Dependable Control of Discrete Systems (DCDS'09)
Bari, 10-12 May 2009

Model-Based Approaches for Railway Safety, Reliability and Security: The Experience of Ansaldo STS

Dr. Francesco Flammini

Ansaldo STS Italy – Innovation Unit
francesco.flammini@ansaldo-sts.com

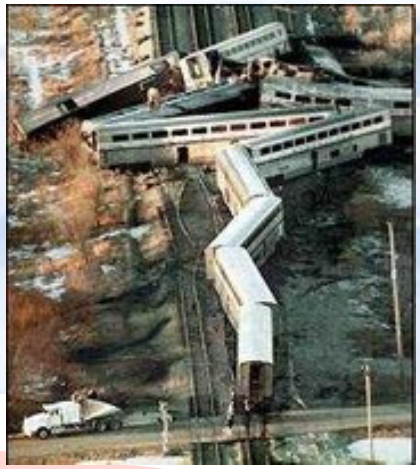
AnsaldoSTS
A Finmeccanica Company

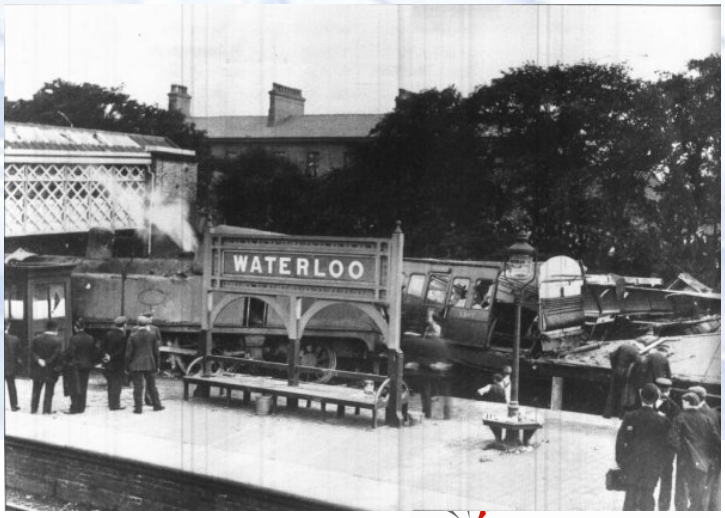
Outline

- Introduction to modern railway control systems
- The need for model-based approaches
- Succesful applications
- Future developments

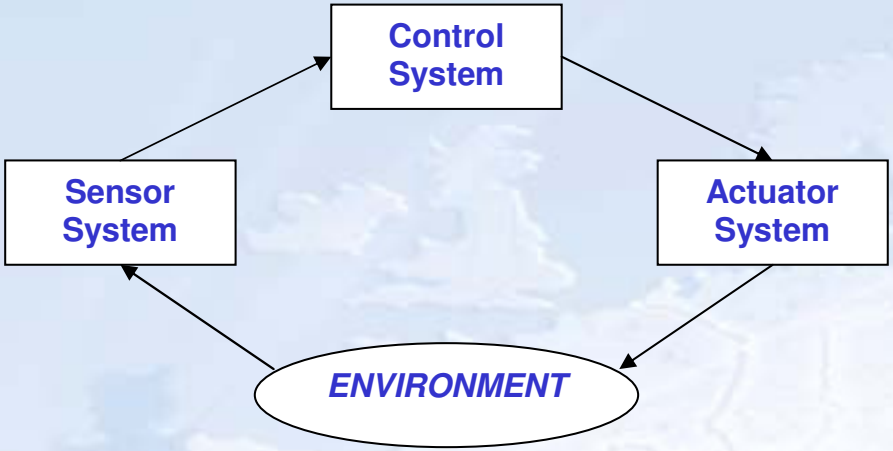
Catastrophic Failures in Railways

- Brief history… (due to speed or signalling)
  - Recent – Metro Rome, 2006
  - Most catastrophic: Amagasaki (Japan), 107 killed, 555 injuried
  - One of the oldest – Waterloo station, 1803
- http://danger-ahead.railfan.net/





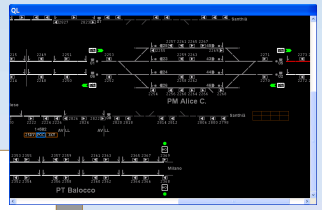
Computer-Based Railway Control Systems



- Safety-Critical Railway Control Systems:
  - Interlocking Systems – management of train route and signals in stations
  - Traffic Management Systems – management of train headways (trackside)
  - Train Control Systems – management of train movement (on-board)
- Evolution from relays based to computer based → more complex failure modes
- Embedded real-time reactive systems increasingly complex:
  - large, distributed, heterogeneous
- Dependability attributes of interest:
  - Reliability Availability Mantainability Safety Security (RAMSS)
- Important to evalutate such attributes in:
  - early development stages to support design choices (*fault forecasting*)
  - verification and validation phase, to demonstrate compliance to RAMSS standard (*assessment / certificafion*)

