Security and Dependability Challenges of IT/OT Integration

Paulo Esteves-Veríssimo
Univ. of Luxembourg, FSTC / SnT

paulo.verissimo@uni.lu
http://staff.uni.lu/paulo.verissimo

CritiX Lab (Critical and Extreme Security and Dependability)

ADA Europe, Lisboa, Portugal, June 2018.

A brief tour of the recent past

Classical CII cyber risk analysis

misconceptions

2005

- physical infrastructures are essentially attackable "physically"
- virtual infrastructures are essentially attackable "virtually"
- they have separate nature and scope
- CII on the other hand have a separate nature from "normal" networks/systems

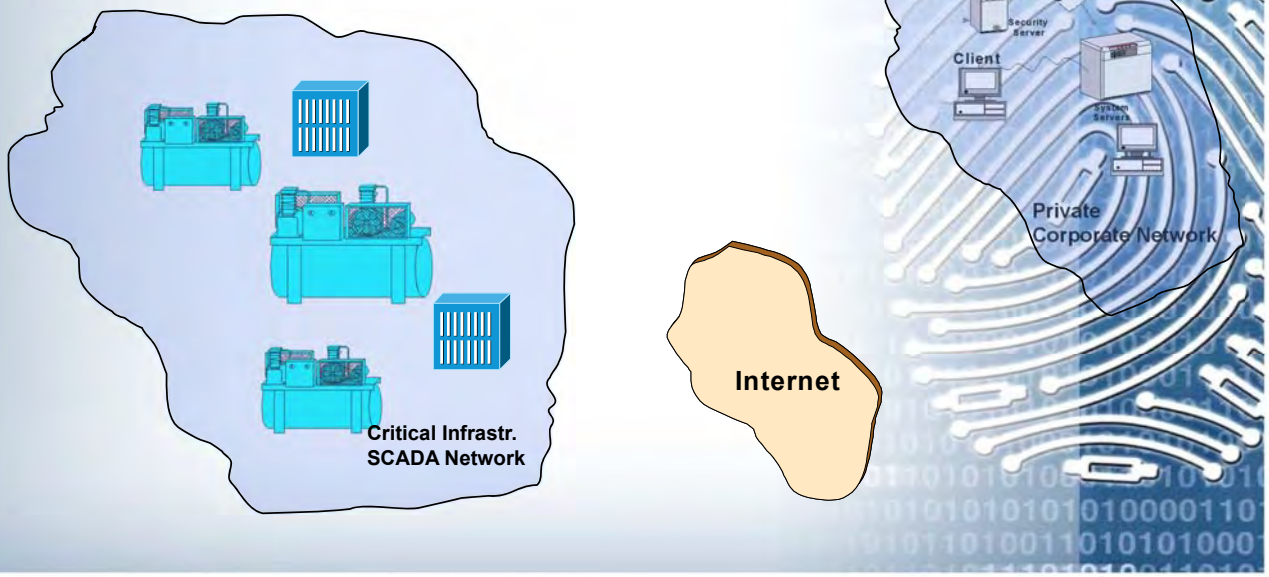
«Today (2005), these are misconceptions to be avoided»

From CIs to CIIs

or the dawn of OT

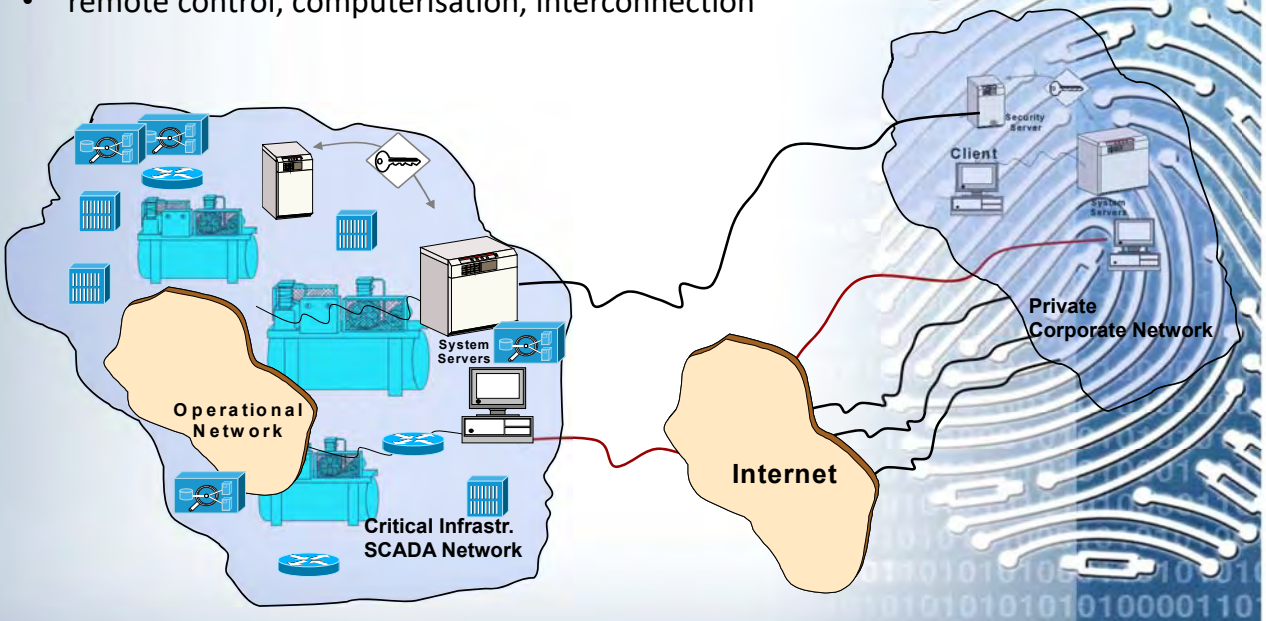
Critical Infrastructures in the old days

- no interconnection, low digital content



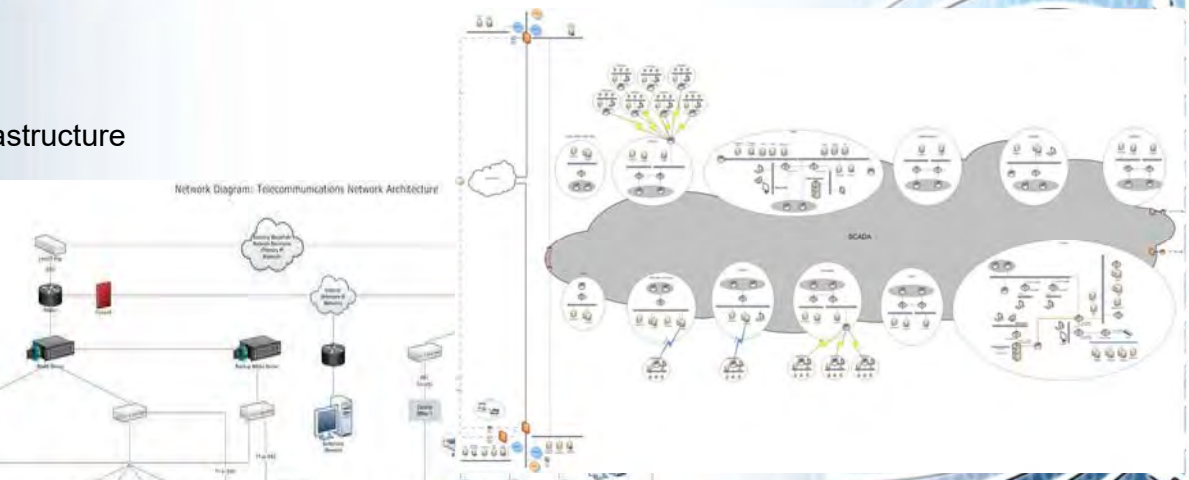
Critical *Information* Infrastructures in the present

- remote control, computerisation, interconnection



IT vs. OT infrastructures
find the differences (?) …

OT infrastructure



IT infrastructure

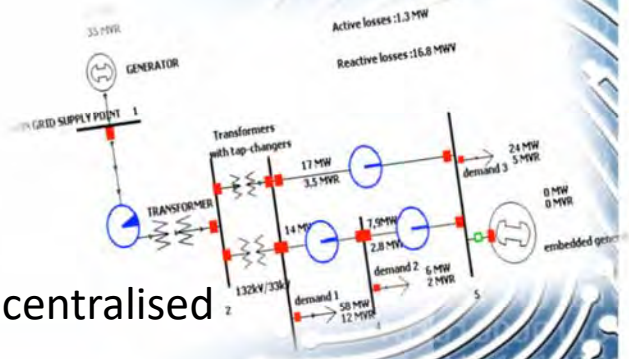
Evolution of CII
or the convergence of IT and OT

- IT and OT look the same
- So, have been analysed and treated the same way

- However, they *just look* the same …
- Some game changers appeared …

The advent of distributed generation

- From --- unidirectional and centralised load flow model
  - production
  - transport
  - distribution

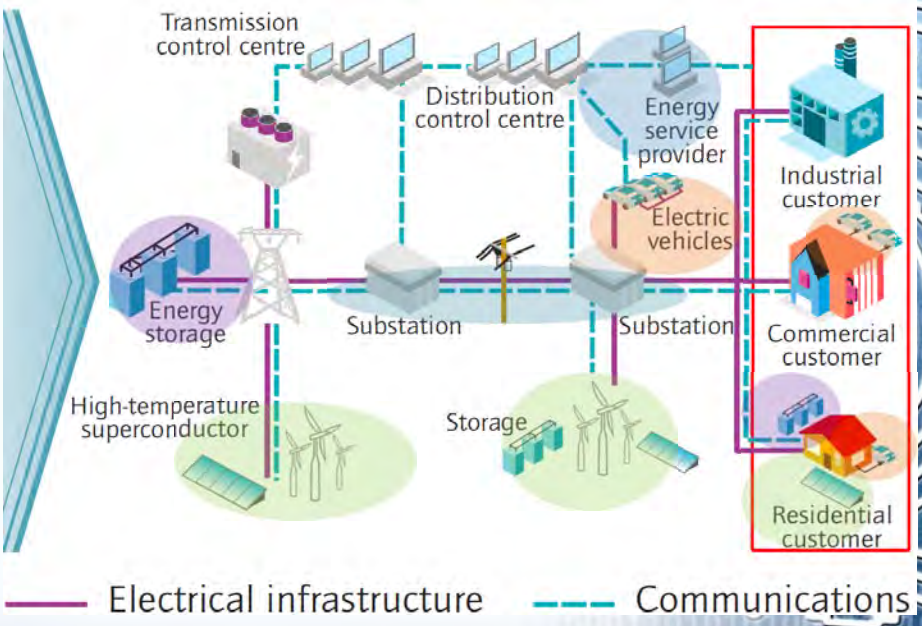


- To --- multidirectional and decentralised load flow model
  - production + transport + distribution

crucial for *security* of energy supply in a distributed generation and renewals-enabled world

The advent of Smart Electrical Grids

- Flexible & distributed generation
- Storage capability
- Electric mobility
- Sophisticated comms infrastructure
- Markets & regulation

