University of Luxembourg

SnT - CritiX

Towards sustainable safety and security in autonomous vehicles

Marcus Völp

marcus.voelp@uni.lu

uni.lu
UNIVERSITÉ DU LUXEMBOURG

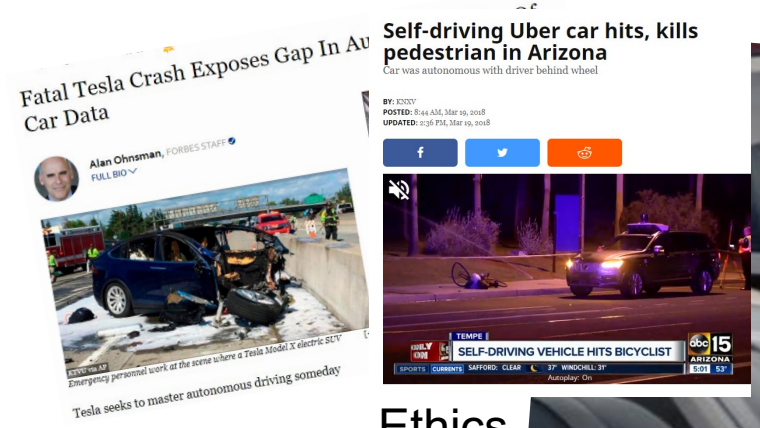
Autonomous driving – the next complexity milestone

securityandtrust.lu

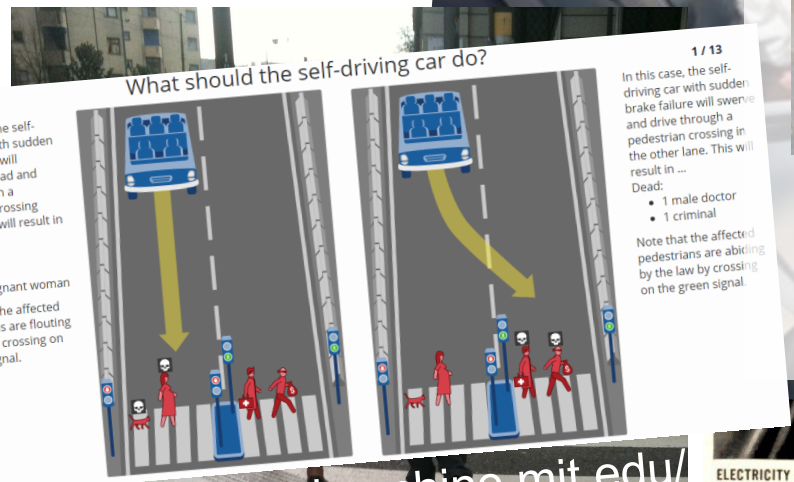
UNIVERSITÉ DU LUXEMBOURG

CRITIX

Acceptance and Reputation



Ethics



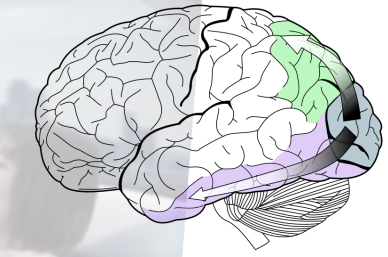
http://moralmachine.mit.edu/

1957
Level 4 autonomy => Level 5

Source: http://paleofuture.com/blog/2010/12/9/driverless-car-of-the-future-1957.html

Implicit Communication

Brain areas involved in human visual perception



Source: Wiki SelKet (CC-BY-SA-3.0)

Recognition not only of regular traffic

Source: Autobild

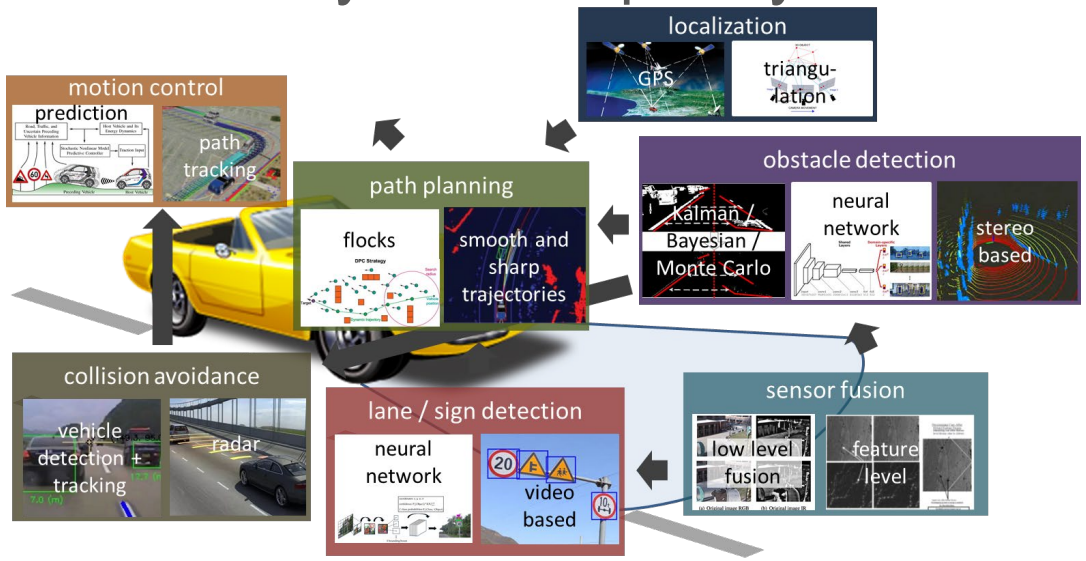
Autonomous driving – the next complexity milestone

securityandtrust.lu

UNIVERSITÉ DU LUXEMBOURG

CRITIX

Functionality vs. Complexity



Components associated with physical control of the vehicle

Components associated with safety

Components associated with entertainment and convenience

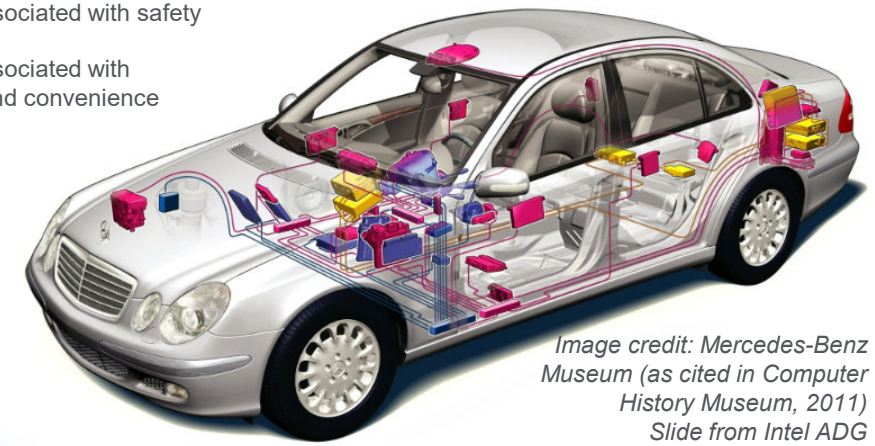


Image credit: Mercedes-Benz Museum (as cited in Computer History Museum, 2011)
Slide from Intel ADG

Complexity of autonomous driving:

- Level 3: 300 MLOC (human supervision)
- Level 5: 1 BLOC+ ?