Automatic Train Protection Systems

HMI



TRAFFIC MANAGEMENT

Radio Block Center

Wide Area Network

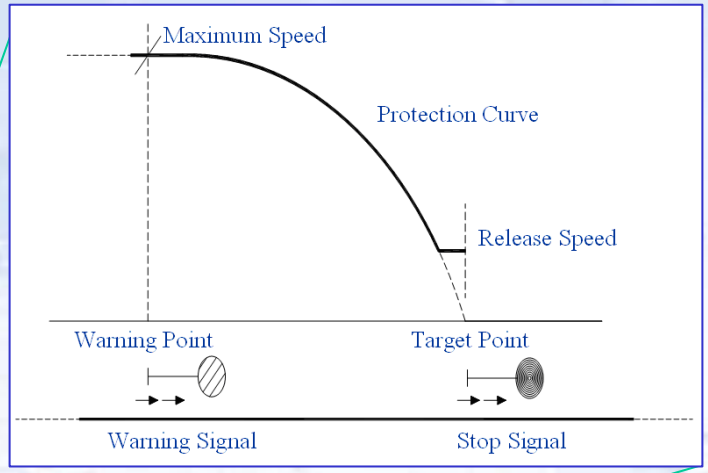
Neighbour RBCs

Base Trans/receiver Station

GSM-R

Train Position Report

Movement Authority with Static Speed Profile



TRAIN CONTROL

ON-BOARD SYSTEM

Air-gap

TRACK CIRCUIT

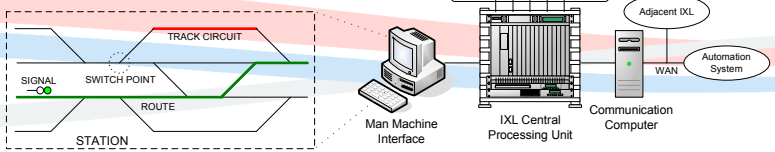
Eurobalise

Balise Telegram with Balise Group identifier

INTERLOCKING

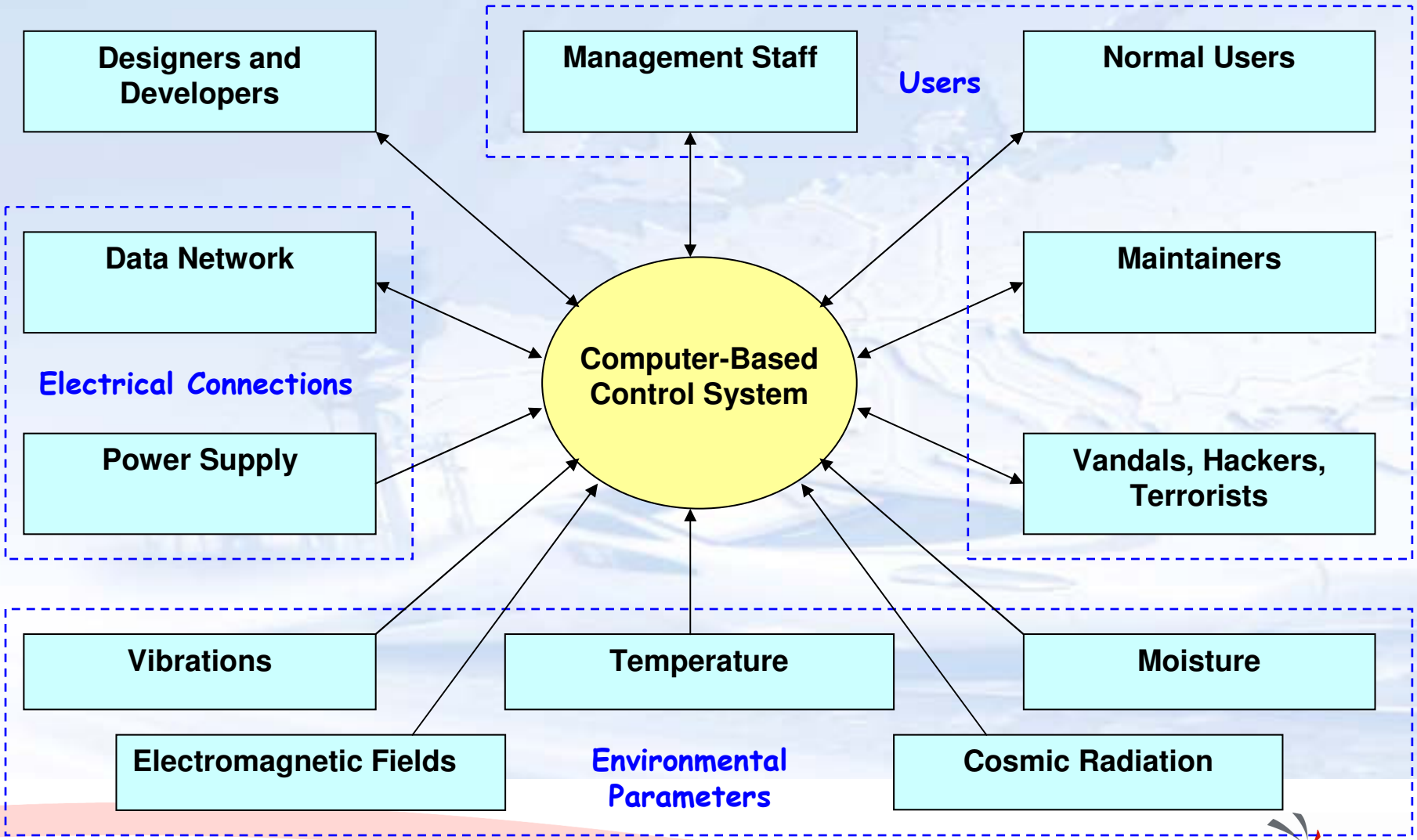
IXLj

IXLk



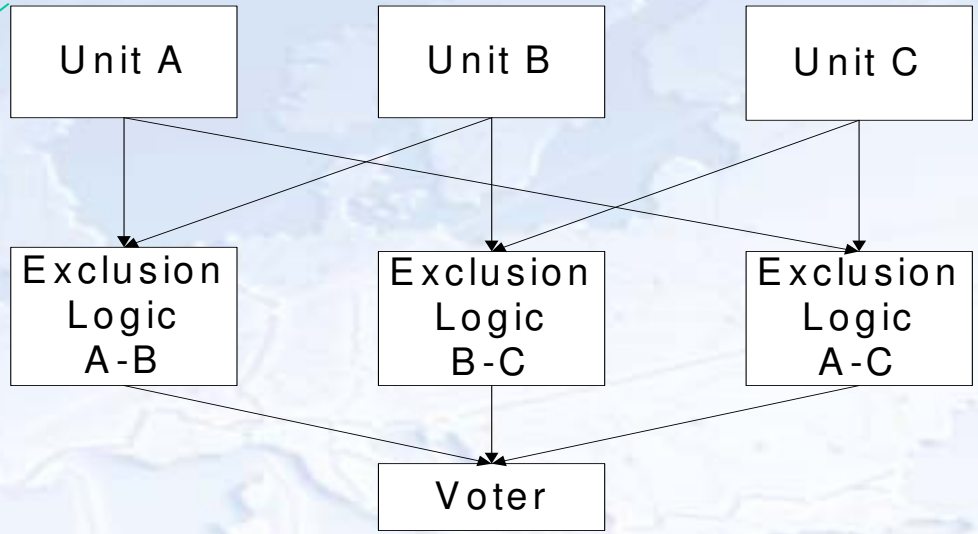
AnsaldoSTS
A Finmeccanica Company

Threats of system dependability



The core of most control systems

- Triple Modular Redundancy (TMR)
- Many other fault-tolerance mechanisms
  - Design diversity
  - Error Correcting Codes
  - Defensive programming
  - …



Objectives of dependability assessment

- Extensive simulation with real systems is unfeasible
- We need to evaluate RAMSS attributes of interest with models as much as possible:
  - Holistic
    - System level failure modes
  - Realistic