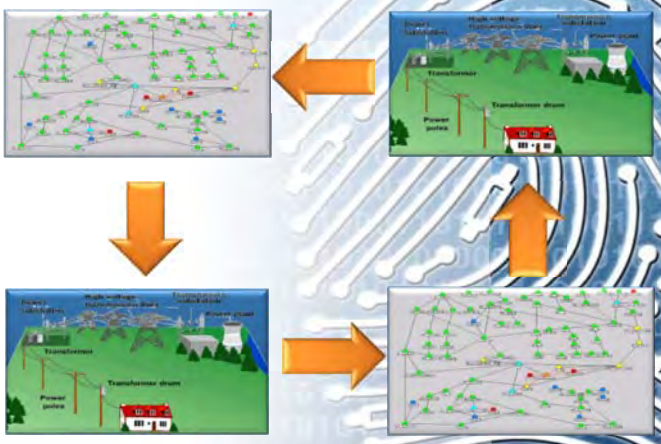


Source: *www.iea.org*

Unexpected interdependencies

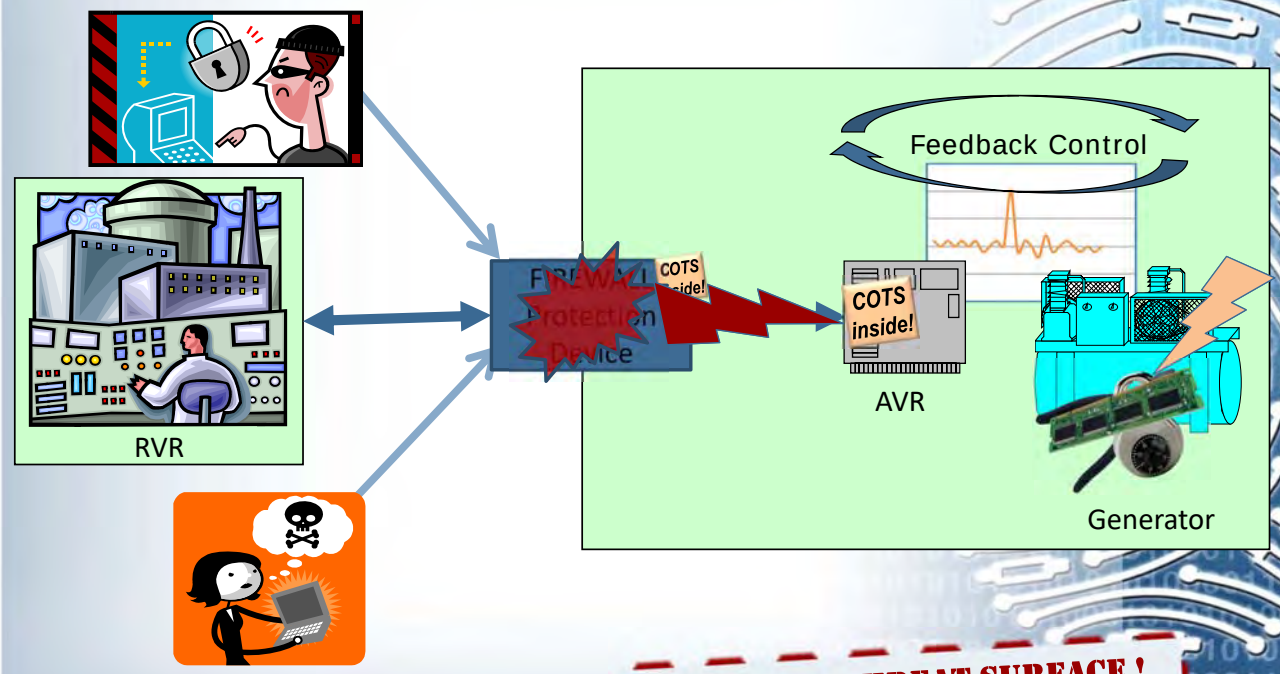
e.g. power grid vs. telecom network

- energy at the root of the infrastructures dependency hierarchy?
- not any longer...



Raise of attacks on Networked Control Systems:

no longer local and closed, proprietary, or dumb



[Bessani et al., IEEE Sec&Priv Mag.'08]

AMPLIFIED THREAT SURFACE !

BANG instead of crash:

The difference between IT and OT

2007

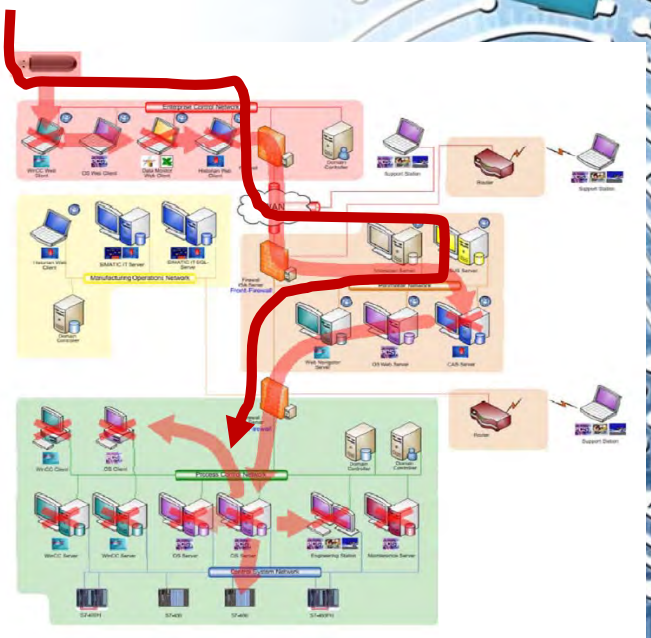
- Simulation of cyber attack, 2007, EUA, DoE Idaho Lab:
  - simulated attack, network based, as if from the Internet, against a power generator.
  - attack shook and destroyed generator

BANG instead of crash:

advanced persistent threats

2009

- ***Stuxnet worm***
- sophisticated piece of computer malware designed to sabotage industrial processes controlled by Siemens SIMATIC WinCC, S7 and PCS 7 control systems
- used both known and previously unknown vulnerabilities to spread; evaded state-of-the-practice security technologies
- self-replicates and spreads in a number of ways: removable drives; LANs; network shares; database servers;
- updates itself through a P2P mechanism within a LAN



Protecting CIIs

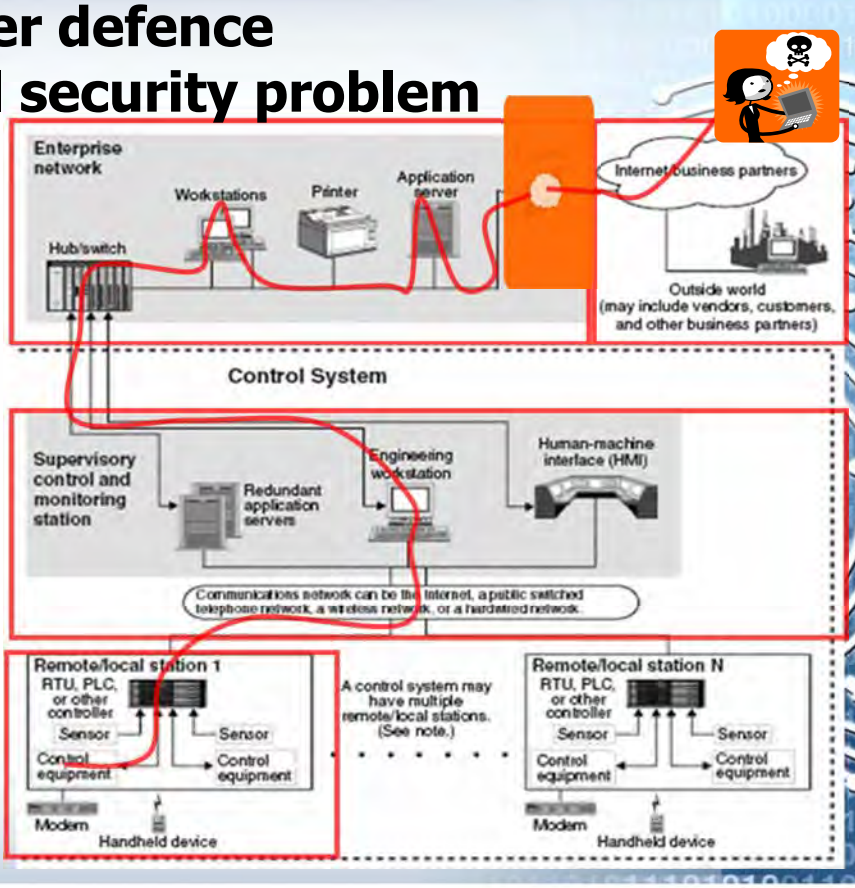
Which solutions ?

Perimeter defence

Classical IT solutions for the OT world

The perimeter defence fundamental security problem

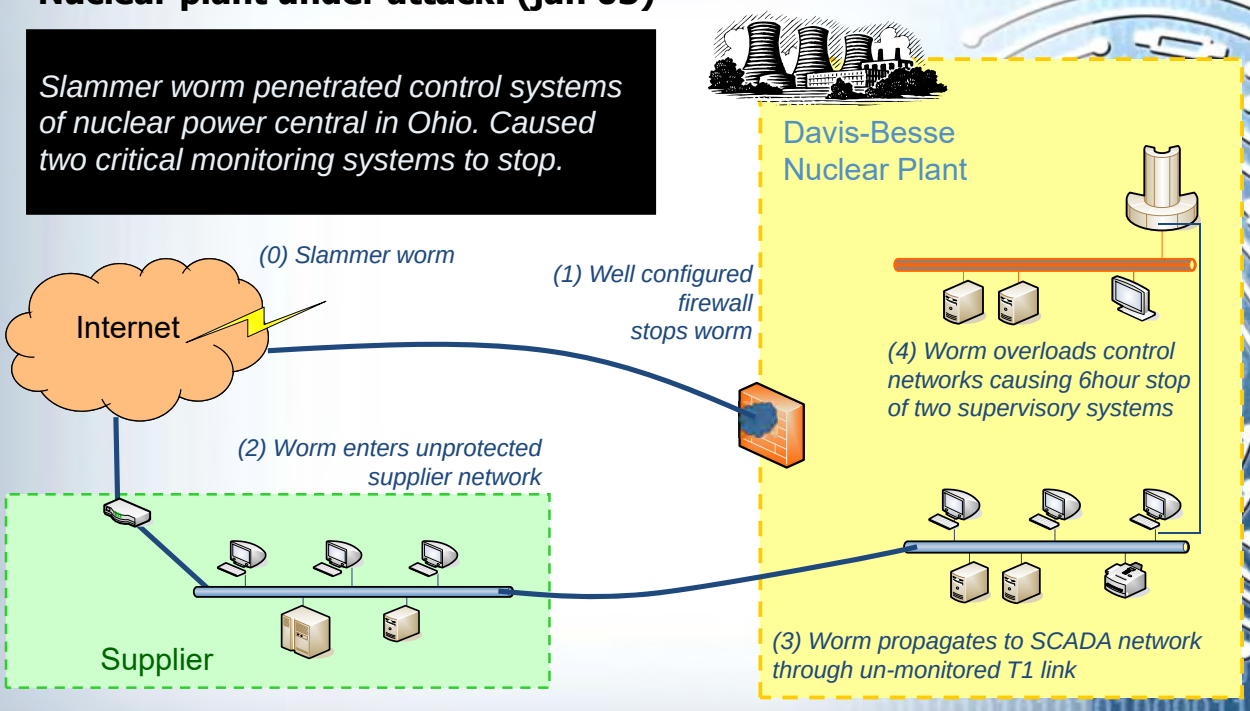
A simple, yet realistic, intrusion scenario



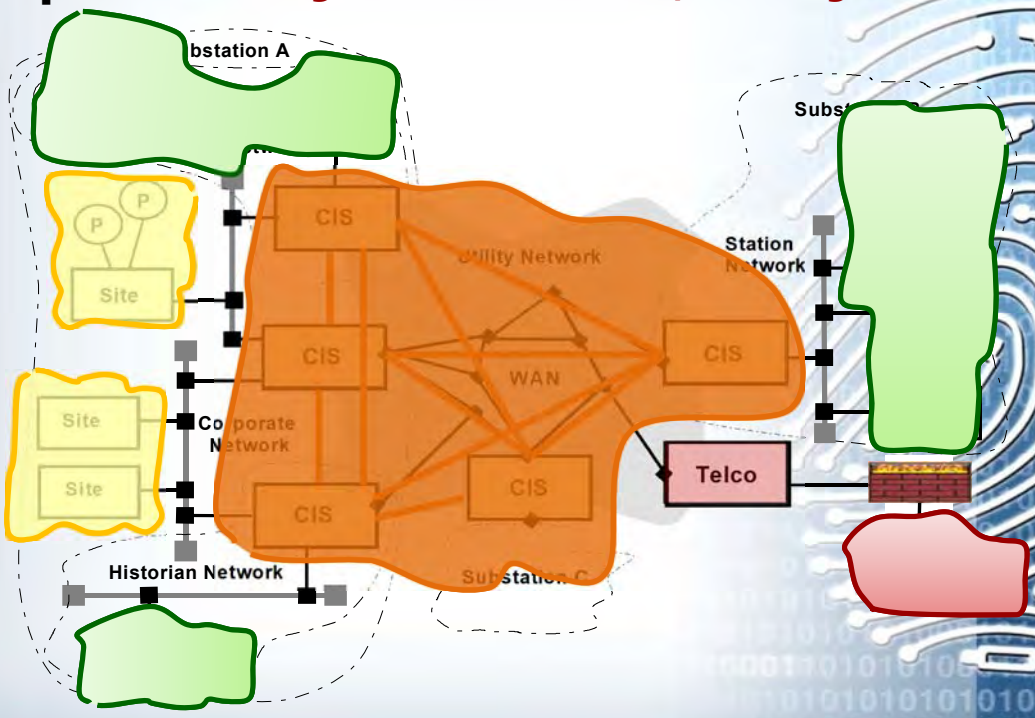
Mind your backyard

Nuclear plant under attack! (jan 03)

Slammer worm penetrated control systems of nuclear power central in Ohio. Caused two critical monitoring systems to stop.



