



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

[Link back to DTU Orbit](#)

Citation (APA):

Fantechi, A., Gnesi, S., Haxthausen, A. E., van de Pol, J., Roveri, M., & Treharne, H. (2016). *SaRDIn - A Safe Reconfigurable Distributed Interlocking*. Poster session presented at The International Conference on Reliability, Safety and Security of Railway Systems, Paris, France.

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal

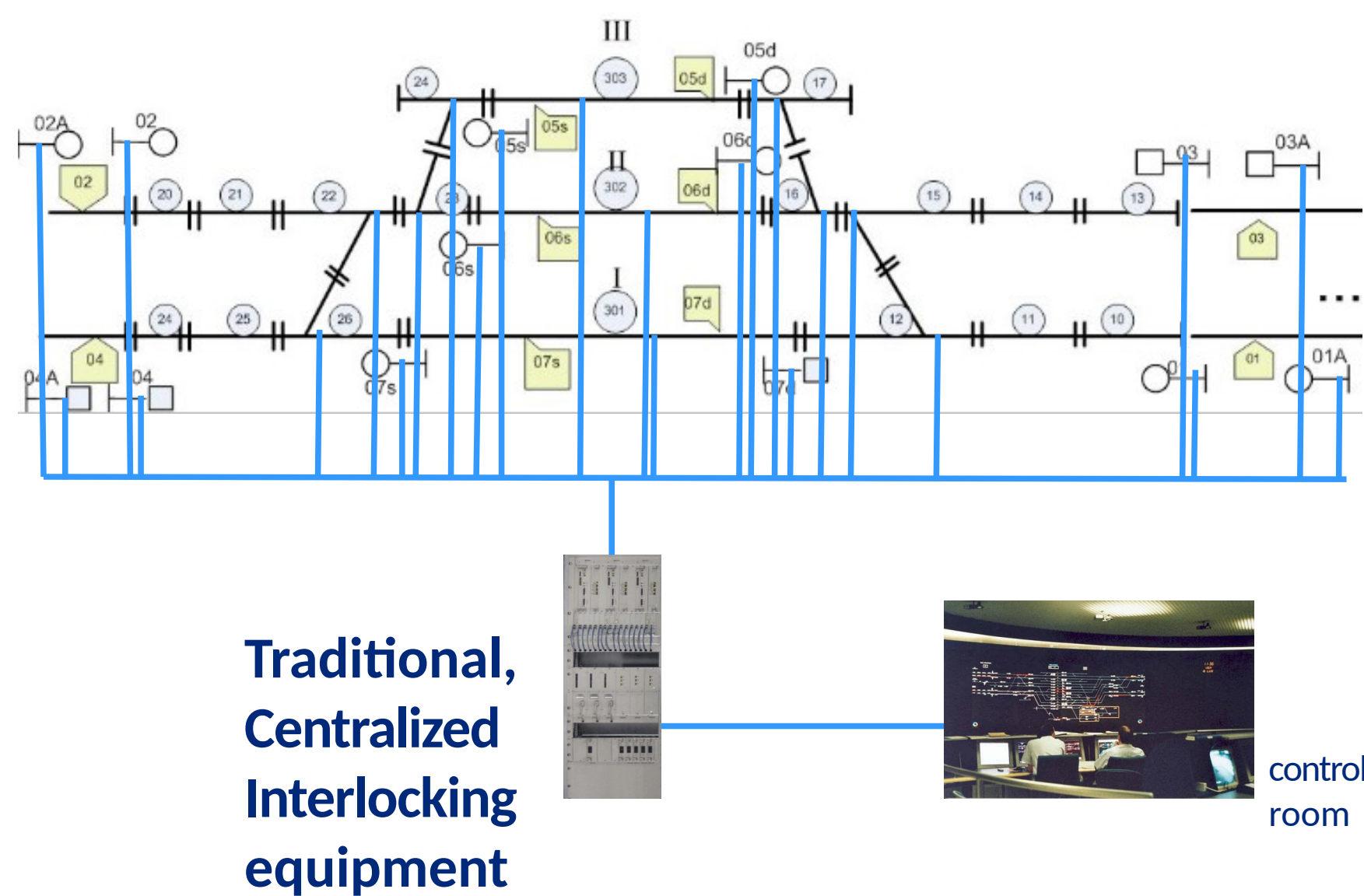
If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

SaRDIn - A Safe Reconfigurable Distributed Interlocking

A. Fantechi^{1,2,3}, S. Gnesi², A. Haxthausen³, J. van de Pol⁴, M. Roveri⁵, H. Treharne⁶
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.