    - Correct behavior with not too many conservative assumptions
  - Maintainable
    - No hyper-skills required to build and modify them
  - Efficient
    - Quick to build and evaluate on normal computers
  - Assessable
    - Readable and low error prone
  - …

New frontiers in dependability modeling

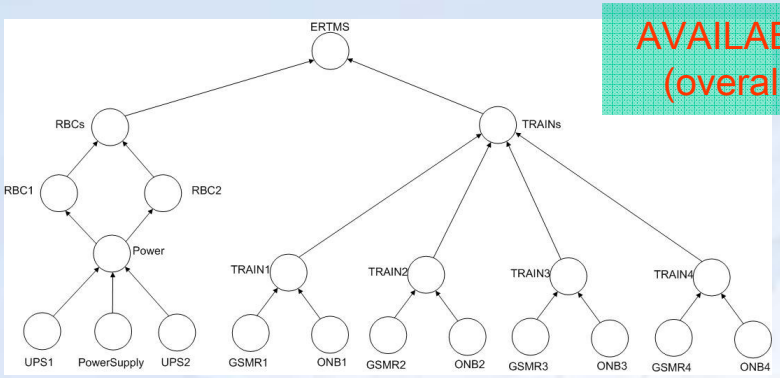
- Multi-paradigm approaches, involving:
  - Multi-formalism modeling
  - Meta-modeling
  - Model-abstraction and transformation
- Choice of the modeling approach most suited to the:
    - Objective of the analysis (performability, security, maintainability, etc.)
    - Constituent subsystems (small embedded device, workstation, etc.)
    - Abstraction layers (hardware, software state-machine, software functions, etc.)
- Advantages:
  - Modular or compositional approach
    - Divide ed impera
    - Incremental, multi-level / hierarchical
    - Reuse (model libraries)
  - They allow for a trade-off among:
    - Ease of use
    - Expressive power
    - Solving efficiency