Fragmentation, Fault Containment, and Defence in depth -- *Working solutions for the IT/OT integrated world !*



CIIs present and future

or the integration of IT and OT

- Are solutions up to the risk level?
- Considering ...
- Complexity of current infrastructures
- degree of vulnerabilities and level of threat ...

- The world is becoming an immense (*interconnected)* infrastructure

Cyberspace today

- immense, interconnected, interdependent infrastructure
- exposure: pressure to be “on-line”
- steadily increasing software vulnerabilities
- powerful adversary actors and sophisticated exploit tools
- targeted attacks and advanced persistent threats
- ***Elevated risk*** in all cyber components

Modern CII cyber risk analysis

status-quo

2005

- cyber-attacks are a common denominator to CI operational risk
- cyber-attacks to CII (incl. energy, telco, Internet, emergency, etc.) will be a pillar of i-warfare/ organized crime
- smaller scale but targeted cyber-attacks to certain CII services (e.g., telco, smart grids) will be a pillar of fraud and extorsion

- All these warnings came to fullfilment (CII high in any cybersecurity agenda, Stuxnet, WannaCry, ...)
- Yet this seemed farfetched in 2005 ...
- Let’s not let History repeat itself...

Ideas for R&D roadmap to solutions

2006

- Investigate architectural configurations that induce ***aprioristic* prevention**
  - of the more severe interaction faults, and attack and vulnerability combinations.
- Investigate middleware devices that achieve ***automatic* tolerance**
  - of remaining faults and intrusions
- Investigate trustworthiness monitoring mechanisms allowing **unforeseen *adaptation***
  - to situations not predicted or that go beyond assumptions

THE MAKINGS OF RESILIENCE !

Designing and architecting for resilience

SnT

dtrust.lu

TIX

1.	we want systems to operate through faults and attacks in a seamless manner, in an automatic way	Preventing and Tolerating Faults and Intrusions
2.	we want systems to endure the fact that operating conditions and environments are everyday more uncertain and/or hostile	Handling Incremental Threat Severity
3.	we want systems to be deployed in unattended manner	Resisting Continued Threats
4.	we want systems to attain very high levels of assurance	Validating and Assessing Assumptions and Mechanisms

(P. Verissimo, N. Neves, M. Correia, "Intrusion-Tolerant Architectures: Concepts and Design",Jun'03, in Architecting Dependable Systems, LNCS. Springer-Verlag, ext. in http://hdl.handle.net/10455/2954)

(P. Verissimo, M. Correia, N. Neves, P. Sousa, "Intrusion-Resilient Middleware Design and Validation",May'09, in Information Assurance, Security and Privacy Services, ser. Handbooks in Info Systems. Emerald)

Is (automatic) resilience really necessary?

- Adm. Michael Rogers, NSA Director and commander of US Cyber Command, said that the question "How, in the midst of degradation and penetration, can we still have confidence in the systems?" is better served by ***focusing on resilience rather than on prevention***.
- [Editor's Note]: This is the new theme for cybersecurity - the ability to ***continue fighting when you're hurt*** is the differentiator between a successful security organization and the one picking up the pieces after an incident and wondering what happened.

FEDERAL TIMES

Print: Subscribe Renew Digital Edition

MOBILITY CYBER FEDERA

Sign up for our free newsletter

IT security shifts from prevention to resiliency

Sep. 22, 2014 - 06:00AM | By AARON BOYD | Comments

Recommend 31 Pin it

AA

Adm. Michael Rogers: Preventing or stopping intruders is only half of the equation for maintaining resiliency.

The discussion on cybersecurity has shifted as CIOs and CTOs come to the realization that no system is immune to attacks and breaches. The conversation is now about "cyber resiliency."

"How, in the midst of degradation and penetration, can we still have confidence in the systems?" Adm. Michael Rogers, NSA director and commander of U.S. Cyber Command, asked at the Billington Cybersecurity Summit in Washington. "Most organizations have tended to put their resources and focus on stopping people from penetrating their systems. I tell organizations that we have got to not only focus on stopping people ... but how are you going to operate and remediate at the same time. That's resiliency."

Architecting and designing for resilience

- comprehensive approach to those threats, from first principles: *"build defence in"*
- simultaneously coping with accidental and malicious faults
- provide protection in an incremental way
- automatically adapt to a dynamic range of severity of threats
- seek unattended and perpetual operation

- ... Let's not let History repeat itself...
- Time to move up the resilience ladder ...

A methodic approach to modular and distributed resilient computing

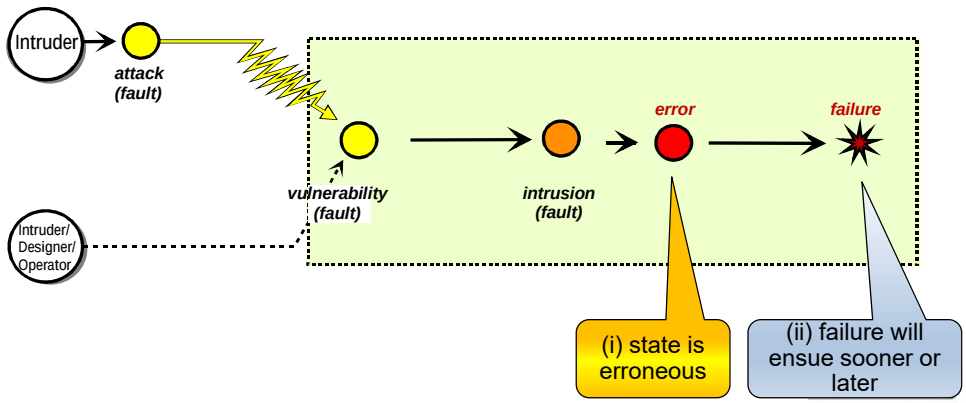
- Fault and intrusion tolerance, or automatic security and dependability
- Handle increasing threat severity
- Resist continued threats

STATE OF THE ART

- Divide-and-conquer to beat extreme threats
- Hybrid models and architectures
- Ultra-reliable trusted components
- High-confidence vertical verification
- Privacy- and integrity-preserving data processing

Attack-Vulnerability-Intrusion *composite* fault model

AVI fault model: *attack + vulnerability→ intrusion → error → failure*

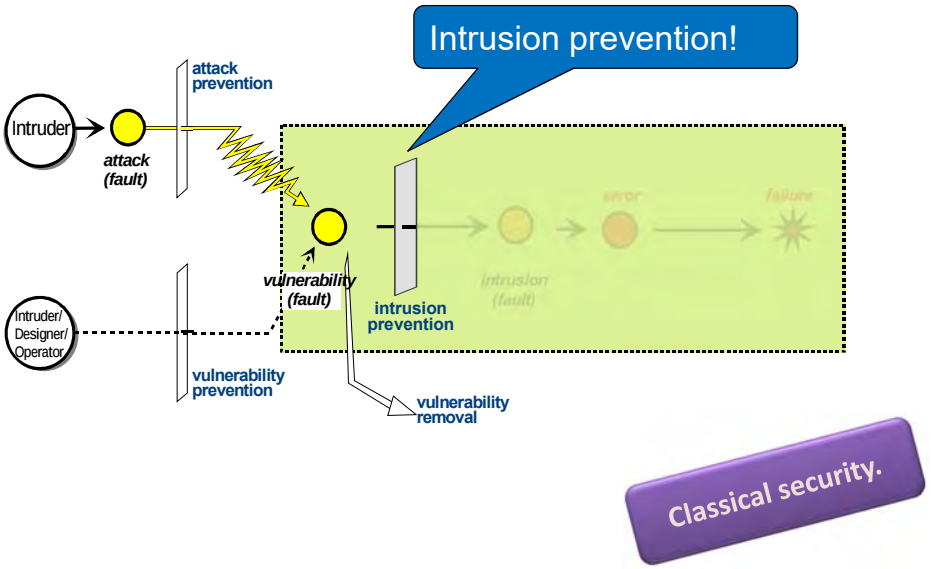


NOTES:
(i) state includes data, code, metadata, configuration variables, etc.
(ii) "failure" means failure of any security property, *when and if perceived by a user*

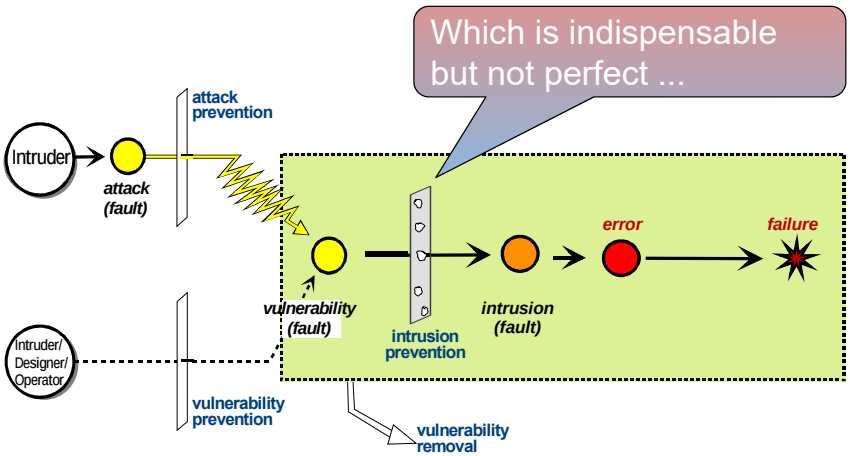
focusing on security for a start …

57

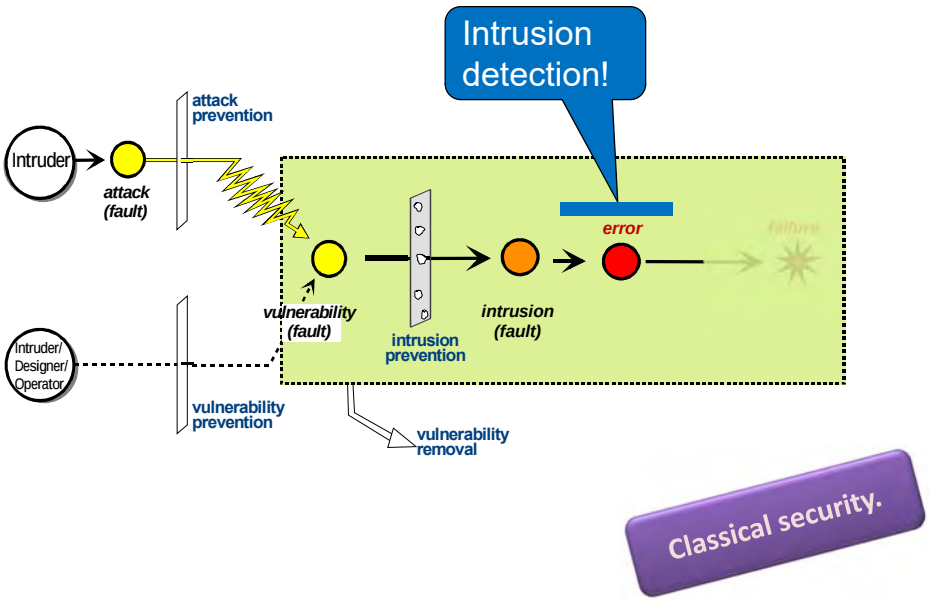
Classical security: Intrusion prevention



