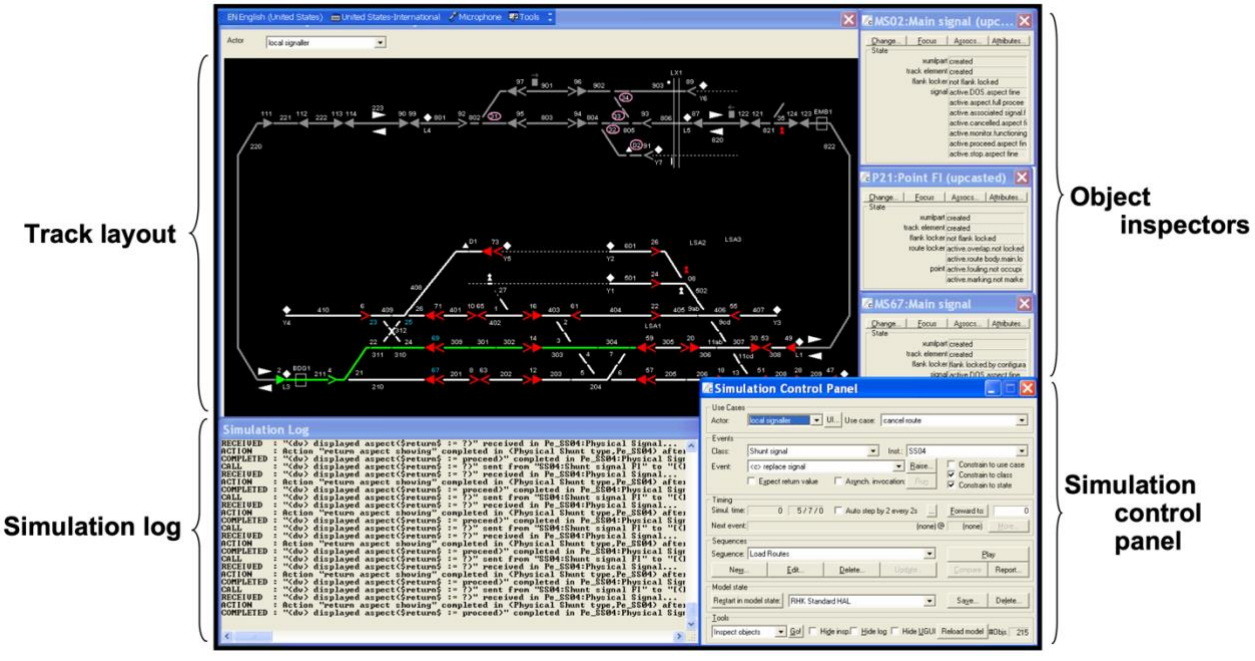


Figure 17. Example of the GENERIS System Simulation and User Interface

9.8. AI-based Automatic Code Generation

Once the system functionality has been fully verified and validated via the system simulation in step 7 of the AIDED© Process, in step 8 the software code for each of the components is generated **automatically** by an appropriate AI system.

Since UML-based modelling tools such as the ARTiSAN/ KnowEnterprise toolset have a **standardised data format** for the export of model information, the data from the state machines developed in step 6 can be read directly by an AI system to generate the software code for each component automatically.

Photo credit: Shutterstock

Figure 18. AI generated software code represents a revolution for high-assurance systems

A listed of the current most frequently used AI tools for the automated generation of software code include the following:

- GitHub Copilot
- PolyCoder (Open-Source Code Generator)
- OpenAI Codex
- Tabnine
- Mutable.ai

The choice of AI tool to be used depends on the needs of the project and must be analysed together with the UML/SysML tool provider for the optimal choice.

9.9. System Integration

In Wikipedia, system integration is defined as follows (Wikipedia System Integration 2023):

> "*In engineering the process of bringing together the component sub-systems into one system (an aggregation of subsystems cooperating so that the system is able to deliver the overarching functionality) and ensuring that the subsystems function together as a system, and in information technology as the process of linking together different computing systems and software applications physically or functionally, to act as a coordinated whole.*"

In step 9 of the AIDED© Process, once the component software has been developed in step 8 of the Process and the necessary hardware has been acquired, the following are the key steps for the system integration:

1. Set up and implementation of the hardware based on the design in step 6 of the AIDED© Process.
2. Loading and integration of the component and application software on the hardware platform.
3. Integration of the external systems or a simulation of those systems which interface with the high-assurance system under development.
4. Integration testing of the complete systems to verify that all components, applications, and interfaces are operating as expected. The degree of detail of the integration testing is determined based on the needs of the project.
5. Rectify and problems or defects that have been detected during preliminary testing.

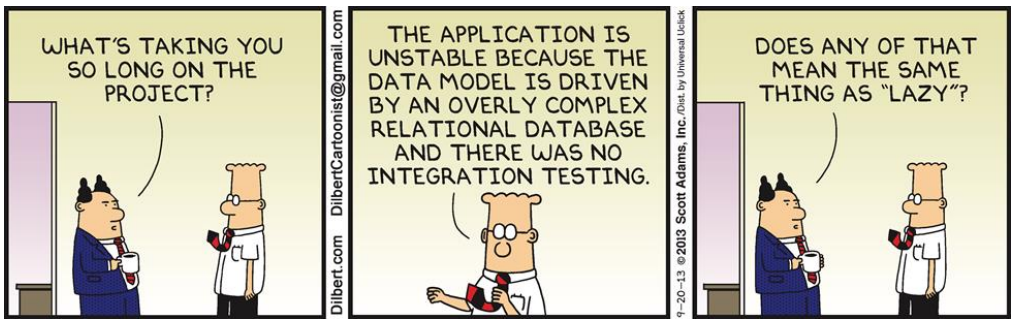


Figure 19. System Integration Testing: Dilbert 2013

9.10. System Testing & Commissioning

In the final step of the AIDED© Process, system functional testing is carried out, involving two phases of testing:

1. System functional testing in the laboratory, using simulators for the external systems, but also the real external systems wherever possible.
2. System functional testing "on location" in the final operational configuration and location, including interfacing with all real external systems.

With the formal approach to system development in the AIDED© Process, a full array of functional testing is not necessary. The testing can be limited to ensure that the high-assurance system is functioning as specified with the external systems.

