Challenges, current solutions and research directions regarding assured autonomy

Paulo Esteves-Veríssimo

Univ. of Luxembourg, FSTC / SnT

paulo.verissimo@uni.lu

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

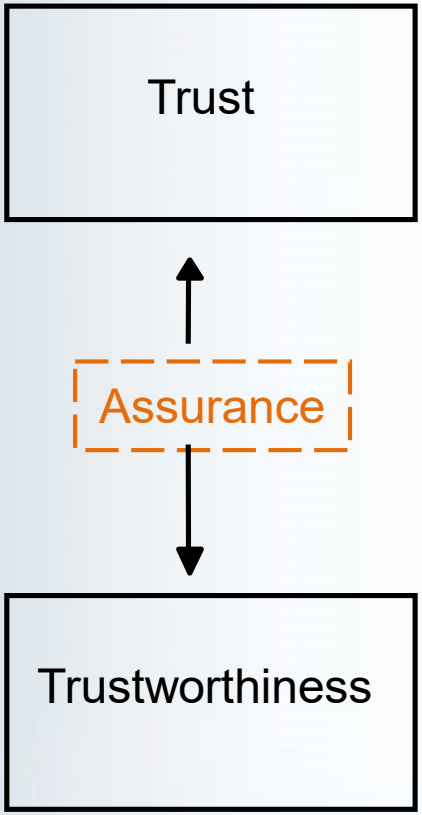
CritiX Lab (Critical and Extreme Security and Dependability)

Panel at 75th IFIP WG10.4 workshop

Champéry, CH

Jan 2019 .

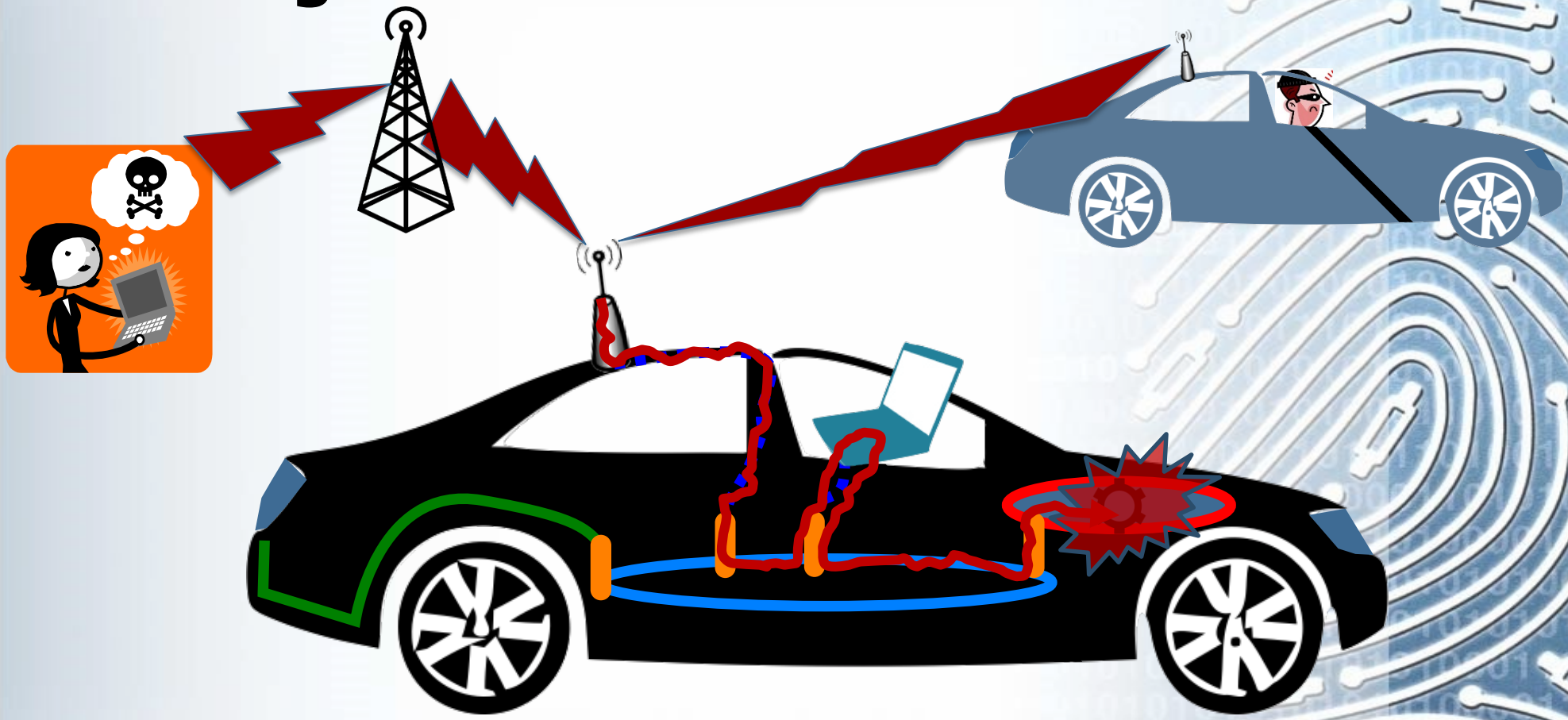
Perspective taken on assurance



- Statements that explicitly define the dependability and security expectations about a system (a set of properties)
-
- Provides justification that the user trust meets system trustworthiness, through assurance evidence and approvals based on evidence
-
- System mechanisms designed and implemented to meet the requirements (enforce the properties)

Autonomous vehicles vs. traditional

Autonomous Vehicles:
no longer mechanical nor isolated



AMPLIFIED THREAT SURFACE !

