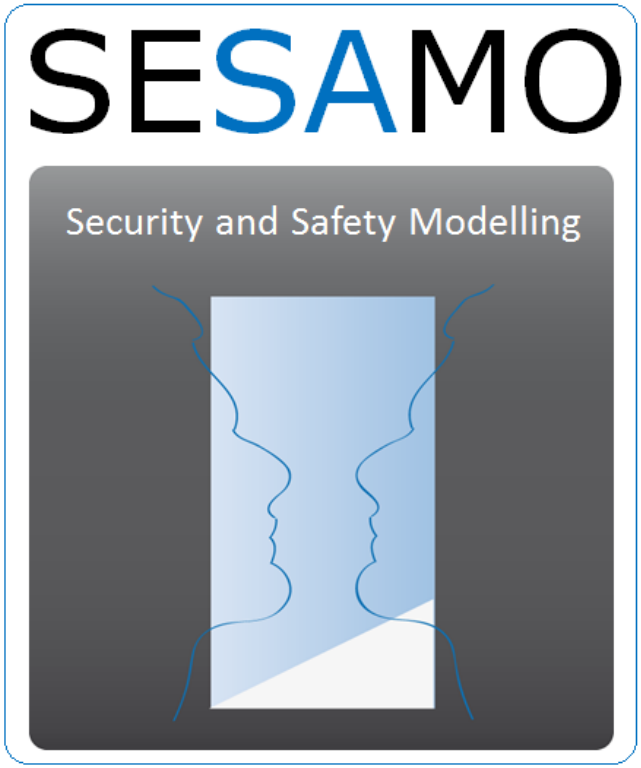


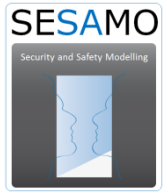
SECURITY AND SAFETY MODELLING

Robert Stroud, Adelard LLP
Lorenzo Strigini, City University

http://sesamo-project.eu

Agenda

- Project overview
- WP1 – Requirements and Use cases
- WP3 – Analysis and assessment



PROJECT OVERVIEW

Overall project figures

- Starting date: May 2012
- Duration: 36 months
- Total costs: 12 million €
- EU contribution: 2 million €
- Total effort: 1100 person months
- 20 partners

SESAMO final goal

Reducing the cost of building safe and secure products

Consortium

- 20 partners
  - 8 countries
  - 13 large industries
  - 1 SME
  - 2 research
  - 4 academia

