Importance of Formal Methods (FMs)

TD2.7: Formal methods and standardisation for smart signalling systems

Invited presentation, Nov 24, 2021
Final Event for OC project 4SecuRail

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No: **101014520**

Antitrust Statement

While some activities among competitors are both legal and beneficial to the industry, group activities of competitors are inherently suspect under the antitrust/ competition laws of the countries in which our companies do business. Agreements between or among competitors need not be formal to raise questions under antitrust laws. They may include any kind of understanding, formal or informal, secretive or public, under which each of the participants can reasonably expect that another will follow a particular course of action or conduct. Each of the participants in this initiative is responsible for seeing that topics which may give an appearance of an agreement that would violate the antitrust laws are not discussed. It is the responsibility of each participant in the first instance to avoid raising improper subjects for discussion, notably such as those identified below.

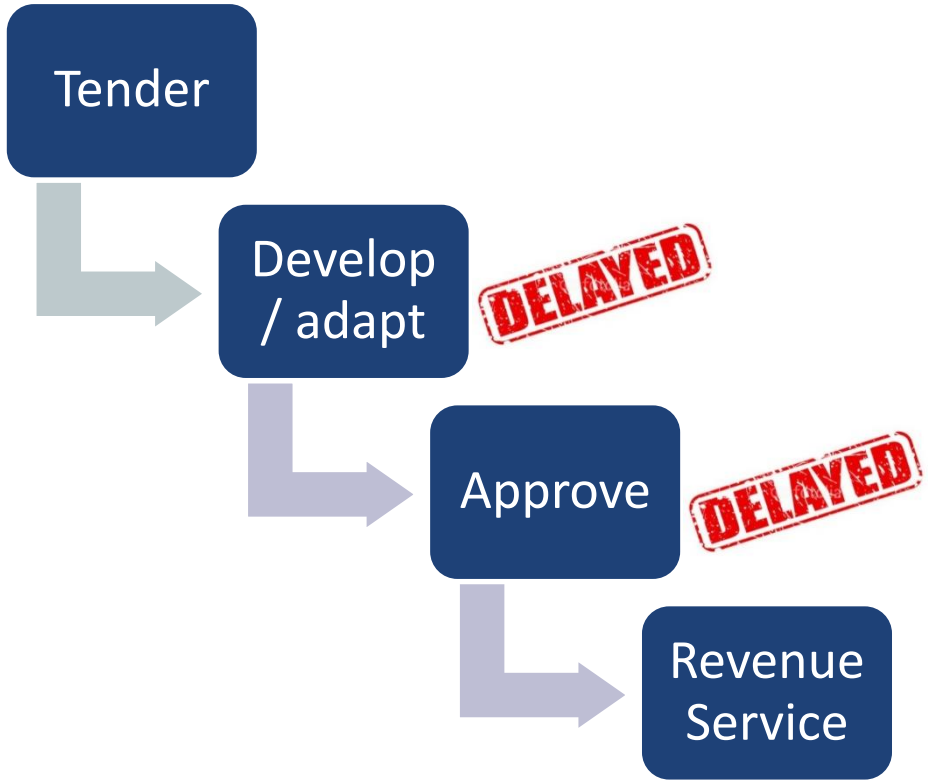
It is the sole purpose of any meeting of this initiative to provide a forum for expression of various points of view on topics (i) that are strictly related to the purpose or the execution of the initiative, (ii) that need to be discussed among the participants of the initiative, (iii) that are duly mentioned in the agenda of this meeting and (iv) that are extensively described in the minutes of the meeting. Participants are strongly encouraged to adhere to the agenda. Under no circumstances shall this meeting be used as a means for competing companies to reach any understanding, expressed or implied, which restricts or tends to restrict competition, or in any way impairs or tends to impair the ability of members to exercise independent business judgment regarding matters affecting competition.

As a general rule, participants may not exchange any information about any business secret of their respective companies. In particular, participants must avoid any agreement or exchange of information on topics on the following non-exhaustive list:

- Prices, including calculation methodologies, surcharges, fees, rebates, conditions, freight rates, marketing terms, and pricing policies in general;
- any kind of market allocation, such as the allocation of territories, routes, product markets, customers, suppliers, and tenders;
- production planning; marketing or investment plans; capacities; levels of production or sales; customer base; customer relationships; margins; costs in general; product development; specific R&D projects;
- standards setting (when its purpose is to limit the availability and selection of products, limit competition, restrict entry into an industry, inhibit innovation or inhibit the ability of competitors to compete);
- codes of ethics administered in a way that could inhibit or restrict competition;
- group boycotts; validity of patents; ongoing litigations.

Why is there a need for formal methods?