Current Cars:

- ~ 100 MLOC (30 MLOC multimedia)
- ~ 100 ECUs

Autonomous driving – the next complexity milestone

securityandtrust.lu

UNIVERSITÉ DU LUXEMBOURG

CRITIX

Functionality vs. Complexity

Components associated with physical control of the vehicle

Safety Certification?

Image credit: Mercedes-Benz Museum (as cited in Computer History Museum, 2011)
Slide from Intel ADG

Over the air updates

https://arstechnica.com/cars/2017/07/gm-to-offer-ota-software-updates-before-2020-but-only-for-a-new-infotainment-platform/

Con

- Le
- Le

Current

- ~ 100
- ~ 100

)

ocessors

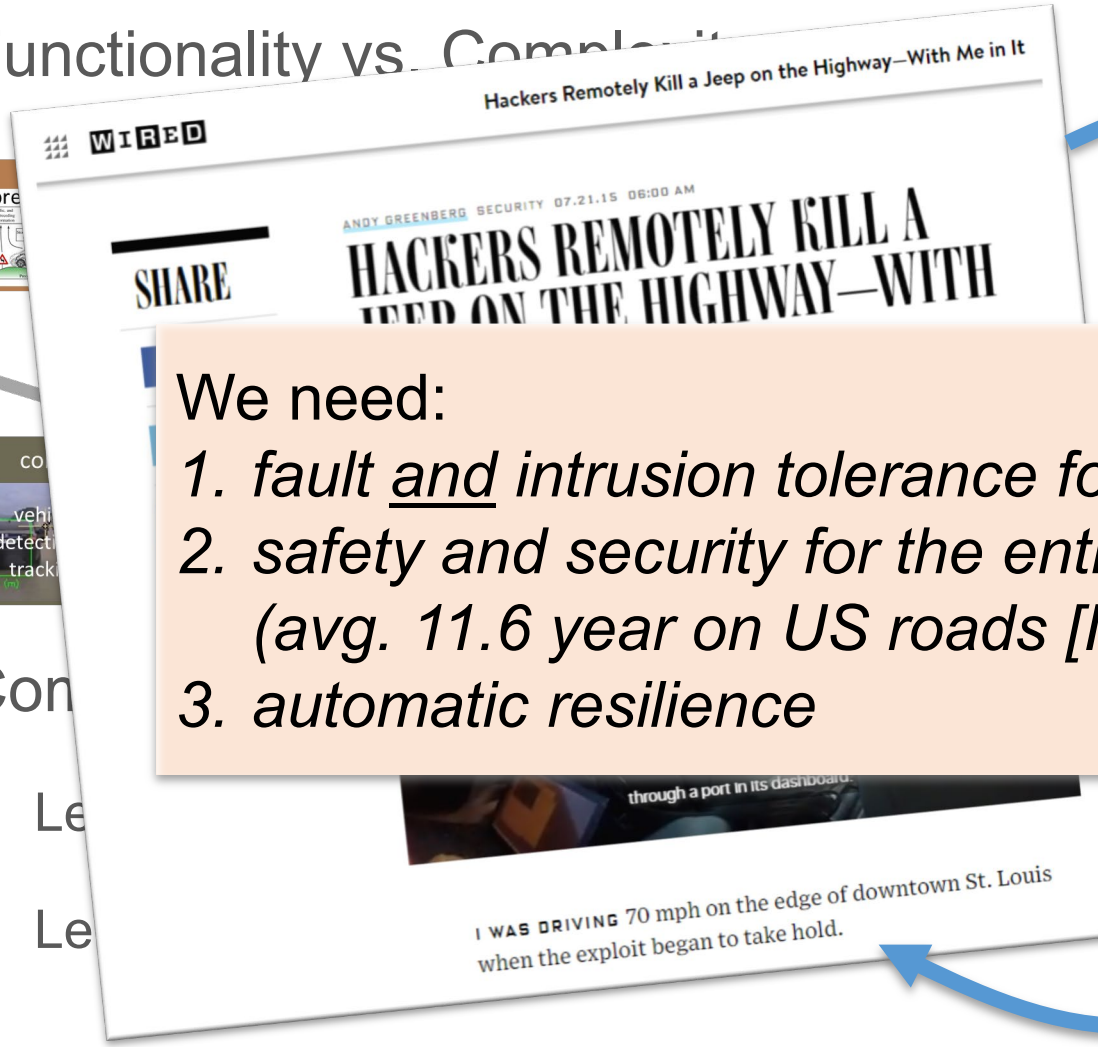
Autonomous driving – the next complexity milestone

securityandtrust.lu

UNIVERSITÉ DU LUXEMBOURG

CRITIX

Functionality vs. Complexity



Safety Certification?

credit: Mercedes-Benz
m (as cited in Computer
History Museum, 2011)
Slide from Intel ADG

We need:

1. *fault <u>and</u> intrusion tolerance for safety critical / real-time systems*
2. *safety and security for the entire lifetime of the car*
   (avg. 11.6 year on US roads [IHS Markit Report '18])
3. *automatic resilience*