By experience, the following stakeholders are involved in the system testing in this phase:

- Supply company test engineers
- Client test engineers and end user experts
- Notified Body expert (see definition below)
- National Safety Authority expert

The following is the European Commission definition of a Notified Body (European Commission 2020):

> "*A notified body is an organisation designated by an EU country to assess the conformity of certain products before being placed on the market. These bodies carry out tasks related to conformity assessment procedures set out in the applicable legislation, when a third party is required. The European Commission publishes a list of such notified bodies*."

Concerning the client representatives in this phase, it is important that the **same client experts** are present for final system testing who carried out the previous validation tasks in the AIDED© Process. The reason for this is that, by experience, if new client experts are introduced in this phase, there is a risk that they will bring in new functional expectations for the system, which have not been previously defined in the client functional requirements. This in turn may delay the final commissioning process for the system until the issues have been clarified.

For the final system functional testing “on location”, even though all external systems interfacing with the high-assurance system under development must be connected, it may be possible or desirable that the behaviour of some secondary external systems not interfacing with the core system be simulated.

In the following example of the testing of the high-assurance ETCS Central Control System, a real On-board Unit (OBU) should be interfaced with the core system (via GSM-R) but the movements of the train itself may be simulated.

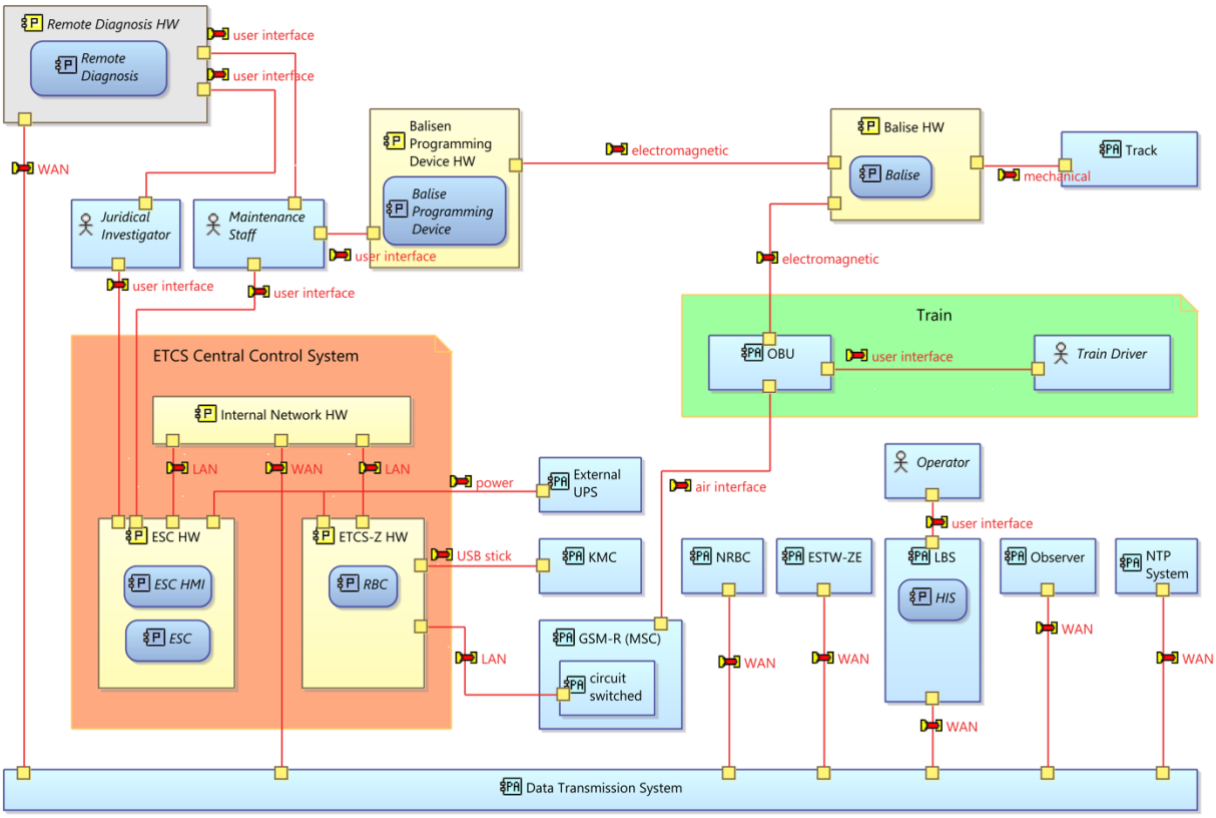


Figure 20. ETCS Central Control System including External Systems

In addition to the final system functional testing, the following **commissioning activities** are carried out in this step of the of the AIDED© Process:

- System Conformity Report is completed by a Notified Body.
- System Acceptance Report/Certificate is issued by the National Safety Authority.
- The high-assurance system is formally handed over to the client.
- The high-assurance system is taken into operational service.

10. System Requirements Management

As with any development of a high-assurance system, in the AIDED© Process the management of the system requirements plays a significant role in every phase of Process (see Figure 6).

In the railway sector, all high-assurance systems are required by the applicable CENELEC standards (CENELEC EN 50126-1:2017, CENELEC EN 50126-2:2017, CENELEC EN 50128:2011, CENELEC EN 50129:2018) to have formal system requirements in order to support the validation, verification and commissioning activities.

As presented in section 9.3 “System Functional Design” and section 9.4 “Logical Architecture Design”, unique in the AIDED© Process is that system requirements are captured and managed **directly in the formal system model** in the UML/SysML tool, without the need for an additional tool such as IBM Rational DOORS® for requirements management.