- To address the challenge to ensure correct behaviour, interoperability, safety and reliability
- Schedules long and unpredictable
  - Errors and omissions are found late
  - Delivery delayed and costs increase
  - Infrastructure manager locked to chosen vendor for long time
  - Systems costly to procure, develop and maintain

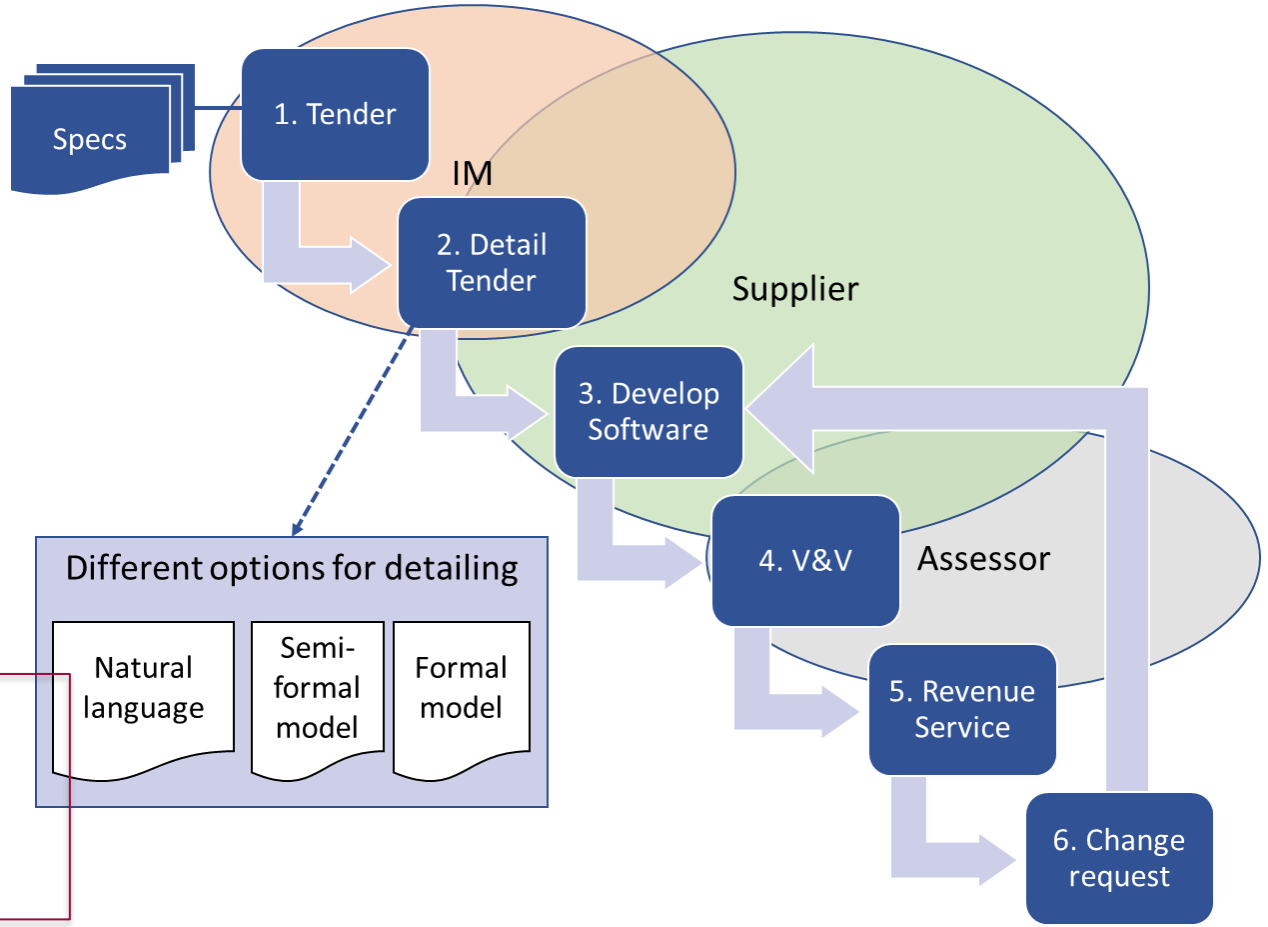


Classification (Taxonomy) of Formal Methods

- **Formal specification**: formalizing system requirements by expressing them in a formal language with a precise and unambiguously defined syntax and semantics.
- **Formal verification**: using a software tool to prove properties of a formal specification, or that a formal model of a system implementation satisfies its specification.
- **Formal development**: using formal methods as an integrated part of a tool-supported system development process.
- **Special purpose:** using customized formal methods tools (“formal apps”) to automate and solve specific tasks, requiring no or limited user intervention.

Life cycle phases relevant for formal methods (FMs)

1. Tender by an IM
2. Detailing of tender requirements
3. Software development
4. Verification & validation of software (compliance to requirements, etc)
5. System entering revenue service
6. Change request resulting in updates to software (phases 3..5 are re-applied)



4SECURail

Studied usefulness of FMs for IMs, based on semi-formal SysML notation (as in EULYNX)

TD2.7's recommendations for use of Formal Methods (FMs)

FMs should be used to ensure important system properties

- Level of trust is significantly higher than for other V&V methods
- FMs can automate tedious V&V tasks
- Along the way, they provide engineers with valuable feedback

Railway control is suited for application of FMs

- High RAMSS demands to be met
- Based on well-understood concepts and principles
- Many FMs success stories exist, e.g. for interlocking and CBTC

FMs have potential for the future in rail

- Increasing number of application targets (software systems)
- Can set benchmark for future system quality and development cycles
- Growing need and interest for FM knowledge from industry

The End