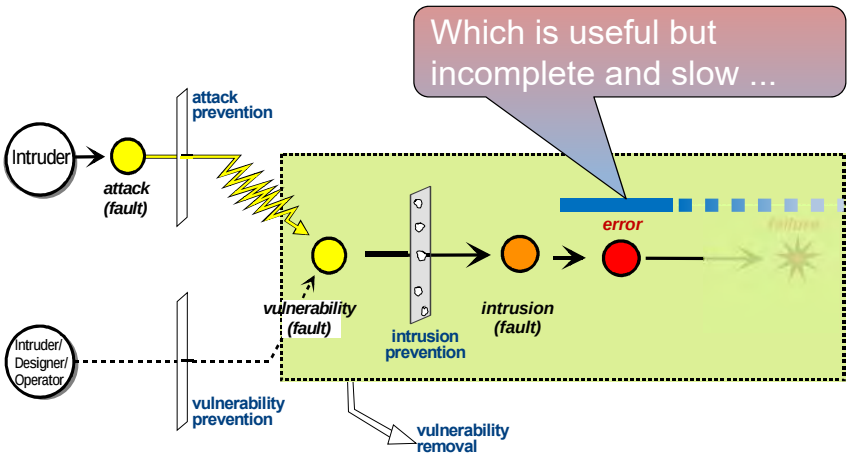
Classical security: Intrusion prevention



Classical security: Intrusion detection



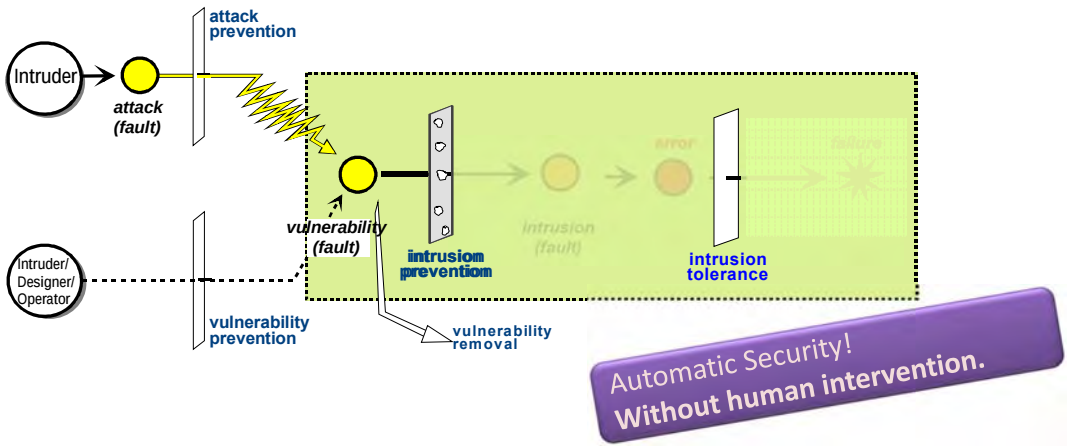
Classical security: Intrusion detection



NOTES:

(i) after intrusion, the system is in the path to failure, so incompleteness or slowliness of intrusion detection and/or processing/mitigation, bears a high risk of failure of a security property as *perceived by a user*

Automatic Dependability and Security

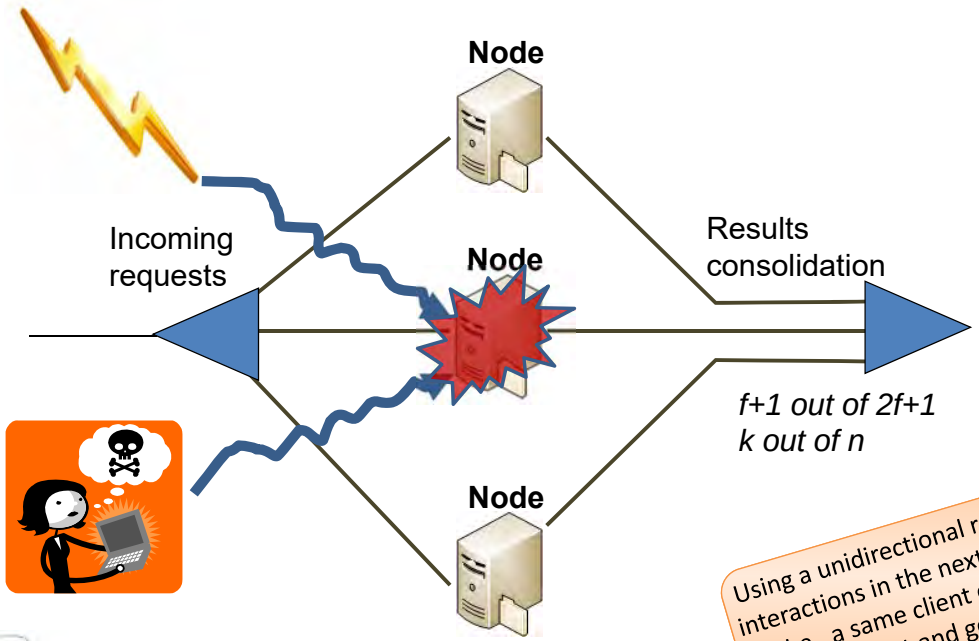


(P. Verissimo, N. Neves, M. Correia, "Intrusion-Tolerant Architectures: Concepts and Design", in Architecting Dependable Systems, LNCS. Springer-Verlag, ext. in http://hdl.handle.net/10455/2954,Jun'03)

Fault and Intrusion Tolerance (FIT)

An abstract solution

Tolerating Faults and Intrusions automatically

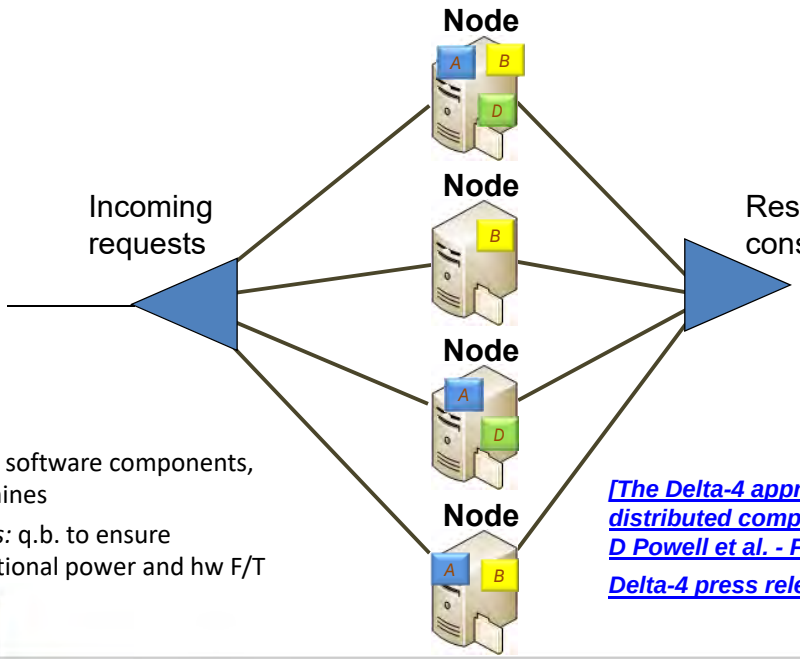


f = max. number of faulty replicas (f=1 in this example)

Using a unidirectional representation of interactions in the next slides, for clarity. I.e., a same client could make the request and get the result.

Fault and Intrusion Tolerance (FIT)

modular and distributed HW/SW F/T (comp. based)



NOTES:

(i) Replicate software components, not machines

(ii) *Machines:* q.b. to ensure computational power and hw F/T

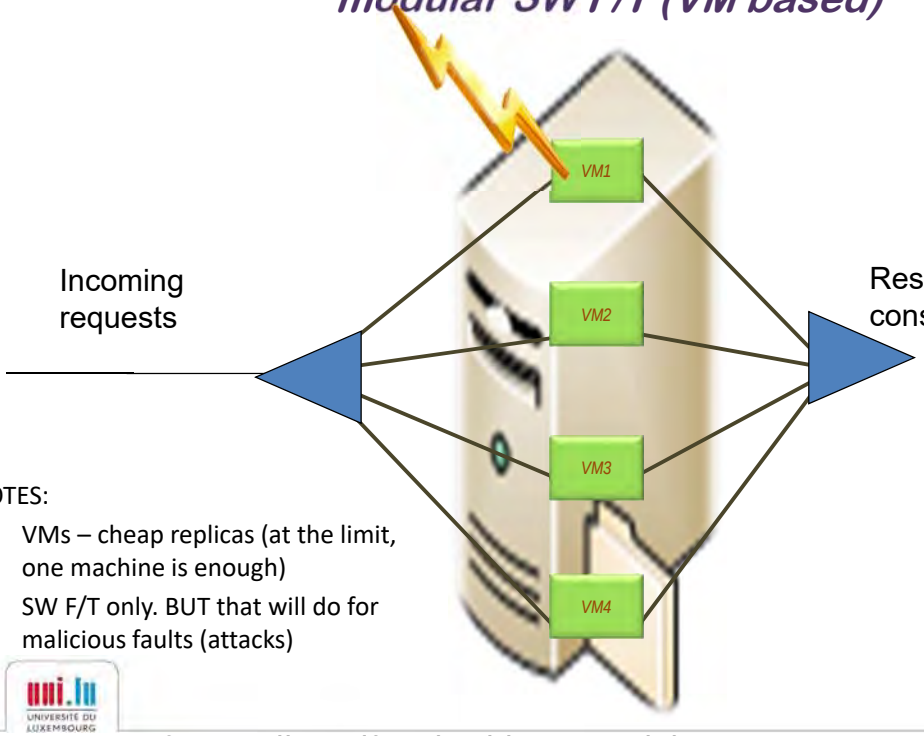
[The Delta-4 approach to dependability in open distributed computing systems. D Powell et al. - FTCS, Tokyo JP, 1988]

Delta-4 press release

3f+1 replicas (f=1 in this example)

Fault and Intrusion Tolerance (FIT)

modular SW F/T (VM based)



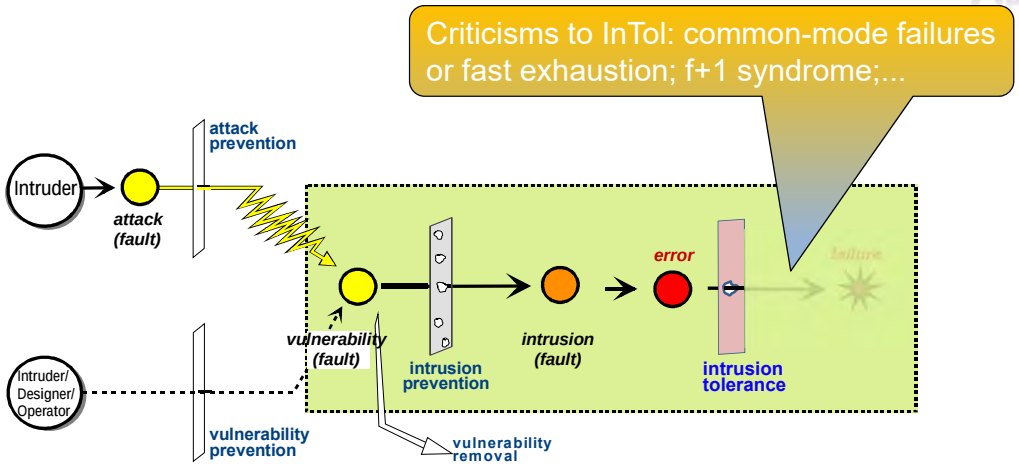
NOTES:

(i) VMs – cheap replicas (at the limit, one machine is enough)

(ii) SW F/T only. BUT that will do for malicious faults (attacks)