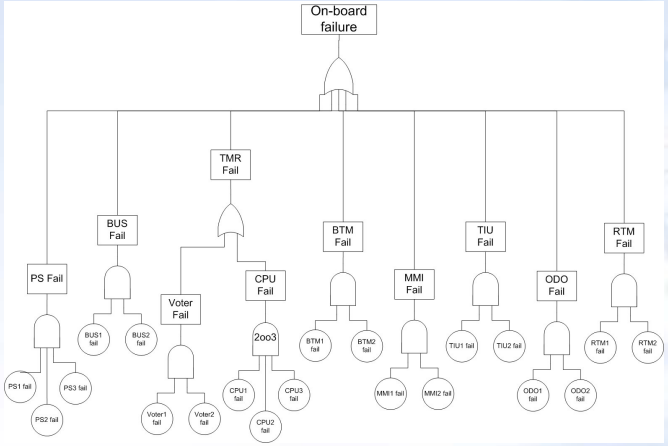
Experience report 1: issues

- Main problem:
  - evaluate system availability with respect to system-level failure modes to demonstrate compliance to RAM requirements
- Unfeasible with traditional single-formalism stochastic modeling approaches:
  - Queueing Networks ➪ limited expressiveness (no failure modeling)
  - Fault Trees ➪ limited expressiveness (no performance modeling)
  - Stochastic Petri Nets ➪ ungovernable complexity and limited efficiency (state space explosion)
  - …
- Further problem:
  - how to evaluate the effect of real-world repair strategies (e.g. preventive maintenance, limited resources, etc)?

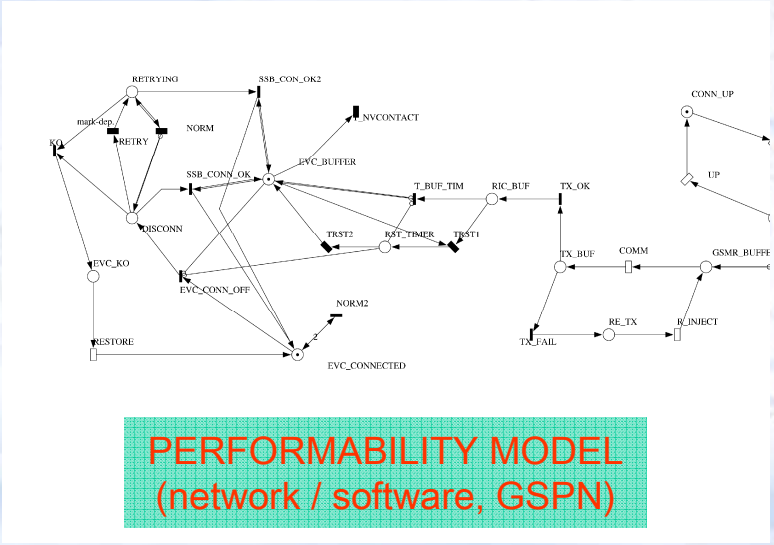
Experience report 1: solution

AVAILABILITY MODEL
(overall system, BN)

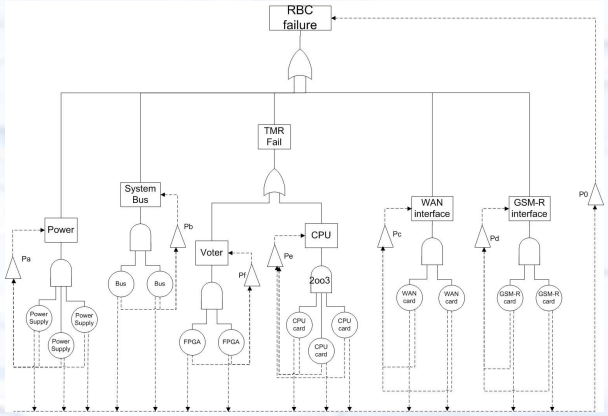




RELIABILITY MODEL
(on-board, FT)



PERFORMABILITY MODEL
(network / software, GSPN)



MAINTAINABILITY MODEL
(trackside, RFT)

- F. Flammini, M. Iacono, S. Marrone, N. Mazzocca: "Using Repairable Fault Trees for the evaluation of design choices for critical repairable systems". In: *Proceedings of the 9th IEEE Symposium on High Assurance Systems Engineering*, HASE'05, Heidelberg, Germany, October 12-14, 2005: pp. 163-172
- F. Flammini, S. Marrone, N. Mazzocca, V. Vittorini: "Modelling System Reliability Aspects of ERTMS/ETCS by Fault Trees and Bayesian Networks". In: *Safety and Reliability for Managing Risk: Proceedings of the 15th European Safety and Reliability Conference* (published in September 1st 2006), ESREL'06, Estoril, Portugal, September 18-22, 2006: pp. 2675-2683

