SaRDIn - A Safe Reconfigurable Distributed Interlocking

Fantechi, Alessandro; Gnesi, S. ; Haxthausen, Anne Elisabeth; van de Pol, J. ; Roveri, M. ; Treharne, H.

Publication date:
2016

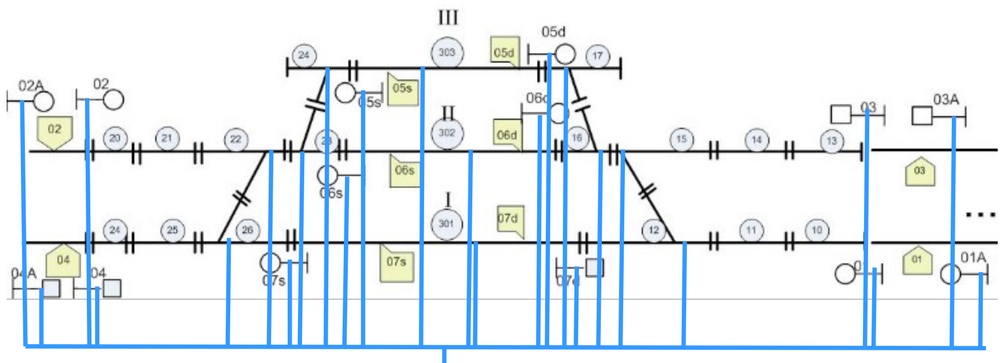
Document Version
Publisher's PDF, also known as Version of record

SaRDIn - A Safe Reconfigurable Distributed Interlocking

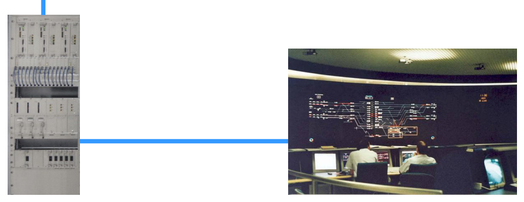
A. Fantechi[1,2,3], S. Gnesi[2], A. Haxthausen[3], J. van de Pol[4], M. Roveri[5], H. Treharne[6]

[1] *Università di Firenze, Dipartimento di Ingegneria dell'Informazione. Firenze. Italy.*
[2] *ISTI-CNR. Pisa. Italy.*
[3] *Danmarks Tekniske Universitet, DTU Compute. Lyngby. Denmark.*
[4] *University of Twente, CTIT. Enschede. The Netherlands.*
[5] *Fondazione Bruno Kessler. Trento. Italy.*
[6] *University of Surrey, Department of Computer Science. Guildford. United Kingdom.*

The concept

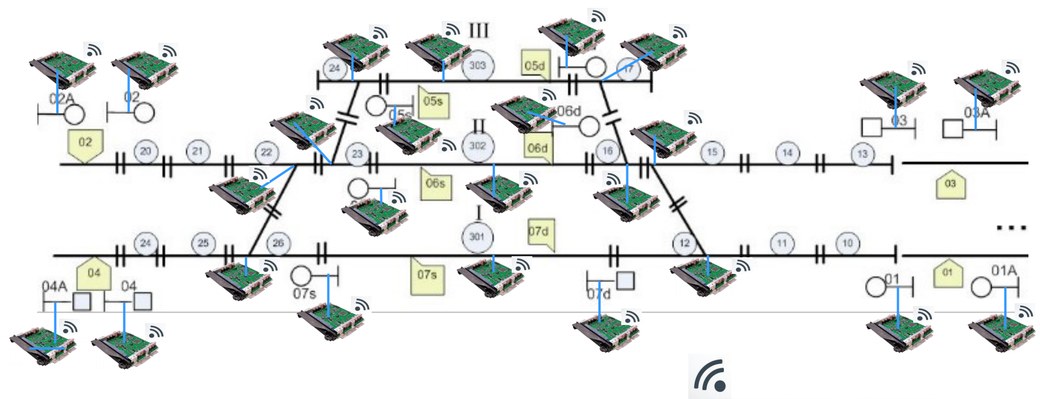


Traditional, Centralized Interlocking equipment



control room

SaRDIn - an innovative concept based on ICT future trends:
Cyber-Physical Systems
Fine-grained distribution of the logic
Distributed autonomous control agents
Emergent global behaviours



- *Interlocking logic distributed in small ECUs that each take control of a physical element*
- *Each distributed item communicates with its adjacent controllers*

control room

ADVANTAGES:

- easier deployment and maintenance,
  - plug-and-play installation
- vendor lock-in avoidance
  - open, standard interlocking protocol stack
  - copper-free communication
- simpler certification process
  - modular formal verification

Challenges

Safety
Communication safety
Consistency of vital distributed information

Reliability, Availability, Maintainability
A high number of distributed elements might decrease global reliability and availability

Distributed configuration and initialisation
Re-configuration at layout changes

Strategies

Safety layer on top of secure wireless communication protocol.
The ***route*** is a global logical notion: a route has to be established by proper cooperation of the distributed elements.
Reserving a route is achieved by a ***distributed consensus algorithm***

*Quantitative **availability** and **capacity** requirements, higher than current centralized interlocking systems.*
Specific (model-based) analyses to assess conformance to such requirements.
***Maintainability**: zero maintenance of the distributed controllers (useful life greater than the associated mechanical equipment)*

Configuration and initialization algorithm guarantees the consistency of distributed replicated information.
Periodic, distributed, check of the integrity and stability of the (local) configuration data
Robust and versatile, plug and play, ***reconfiguration*** algorithm for layout changes: each controller autonomously discovers its new configuration by communicating with the neighbours.

SaRDIn strengths

Standard off the shelf distributed controllers

Open standard protocols:
Route reservation
Configuration
Re-configuration

Formal verification that the algorithms maintain safety
→ Basis for plug and play *certified* controllers: proof that the correct installation of such controllers within the standard interlocking protocol guarantees safety

RSSR2016 - International Conference
Reliability, Safety and Security of Railway Systems: Modelling, Analysis, Verification and Certification
June 28-30, 2016
Espace du Centenaire, Maison de la RATP, Paris, France

VILLUM FONDEN
RobustRailS