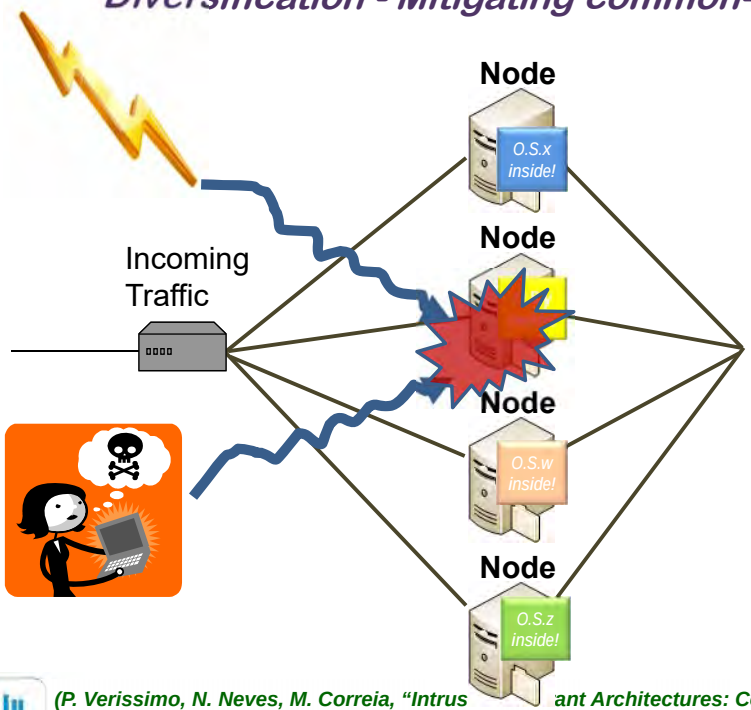
3f+1 replicas (f=1 in this example)

Automatic Dependability and Security: intrusion tolerance



Fault and Intrusion Tolerance (FIT)

Diversification - Mitigating common-mode faults

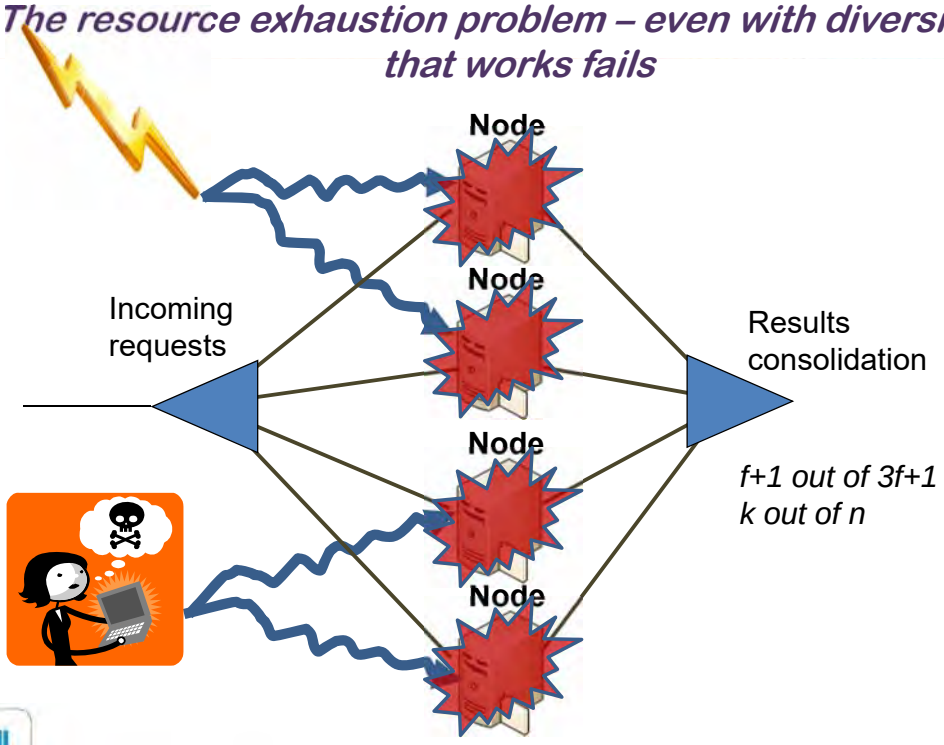


f = max. number of faulty replicas (f=1 in this example)

(P. Verissimo, N. Neves, M. Correia, "Intrus ant Architectures: Concepts and Design", in Architecting Dependable Systems, LNCS. Springer-Verlag, ext. in http://hdl.handle.net/10455/2954,Jun'03)

Fault and Intrusion Tolerance (FIT)

The resource exhaustion problem – even with diversity, all that works fails

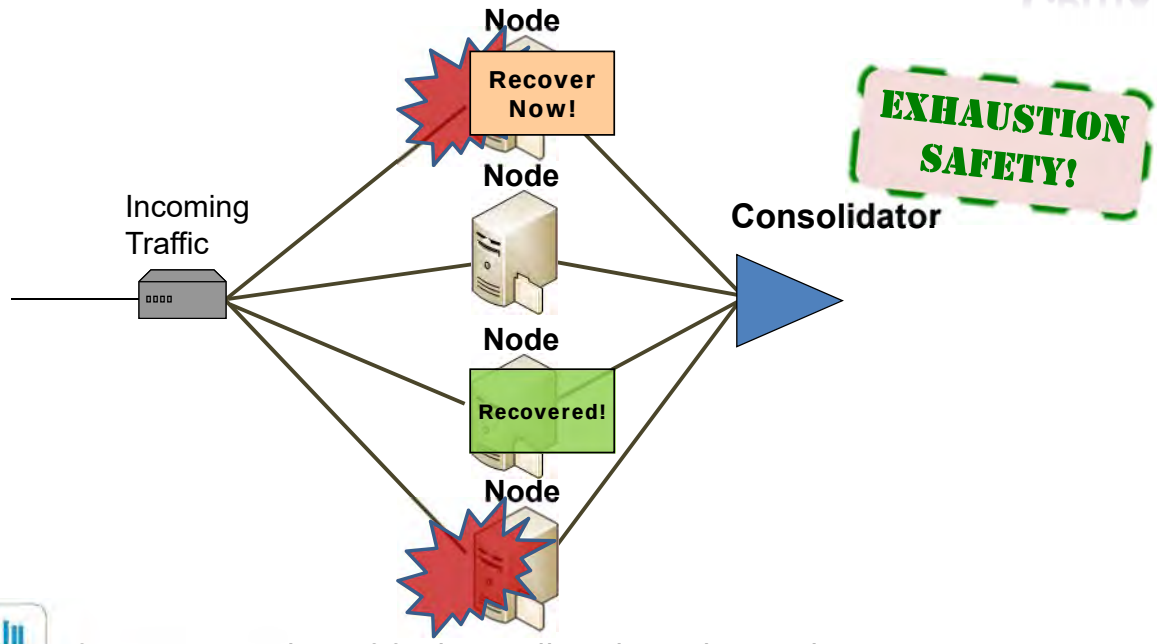


f = max. number of faulty replicas (f=1 in this example, was exceeded)

Proactive and Reactive Recovery (PRR)

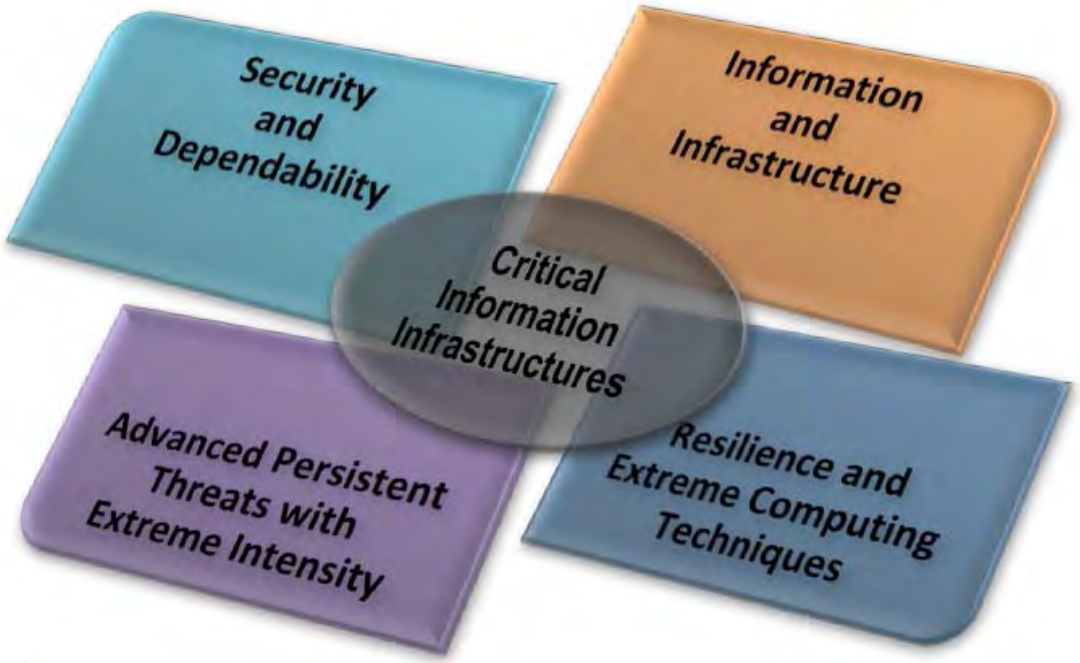
Resisting Continued Threats

Seeking (unattended) perpetual execution



f = max. number of faulty replicas in an interval *Tr*

CritiX: Meeting the Challenges of Critical Dependability and Security

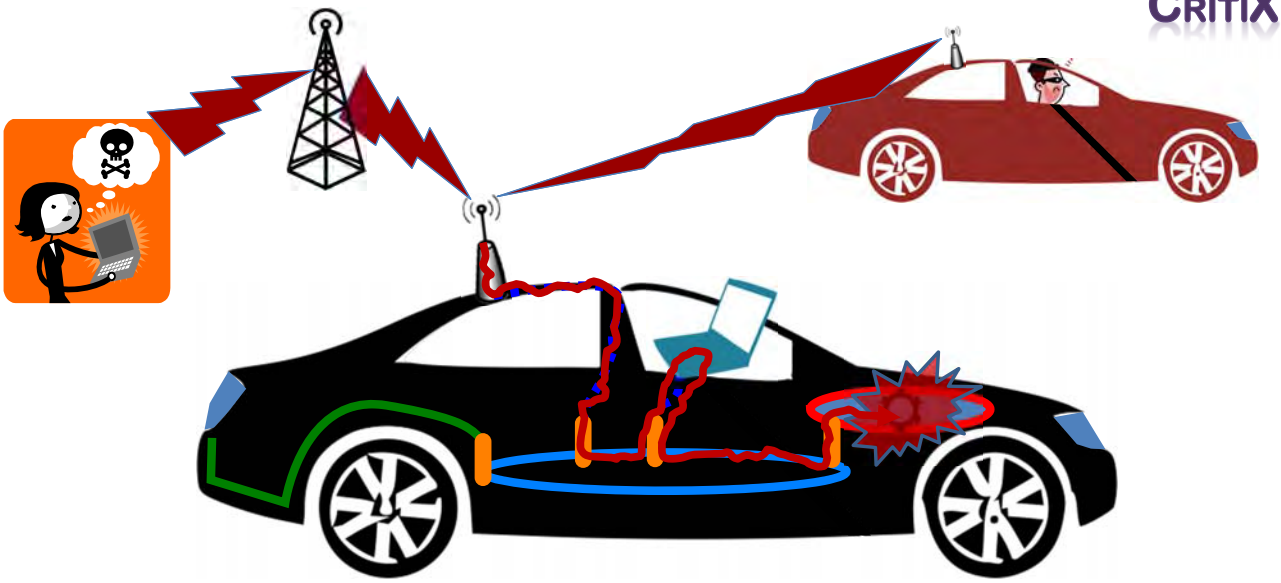


Emerging challenges in IT/OT Integration:

The Autonomous and Cooperative Vehicles Ecosystem !