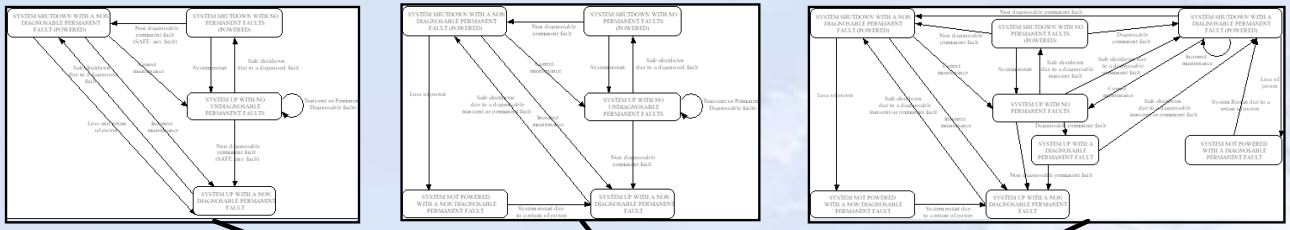
Experience report 2: issues

- Main problem:
  - evaluate TMR safety in presence of imperfect maintenance
- Existing GSPN model assuming perfect maintenance hardly extensible
  - Low maintenability
  - Very limited efficiency
- No other single formalism approach usable to solve the overall problem
- Further problem:
  - how to improve the maintenability of the existing GSPN-based safety model?

Experience report 2: solution

Finite State Machine OR Continuous Time Markov Chain OR Timed Automata at different levels of detail

REPAIR MODELS (environmental & human factors, CTMC)



Maintenance model implementation

Choice of the model

Maintenance Model Interface

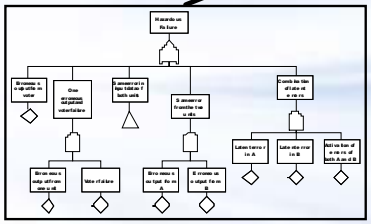
Operational Status (OK, KO, Up with fault, etc.)

Composition

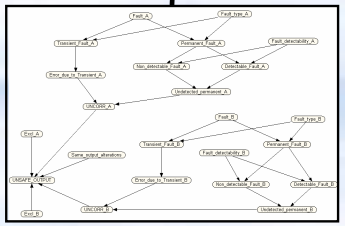
Fault Events (Transient, Permanent, etc.)

Failure Model Interface

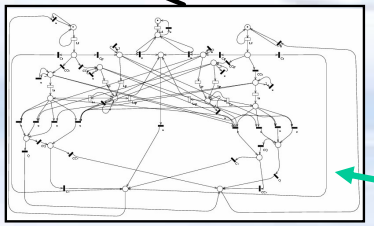
Choice of the model



Fault Tree



Bayesian Network



GSPN

Failure model implementation

EXISTING SAFETY MODEL (hardware, GSPN)

+ expressiveness, complexity, realism
- solving efficiency, readability, maintainability

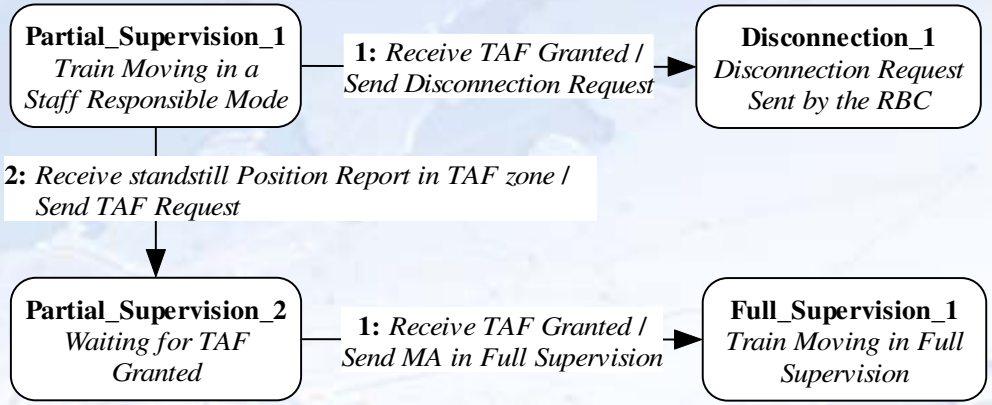
• F. Flammini, S. Marrone, N. Mazzocca, V. Vittorini: "A new modelling approach to the safety evaluation of N-modular redundant computer systems in presence of imperfect maintenance". In: Reliability Engineering & System Safety (Elsevier) – special issue on ESREL'07 selected papers. DOI: 10.1016/j.ress.2009.02.014

Experience report 3: issues

- Main problem:
  - perform system functional verification of the European Railway Traffic Management System / European Train Control System (ERTMS/ETCS)
- Issues:
  - extensive testing unfeasible due to system complexity (test-case number explosion)
  - testing required for both nominal and degraded conditions
  - unstable system requirements specification
- Further problem:
  - How to detect missing requirements in order to improve system specification? (validation)