Con

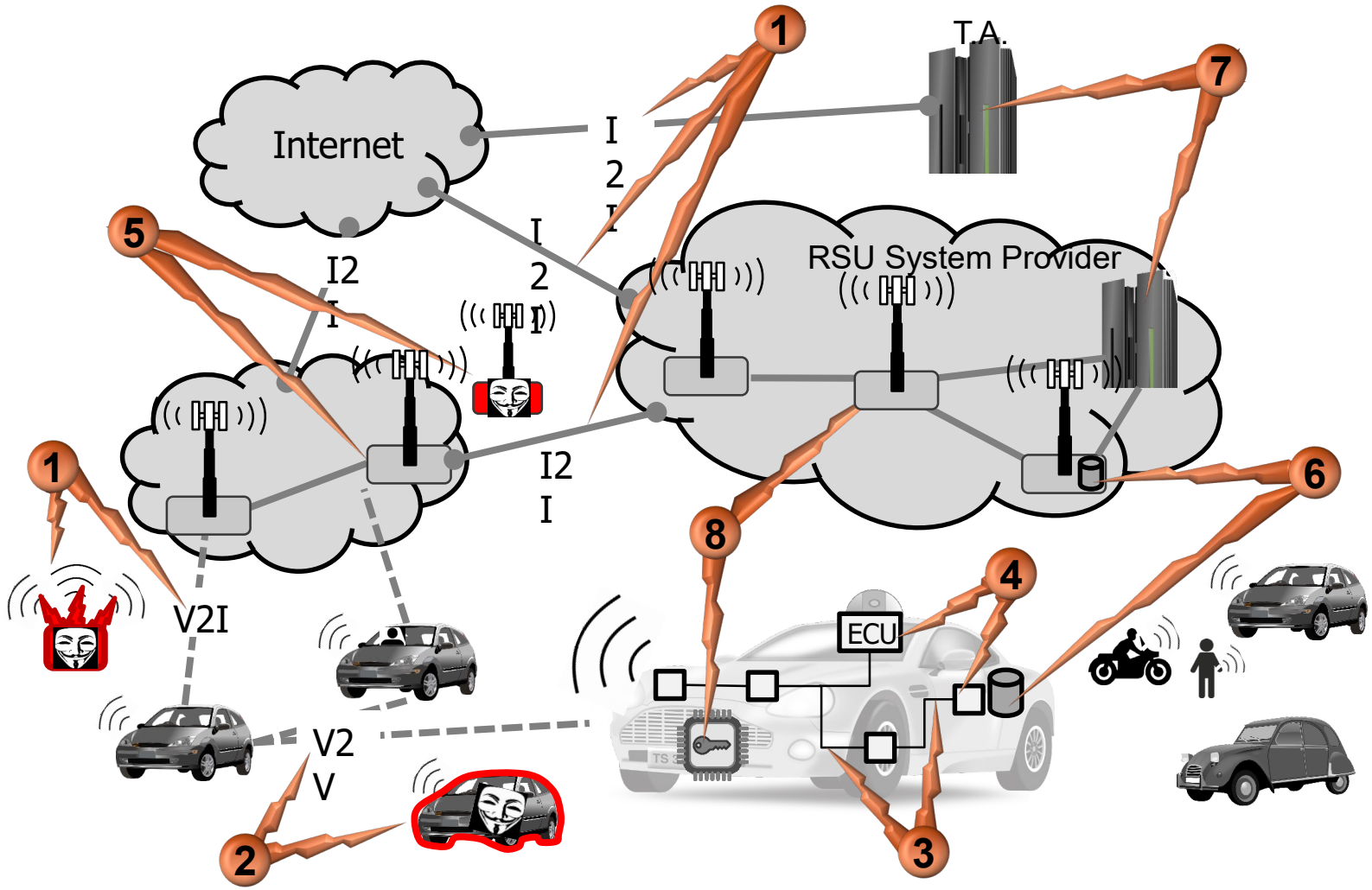
- Le
- Le
- ~ 100
- ~ 100

)

ocessors

https://arstechnica.com/cars/2017/07/gm-to-offer-ota-software-updates-before-2020-but-only-for-a-new-infotainment-platform/

Threat Vectors on autonomous and cooperative vehicle ecosystems



Threat Vectors:

1. Attacks on global V2I/I2I communication infrastructure
2. Attacks on local V2V communication infrastructure
3. Attacks on in-vehicle communication infrastructure
4. Attacks on vehicle computing nodes' software
5. Attacks on road-side units'software
6. Attacks on sensors and control-sensitive data
7. Attacks on authentication mechanisms
8. Physical-level attacks

[Lima et al. “Towards Safe and Secure Autonomous and Cooperative Vehicle Ecosystems”, CPS-SPC 2016]