X-by-wire Networked Vehicles: no longer mechanical or isolated

securityandtrust.lu
CritiX

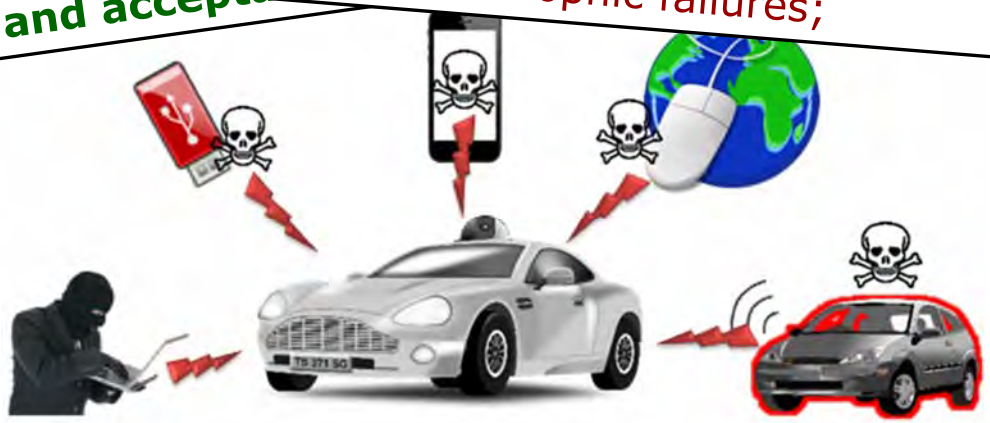


[I. Lima et al., ACM CPS-SP@CCS'16]

AMPLIFIED THREAT SURFACE !

The safety-security gap in vehicles

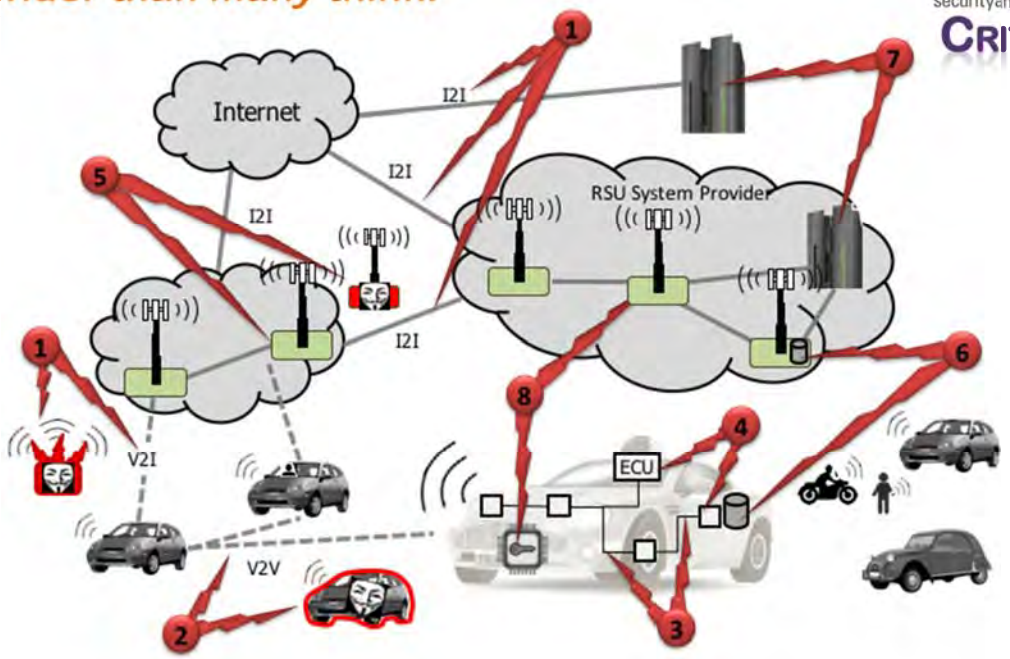
Vulnerabilities in a car **will** lead, rather sooner than later, to catastrophic failures;



AMPLIFIED THREAT SURFACE !

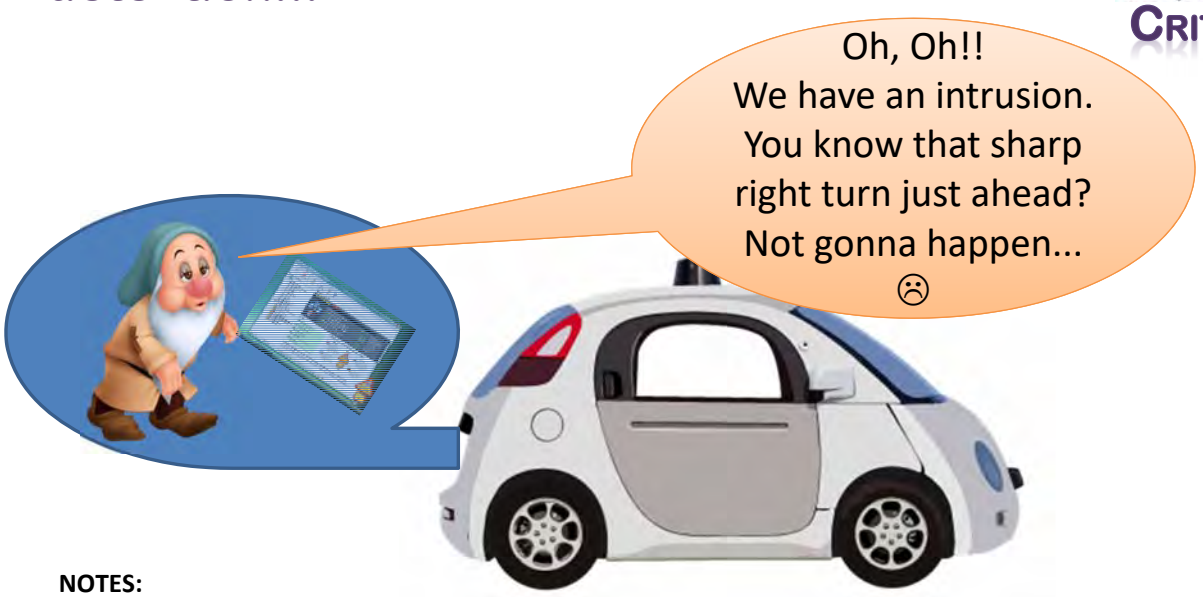
Autonomous vehicle ecosystem threat plane

perhaps wider than many think!



Towards Safe and Secure Autonomous and Cooperative Vehicle Ecosystems. *Lima, A; Rocha, F; Volp, M; Verissimo, P. in Proc's 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy (2016, October) @CCS, Vienna-Austria*

Autonomous driving with intrusion detection...



NOTES:

(i) after intrusion, the system is in the path to failure, so incompleteness or slowliness of intrusion detection and/or processing/mitigation, is the path to catastrophe.

(ii) IDS are at best useful as off-line fault diagnosis

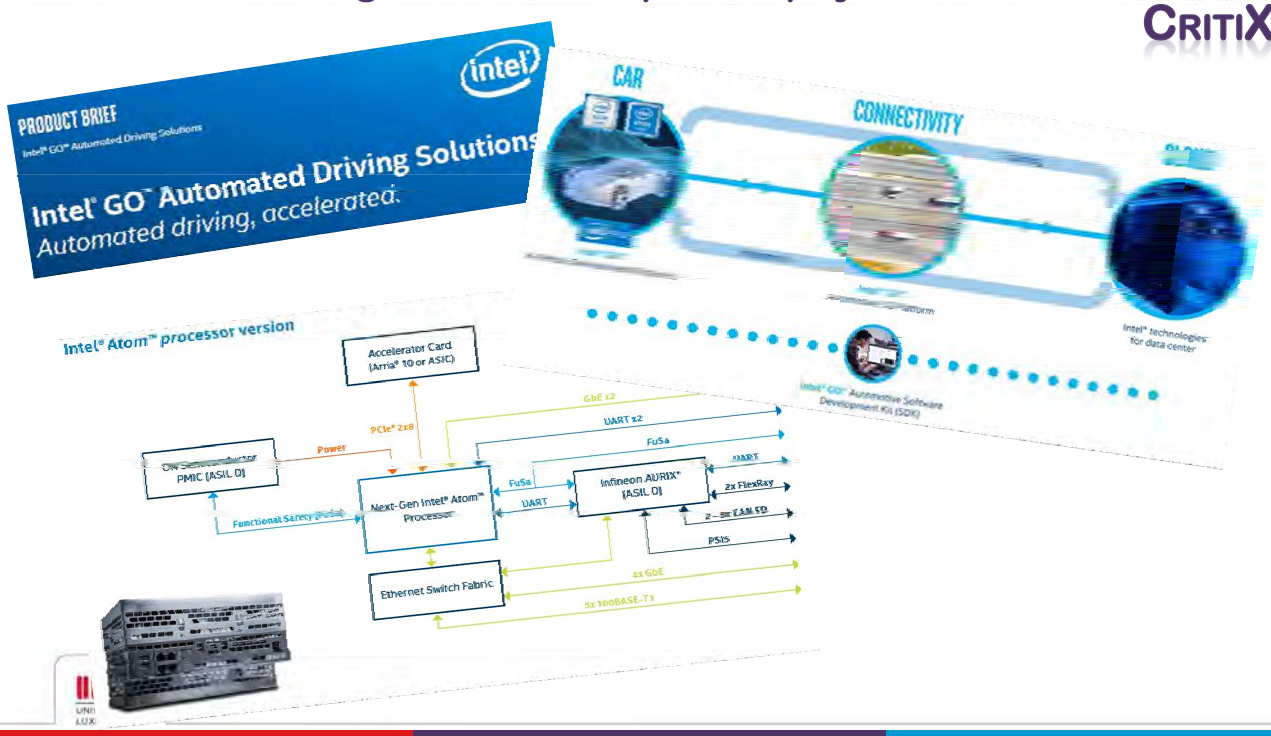
Research strategy enablers for safe and secure RTES

- **Powerful architectures** (e.g. manycores), capable of: high-power computing, enabling security/safety defenses
- **Automatic resilience** mechanisms for safety and security (hypervisors, gateways, trusted components, enclaves)
- **Secure and dependable *real-time* communication**, despite accidents and attacks

Research strategy enablers for safe and secure RTES

- **Powerful architectures** (e.g. manycores), capable of: high-power computing, enabling security/safety defenses
- **Automatic resilience** mechanisms for safety and security (hypervisors, gateways, trusted components, enclaves)
- **Secure and dependable *real-time* communication**, despite accidents and attacks

Intel GO Automated Driving Solutions:
seems to be aligned with this philosophy



Intel Collaborative Research Institute for
Collaborative Autonomous & Resilient Systems (CARS)

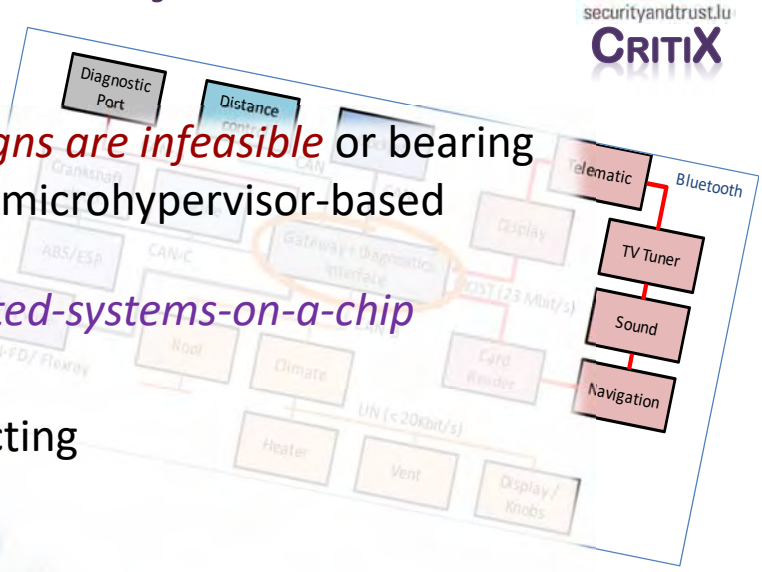
PRESS RELEASE: ***http://www.icri-sc.org/news/press-releases/detail/artikel/leading-european-cybersecurity-research-organizations-and-intel-labs-join-forces-to-conduct-research/***

http://www.icri-sc.org/resilient-autonomy/mission/

Research strategy enablers for safe and secure RTES

- **Powerful architectures** (e.g. manycores), capable of: high-power computing, enabling security/safety defenses
- **Automatic resilience** mechanisms for safety and security (hypervisors, gateways, trusted components, enclaves)
- **Secure and dependable *real-time* communication**, despite accidents and attacks