The following is an example of the capturing and linking of requirements to functions in the system model, with the requirements listed on the right side of the diagram:

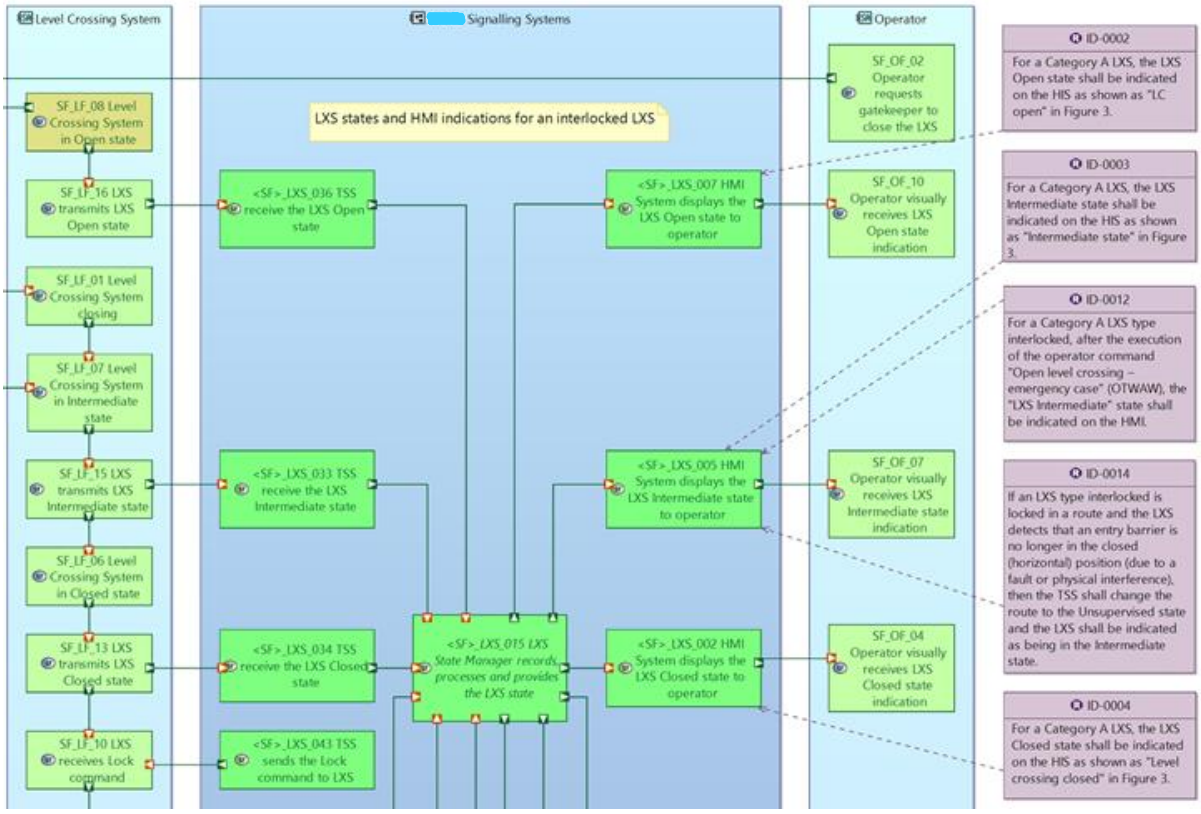


Figure 21. Example of linking SSS Requirements with Functional Objects in the Model

For high-assurance systems, the requirements are normally either:

- **system requirements** delivered by the client, or
- detailed **SSS requirements** developed by the supply company,

or both of the above. If both types of requirements are present in a project, they can be labelled as client or SSS requirements both in the requirement ID as well as in the appropriate attribute in the requirement object in the system model.

In addition, in the AIDED© Process the requirements are categorised in two major groups:

- **Functional requirements**
- **Non-functional requirements** (e.g., performance requirements, environmental requirements, reliability requirements, maintenance requirements, etc.)

As with functional requirements, the non-functional requirements are fully captured and managed in the system model. Non-functional requirements can be linked with the overall system as well as with the appropriate physical components in step 5 of the AIDED© Process (see Figure 14) and can be verified for fulfilment in the system model accordingly.

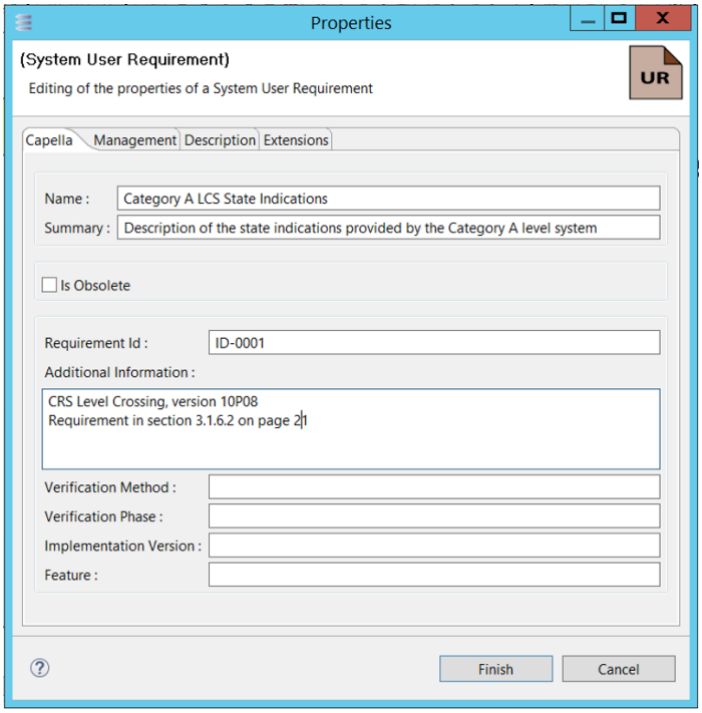


Figure 22. Example of the Requirement Verification Attributes available in Capella

As mentioned in previous sections, since verification is principally automated in the AIDED© Process for the verification steps illustrated in Figure 6, this results in **significant time and cost saving** compared to the manual requirement verification carried out by supply companies in the railway industry today.

11. Agile Scrum Framework

As defined in Wikipedia (Wikipedia Agile 2024), in system and software development, Agile practices include requirements, discovery and solutions improvement through the collaborative effort of self-organising and cross-functional teams with their customer(s)/end user(s). The Agile principles include a broad range of system development methods, the most popular of these being Scrum and Kanban.

Classically, the Scrum Agile method was applied primarily within the scope of software development teams.

An important innovation of the AIDED© Process compared to conventional approaches is that the Scrum method is applied in **all steps** of the system development Process (see also Figure 6). This provides a solid framework for the organisation, allotment and tracking of teamwork and progress on a daily basis.

In addition, as described in the article "Agile vs. Scrum: Which Should You Use, and Why?" (Coursera 2023), in the AIDED© Process the overall project management of the development of a high-assurance system is carried out based on Agile principles.