Outline

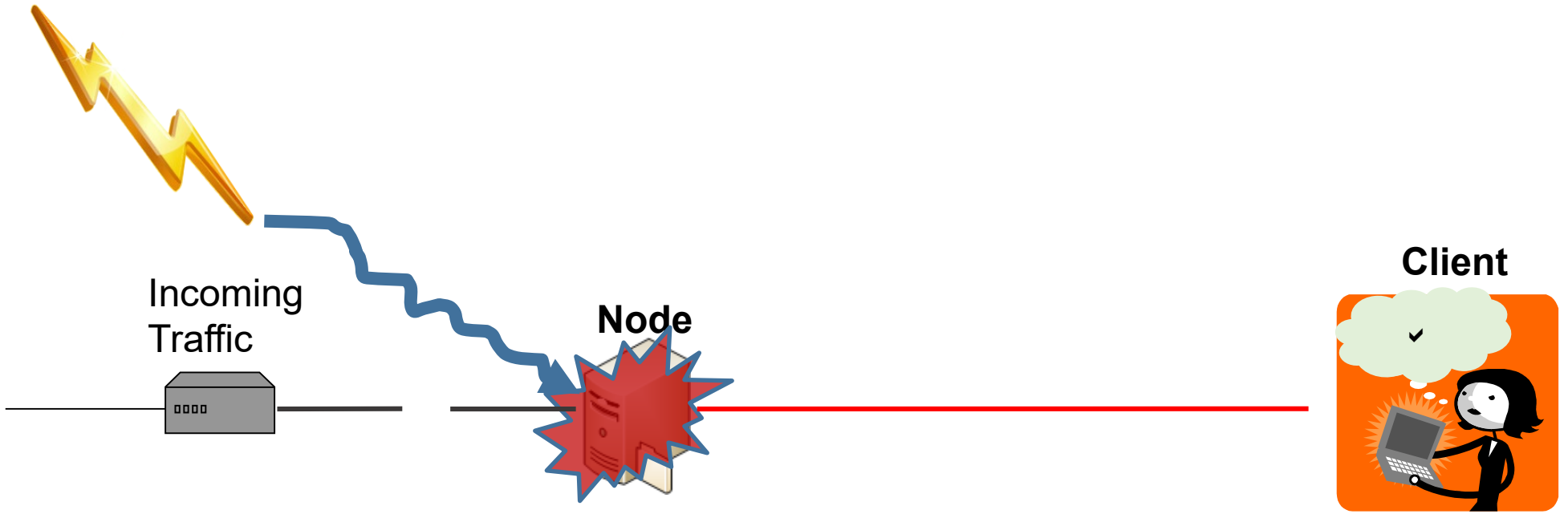
securityandtrust.lu

UNIVERSITÉ DU LUXEMBOURG

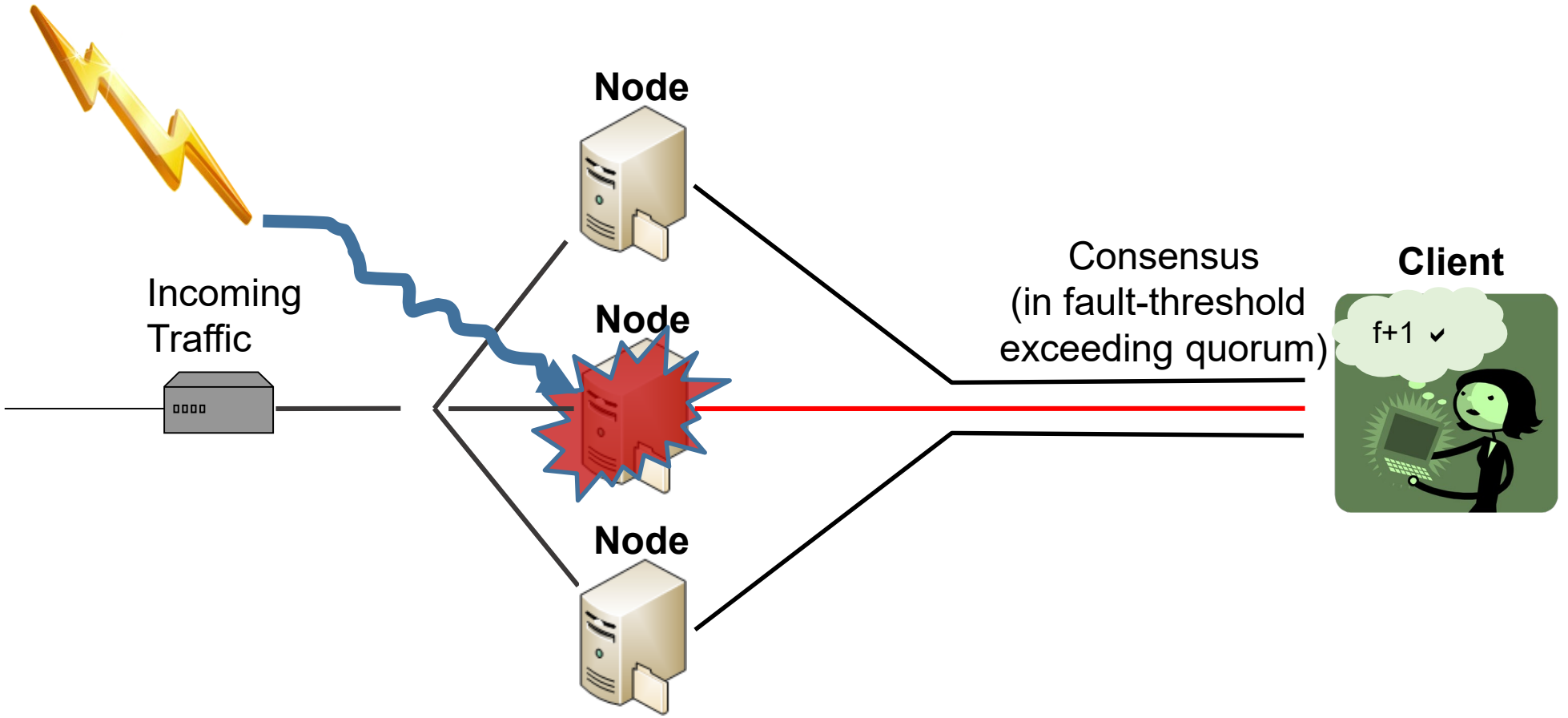
CRITIX

- Motivation
- What we all know: FIT / Resilience
- Full compromise of swarm individuals is intolerable
- Intra Vehicular Systems
- Towards Sustainable Safety and Security
  - Surviving perception / maneuver planning unavailabilities
  - Lifecycle for safeguarding safety and security
- Conclusions