Case for a holistic approach:

Individualistic cars will worsen safety

Second Tesla autopilot crash under federal scrutiny

by Chris Isidore @CNNMoney July 7, 2016

Another week, another Tesla crash involvi Autopilot

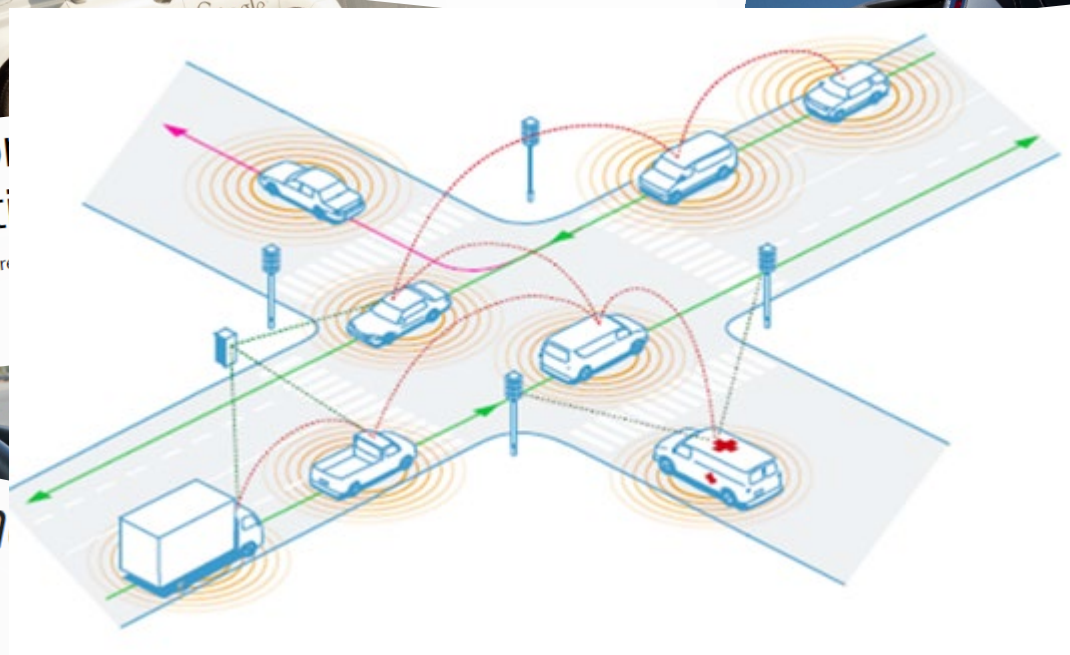
By Yoni Heisler on Aug 19, 2016 at 4:30 PM

Uber self-driving car kills pedestrian in first fatal autonomous crash

self-driving Uber

Case for a holistic approach:
Individualistic cars will worsen safety

Cooperation is key!



TECHNOLOGY NEWS | Mon Feb 29, 2016 | 6:31pm EST

Google says it
after self-drivir

Secou
scruti
by Chris Isidor

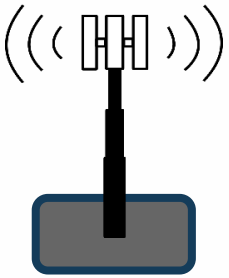
Another week, an
Autopilot
By Yoni Heisler on Aug 19, 2016 at 4:30 PM

