# SARA component approach for the development of railway safety-critical applications

Marc Sango, Laurence Duchien, Christophe Gransart

# SARA component approach for the development of railway safety-critical applications

Marc Sango, Laurence Duchien, Christophe Gransart
Univ Lille Nord de France - IFSTTAR - INRIA - Univ Lille 1 - LIFL, UMR CNRS 8022
marc.sango@ifsttar.fr, laurence.duchien@inria.fr, christophe.gransart@ifsttar.fr

## Context, challenges and proposal

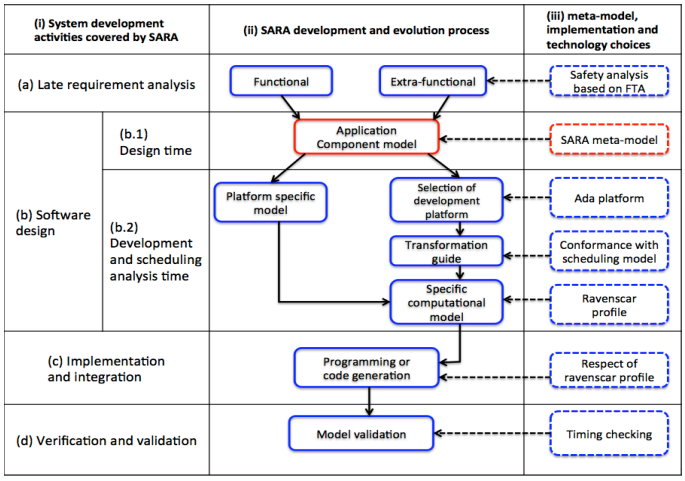
**Context:** To provide high availability, software control applications, such as on-board train supervision applications must be fault-tolerant. The idea to guarantee dependability requirements is to enhance the established approaches like the CBSE with fault tolerance mechanisms (e.g., replication techniques or degraded modes of operation) [1]. Furthermore, due to the nature of safety-critical software and its certification requirements, dependability requirements must be traceable along the development process in order to facilitate the certification process [2]. This context raises the following challenges.

**Challenge 1** (separation of concerns). In order to ensure that critical requirements are properly implemented, dependability requirements have to be separated from other requirements at each stage of software life-cycle

**Challenge 2** (traceability of concerns) In order to facilitate the certification process, dependability requirements have to be separated and traceable at each stage of software life-cycle, from requirement analysis to component instance.

**Proposal :** Our contribution consists of an integrated component-based development and evolution process in order to enforce and trace dependability requirements during the entire development process

## SARA approach

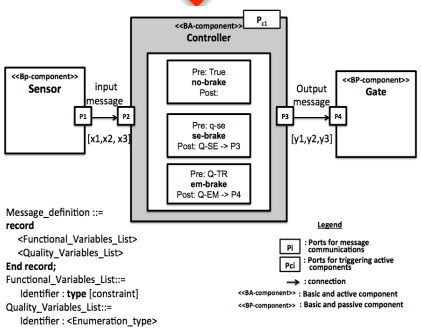



Our approach consists of four phases:
(a) The late requirement analysis phase, which consists in separating functional requirements from extra-functional requirements. We focus on dependability requirements, particularly, the degraded modes of operation.
(b) The software design phase that contains two steps:
(b.1) In the design time step, we model the requirements by components. We use the software component-based model [2],
(b.2) In the development and scheduling analysis time step, we choose an appropriate development method for safety-critical systems.
(c) The implementation and integration phase, which consists in implementing or generating the code in Ada Ravenscar profil.
(d) The verification and validation phase, which consists in checking the temporal dependability requirements.

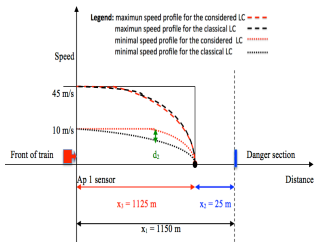
## Experimental evaluation

Requirement Analysis → Sofwatre component design → Implementation → Simulation evaluation

Example of on-board train speed application requirements:
**Functional requirement (R1):** "Calculation of a speed profile taking into account the train running / braking characteristics which are known on-board and the track description data" (ERTMS/ETCS specification)
**Dependability requirement (R2):** "In case only the application of (the non-vital) service brake has been commanded and the service brake fails to be applied, the emergency brake command shall be given".
**Temporal dependability requirement (R3):** "once closed and when there is no train approaching meanwhile, the LC must be kept closed at least (Tbegin) and at most (Tend), where Tbegin and Tend are the time limits"




The model implementation based on the SARA's API (the open availability code, Sara2Ada and Sara2Ravenscar is available in http:// urls.fr/sara).




## Conclusion

- Based on some chosen benchmarks at rail-road level crossing area, a running example is evaluated throughout our component-based development and evolution process.
- The complete process shows that our two challenges, the traceability and the separation of functional and dependability requirements can be maintained during both the development and evolution process.

## Future works

- Transformation of SARA components to timed automata model
- Towards the formal verification of safety application model

## References

- [1] Q. Enard, M. Stoicescu, E. Balland, C. Consel, L. Duchien, J.-C. Fabre, and M. Roy. Design-driven development methodology for resilient computing. In CBSE '13, pages 59–64, 2013
- [2] M. Sango, C. Gransart, and L. Duchien. Safety component-based approach and its application to ERTMS/ETCS on-board train control system. In TRA2014 Transport Research Arena 2014, Paris, France, April 2014.