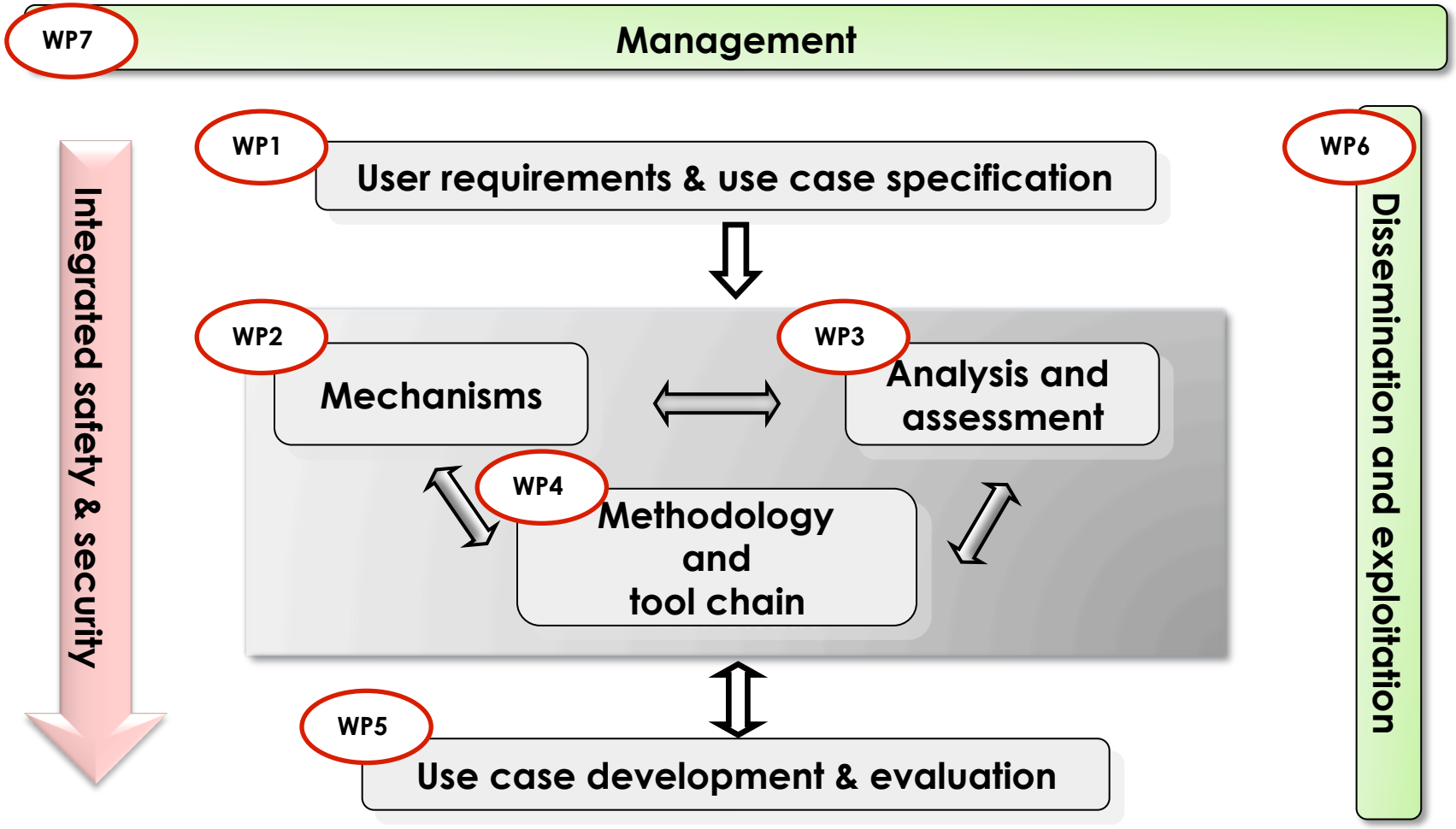
Project summary

- SESAMO addresses:
  - … the root problems arising with the convergence of safety and security in embedded real-time (and therefore time-critical) systems …
  - … subtly and poorly understood interactions between functional safety and security mechanisms …
  - … the absence of a rigorous theoretical and practical understand of safety and security feature interaction …