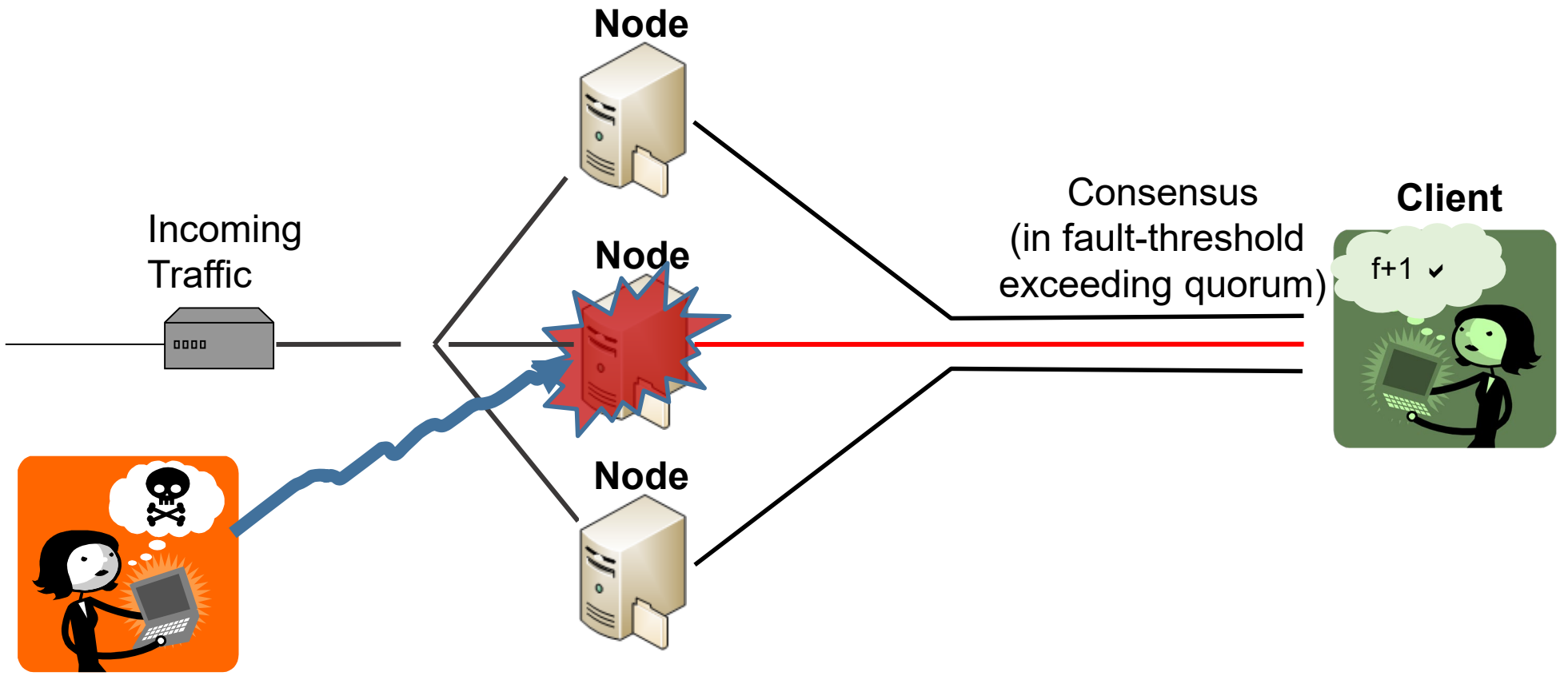
Fault and Intrusion Tolerance



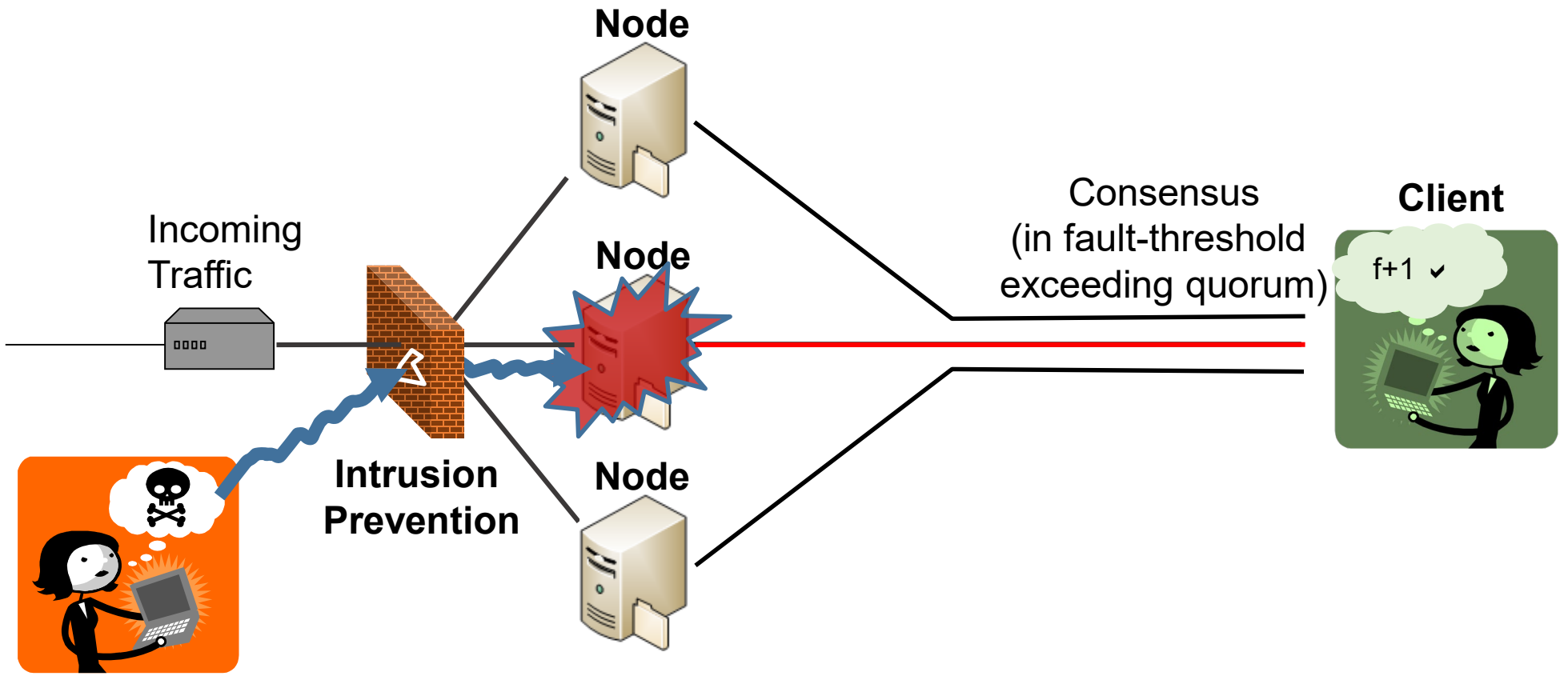
Fault and Intrusion Tolerance



Fault and Intrusion Tolerance

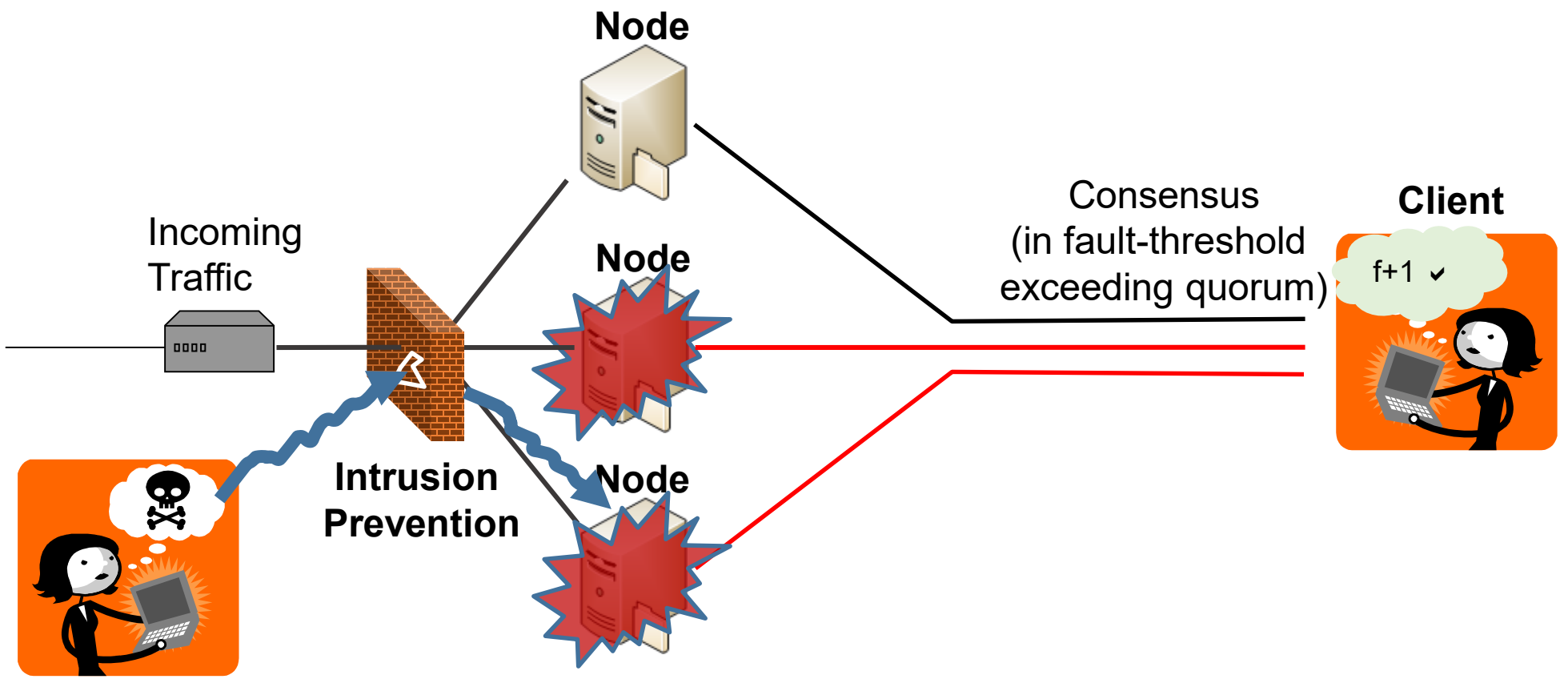