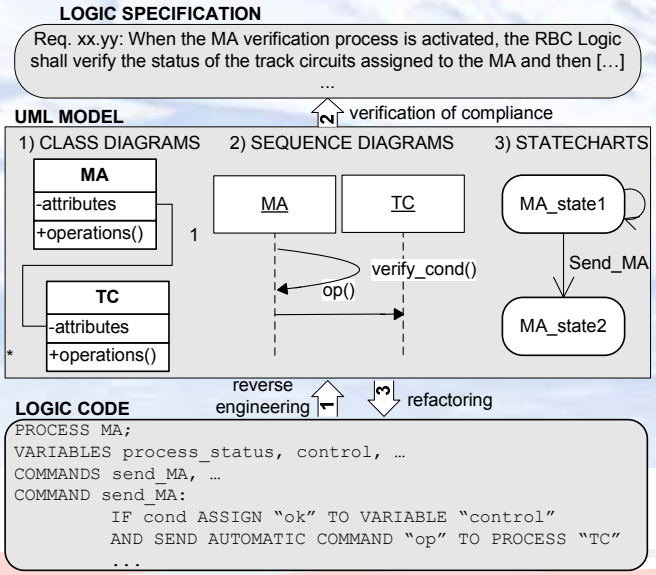
Experience report 3: solution

1. Model-based testing (dynamic verification)
   - Automatic generation and reduction of the test-suite using reference abstract models like Finite State Machines



- F. Flammini, N. Mazzocca, A. Orazzo: "Automatic instantiation of abstract tests to specific configurations for large critical control systems". In: Journal of Software Testing, Verification & Reliability (STVR), Vol. 19, Issue 2, pp. 91-110
- F. Flammini, P. di Tommaso, A. Lazzaro, R. Pellecchia, A. Sanseviero: "The Simulation of Anomalies in the Functional Testing of the ERTMS/ETCS Trackside System". In: Proceedings of the 9th IEEE Symposium on High Assurance Systems Engineering, HASE'05, Heidelberg, Germany, October 12-14, 2005: pp. 131-139

2. Model-based code inspection (static verification)
   - Use of UML-based reverse engineering and refactoring



- C. Abbaneo, F. Flammini, A. Lazzaro, P. Marmo, N. Mazzocca, A. Sanseviero: "UML Based Reverse Engineering for the Verification of Railway Control Logics". In: IEEE Proceedings of Dependability of Computer Systems, DepCoS'06, Szklarska Poręba, Poland, May 25-27, 2006: pp. 3-10

Experience report 4: issues

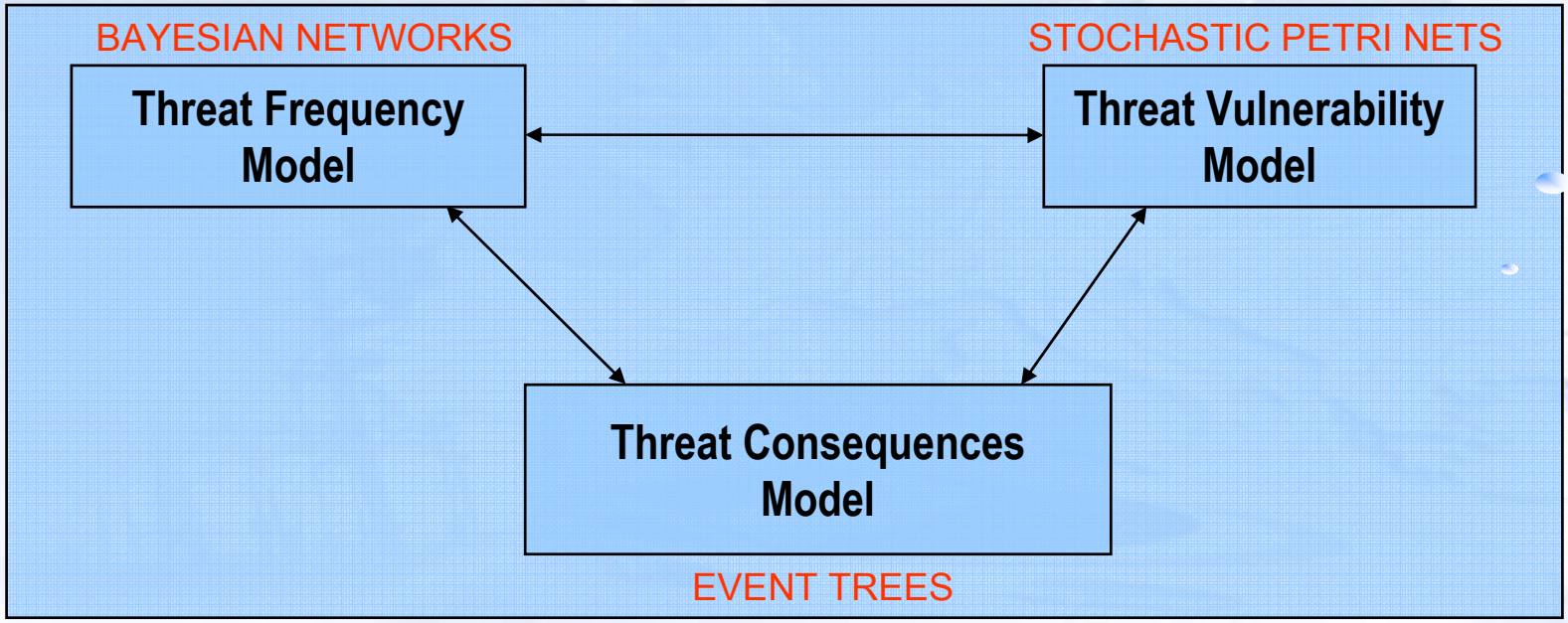
- Main problem:
  - Quantitative security risk assessment to support the design of protection mechanisms and evaluate the return on investment
- Issues:
  - Traditional reliability modeling formalisms (e.g. Fault Trees) inadequate for security modeling (e.g. no support for interdependant basic events)
  - Complexity in vulnerability modeling
- Further problem:
  - How to demonstrate to the customer the optimality of security system design (e.g. size of subsystems)?