The following is an overview of the basic principles of the Scrum method, as applied in the AIDED© Process (Wikipedia Scrum 2024):

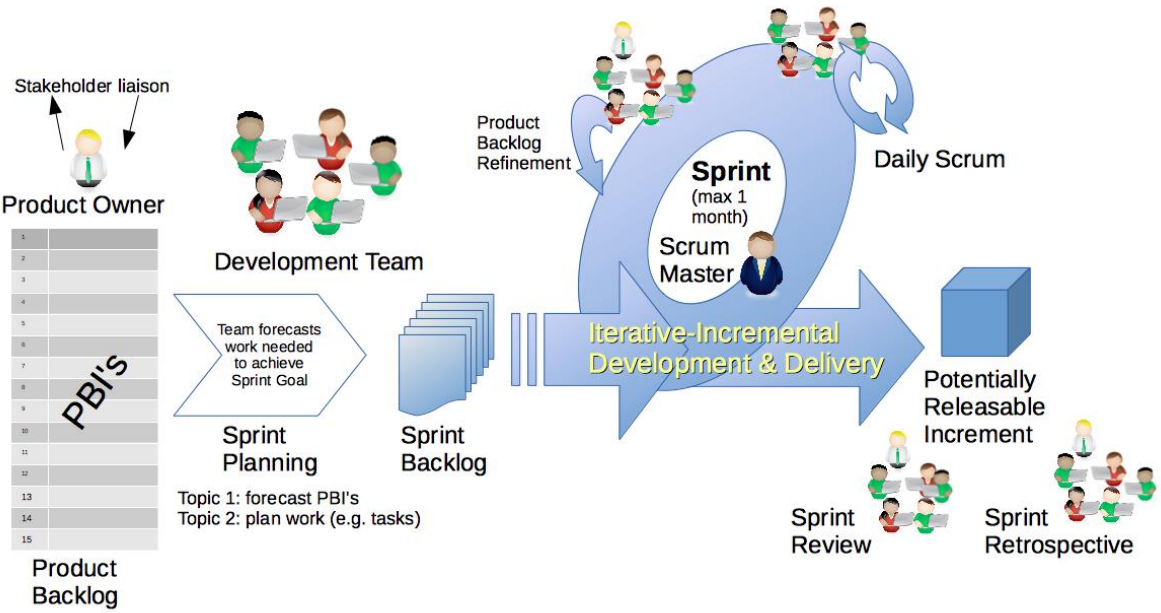


Figure 23. Overview of the Scrum Method Environment

The following are some of the key advantages of the Scrum method from the perspective of the AIDED© Process:

- Work in each step of the Process is broken down into manageable tasks (Product Backlog Issues (PBI's)) that can be completed by the Development Team in a sprint (2 to maximum 4 weeks). This in turn provides success for the Development Team at the end of each sprint, keeping the motivation in the team high.
- In the Sprint Planning Meetings, the Development Team is actively involved in the planning of and commitment to the tasks to be completed in the next sprint.
- Via the Daily Scrum the team can coordinate their work and address problems or roadblocks on a daily basis.
- If the tasks committed in a sprint are completed earlier than planned by a Development Team member, new tasks can be picked up immediately from the Product Backlog.
- In the Review and Retrospective Meetings at the end of every sprint, the Development Team can propose changes toward the Product Owner, the project management as well as other stakeholders to continuously improve the product and the process.
- Since all PBI's (both planned and completed), responsibilities and project progress are captured in a tool such as Jira, there is full transparence for the project management and other key project stakeholders concerning the planning and progress of work by the Development Team.
- The Scrum method supports the Development Team and the project management to adapt the project work based on new information or knowledge in the project or to mirror new priorities.

The issue of team motivation is a particularly important theme since this is a key factor in the success of a project. As per the article by Dan Cable concerning "Why People Lose Motivation…" (Cable 2018), the Scrum method strongly supports the three key areas that leaders should focus on concerning employee motivation:

- Making employees feel comfortable about expressing themselves.
- Creating an environment in which experimentation is valued.
- Helping employees feel a sense of purpose.

12. Automated Generation of Documents

Based on the author's experience in the field, tens of thousands of hours are spent by supply companies for the manual generation of documents in the conventional process for the development of a high-assurance system.

The intention of the AIDED© Process is that all document contents are captured within the system model and that project documents are then generated directly and automatically from the system model. This innovative approach has the following important advantages:

- Document content is captured in the model in small units, i.e., each text object (e.g., a paragraph), diagram, term, abbreviation, stakeholder, etc. is an object in the model, and thus can be used in any number of documents as needed.
- Any changes to an object in the model are automatically updated in all documents using the text object.
- The standardised terms and abbreviations in the model (see step 1 in the AIDED© Process in section 9.1) can be used in the text objects. With this,
    - A glossary of terms and abbreviations can be generated automatically when generating a document from the model.
    - Any term or abbreviation used in a document is automatically hyperlinked to its definition in the document.
    - An index of terms and abbreviations can be generated automatically at the end of the document.
    - Any change to a term or abbreviation will be automatically updated in all documents using the term or abbreviation.
- The automatically generated documents include but are not limited to:
    - A title page
    - A document approvals section
    - A history of the document
    - A table of contents, including hyperlinks to each section in the document
    - A list of figures, including hyperlinks to each figure in the document
    - A list of tables, including hyperlinks to each table in the document
    - A glossary of all terms and abbreviations used in the document.

- All terms and abbreviations are highlighted and hyperlinked to the glossary of terms and abbreviations.
- A listing of all reference documents
- An index with all terms and abbreviations used in the document.

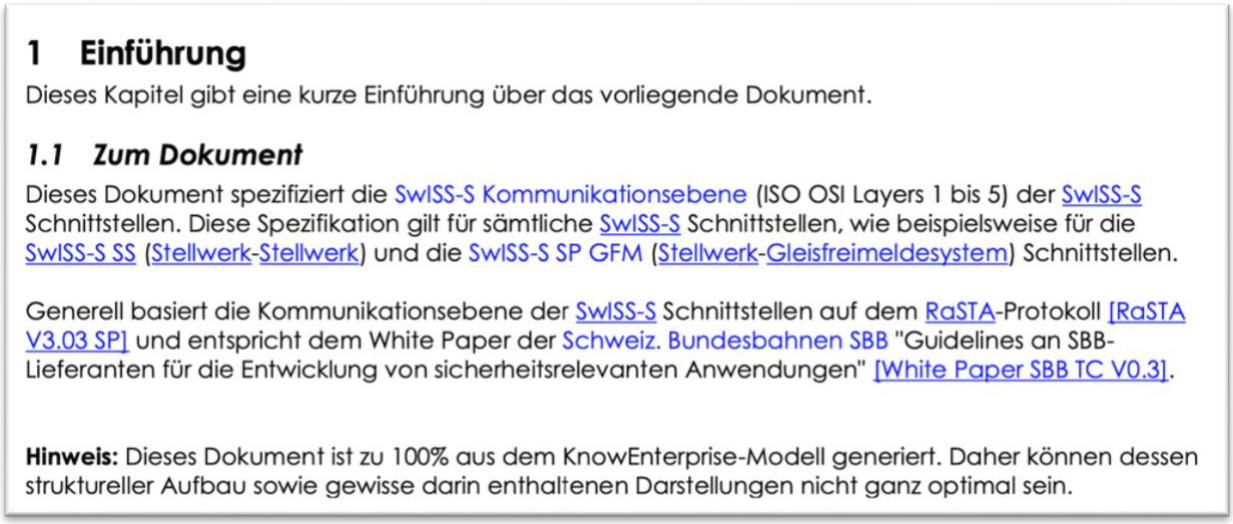
Based on the author's experience, a 40-page, perfectly formatted document with the aforementioned content can be developed from scratch within 3 to 4 hours. The automatic document generation time for a 40-page document is about 5 minutes.