Fault and Intrusion Tolerance



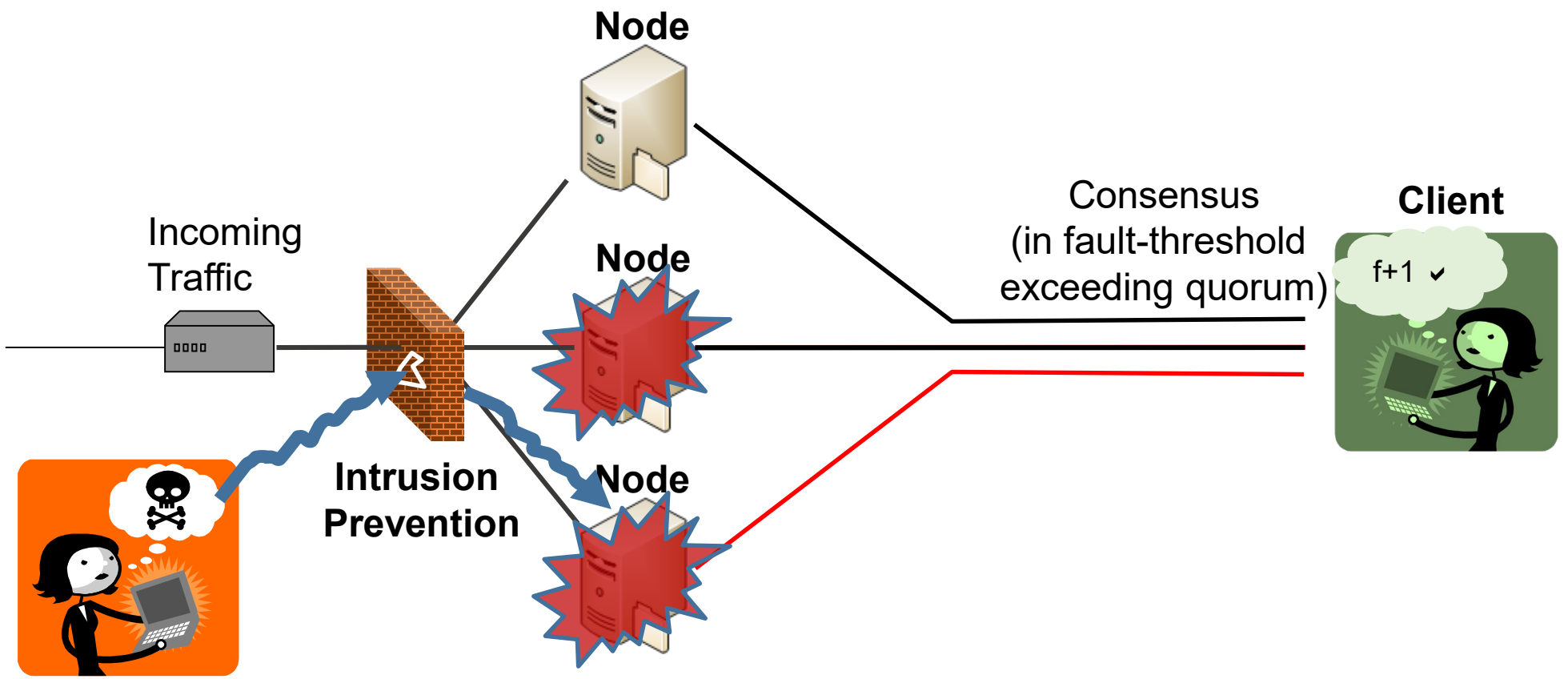
Fault and Intrusion Tolerance

P. Sousa et al. – Exhaustion Failure



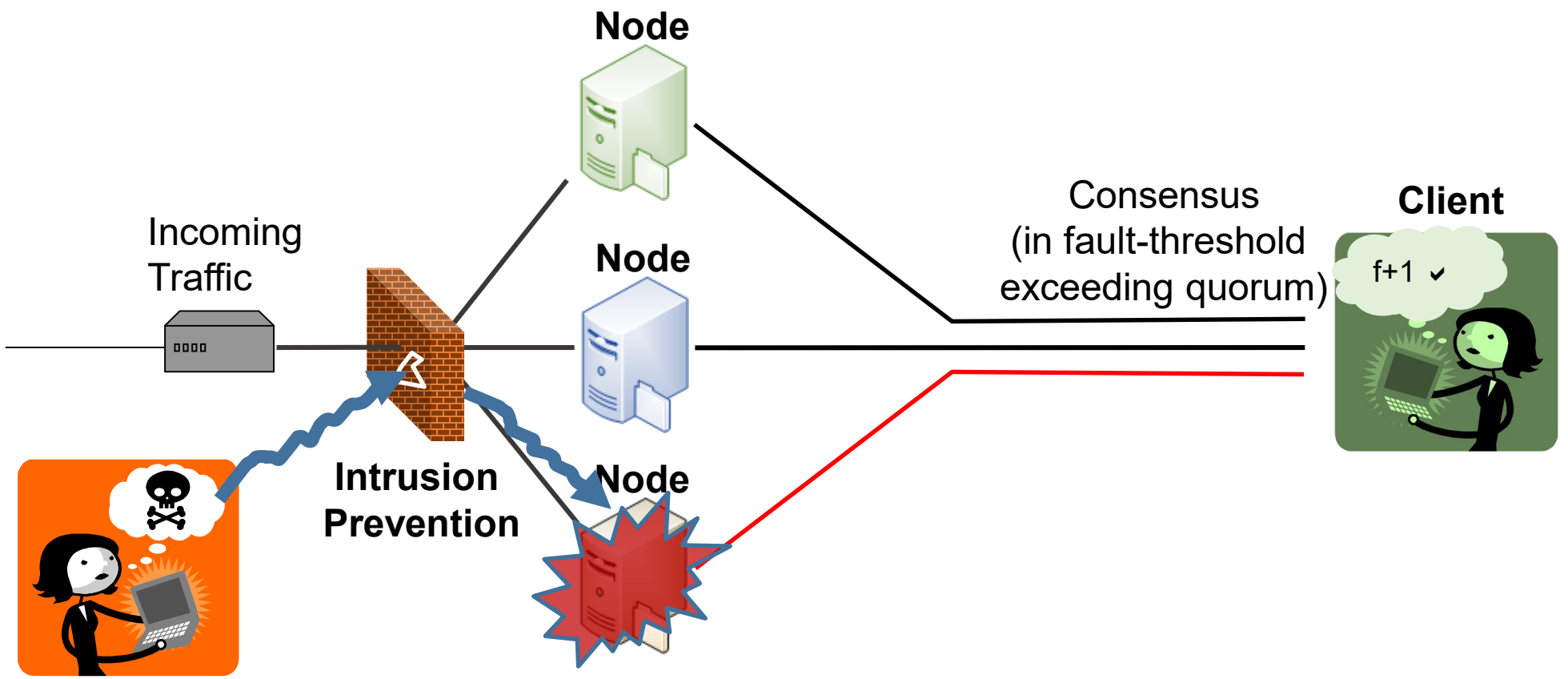
Fault and Intrusion Tolerance