Experience report 4: solution

$$R = P \cdot V \cdot D$$

RISK MODEL

WORK IN PROGRESS

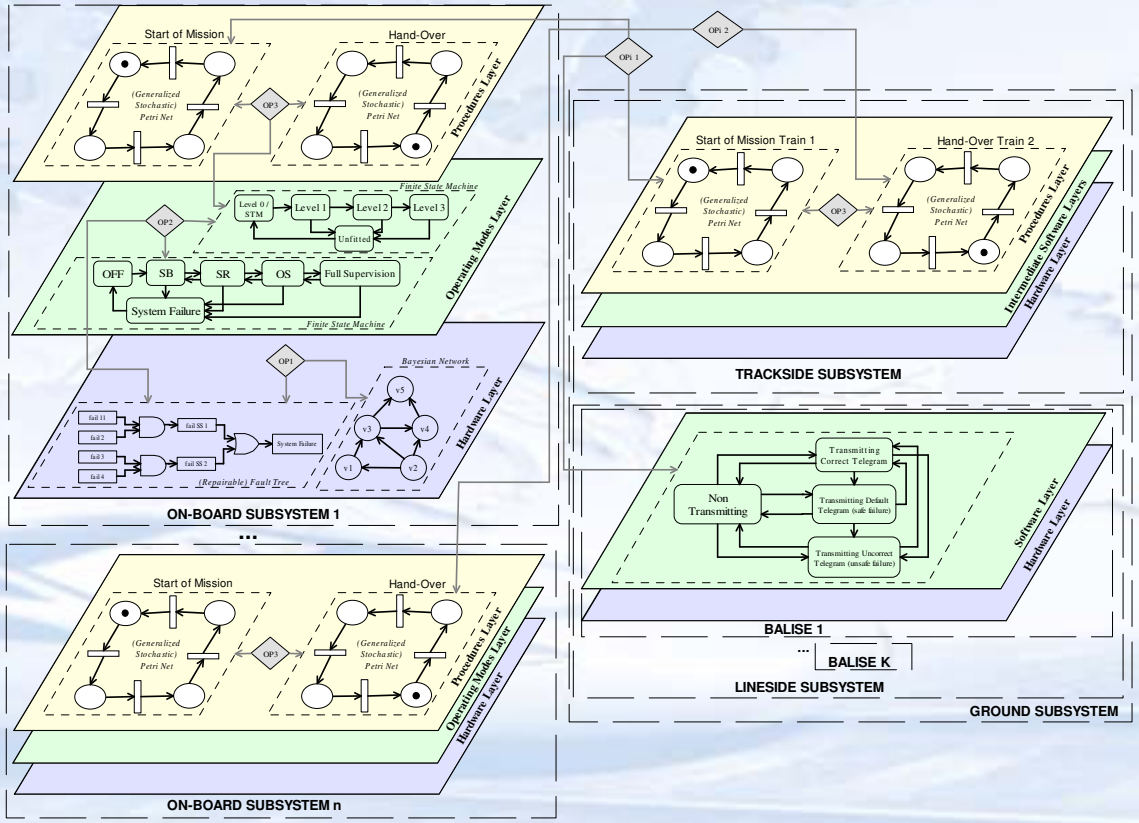


- We have already implemented a genetic algorithm to automatically maximize the return on investment while fulfilling external budget constraints