An example of this is the "*SwISS-S V1.2 Spezifikation Layer 1-5*" document in Annex 3. All text elements, chapter sections, diagrams, tables, terms and abbreviations, reference documents, etc. are contained in the SwISS model in the ARTiSAN/ KnowEnterprise toolset.

This means that any of these elements only needs to be developed once within the model and then can be reused by any other project document requiring that element. Any update to an element (e.g. a version update of a reference document) is automatically updated in all documents using the reference.

By experience, thanks to the AIDED© Process the effort for document development can be reduced by up to 80%.

The following is a screenshot from a document developed by the author and generated automatically from a system model developed with the ARTiSAN/KnowEnterprise toolset, with hyperlinked terms in blue and further model elements in blue/underlined (from Annex 3, page 5).



1 Einführung

Dieses Kapitel gibt eine kurze Einführung über das vorliegende Dokument.

1.1 Zum Dokument

Dieses Dokument spezifiziert die SwISS-S Kommunikationsebene (ISO OSI Layers 1 bis 5) der SwISS-S Schnittstellen. Diese Spezifikation gilt für sämtliche SwISS-S Schnittstellen, wie beispielsweise für die SwISS-S SS (Stellwerk-Stellwerk) und die SwISS-S SP GFM (Stellwerk-Gleisfreimeldesystem) Schnittstellen.

Generell basiert die Kommunikationsebene der SwISS-S Schnittstellen auf dem RaSTA-Protokoll [RaSTA V3.03 SP] und entspricht dem White Paper der Schweiz. Bundesbahnen SBB "Guidelines an SBB-Lieferanten für die Entwicklung von sicherheitsrelevanten Anwendungen" [White Paper SBB TC V0.3].

Hinweis: Dieses Dokument ist zu 100% aus dem KnowEnterprise-Modell generiert. Daher können dessen struktureller Aufbau sowie gewisse darin enthaltenen Darstellungen nicht ganz optimal sein.

Figure 24. Example of Hyperlinked Elements in an Automatically Generated Document

13. Implementing the AIDED© Process in a Large Organisation

Implementing the AIDED© Process in a large corporation or organisation for the development of a high-assurance system can be a challenge based on several factors:

- The development of a high-assurance system is normally carried out within the scope of a (client) project with a fixed time schedule and a limited budget. Neither the company management nor the development team are motivated to implement a new process in this environment.
- The management board members of the organisation do not understand the methods and advantages of the AIDED© Process.
- The organisation does not have the necessary skilled experts to implement the AIDED© Process.

In order to mitigate these factors, the following steps are proposed for the implementation of the AIDED© Process in an organisation:

1. At least one senior executive in the organisation should understand the AIDED© Process and its advantages and be prepared to support its implementation on long-term basis.
2. A first project should be chosen which does not have fixed time and budget restrictions, for example, a project within the organisation. This need not be the development of a high-assurance system since the AIDED© Process can be applied to any system development.
3. The management board should guarantee that a generous budget is provided for the project, including the possibility to extend the budget if needed.
4. The development of the system should not be time-critical, the work should be regarded as a research project, but with a concrete product/system as its output.
5. Start with one small, skilled team who will work on the dedicated project for a specific system using the AIDED© Process.
6. The development team members must be skilled and experienced in advanced formal system modelling and tools as required for the Process.
7. A formal system modelling coach who understands the aims and intentions of the AIDED© Process should be made available to the development team.

8. A formal system modelling quality manager should be integrated in the development team to ensure a unified approach to the system modelling carried out by the team. This may be the same person as the modelling coach above.

9. The Scrum environment as per Figure 23 should be set up for the development team, including a Product Owner, a Scrum Master and a Scrum management tool such as Jira®.

10. Reporting to the management board concerning the progress, problems, and issues in the project should be carried out on a regular basis (e.g., monthly), for example, by the Product Owner, the modelling coach, and the team leader.

11. If the management board is satisfied with the results of the AIDED© Process, the method can be migrated to additional teams to be trained in the process, its methods and tools.

12. This is a transition to a new era in system design and engineering and should be regarded as such by the management board.

The importance of the role of the management board in driving innovation is emphasised in the article from McKinsey "The innovation commitment" (Cohen, Quinn & Roth 2019):

"*Setting aspirations and making tough resource-allocation and portfolio choices are areas where a company's top leaders play a unique and disproportionate role in creating change.*"

Photo credit: lumapps

Figure 25. Coaching is a key aspect in the AIDED© Process.

14. The Future of the Workplace and the AIDED© Process

With the advent of hybrid and remote working given a major boost during the COVID pandemic and gaining importance of AI applications in the workplace, there is little doubt that the workplace as we know it from the 2010s will change radically in the coming years and decades.

This is summarised excellently in the Forbes article "Navigating The Future Of Work And Leadership By Embracing Change And Transformation" (Lundberg 2024):

> "*The future of work and leadership heralds an era of unprecedented, fast-paced changes and exponential opportunities. As we navigate through this transformative period, the impact of evolving technologies, shifting workforce demographics and the redefinition of traditional work environments is profoundly reshaping how we lead and operate.*"

The AIDED© Process embraces these changes fully. With the following features, the Process fully supports **hybrid and remote working models**, whereby development team members can be located anywhere in the world:

- The development team works on a common system model with a tool that can be accessed via the internet from anywhere in the world,
- The possibility to communicate face-to-face via online systems such as Zoom, and
- The possibility of senior management to monitor the progress of work on an on-going basis via a Scrum management tool such as Jira®,

The remote working model has the following advantages.