P. Sousa et al. – Exhaustion Failure



Fault and Intrusion Tolerance

P. Sousa et al. – Exhaustion Failure



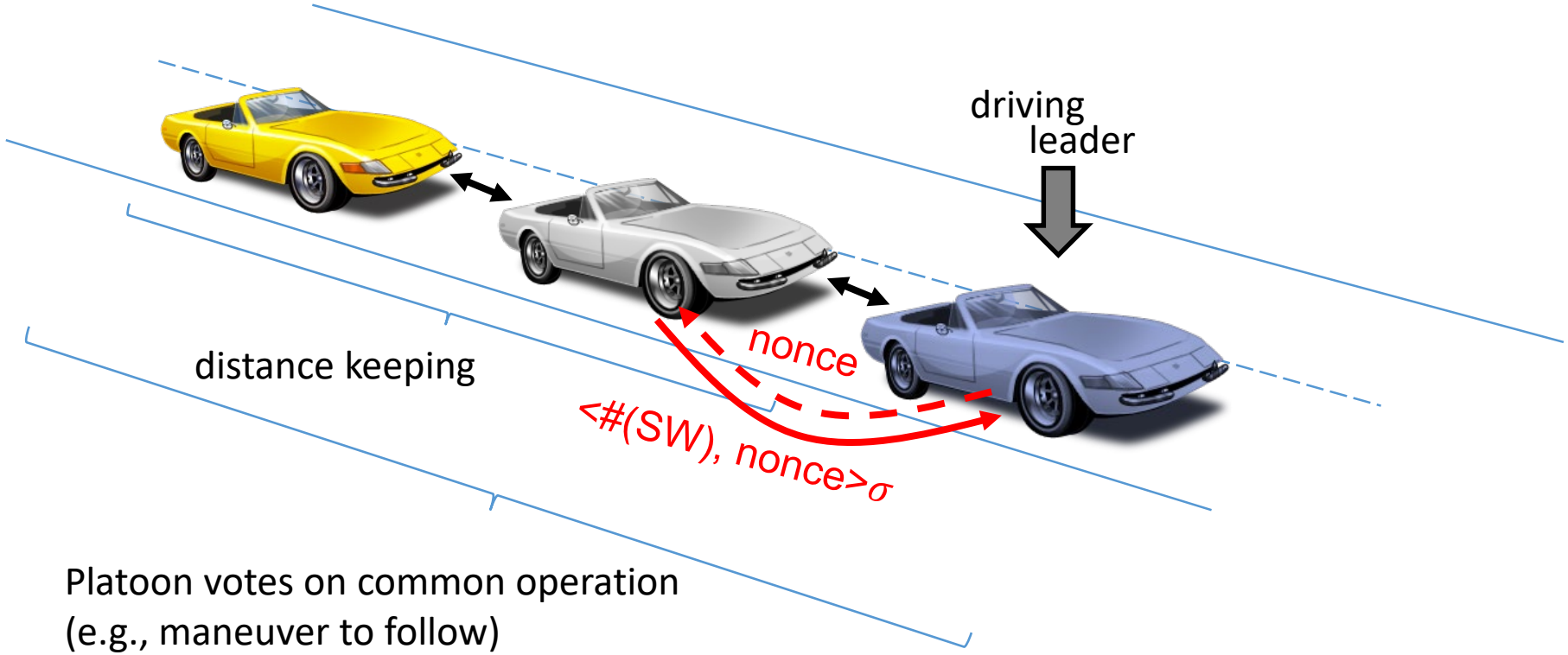
Full compromise of swarm individuals is intolerable