Uber self-driving car kills pedestrian in first
fatal autonomous crash

Autonomous Vehicle Ecosystem

- Components

S-Vehicles



Road Side Unit

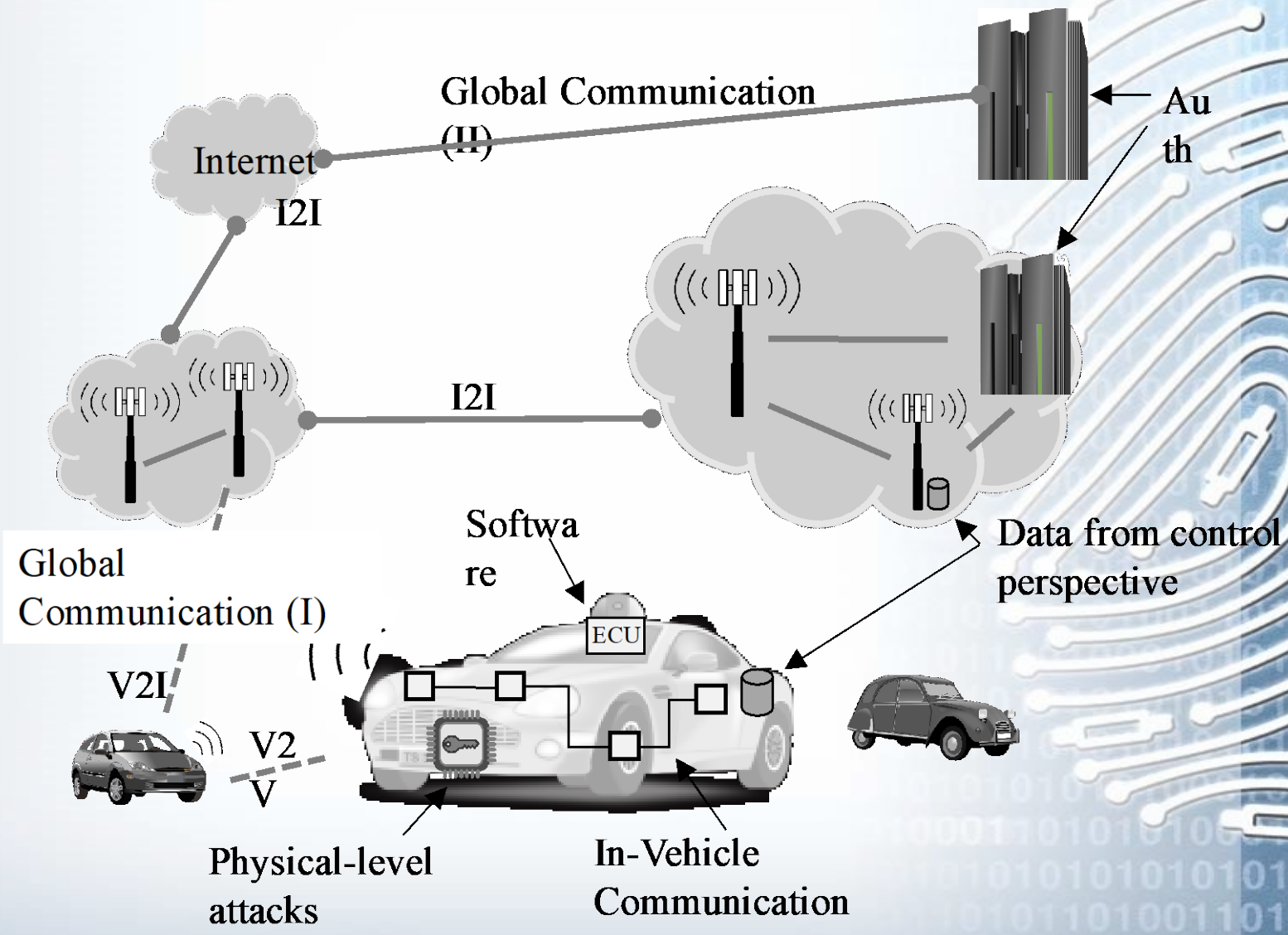
Trusted Authority

Other
s-Components

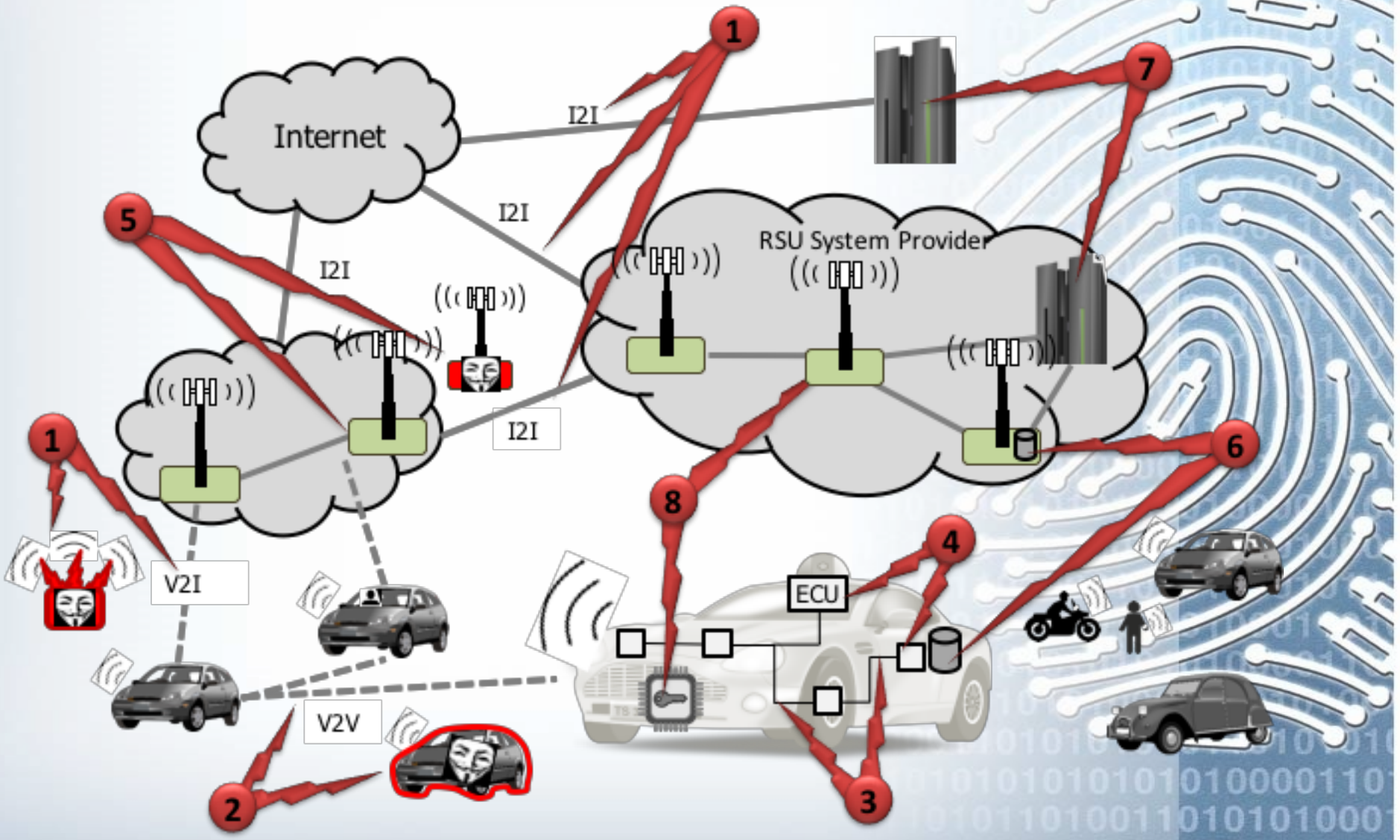
Environment

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

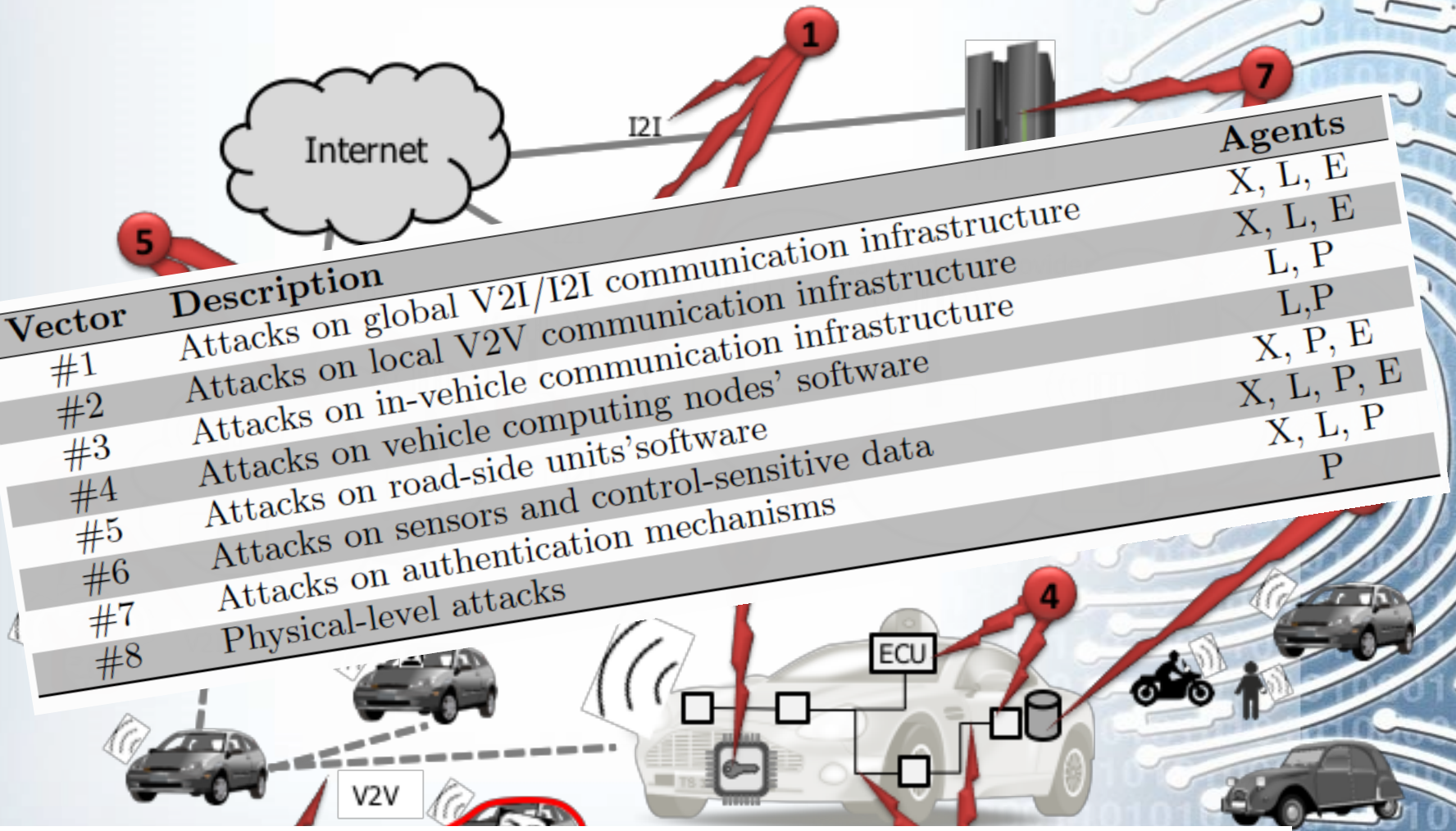
Autonomous Vehicle Ecosystem



Autonomous vehicle ecosystem threat plane perhaps wider than many think



