FORUM STIC Paris-Saclay 2013

Labex DigiCosme — digiteo Recherche en sciences & technologies de l'information — SystemX Institut de Recherche Technologique

Fateh GENAB, Elie SOUBIRAN

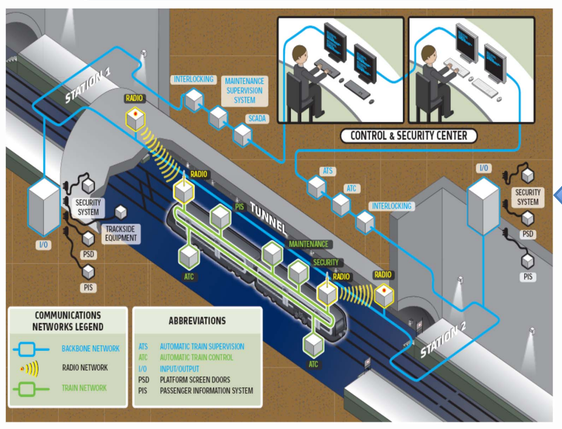
N°5.2 Safe and Reliable embedded Systems

context

Constrained systems:

- Strict normative referential (EN50126/128), specific exploitation rules
- Operator: requirements regarding capacity, performance, safety, availability, and maintainability
- Passenger: comfort, service availability…

Railway Transport Systems

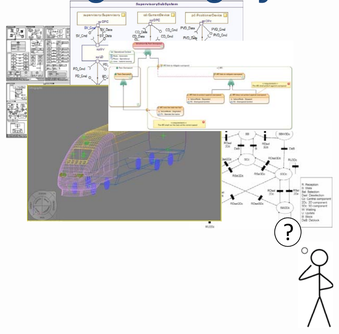


Complex systems:

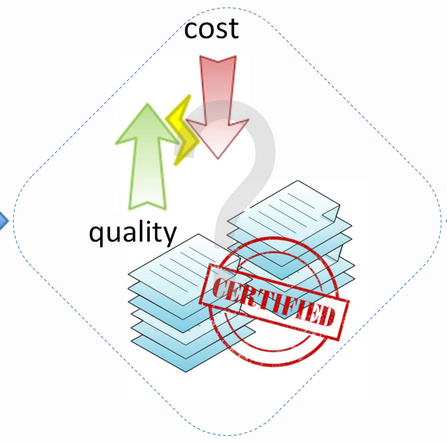
- Heterogeneous systems: Train control, passenger information, maintenance and supervision…
- Users: operators, passengers, maintenance teams
- Distributed intelligence and safety functions

Challenges

Signalling system engineering:



- Different metier
- Different formalisms
- Concurrent engineering
- Costly validation & verification
- Costly RAMS analysis
- Trace everything!



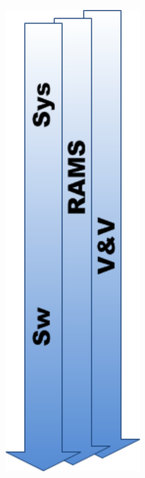
Need of innovative equipment:

- Safe and available computing units
- Efficiency: more operational needs → more services → more functions
- Genericity: shall be used for different sub-system at a lesser cost

Innovations

Process and interoperable tools

- Interoperable referential for specification and analysis
- Formal tools for RAMS analysis, verification and validation
- Traceability and refinement of non-functional requirements
- Architecture optimisation (LP, GA…)
- Synchronous language for SW specification
- Capitalize models, components for reuse concern



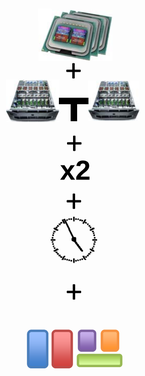
RT constraints pull up

PIL, HIL

Configuration

Application deployment

Safe and available execution platform combining:



- Multi-Cores: increased performance
- Voting systems: safety architecture
- Redundancy of voting systems: availability
- RTOS: isolation and scheduling of applications
- Middleware: Services, abstraction of the composite structure, abstraction of the lower levels

Results

start May 2013

Demonstrator of a framework for system and software conception

Integrate tools such as SysML, Scade, Syndex, Simfia - Altarica, OCL, HOL-TestGen, Diversity, Alcool…
Code generation and aided configuration for the execution platform

Demonstrator of an execution platform for railway applications

SoC Scaleo Chip, Kron-OS/PharOS, Railway specific Middleware

End May 2016

Contact: elie.soubiran@irt-systemx.fr

Financial support: Investissements d'avenir — Trusted Labs — Scaleo chip — apsys — SystemX — ALSTOM — ESTEREL Technologies — KRONO-SAFE

Academic support: Mines Télécom — Laboratoire de recherche en informatique — cea — Inria