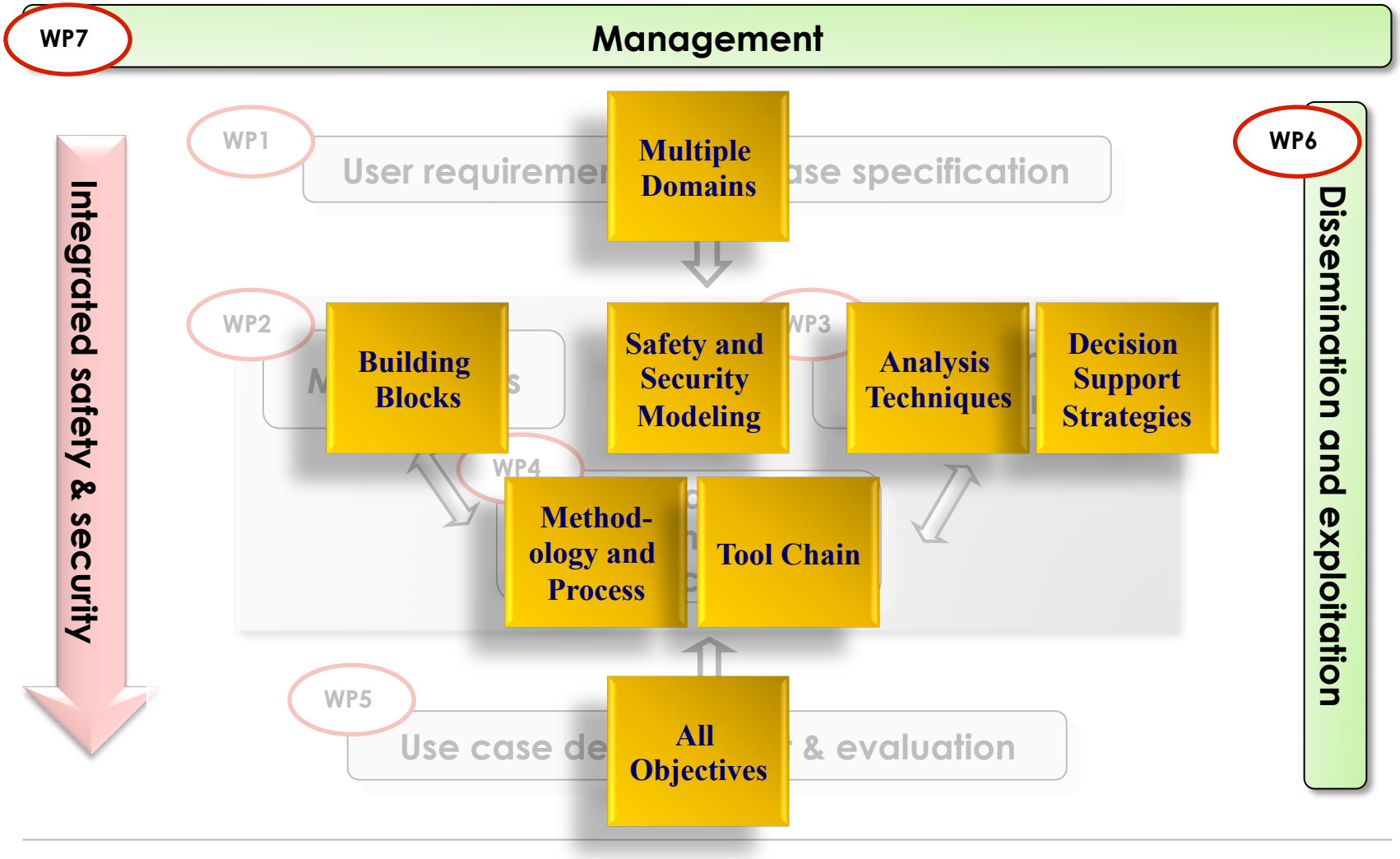
Proposed solution

- SESAMO proposes:
  - … to develop a component-oriented design methodology based upon model-driven technology …
  - … jointly addressing safety and security aspects and their interrelation for networked embedded systems …
  - … in multiple domains (e.g., avionics, transportation, industry control)