Autonomous vehicle ecosystem threat plane perhaps wider than many think



Vector	Description	Agents
#1	Attacks on global V2I/I2I communication infrastructure	X, L, E
#2	Attacks on local V2V communication infrastructure	X, L, E
#3	Attacks on in-vehicle communication infrastructure	L, P
#4	Attacks on vehicle computing nodes' software	L,P
#5	Attacks on road-side units'software	X, P, E
#6	Attacks on sensors and control-sensitive data	X, L, P, E
#7	Attacks on authentication mechanisms	X, L, P
#8	Physical-level attacks	P

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

Contributions to certification mindset change (I)

Traditional certification mindset

Faults in a well designed car lead to an **infinitesimal and acceptable** probability of catastrophic failure

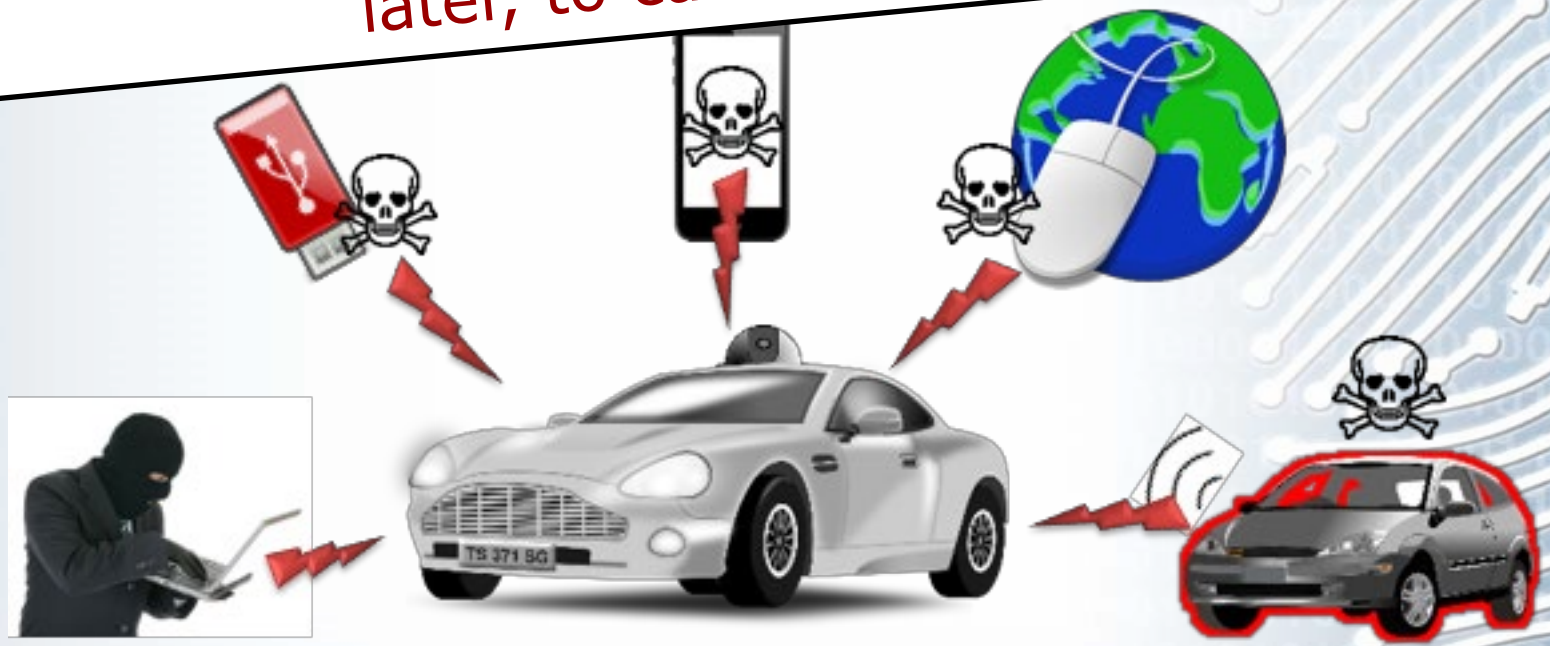
Code-size gap in vehicle ecosystems

Faults in a well designed car may imply a **non-negligible** probability of catastrophic failure