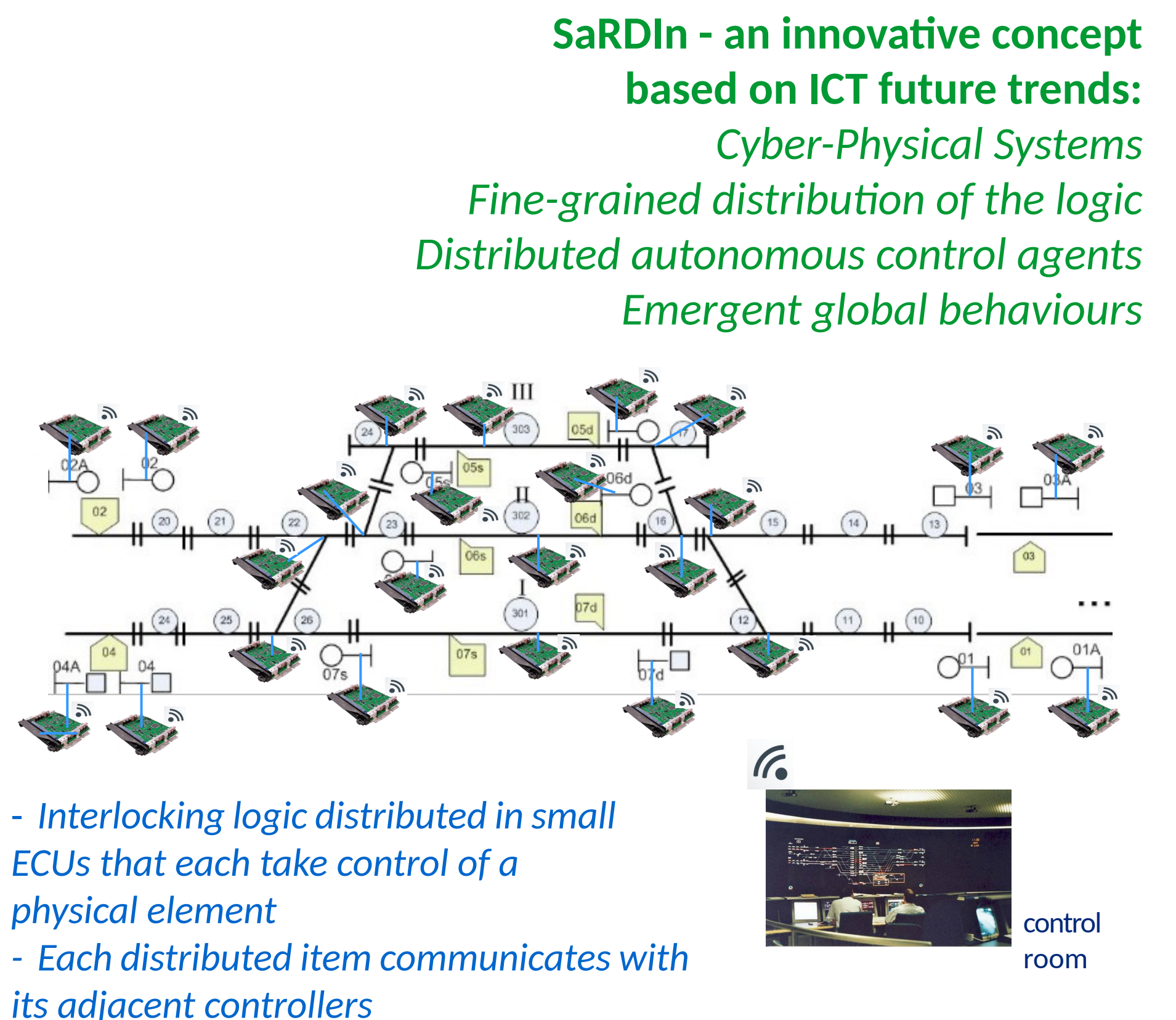
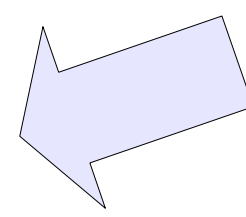
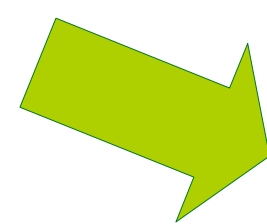


The concept



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