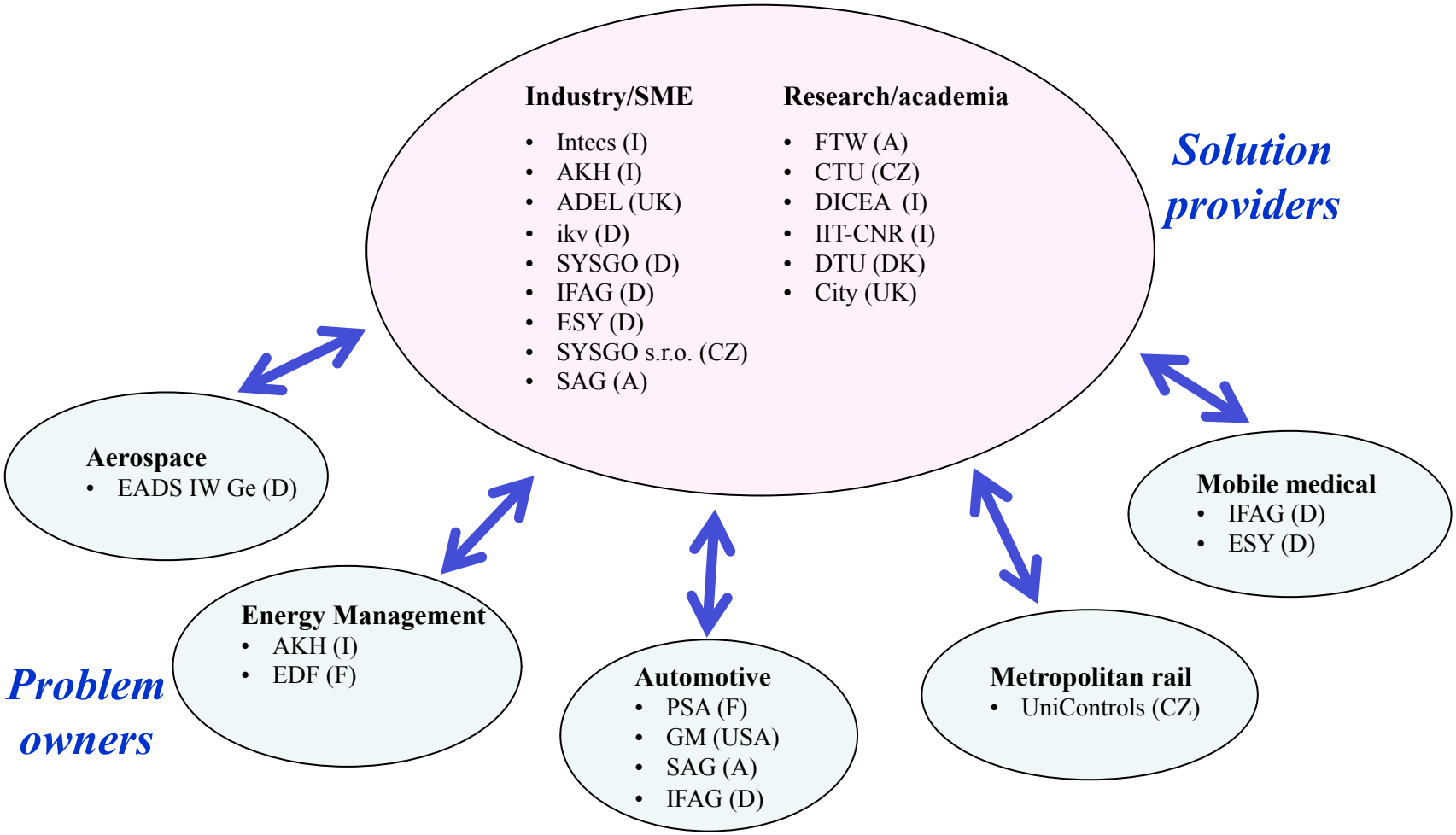
Objectives & Workpackages



Objectives & Workpackages

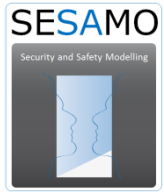


Structure of consortium



Use cases

- Avionics – EADS
- Automotive e-motor – Infineon / ikv
- Industrial drive – Siemens
- Car infotainment – Peugot Citroën
- Medical – Infineon / eesy-id
- Railway – Unicontrols / SYSGO
- Smart grid – EDF / FTW
- Oil & gas – Akhela



WP1 – REQUIREMENTS AND USE CASES

WP1 objectives

- Identification of process and methods requirements with regard to functional safety and security
- Analysis of related functional safety and security analysis standards
- Elaboration of use case scenarios and reflection of user requirements to drive the proof of concept

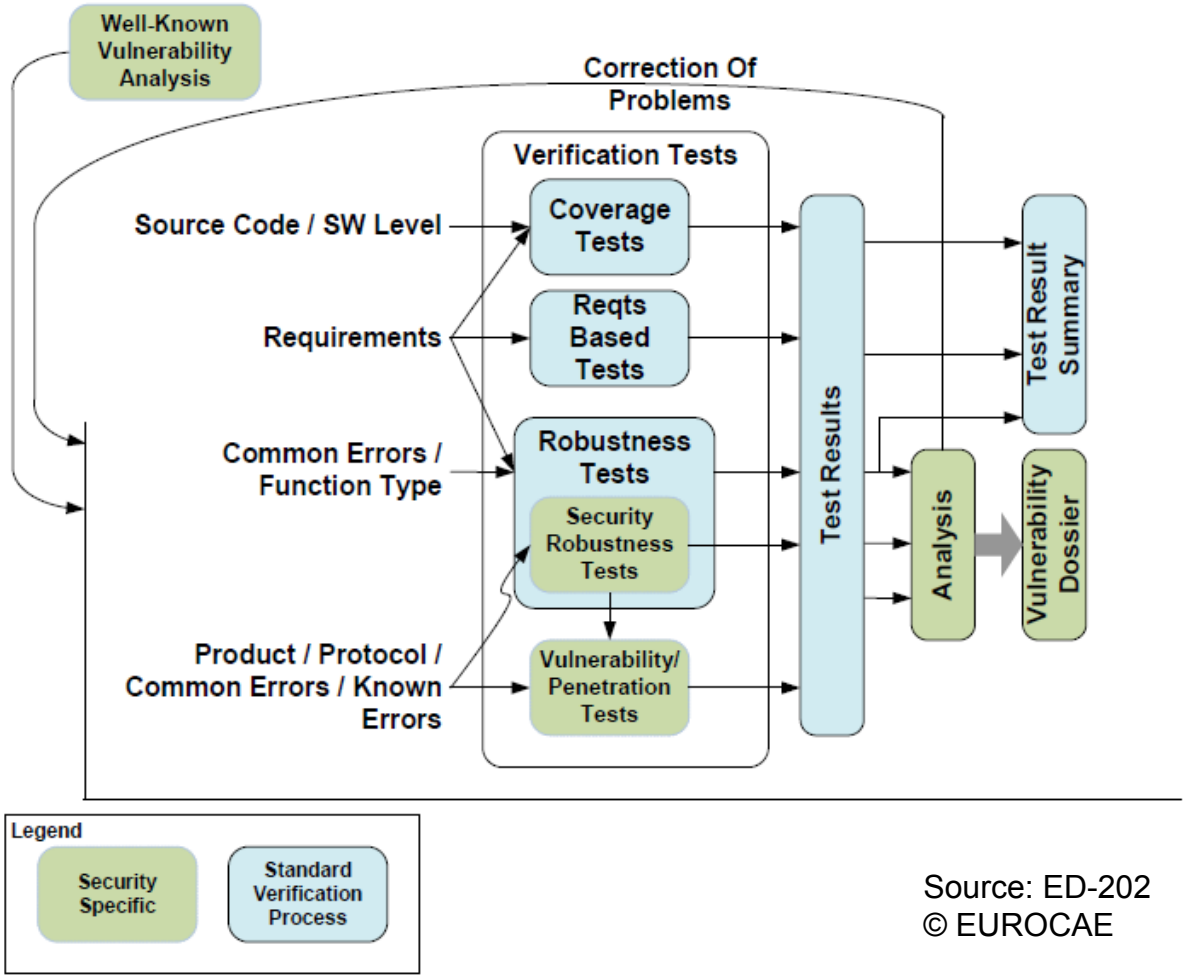
Observations - requirements

- Priorities for information security:
  - Confidentiality / Integrity > Availability
- Priorities for embedded systems:
  - Availability / Integrity >> Confidentiality
- Additional requirements:
  - Autonomous
  - Timeliness
  - Isolation
  - Safety > Security

Observations - process

- Safety is far better understood than security from both a process and a product perspective
- Some debate about how best to combine safety and security
- Not clear that applying separate safety and security processes will converge
- Hence, desirable to develop an integrated process for building a safe and secure system

Example – verification tests



Source: ED-202
© EUROCAE

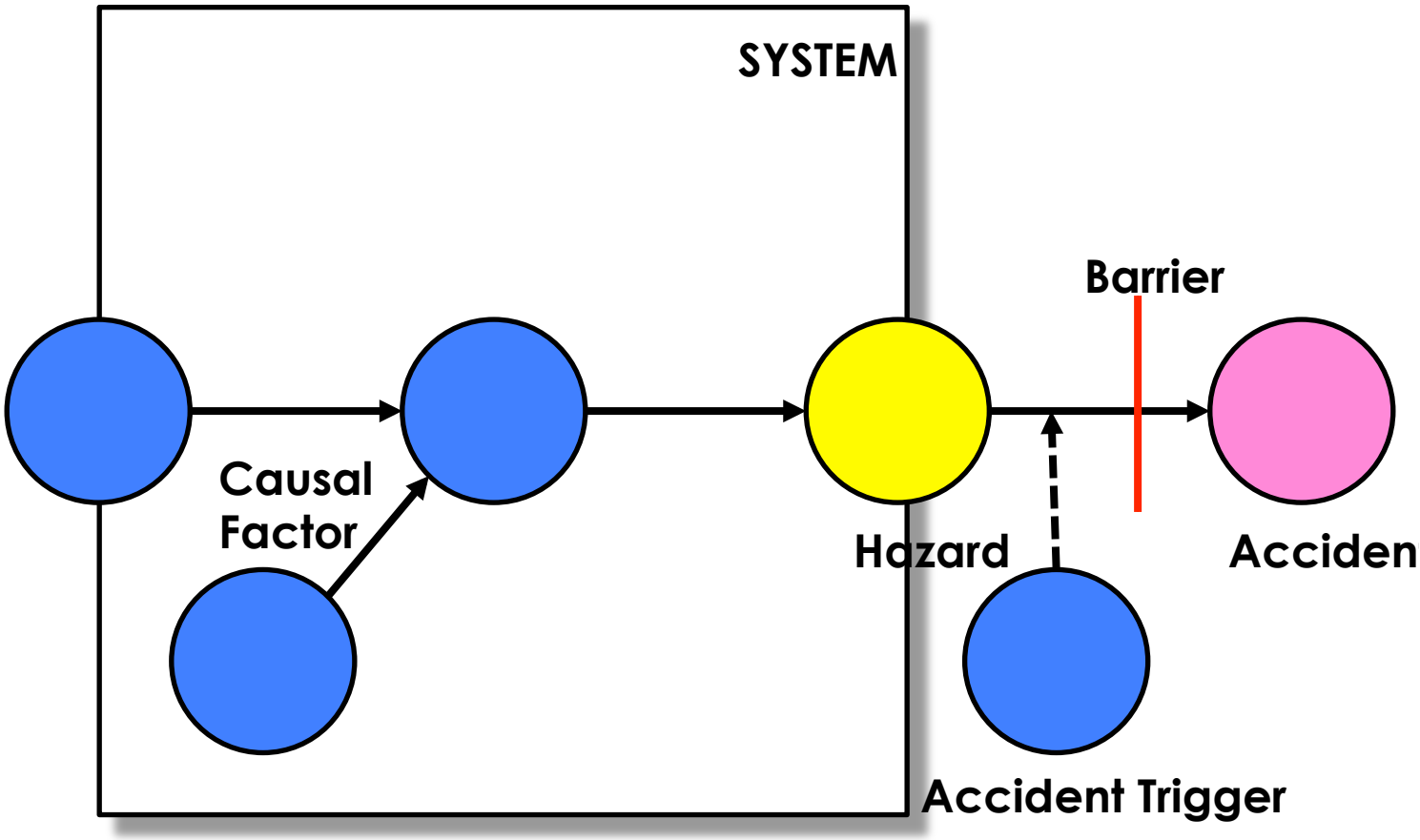
Observations - standards

- Most security standards are concerned with information security:
  - ISO 2700x
- However, some new standards are emerging for control system security:
  - ISA 99 / IEC 62443
  - NIST 800-82
- The Common Criteria deal with security assurance rather than secure development

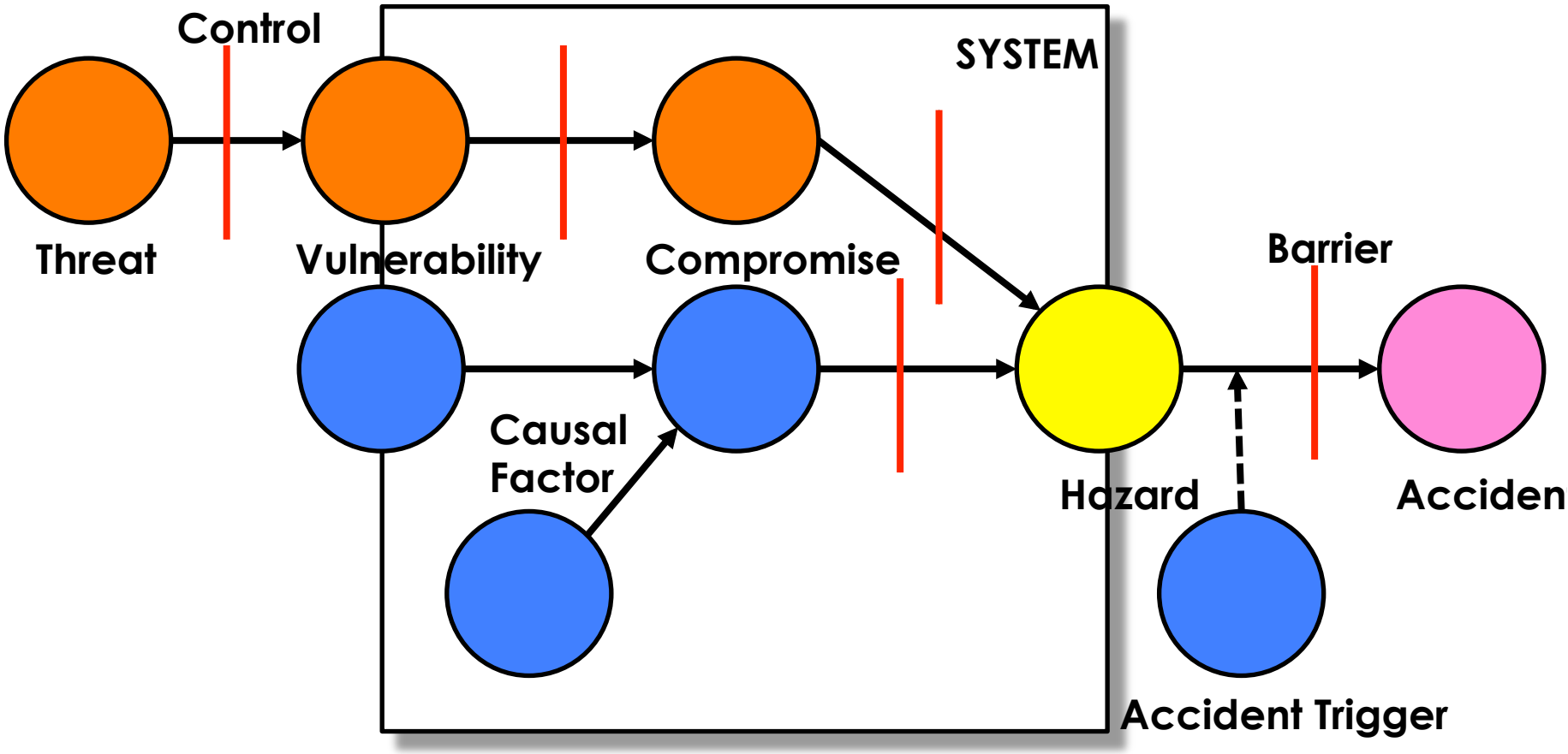
Security-informed safety

- Security requirements are beginning to appear in safety standards
- Clause 1.2 k) of IEC 61508-1:2010:
  - *"requires malevolent and unauthorised actions to be considered during hazard and risk analysis. […]"*
- Similarly, draft EN 50126-5:2012 states:
  - *"The Safety Case shall demonstrate that […] misuse-based failures on external interfaces do not adversely impact on the safety integrity of the system"*