S-Vehicles

Safety-security gap in vehicle ecosystems

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



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

Safety-security gap in vehicle ecosystems

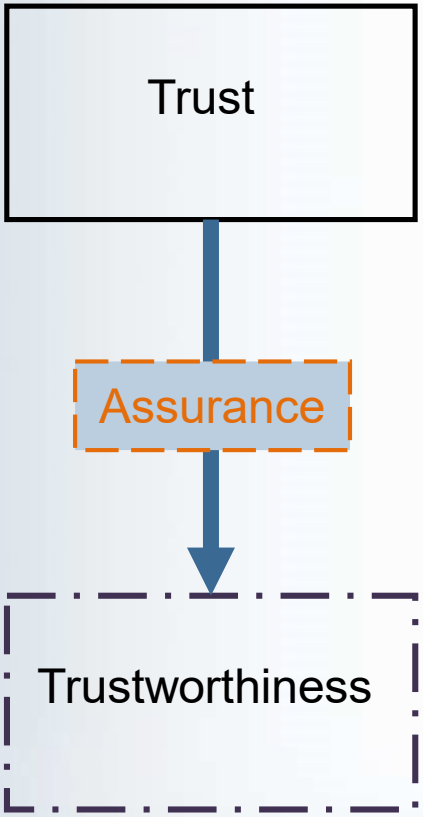
Faults in a well designed car lead to an **infinitesimal and acceptable** probability of catastrophic failure;

Faults in a well designed car may imply a **non-negligible** probability of catastrophic failure

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

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

Perspective taken on assurance: how does the scenario change it

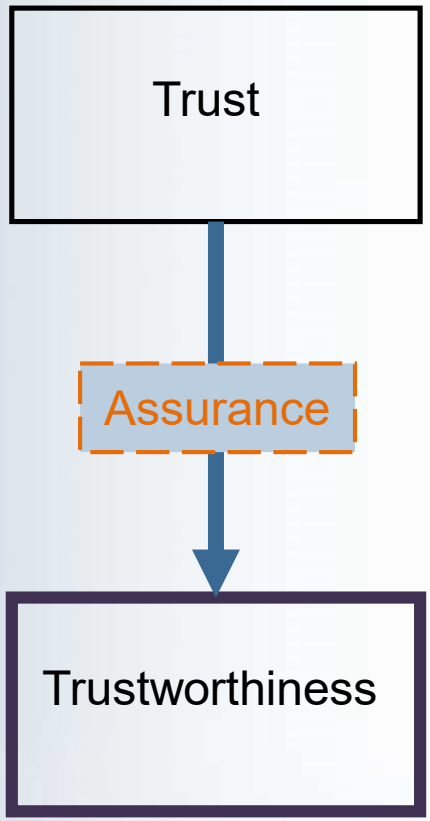


- Statements that explicitly define the dependability and security expectations about a system (a set of properties)
-
- Provides justification that the user trust meets system trustworthiness, through assurance evidence and approvals based on evidence
-
- System mechanisms designed and implemented to meet the requirements (enforce the properties)

Perspective taken on assurance:
weakening the trust-trustworthiness link

- Statements that explicitly define the dependability and security expectations about a system (a set of properties)
-
- Provides justification that the user trust meets system trustworthiness, through assurance evidence and approvals based on evidence
-
- System mechanisms designed and implemented to meet the requirements (enforce the properties)