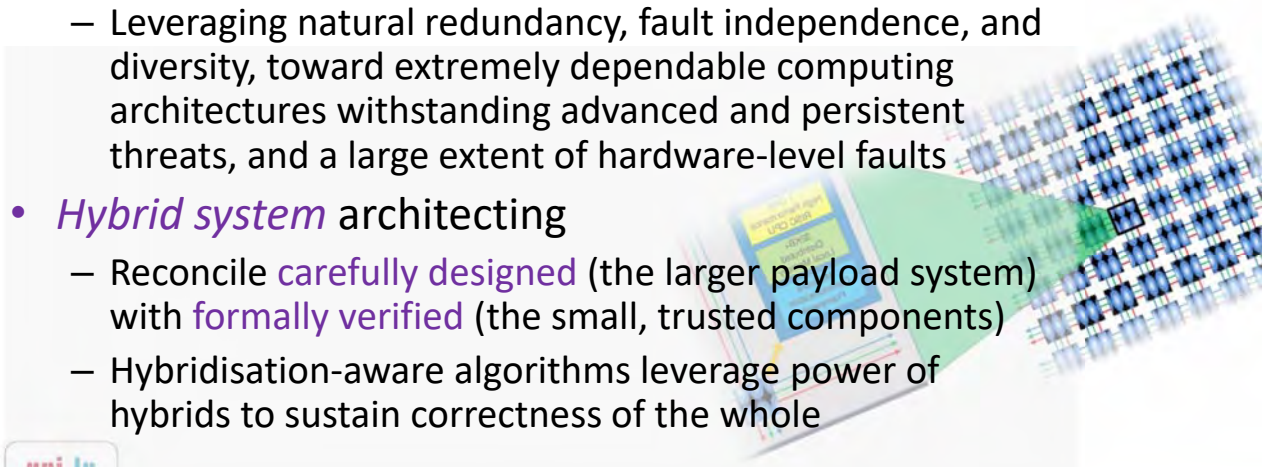
Ultra-reliable trusted components
Dependable Hypervisor and Manycore Architectures



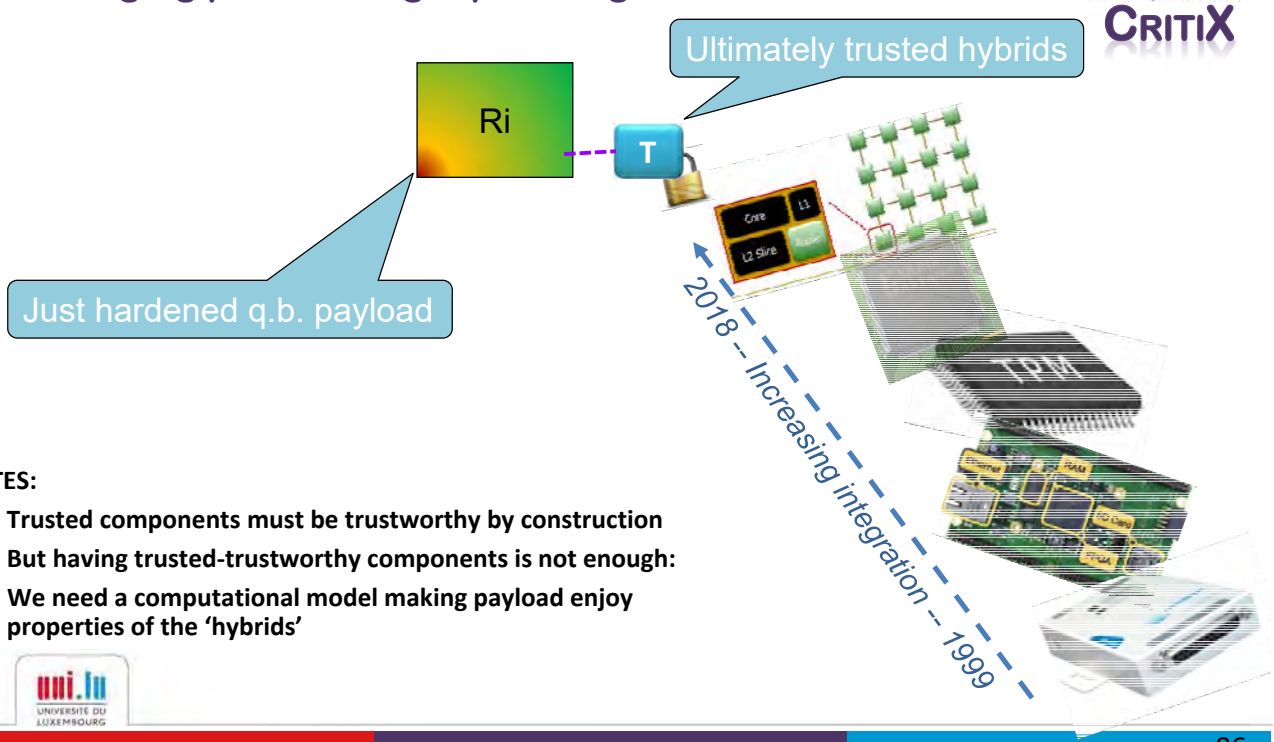
- *Fault-free system designs are infeasible* or bearing extreme costs, even if microhypervisor-based
- Manycores as *distributed-systems-on-a-chip*
- *Hybrid system* architecting

Ultra-reliable trusted components
Dependable Hypervisor and Manycore Architectures

- *Fault-free system designs are infeasible* or bearing extreme costs, even if microhypervisor-based
- Manycores as *distributed-systems-on-a-chip*:
  - Leveraging natural redundancy, fault independence, and diversity, toward extremely dependable computing architectures withstanding advanced and persistent threats, and a large extent of hardware-level faults
- *Hybrid system* architecting
  - Reconcile carefully designed (the larger payload system) with formally verified (the small, trusted components)
  - Hybridisation-aware algorithms leverage power of hybrids to sustain correctness of the whole



Divide-and-conquer I: **Hybrid models and architectures**
Leveraging power at right place right time



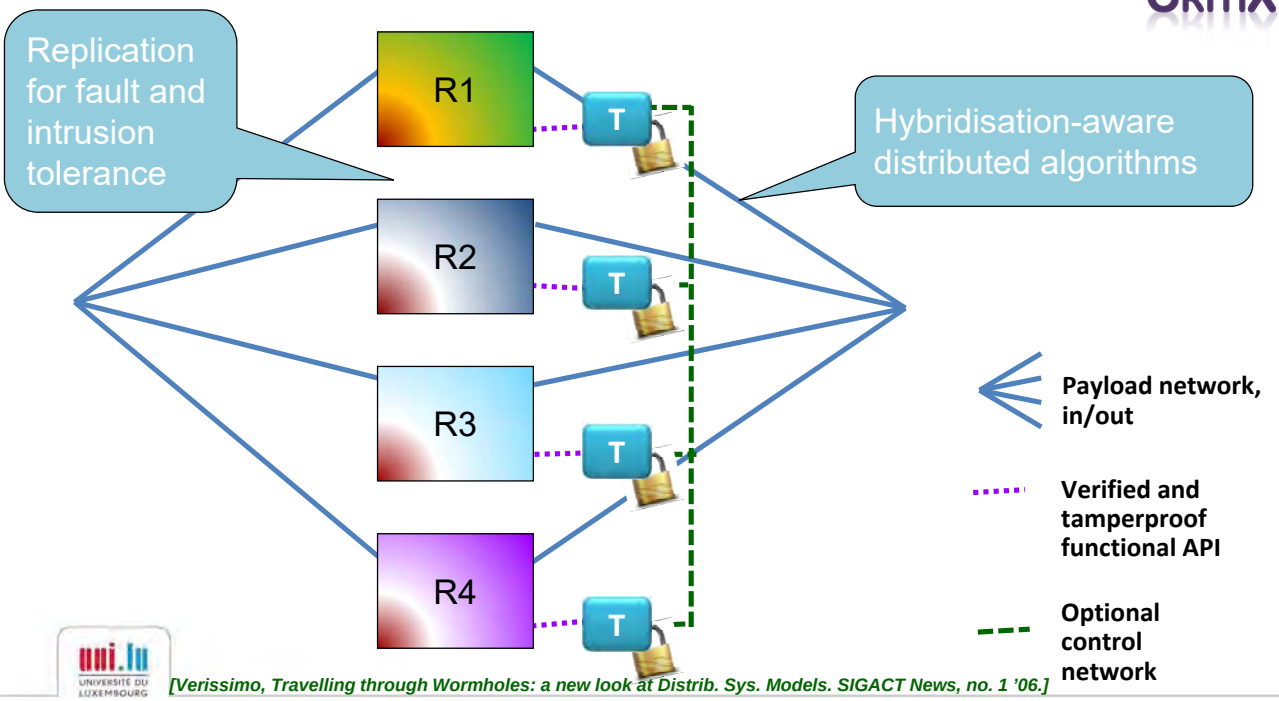
NOTES:

(i) Trusted components must be trustworthy by construction

(ii) But having trusted-trustworthy components is not enough:

(iii) We need a computational model making payload enjoy properties of the 'hybrids'

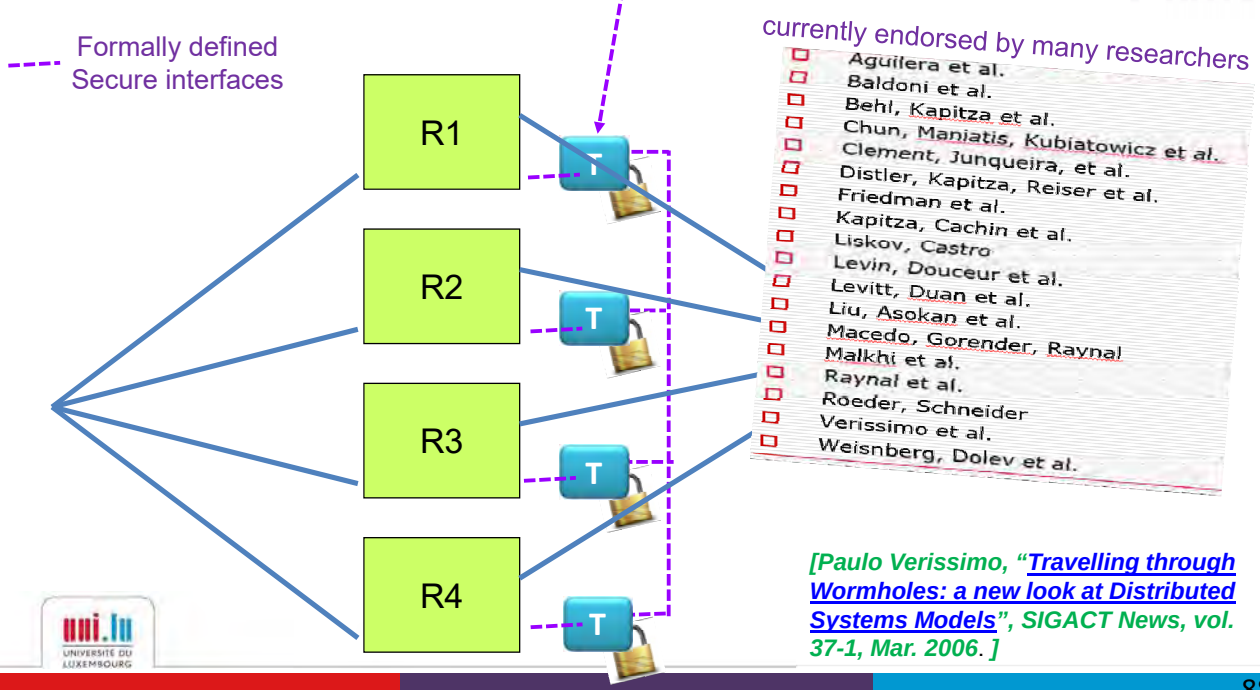
Divide-and-conquer I: Hybrid models and architectures
Leveraging power at right place right time



[Verissimo, Travelling through Wormholes: a new look at Distrib. Sys. Models. SIGACT News, no. 1 '06.]