securityandtrust.lu

UNIVERSITÉ DU LUXEMBOURG

CRITIX

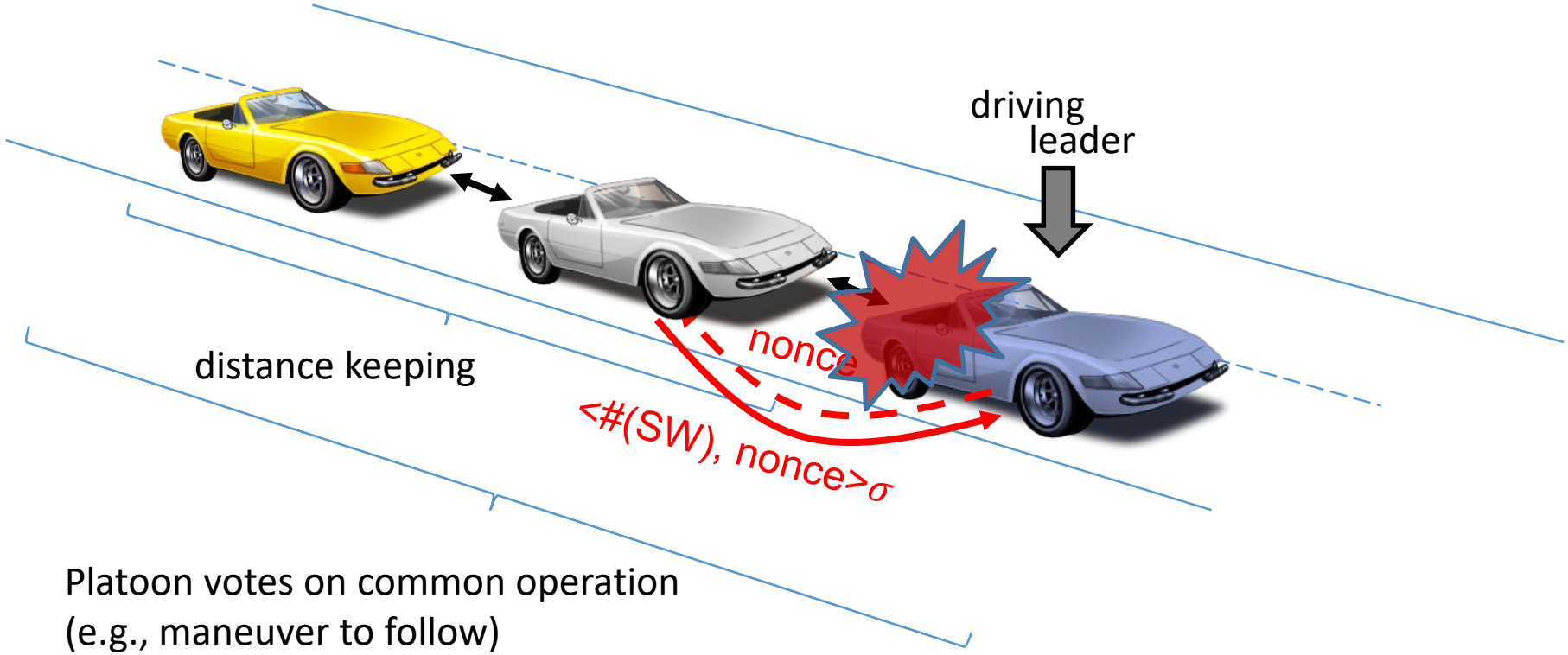
- Platoon of Cars



Platoon votes on common operation
(e.g., maneuver to follow)

Full compromise of swarm individuals is intolerable

- Platoon of Cars

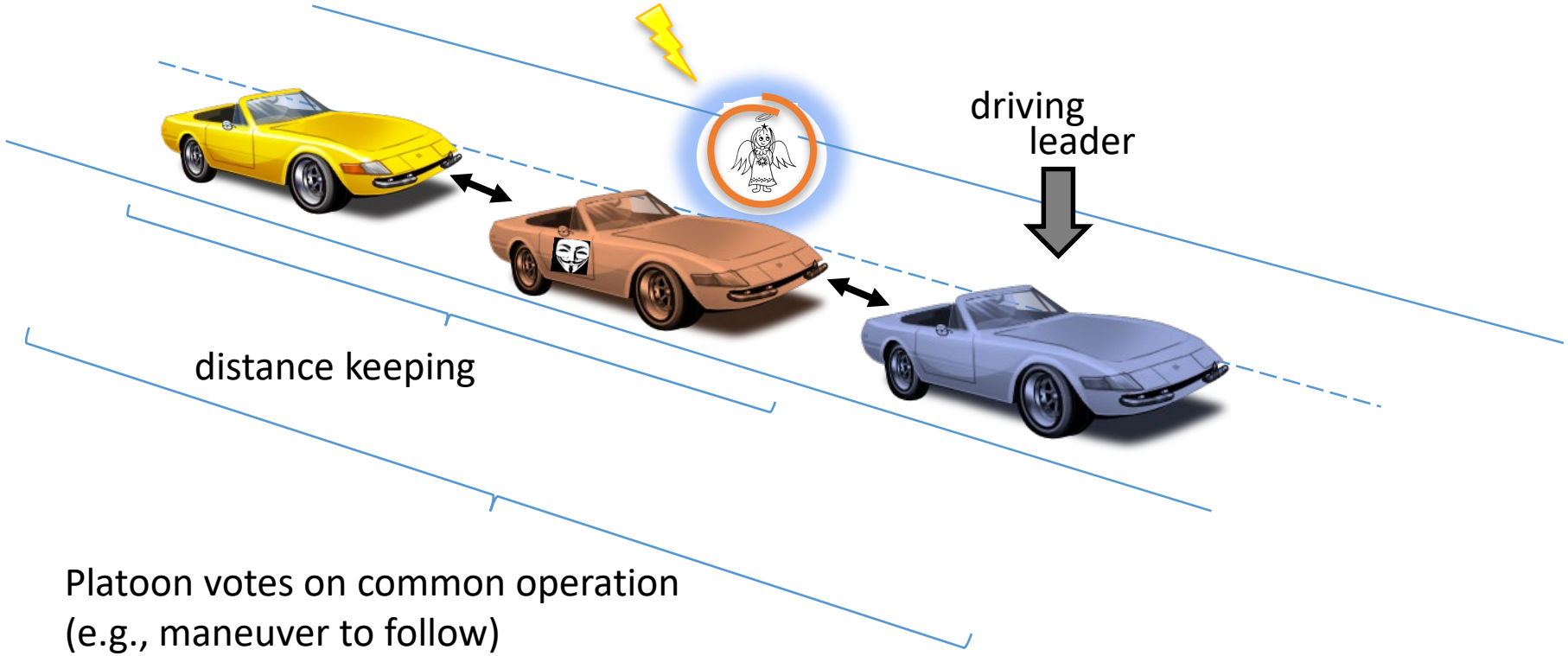


Platoon votes on common operation
(e.g., maneuver to follow)

Full compromise of swarm individuals is intolerable

Towards Sustainable Safety and Security

- