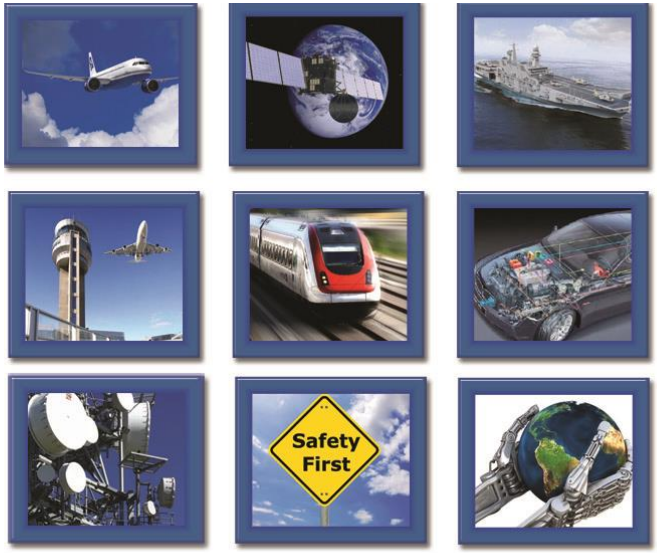
intecs

the Brainware company

Automotive SPIN



12 November 2015

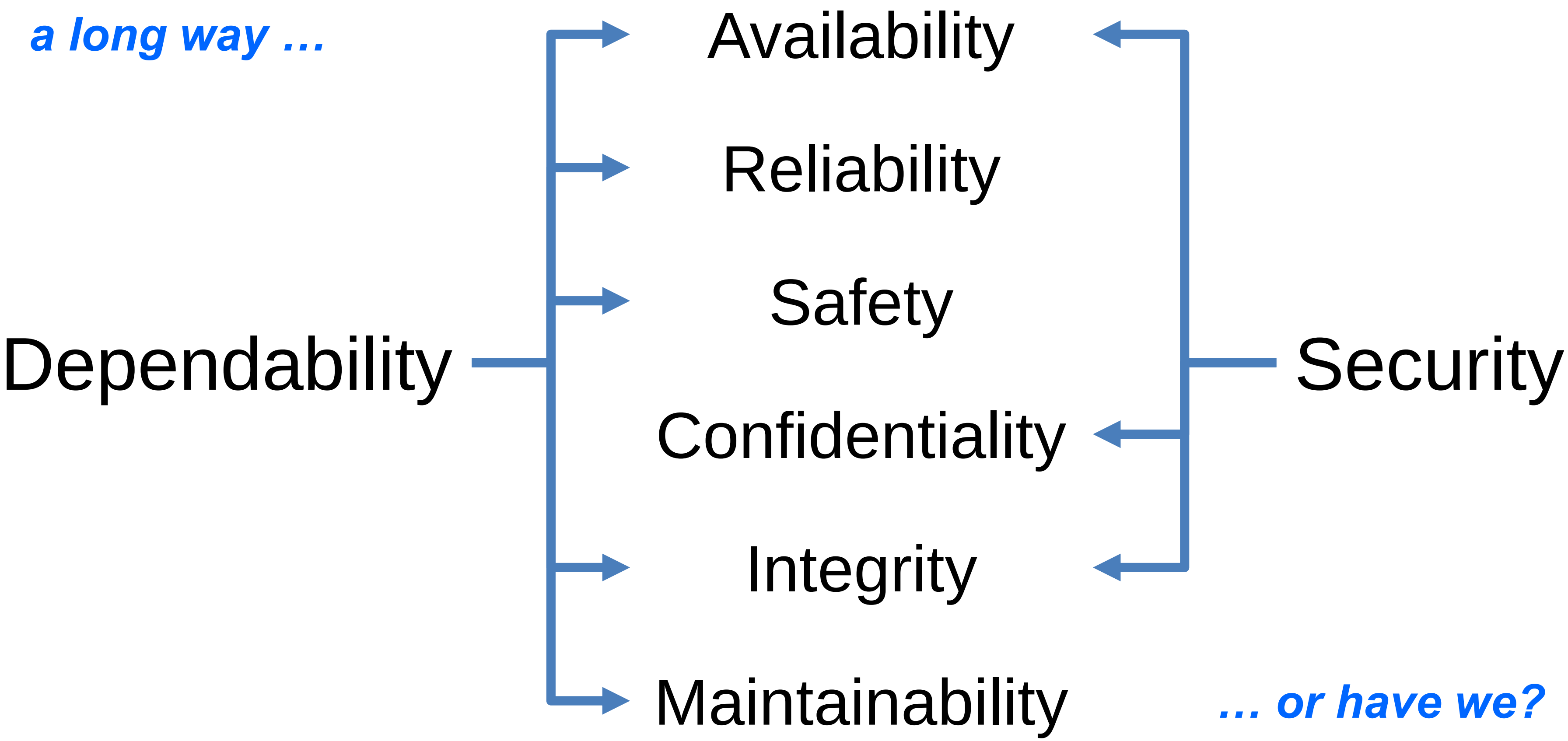
Integration of Safety & Security in Automotive Electronic Systems

John Favaro

john.favaro@intecs.it

A Balance of Attributes

We have come a long way …



Dependability

Availability

Reliability

Safety

Confidentiality

Integrity

Maintainability

Security

… or have we?

(Basic Concepts and Taxonomy of Dependable and Secure Computing, Avizienis et al.)

The Problem

INTECS PROPERTY - REPRODUCTION FORBIDDEN

Optimization

- Automotive electronics systems are heavily optimized
  - Down to the very last microsecond, gram, penny, ampere
  - For cost, weight, power, performance, …
- If you come in with security separately, it’s already too late
  - Only expensive solutions available

Safety & Security in ISO 26262

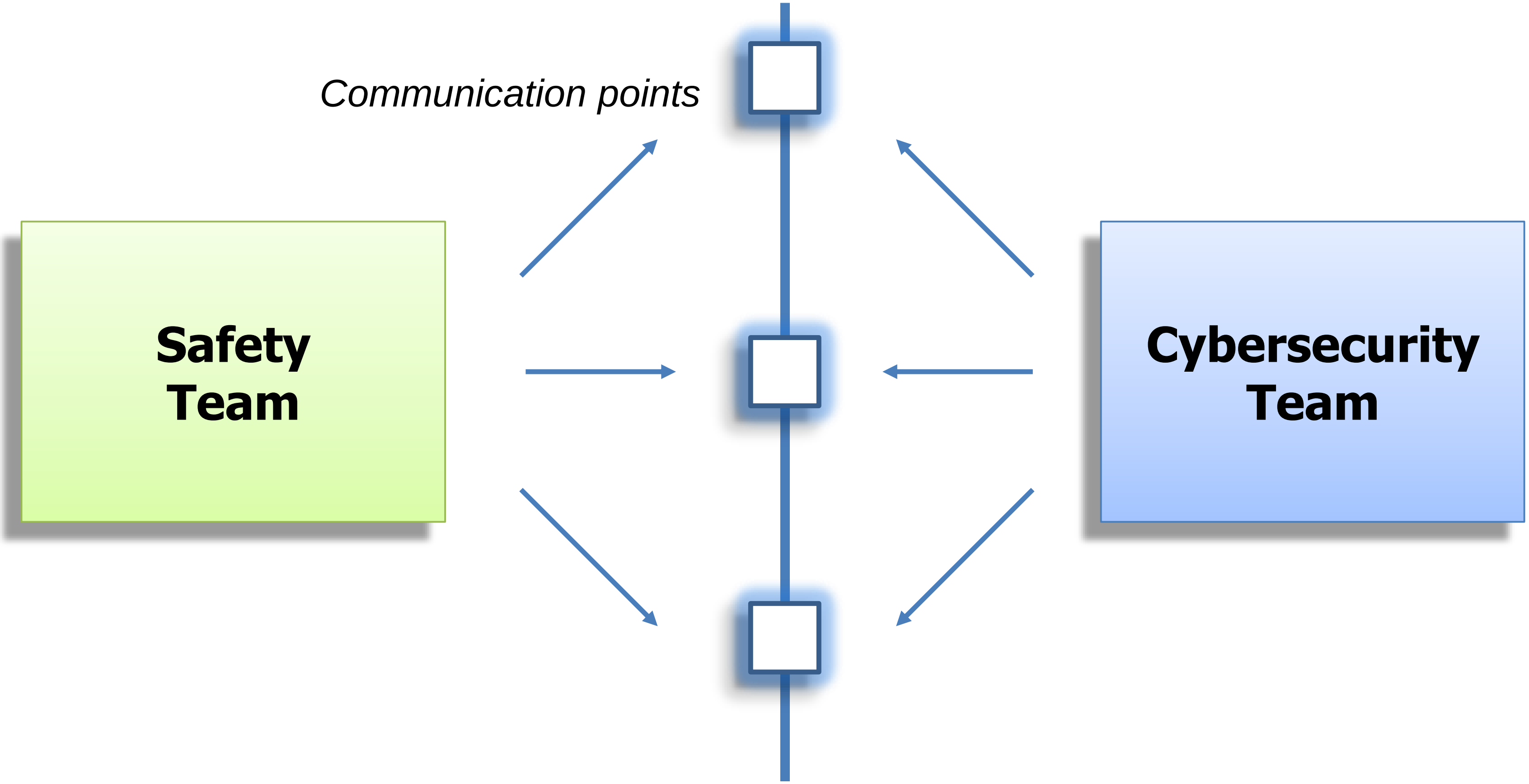
- 1st edition published November 2011
- Work on 2nd edition begin in 2015
  - Publication foreseen in 2017
- No cybersecurity in the 1st edition
  - IEC 61508 has an embryonic approach
  - For the 2nd edition of ISO 26262, an SAE task force is elaborating an approach
  - J3061 “Cybersecurity Guidebook”

(Thanks to G. Sartori for current information on WG activity status)

Separate Teams

- The task force has decided not to add security requirements to ISO 26262
  - Safety team / security team
  - Separate lifecycles, separate activities
- Elaborating a document describing the approach
  - *Guidance on Potential Safety-Cybersecurity Interface Points (Informative)*

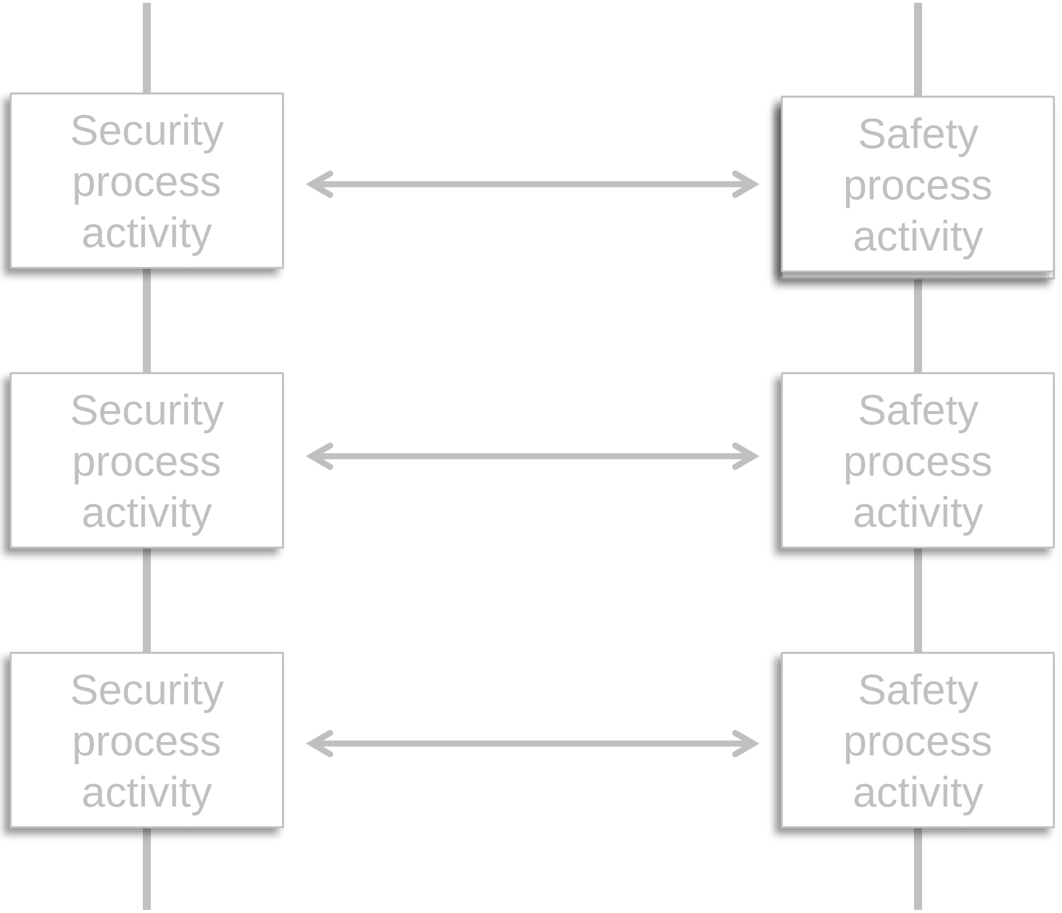
An Interface



Safety Cybersecurity Interface (SCI)

From Conceptual to Practical

The Standard will go no further than this


Security process activity
Safety process activity
Security process activity
Safety process activity
Security process activity
Safety process activity

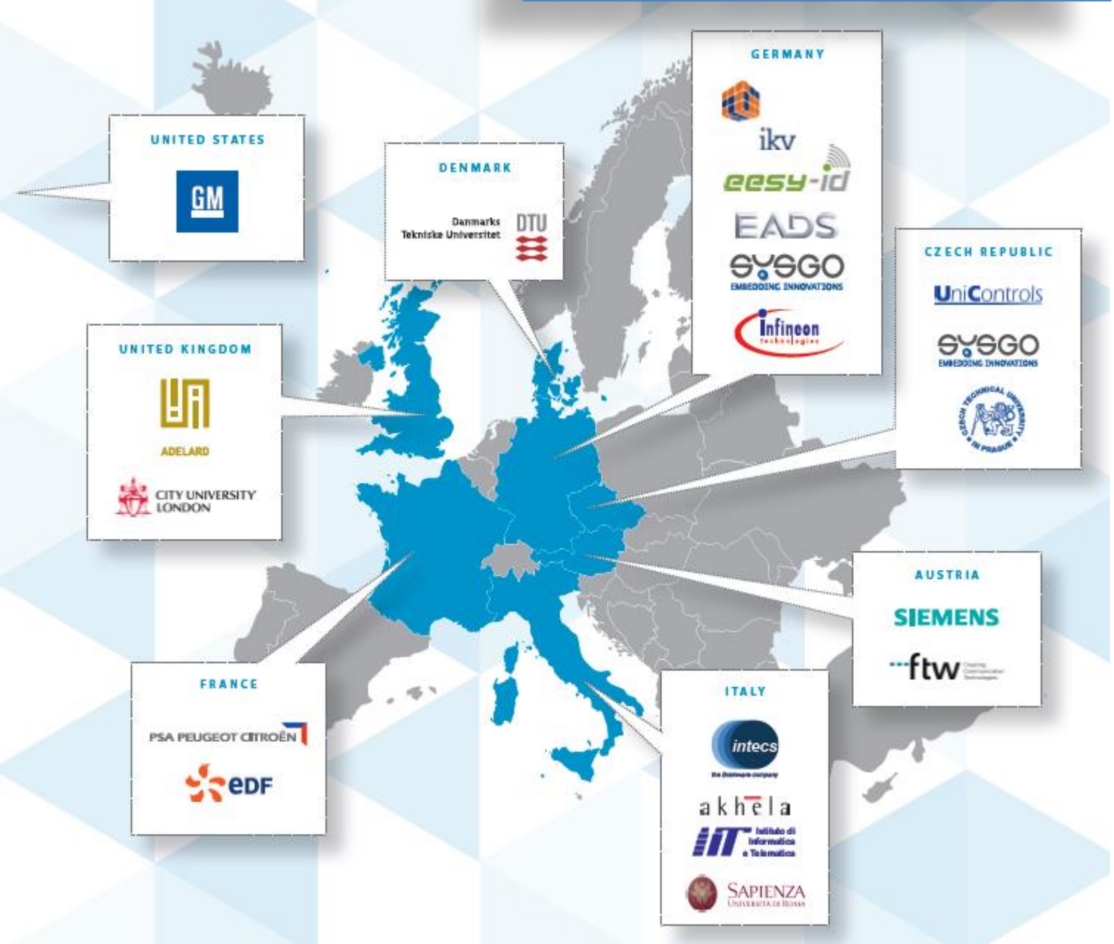
How to work within this context?

SESAMO Consortium

Coordinator: Intecs

- 20 partners
  - 8 countries
  - 13 large industries
  - 1 SME
  - 2 Research
  - 4 Academia

OEMs: GM, PSA



What is SESAMO?

- 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 understanding of safety & security feature interaction

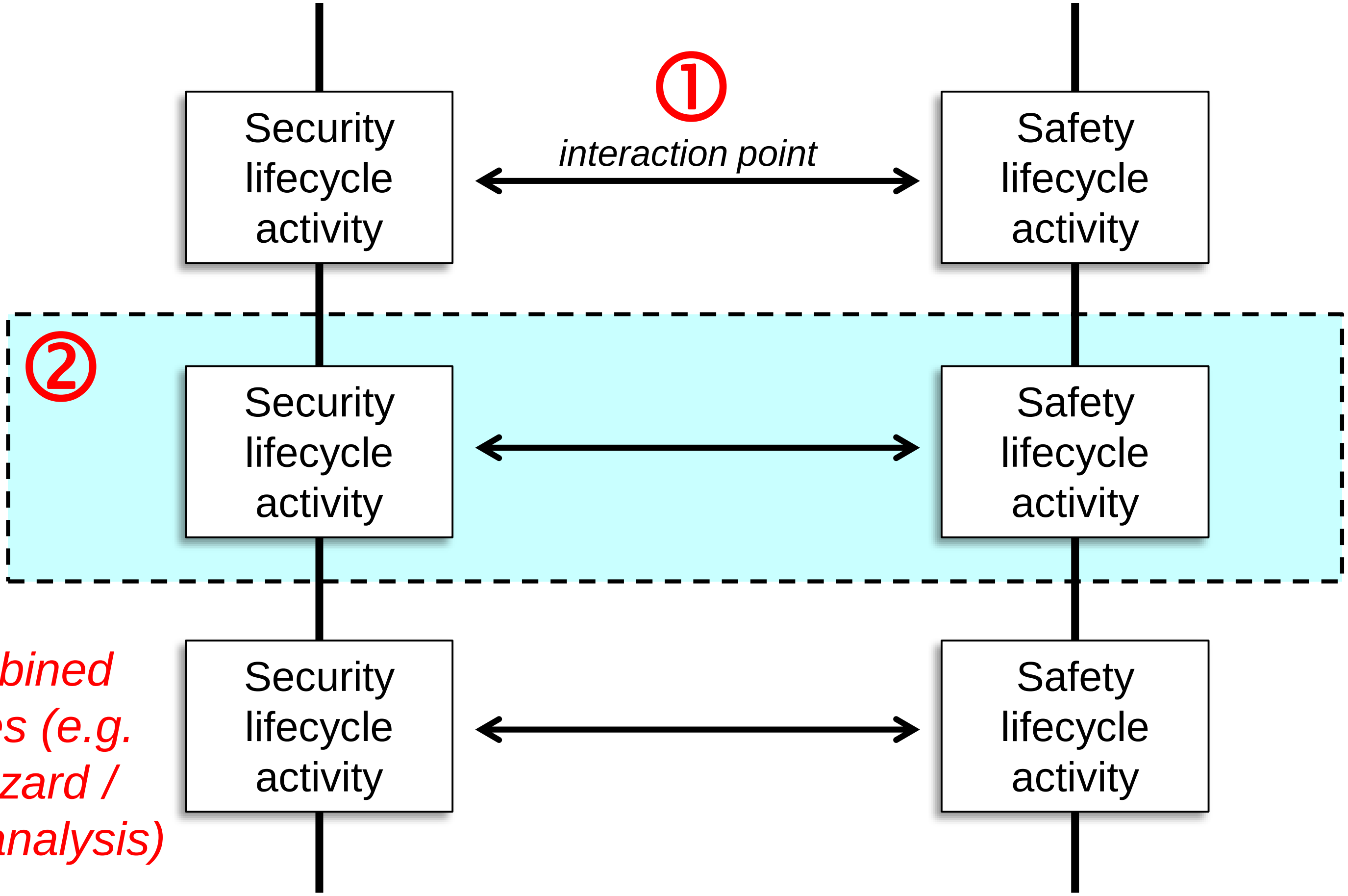
The Integrated Methodology

Aligned Processes

- We propose similarly structured and aligned processes but not necessarily a fully integrated process
  - Allows to consider security from beginning – not added at a later stage when it is too late
  - Leads to “Security informed Safety”
- **Weak Interactions**
  - Identify **common building blocks** in the construction of safe and secure automotive systems
  - Provide trade-off analyses for synergies, interference, etc.
- **Strong Interactions**
  - Identify **common activities** in aligned processes (e.g. hazard and threat analysis) and create joint activities)

SESAMO Integrated Approach

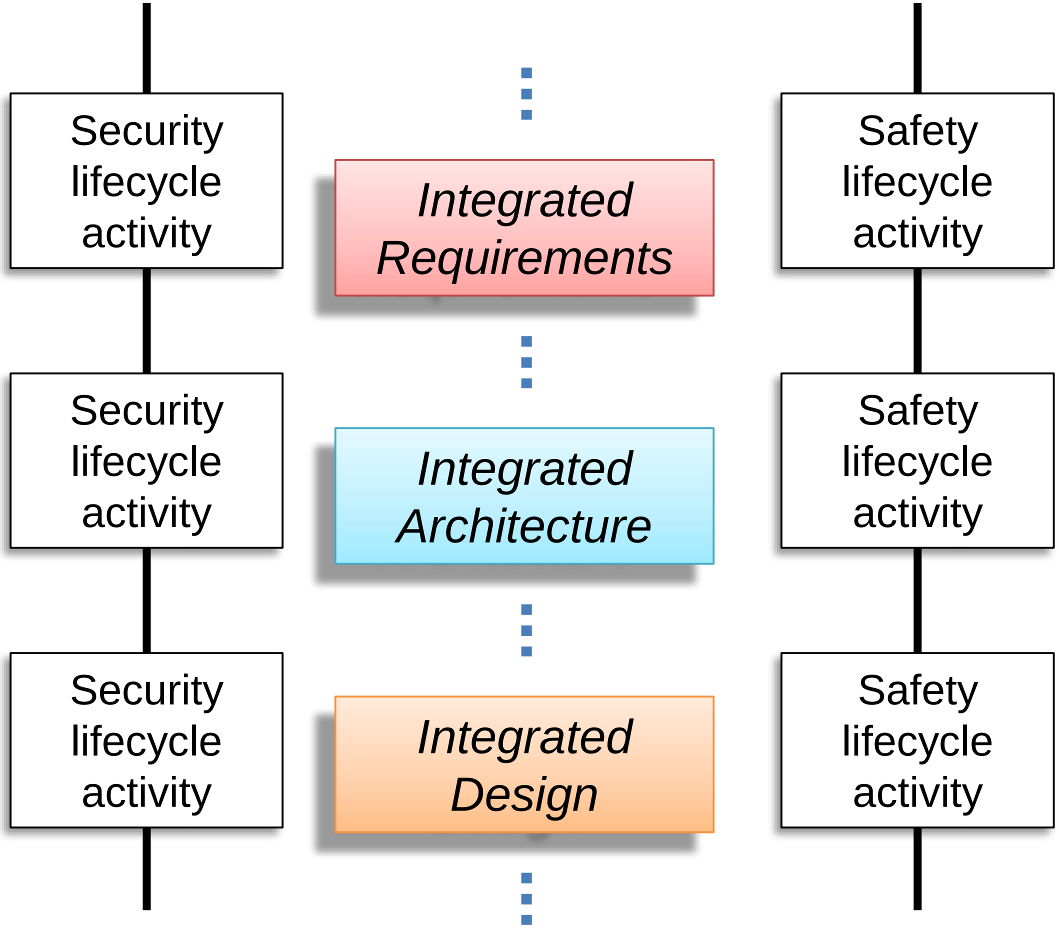
1. Tradeoff analysis (e.g. effect of chosen security mechanism on safety)