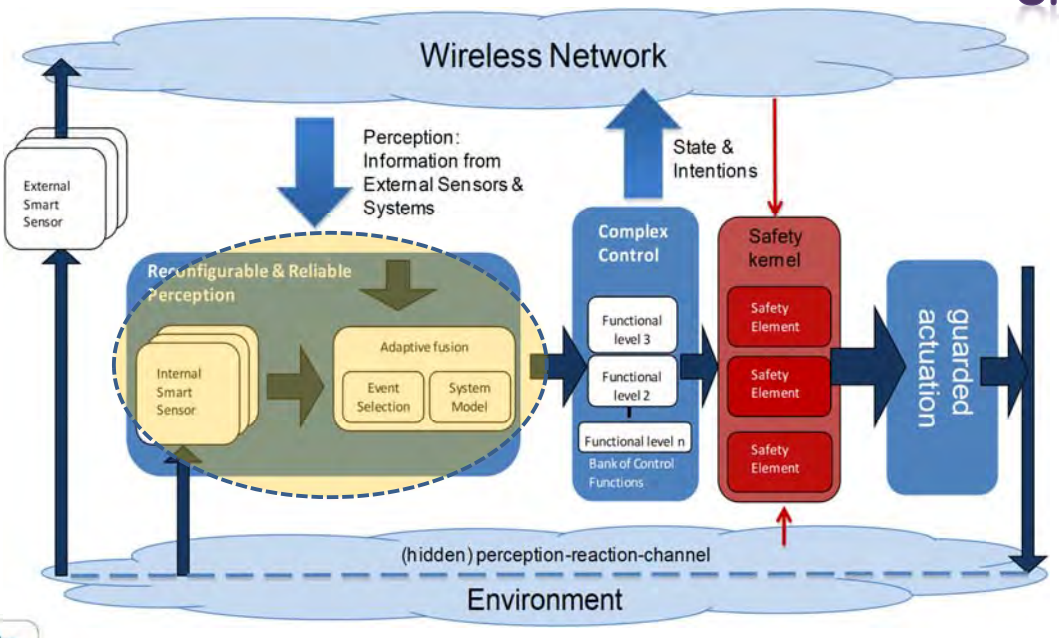
Divide-and-conquer I: Hybrid models and architectures
Leveraging power at right place right time

Leveraging trusted-trustworthy components (aka TEE) with the right set of simple functions (failure detectors, monotonic counters, reliable timers and clocks, PRG, signatures, indelible logs, binary cons.

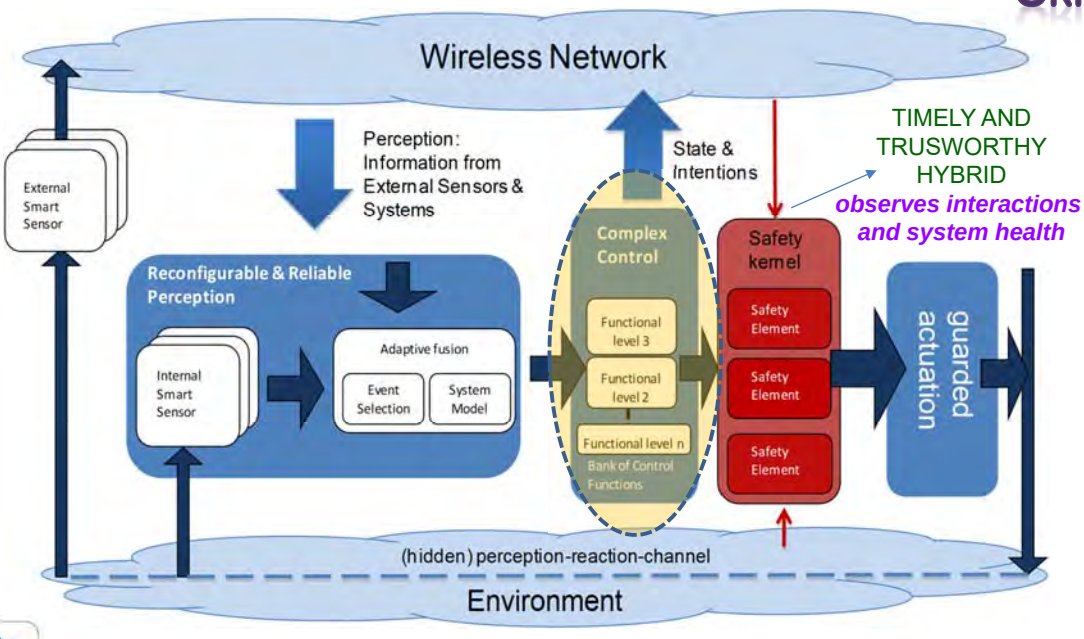


[Paulo Verissimo, "Travelling through Wormholes: a new look at Distributed Systems Models", SIGACT News, vol. 37-1, Mar. 2006.]

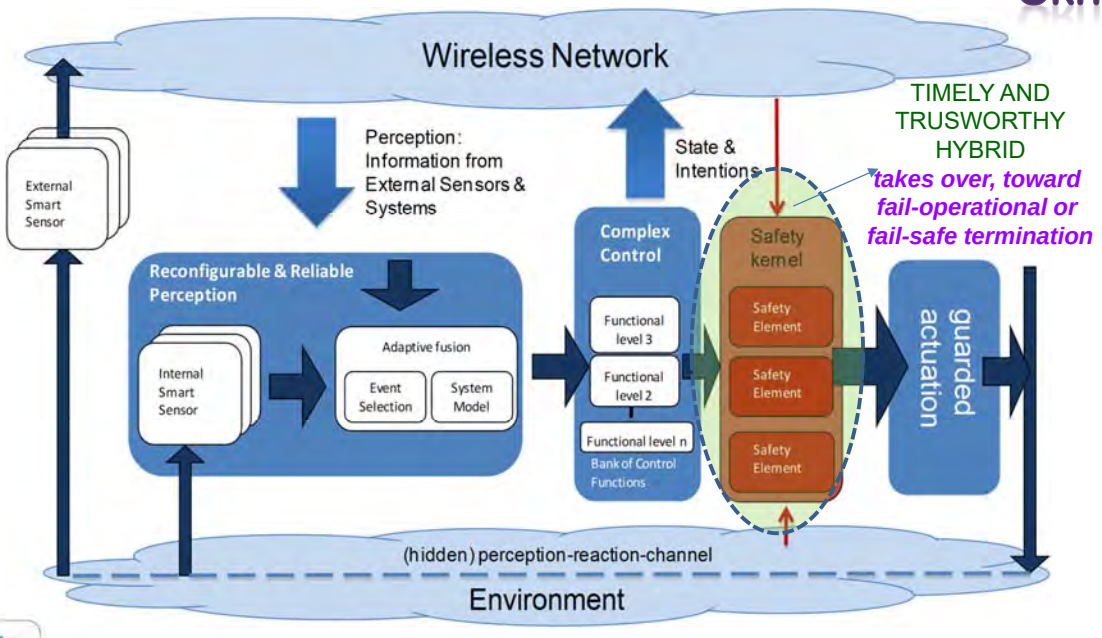
KARYON architectural view: proof of concept of hybridisation for safety



KARYON architectural view: proof of concept of hybridisation for safety



KARYON architectural view: proof of concept of hybridisation for safety



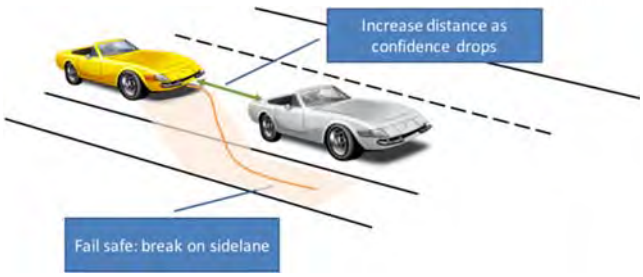
KARYON architectural view: proof of concept of hybridisation for safety

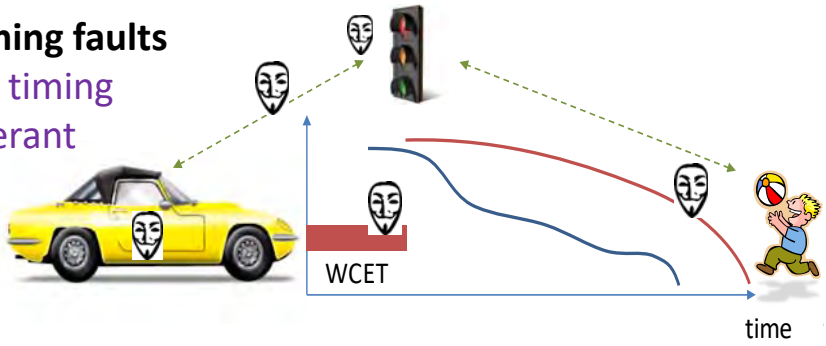
Research strategy enablers for safe and secure RTES

- **Powerful architectures** (e.g. manycores), capable of: high-power computing, enabling security/safety defenses
- **Automatic resilience** mechanisms for safety and security (hypervisors, gateways, trusted components, enclaves)
- **Secure and dependable *real-time* communication**, despite accidents and attacks

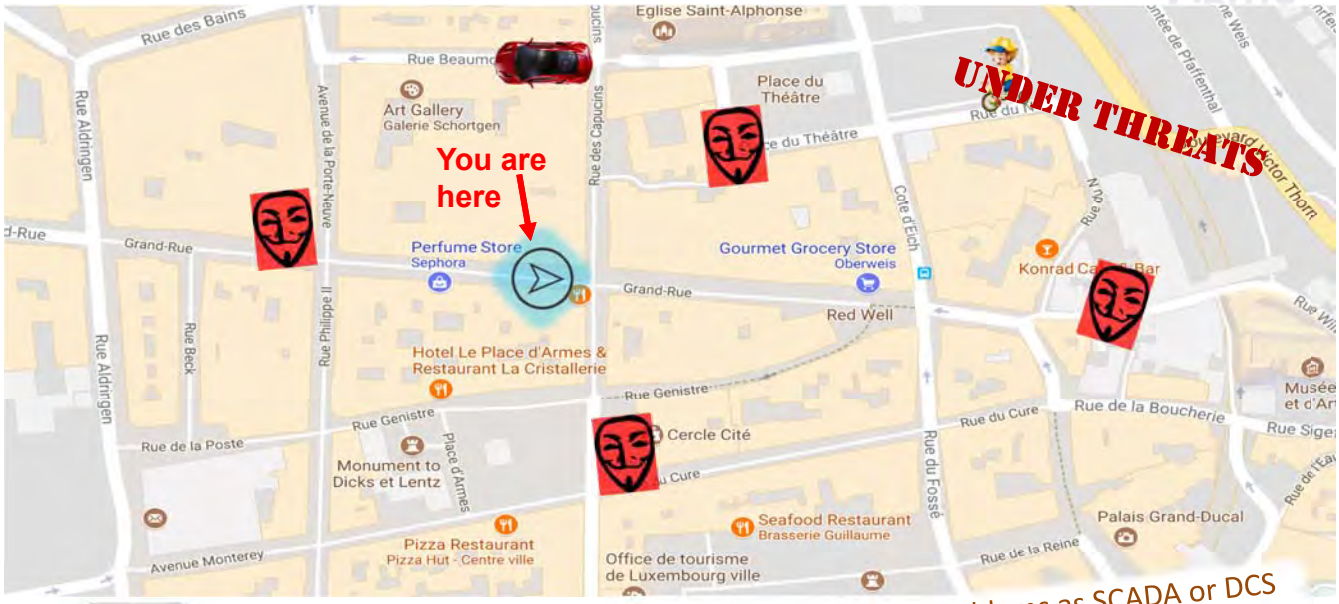
Integrating security into safety-critical real-time distributed control systems

- **collaboration and consensus with real-time constraints, under accidental and malicious threats**
  - Byzantine-resilient **Real-time** Reliable Broadcast
  - **deadline misses as timing faults** masked through novel timing fault and intrusion tolerant algorithms





Application- and context-aware protocols for security- and safety-critical R/T ops.



- Similar but tougher problems as SCADA or DCS

Paulo Esteves-Veríssimo
University of Luxembourg Faculty of Science, Technology and Communication
and SnT, the Interdisciplinary Centre for Security, Reliability and Trust

paulo.verissimo@uni.lu
http://staff.uni.lu/paulo.verissimo

CRITIX @SnT
Critical and Extreme Security and Dependability
http://wwwen.uni.lu/snt/research/critix

We're hiring
bright post-docs and PhD students
willing to address these challenges!