- F. Flammini, A. Gaglione, N. Mazzocca, C. Pragliola: "Quantitative Security Risk Assessment and Management for Railway Transportation Infrastructures". In: Proc. 3rd International Workshop on Critical Information Infrastructures Security, CRITIS'08, Frascati (Rome), Italy, October 13-15, 2008: pp. 213-223
- F. Flammini, V. Vittorini, N. Mazzocca, C. Pragliola: "A Study on Multiformalism Modelling of Critical Infrastructures". In: Proc. 3rd International Workshop on Critical Information Infrastructures Security, CRITIS'08, Frascati (Rome), Italy, October 13-15, 2008: pp. 395-402

Future developments

- Methodology
  - Definition of appropriate multiformalism composition operators
- Applications
  - New case-studies, e.g. system level safety evaluation



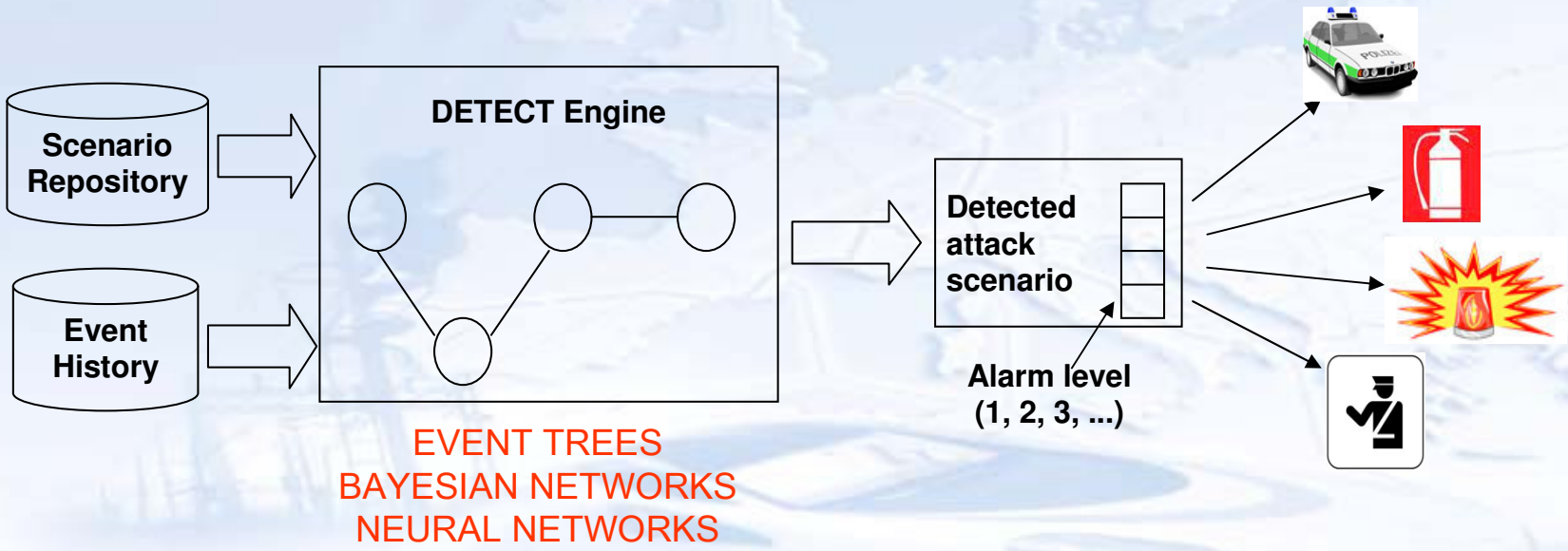
- G. Di Lorenzo, F. Flammini, M. Iacono, S. Marrone, F. Moscato, V. Vittorini: "The software architecture of the OsMoSys multisolution framework". In: Proc. 2nd International Conference on Performance Evaluation Methodologies and Tools, VALUETOOLS'07, Nantes, France, October 23-25, 2007: pp. 1-10

- Are models useful only for dependability prediction and assessment?

Experience report 5: issues

- Main problem:
  - On-line detection of threats for early warning and decision support
- Issues:
  - Integration and reasoning of multi-sensor data
  - Need for real-time detection models
- Further problem:
  - How to quantify uncertainity?

Experience report 5: solution



- F. Flammini, A. Gaglione, N. Mazzocca, C. Pragliola: "DETECT: a novel framework for the detection of attacks to critical infrastructures". In: Safety, Reliability and Risk Analysis: Theory, Methods and Applications – Martorell et al. (eds), Proceedings of ESREL'08, Valencia, Spain, 22-25 September 2008: pp. 105-112
- F. Flammini, A. Gaglione, N. Mazzocca, V. Moscato, C. Pragliola: "Wireless Sensor Data Fusion for Critical Infrastructure Security". In: Advances in Soft Computing Vol. 53: Proc. International Workshop on Computational Intelligence in Security for Information Systems, CISIS'08, Genoa, Italy, October 23-24, 2008: pp. 92-99

Thank you for your kind attention

Questions?

AnsaldoSTS
A Finmeccanica Company