Perspective taken on assurance:
bringing trustworthiness back high up

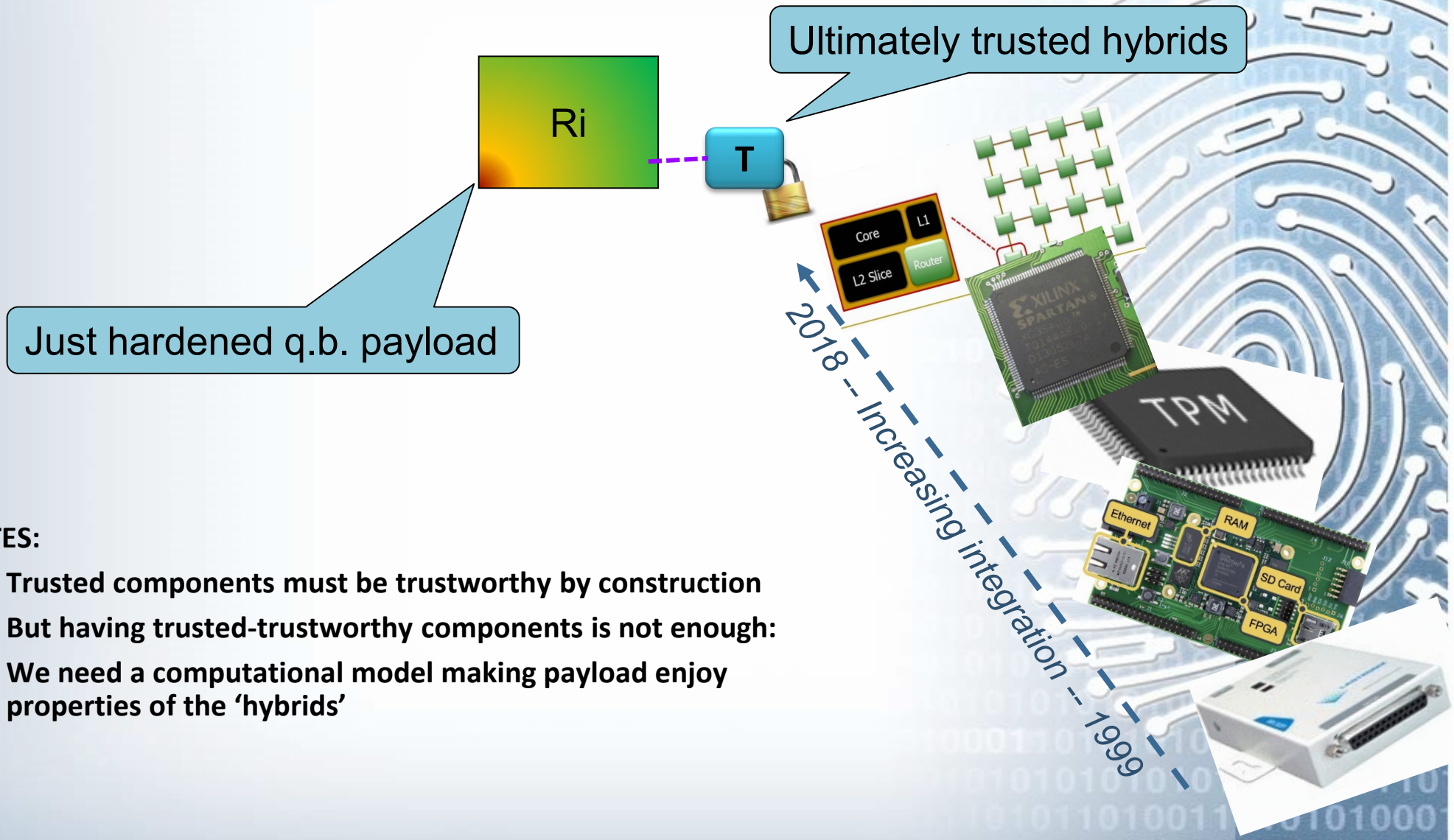


- Statements that explicitly define the dependability and security expectations about a system (a set of properties)
-
- Provides justification that the user trust meets system trustworthiness, through assurance evidence and approvals based on evidence
-
- System mechanisms designed and implemented to meet the requirements (enforce the properties)

Contributions to certification mindset change (II)

Divide-and-conquer I: **Hybrid models and architectures**

Leveraging power at right place right time



NOTES:

(i) **Trusted components must be trustworthy by construction**

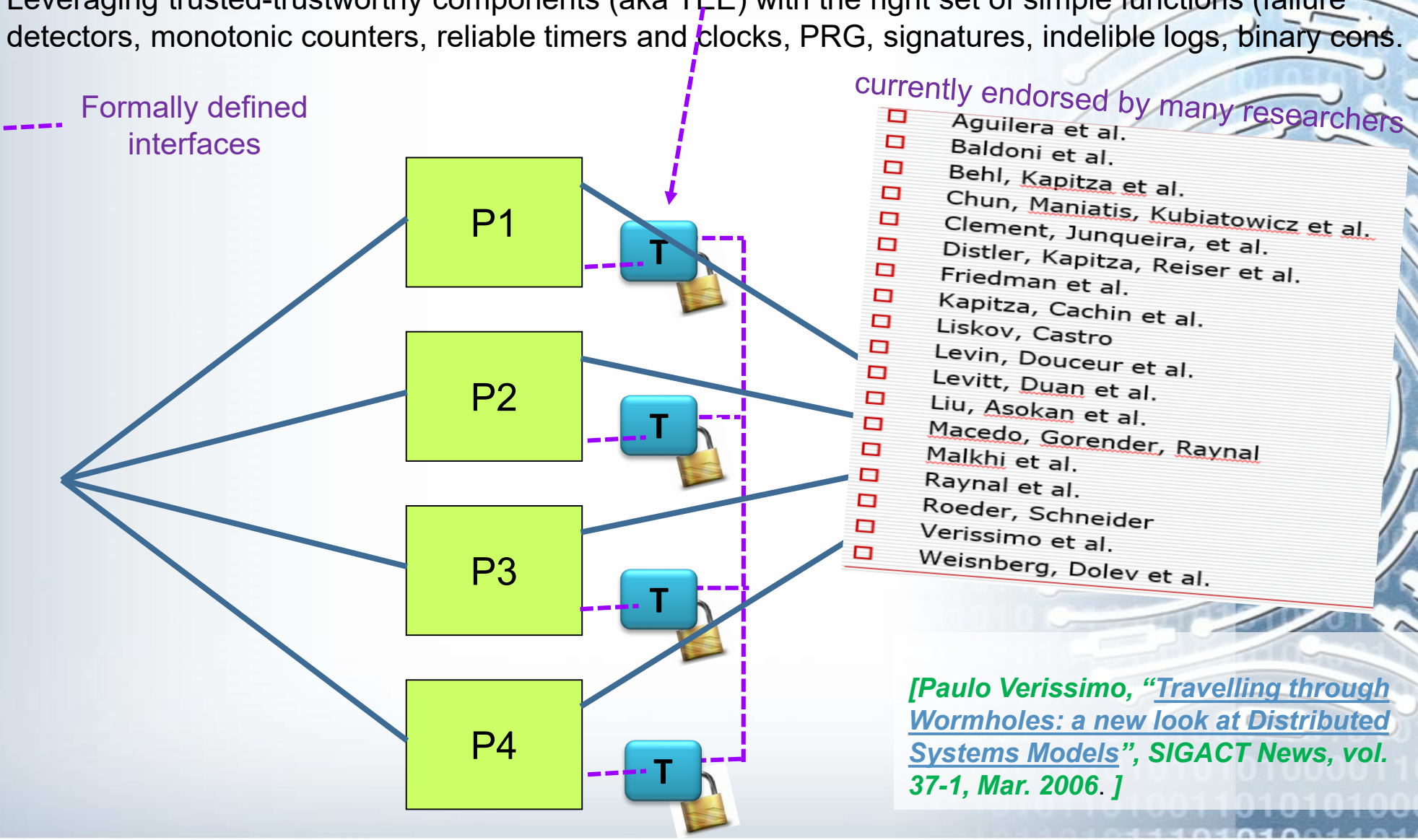
(ii) **But having trusted-trustworthy components is not enough:**