- A company is no longer tied to local resources where the company is located, but has access to the best and most experienced resources worldwide.
- Team members have more free time available and contribute to a more sustainable world since they do not have to travel to and from work daily.
- It supports the desire of younger generations of the team to work as "digital nomads". (See "How to Become a Digital Nomad". (Hennigan 2023))

In addition, these factors contribute to increase the motivation of the development team members, as previously mentioned, a key factor in the success of a project.

The AIDED© Process also embraces the second major change in the work environment in the coming years, the use and application of **new AI tools and systems**.

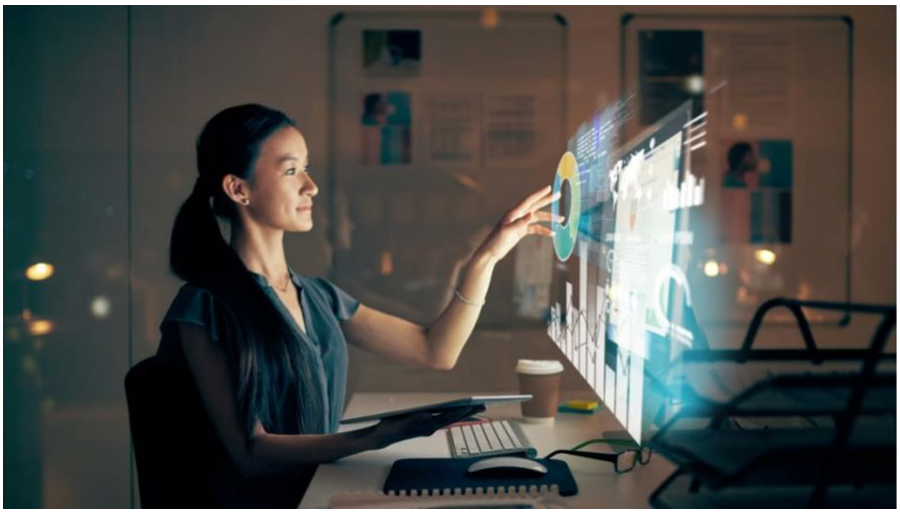


Figure 26. The application of AI systems will radically change the work environment.

The most predominant aspect of AI in the AIDED© Process is the use of an AI tool for automatic code software code generation in step 8 of the Process (see section 9.8). The application of the disruptive AI technology certainly makes AIDED© a disruptive process, since it makes conventional software developers practically obsolete and shifts the focus of work to the system experts in their respective fields, as illustrated in the example below.

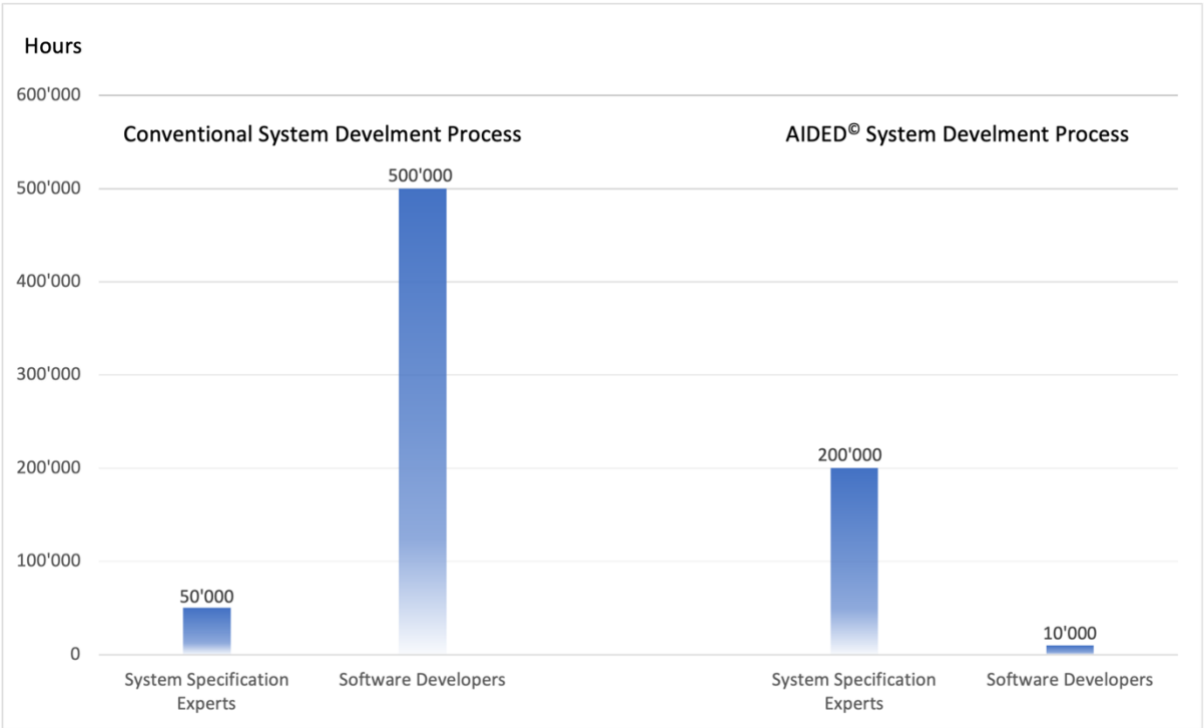


Figure 27. The AIDED© Process shift from software development to system specification.

A further benefit of the AIDED© Process illustrated in Figure 27 on the previous page is the significant reduction of effort required for the development of a high-assurance system. In the example, the overall effort is reduced from 550,000 hours (from the author's experience, a feasible value for high-assurance system development) to 210,000 hours, a reduction in effort of circa 60% or just over 210 person-years.