①
interaction point
Security lifecycle activity
Safety lifecycle activity
②
Security lifecycle activity
Safety lifecycle activity
Security lifecycle activity
Safety lifecycle activity

2. Combined activities (e.g. joint hazard / threat analysis)

INTECS PROPERTY - REPRODUCTION FORBIDDEN

Single Set of Work Products


Security lifecycle activity
Integrated Requirements
Safety lifecycle activity
Security lifecycle activity
Integrated Architecture
Safety lifecycle activity
Security lifecycle activity
Integrated Design
Safety lifecycle activity

Building Blocks

Design solutions and architectural patterns	Components	Algorithms and protocols	
Redundancy and diversity	Run-Time Monitoring	Encryption and decryption	Node authentication
Partitioning (Space/Time)		Signature generation and verification	Protocols for real-time communications
		Integrity protection	Checksums
		…	…

Example: Space-Partitioning

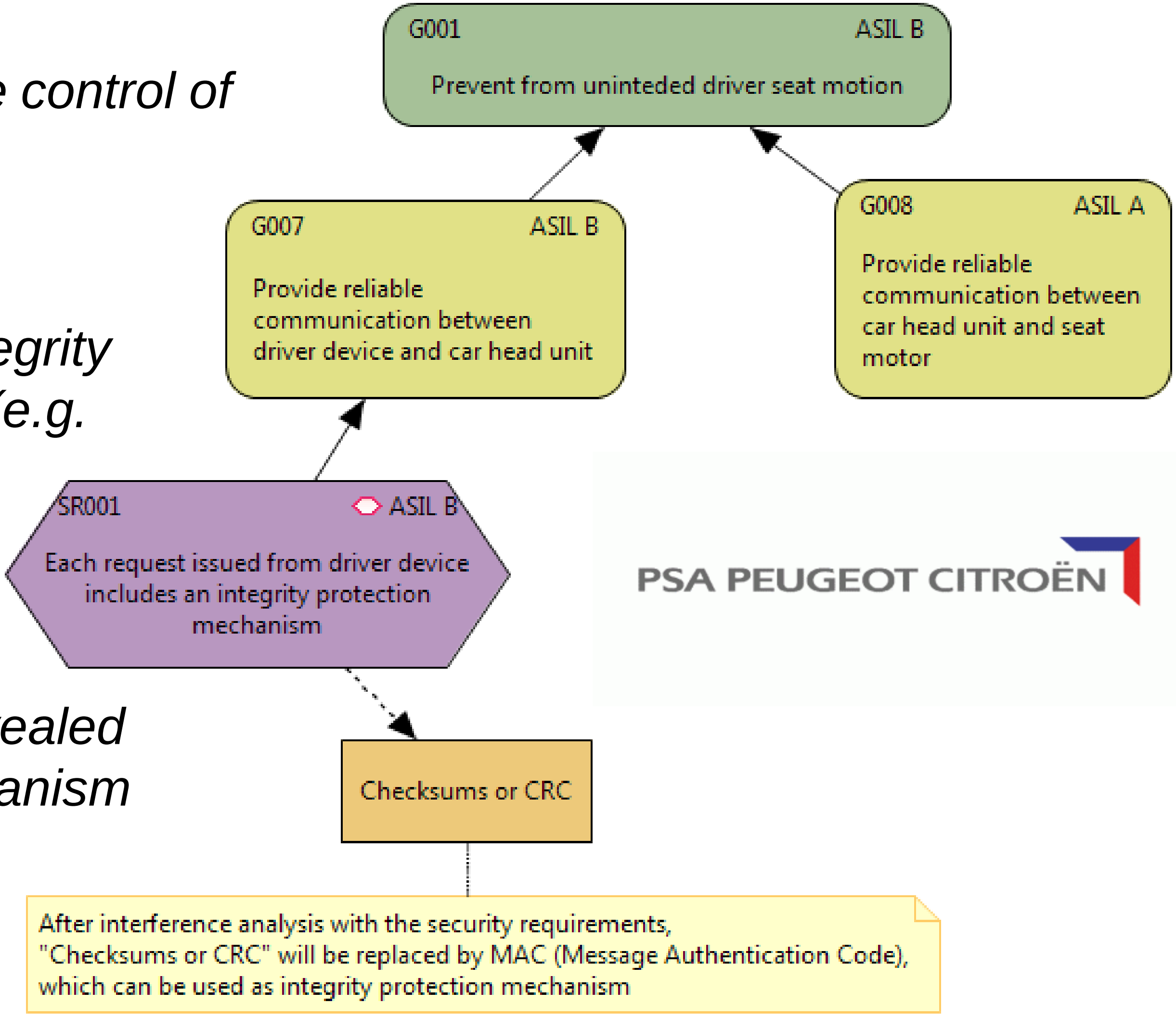
	Safety	Security
Trade-offs	➢ Increased execution time of each application through context switches ➢ Limited communication interface between secure and unsecure system increases Worst Case Execution Time (WCET) of command processing	➢ Additional communication interface between secure and unsecure system increases potential of attacks
Synergies	➢ Space partitioning of secure system prevents fault propagation of unsecure system components	➢ Space partitioning protects secure system from security attacks of unsecure system