(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

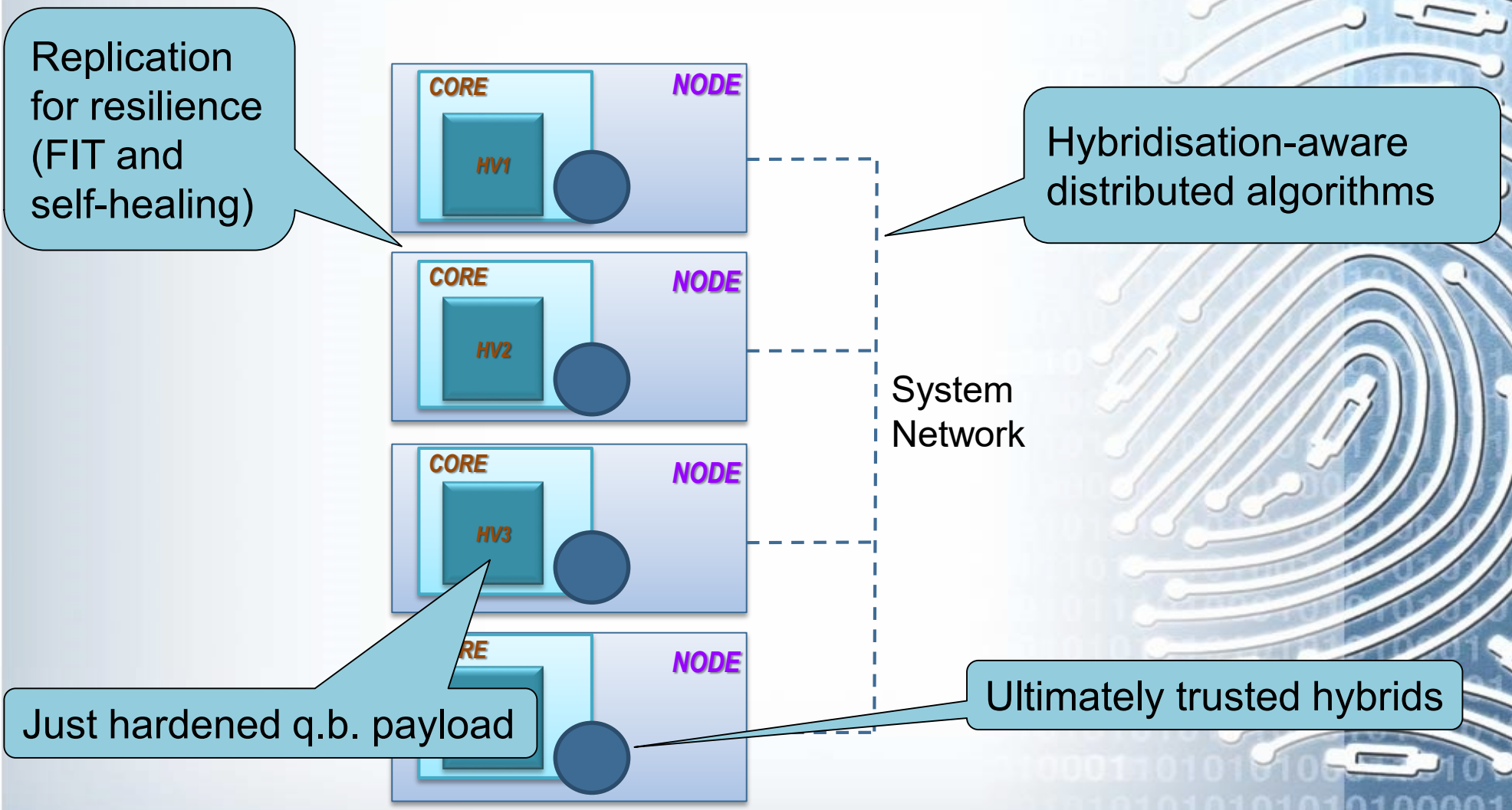
Leveraging trusted-trustworthy components (aka TEE) with the right set of simple functions (failure detectors, monotonic counters, reliable timers and clocks, PRG, signatures, indelible logs, binary cons.



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

Hybrid models and architectures for VLSI FIT

Leveraging power at right place right time



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