A change already happening in the workplace and which will play an important role in the future is the **contracting of staff and experts who are not permanent employees of the company**, and as mentioned, the increased **application of AI and automation systems**. This is exemplified well in Ravin Jesuthasan's article "*The 8 Ways Companies Get Work Done, and How to Align Them"*(Jesuthasan 2019) in which the following eight sources of labour in the (future) workplace are described:

- **Employees.** Still the primary source of work for most organisations, employment is usually either part-time or full-time.
- **Independent contractors.** A common work option since the third industrial revolution (Markillie 2012), independent contractors play a vital role in augmenting the employee population.
- **Gig workers.** A rapidly growing source of labour, gig workers typically take on short-term assignments and projects.
- **Outsourcers.** Another hallmark of the third industrial revolution, the outsourcing of entire processes is typically done for efficiency and/or labour arbitrage reasons.
- **Alliances with start-ups and other companies.** These are an increasingly important means for sharing risk and accessing new capabilities.
- **Volunteers.** Typically, they are used for crowdsourcing innovation or promoting brands on social media.
- **Smart automation.** This is often used to refer to artificial intelligence [AI] (such as machine learning and natural language processing) and robotic process automation, which can substitute highly repetitive, rules-based work, augment existing employee capabilities, and also create demand for new human skills.
- **Robotics.** Affects work in much the same way as artificial intelligence, but in the physical sphere.

The AIDED© Process fully supports this diversified workforce in the processes, methods and tools described in this paper. Gig workers and robotics may not be particularly applicable in the AIDED© Process but this will depend on the individual project.

15. Conclusion

The AIDED© Process represents a revolution in the approach, methods, and tools for the development of high-assurance systems in the railway sector, offering the following key advantages over conventional system development:

- ✓ The development time of a high-assurance system, from concept to system acceptance, is reduced from 8-10 years to between 3 to 4 years.
- ✓ System development costs are significantly reduced.
- ✓ The client validation of the system specification and development is an ongoing process.
- ✓ Most system verification activities are automated in the model, thus reducing costs for manual verification.
- ✓ The "Reusability" of the AIDED© process system model contributes to the sustainability of the project work by reducing the effort and energy required to develop high-assurance systems, since:
  - Model elements such as terms, abbreviations, text elements, diagrams, etc. can be reused for a number of different applications within the system model.
  - The complete system model can be reused for other clients by creating a clone of the system model and simply adapting it for the new client.
- ✓ Via the model-steered system simulation the client can test and validate the functions of the final system before any software code is developed.
- ✓ Since software code is generating automatically respectively directly from the system model, human-created software errors and the debugging of those errors is completely eliminated.
- ✓ Since all project documents can be generated directly from the system model with an appropriate UML/SysML toolset:
  - A high quality and consistency of the documents is guaranteed.
  - The high costs for document development typical in the development of high-assurance systems can be significantly reduced.

The factors above all contribute to **significantly improve the sustainability** of a company applying the AIDED© process as well as the sustainability of their high-assurance system products.

The significant cost and time reductions achieved by the AIDED© process also makes a high-assurance system product of a company which uses the process, highly competitive in the market, or to quote Laura Furstenthal, Martin Hirt, and Erik Roth in their article "*Innovation: Your launchpad out of the COVID-19 crisis"* (Furstenthal, Hirt & Roth 2021):

> *"We know that those who prioritize innovation and maintain a through-cycle perspective emerge from crises stronger, with a foundation for continuing outperformance. Accordingly, innovation that pivots products and services to new customer priorities and makes the organization more responsive to new market opportunities should be a key ingredient of any COVID-19 exit strategy."*

The attributes in the quote above certainly apply to the AIDED© process.

It is also important to note that the AIDED© process is not restricted to the railway sector, it can be applied in any industry for the development of software and hardware systems, including non-high-assurance system applications.

Looking into the future of the AIDED© process, further development of AI systems in the coming years may also make it possible that the development of the system modelling in the process can be supported and accelerated by an appropriate AI system. The concept is that the development team would provide natural language or written requirements inputs to the AI system, which would then automatically and within minutes provide a first draft of a model for a particular feature. From this, the development team can then adapt and refine the model to meet the functional requirements of the client. It is estimated that this could reduce the time needed for system modelling in the AIDED© process by up to 50%

And finally, to paraphrase a quote attributed to George Bernhard Shaw (goodreads 2016):

> "*Experts who know that something cannot be done are kindly requested not to interrupt those who are already doing it.*"

Abbreviations

The following abbreviations and acronyms are referenced in this document:

Abbreviation	Term
AIDED©	Advanced Integrated Design, Engineering and Development (process)
CENELEC	European Committee for Electrotechnical Standardisation
CRS	Customer Requirement Specification
DAL	Design Assurance Level
ETCS	European Train Control System
FAP	Fahrstrassen-Anpassung (English: Route Adaption)
ID	Alpha-numeric identification code
IXS	(Railway) Interlocking System
GSM-R	Global System for Mobile Communications – Railway
LX/LXS	Level Crossing System
Maglev	Magnetic Levitation
MBSE	Model-based System Engineering
MTMS	Maglev Train Management and Safety (system)
OBU	(ETCS) On-board Unit
RAMS	Reliability, Availability, Maintainability and Safety
SBB	Schweizerische Bundesbahnen (Swiss Federal Railways)
SSS	System/Subsystem Specification
SysML	Systems Modelling Language
TCS	(Railway) Traffic Control System

Abbreviation	Term
TMS	Traffic Management System
UI	User Interface
UIC	International Union of Railways (Union internationale des chemins de fer)
UML	Unified Modelling Language

Table 4. List of Abbreviations

References

Anthony, S.D. (2017) *To Reinvent Your Firm, Do Two Things at the Same Time* [online] Harvard Business Review. Available at: https://hbr.org/podcast/2017/04/to-reinvent-your-firm-do-two-things-at-the-same-time [Accessed 31 January 2024].

Arbour Group® (2015), "*Verification vs Validation - What's the Difference?*" [online] Available at: https://www.arbourgroup.com/blog/2015/verification-vs-validation-whats-the-difference/ [Accessed 12 January 2024].

Cable, D. (2018) *Why People Lose Motivation - and What Managers Can Do to Help* [online] Harvard Business Review. Available at: https://hbr.org/2018/03/why-people-lose-motivation-and-what-managers-can-do-to-help [Accessed 31 January 2024].

Cohen, D., Quinn, B. and Roth, E. (2019) *The innovation commitment* [online] McKinsey & Company. Available at: https://www.mckinsey.com/capabilities/strategy-and-corporate-finance/our-insights/the-innovation-commitment [Accessed 20 March 2024].

CENELEC EN 50126-1:2017, "*Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS), Part 1: Generic RAMS Process*", CENELEC; not available on-line, must be purchased.

CENELEC EN 50126-2:2017, "*Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS), Part 2: Systems Approach to Safety*", CENELEC; not available on-line, must be purchased.