A Practical Example

Remote smartphone control of driver seat position

Safety requirement: integrity protection mechanism (e.g. Checksums or CRC)

Interference analysis revealed synergy with MAC mechanism for security



G001 ASIL B

Prevent from uninteded driver seat motion

G007 ASIL B

Provide reliable communication between driver device and car head unit

G008 ASIL A

Provide reliable communication between car head unit and seat motor

SR001 ASIL B

Each request issued from driver device includes an integrity protection mechanism

Checksums or CRC

After interference analysis with the security requirements, "Checksums or CRC" will be replaced by MAC (Message Authentication Code), which can be used as integrity protection mechanism

PSA PEUGEOT CITROËN

Conclusions

- Successful automotive safety and security is strongly dependent on the methodology
  - For disciplined, well constructed development
  - For convincing argumentation in assessment
- The methodology must integrate safety and security
  - But the standards are lagging behind
- The SESAMO integrated methodology takes a model based approach
  - provides extensive tool support for the methodology – essential for traceability
- Provides a practical approach and a roadmap to future integration in both standards and practice

THANK YOU !

Roma
Sede Legale; Salita del Poggio Laurentino 7; I– 00144 Roma;
tel +39 06 20 39 28 00; fax +39 06 20 39 28 58

Pisa
Via Umberto Forti Trav. A5; Loc. Ospedaletto; I–56121 Pisa;
tel +39 050 96 57 411; fax +39 050 96 57 400

Fusaro (NA)
Via Giulio Cesare, 105; I-80070 Bacoli (NA);
tel +39 081 52 72 854; fax +39 081 52 72 828

Napoli
Via Giovanni Porzio, 4; Centro Direzionale Isola F4; I- 80143 Napoli;
tel +39 081 73 48 087; fax +39 081 73 48 296

Milano
Via Archimede 10; I- 20129 Milano;
tel +39 02 55 19 47 65; fax +39 02 55 18 0041

Torino
corso Marche 79; I-10147 Torino;
tel +39 349 4719515

Cagliari
Via Sonnino, 46; I–90125 Cagliari;
tel +39 070 668 593; fax +39 070 668 594

Genova
Via Federico Avio 4; I-16151 Genova;
tel +39 010 6466052; fax +39 010 6438884

L'Aquila
S.S. 17 Località Boschetto 67100 L'Aquila
tel +39 0862 3441; fax +39 0862 344527

Munich
Josephsspitalstraße 15; D-80331 München

Paris
73, Boulevard Haussmann; F-75008 Paris

Toulouse
55, Avenue Louis Breguet; Bat. 7 – Bureau 24; F–31400 Toulouse;
tel +33 (0)5 612 03 299; fax +33 (0)5 612 03 297

www.intecs.it