Safety analysis (Yellow book)



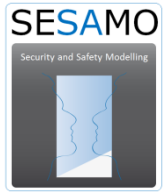
Safety and Security analysis



Safety case challenge

- *"The safety case shall demonstrate the appropriateness [...], of the following:*
  - *Choice of cryptographic techniques*
  - *Choice of cryptographic architectures*
  - *Management activities*
- *Reasonable assumptions shall be described about the nature, motivation, financial and technical means of an attacker [...]"*

Clause 7.3.8.2, EN 50159:2010



WP3 – ANALYSIS AND ASSESSMENT TECHNIQUES

WP3 - Objectives

- Goal of WP3 is to provide

  qualitative and especially quantitative techniques for the analysis and assessment of safety and security properties, both separately and in integrated ways

  - linked to WP2, feeding into WP4
  - first surveyed techniques brought in by partners to address various SESAMO challenges
  - working on demonstration of techniques applied to use cases

Managing the "clashes"

- managing coexistence and trade-offs between safety/security requirements
  - different processes for safety/security oriented development
  - "metrics": standard-oriented, risk-oriented
- directions explored:
  - integration of processes for safety and security
  - design analysis techniques that combine the two kinds of issues
  - probabilistic analyses that capture both concerns

Wide range of techniques

- design-oriented analyses for verification
- extending structured development process to include security as well as safety
- organising the evidence that supports trust in the safety / security properties
- probabilistic analysis for informing design/ assessment in quantitative risk terms
  - with application to specific design trade-offs
  - with techniques to master full-scale system complexity in use cases

Techniques being studied

Techniques/methods	*Use case applications now studied*
Stochastic action networks	Trade-offs, automotive and medical use cases
Preliminary Interdependence Analysis	Complex security/safety interdependences in oil/gas use case
BDMP based analysis	Smart grid use case
Proofs of information trustworthiness / use match	Partitioning (e.g. Aviation use case), auto infotainment
Schedulability analysis	Trade-offs in communication
FTA, FMECA, HAZOP, ...	Extending to cover safety and security: automotive, industrial drive, rail
Security-informed safety cases	Aviation use case

Some examples ..

... in pictures

Modelling attacker strategies

- so as to assess system design wrt attack

$t = N$
for all $s^N \in S$ **do**
  $u^N(s^N) = r^N(s^N)$
end for
while $t > 1$ **do**
  $t = t - 1$
  for all $s^t \in S$ **do**

$$u^t = \max_{a \in A_{s^t}} \left\{ r^t(s^t, a^t) + \sum_{a_{ij} \in A_i} \mathbf{Pr}_{ij}^t \cdot u^{t+1}(s_j) \right\}$$

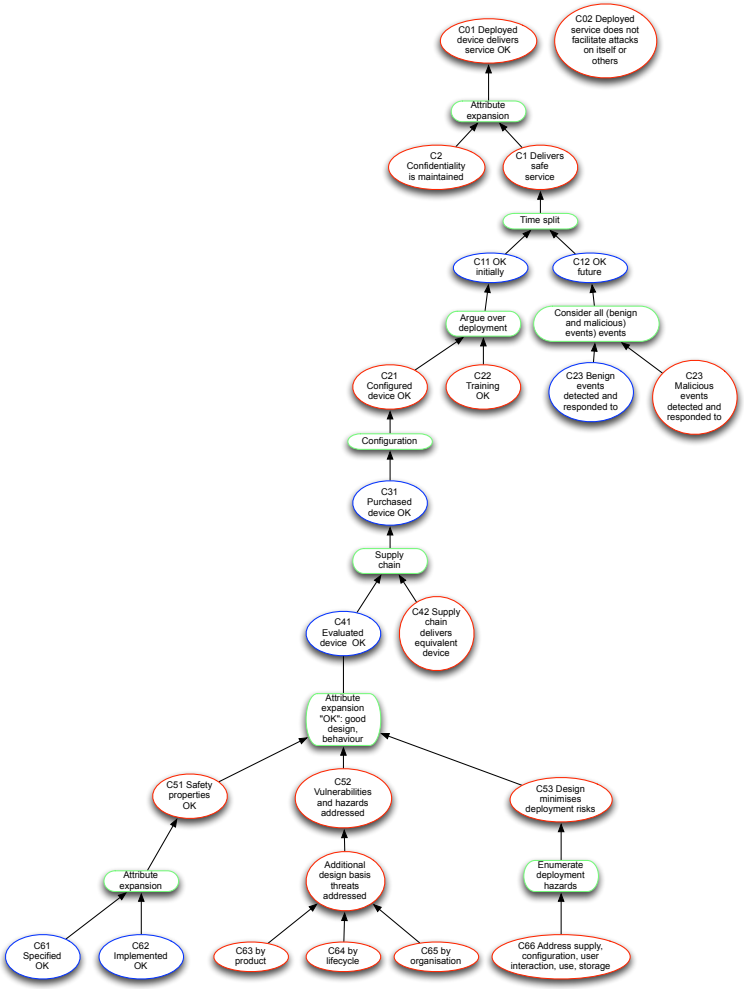
$$A^*_{s^t,t} = \arg\max_{a \in A_{s^t}} \left\{ r^t(s^t, a^t) + \sum_{a_{ij} \in A_i} \mathbf{Pr}_{ij}^t \cdot u^{t+1}(s_j) \right\}$$