CENELEC EN 50128:2011, "*Railway Applications - Communication, signalling and processing systems – Software for railway control and protection systems*", CENELEC; not available on-line, must be purchased.

CENELEC EN 50129:2018, "*Railway Applications - Communication, signalling and processing systems - Safety-related electronic systems for signalling*", CENELEC; not available on-line, must be purchased.

CENELEC EN 50159:2010, "*Railway Applications - Communication, signalling and processing systems - Safety-related communication in transmission systems*", CENELEC; not available on-line, must be purchased.

Coursera (2023), "*Agile vs. Scrum: Which Should You Use, and Why?*" [online] Coursera staff, Available at: COURSERA, [Accessed 12 March 2024].

DO-178C/ED-12C (2012), "*Software Considerations in Airborne Systems and Equipment Certification*", RTCA Incorporated, not available on-line, must be purchased.

DO-254 / EUROCAE ED-80 (2000), "*Design Assurance Guidance for Airborne Electronic Hardware*", RTCA Incorporated and EUROCAE, not available on-line, must be purchased.

European Commission (2020), "*Internal Market, Industry, Entrepreneurship and SMEs, Notified Bodie*s" [online] Available at: https://single-market-economy.ec.europa.eu/single-market/goods/building-blocks/notified-bodies_en [Accessed 7 March 2024].

Furstenthal, L., Hirt, M. and Roth, E. (2021) "*Innovation: Your launchpad out of the COVID-19 crisis"* [online] McKinsey & Company. Available at: https://www.mckinsey.com/capabilities/strategy-and-corporate-finance/our-insights/innovation-your-launchpad-out-of-the-covid-19-crisis [Accessed 1 February 2024].

goodreads (2016), "*George Bernhard Shaw > Quotes*" [online] Available at: https://www.goodreads.com/quotes/7424287-people-who-say-it-cannot-be-done-should-not-interrupt [Accessed 22 March 2024].

Hennigan, R. (2023), "*How to Become a Digital Nomad*", [online] Harvard Business Review, Available at: https://hbr.org/2023/02/how-to-become-a-digital-nomad
[Accessed 21 March 2024].

Jesuthasan, R. (2019) *The 8 Ways Companies Get Work Done, and How to Align Them* [online] Harvard Business Review. Available at: https://hbr.org/2019/08/the-8-ways-companies-get-work-done-and-how-to-align-them [Accessed 31 January 2024].

Koenig, N. (2023), "*PhD by Portfolio, Module 1, Assignment LO4: Develop new or processes at the forefront of work*." Available at: SSBR Classroom.

Koenig, N. (2024), "*PhD by Portfolio, Module 2, Assignment LO4: Develop new ideas or processes at the forefront of work in relation to problem solving and decision making*." Available at: SSBR Classroom.

Lundberg, I. (2024), "*Navigating The Future Of Work And Leadership By Embracing Change And Transformation*", [online] Forbes Coaches Council, Available at: https://www.forbes.com/sites/forbescoachescouncil/2024/01/30/navigating-the-future-of-work-and-leadership-by-embracing-change-and-transformation/?sh=724d452464cb [Accessed 18 March 2024].

Markillie, P. (2012), "*A third industrial revolution*", [online] The Economist, Available at: https://www.economist.com/special-report/2012/04/21/a-third-industrial-revolution [Accessed 22 March 2024].

MSc-IT Study Material (2011), "*The benefits of using formal models, Chapter 4. An Introduction to Analysis and Design*" [online] Computer Science Department, University of Cape Town, Available at: https://www.cs.uct.ac.za/mit_notes/software/htmls/ch04s06.html [Accessed 13 February 2024]

Project Management Institute (2013), "*The High Cost of Low Performance: The Essential Role of Communications*", [online] Available at: https://www.pmi.org/-/media/pmi/documents/public/pdf/learning/thought-leadership/pulse/the-essential-role-of-communications.pdf [Accessed 15 January 2024].

Tannam, E. (2019), "*What are the benefits of white-box models in machine learning?*" [online] Silicon Republic, Available at: https://www.siliconrepublic.com/enterprise/white-box-machine-learning#:~:text=White%2Dbox%20models%20are%20the,process%20has%20to%20be%20transparent. [Accessed 19 February 2024].

Wikipedia Agile (2024), "*Agile software development*" [online] Wikimedia Foundation, Inc., Available at: https://en.wikipedia.org/wiki/Agile_software_development#cite_note-AgileManifesto-4 [Accessed 30 January 2024]

Wikipedia Digital Prototyping (2023), "*Digital Prototyping*" [online] Wikimedia Foundation, Inc., Available at: https://en.wikipedia.org/wiki/Digital_prototyping [Accessed 27 March 2024]

Wikipedia Scrum (2024), "*Scrum (software development)*" [online] Wikimedia Foundation, Inc. (Diagram: Dr Ian Mitchell), Available at: https://en.wikipedia.org/wiki/Scrum_(software_development) [Accessed 12 March 2024]

Wikipedia System Integration (2023), "*System integration*" [online] Wikimedia Foundation, Inc., Available at: https://en.wikipedia.org/wiki/System_integration#:~:text=System%20integration%20is%20defined%20in,a%20system%2C%20and%20in%20information [Accessed 6 March 2024]

Annexes

Annex 1 SwissRapide AG, "*Strategic Plan for the Alberta Ultra-Highspeed Maglev Rail Project Calgary - Edmonton*", 15 September 2023 (Niklaus H. König, SSBR PhD by Portfolio, Module 1, Assignment LO4)

Annex 2 SwissRapide AG, "*Guideline for the Founding of an SPV Company for the Alberta Ultra-Highspeed Maglev Rail Project in Calgary, Alberta*", 16 January 2024 (Niklaus H. König, SSBR PhD by Portfolio, Module 2, Assignment LO4)

Annex 3 SwISS Konsortium, "*SwISS - Stellwerk Interface Standard SBB, SwISS-S V1.2 Spezifikation Layer 1-5*", For: Swiss Federal Railways SBB AG, 22 February 2015

Annex 4 SwISS Konsortium, "*SwISS - Stellwerk Interface Standard SBB, SwISS SSA 2.0 Spezifikation*", For: Swiss Federal Railways SBB AG, 18 November 2011

Annex 5 Euro-Interlocking Project, *GENERIS UML Model*, International Union of Railways (UIC), June 2008