  end for
end while

- evolving to probabilistic analysis, e.g. number of steps to violation

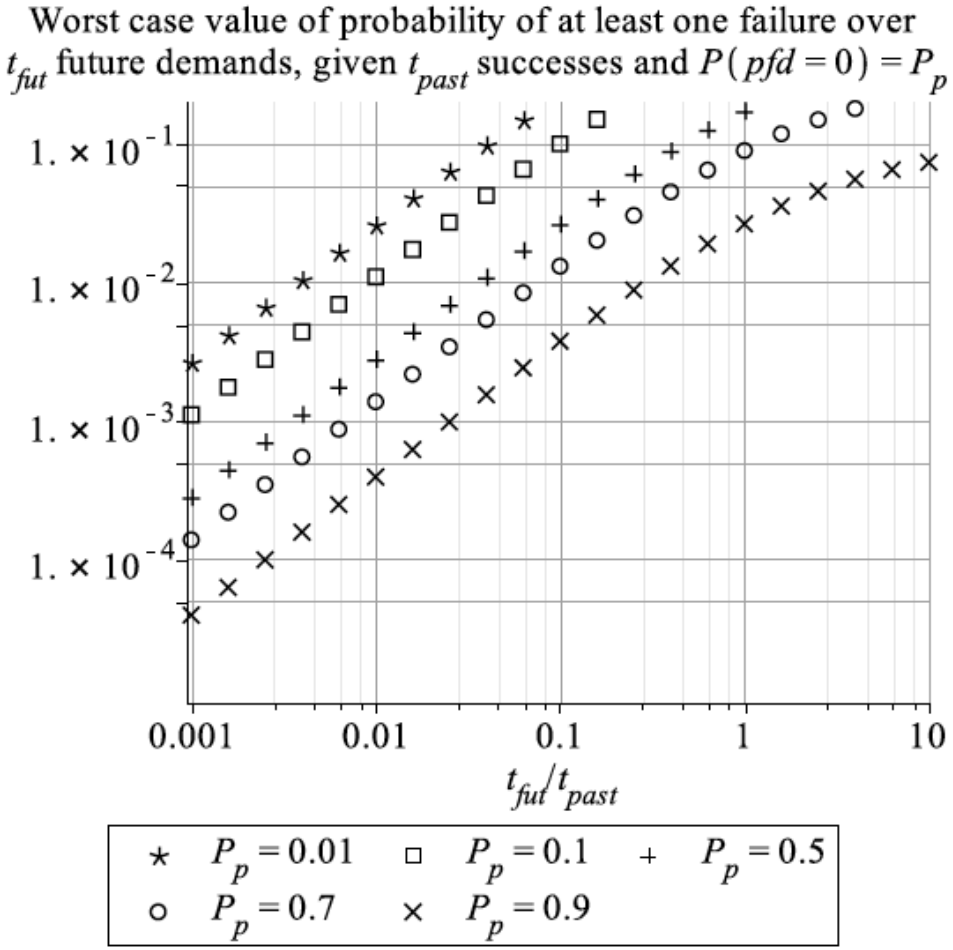
Security-Informed Safety Case

- What impact does security have on the safety case?
- considerations include e.g.:
  - Supply chain integrity
  - Malicious events post deployment
  - Design changes to address user interactions, training, configuration, vulnerabilities
  - Additional functional requirements that implement security controls
  - Possible exploitation of the device/service to attack itself or others



Inference from operation and process evidence

- integrating knowledge that developers "ticked all the boxes"
- with failure-free operation
- for conservative prediction of risk



PIA integration example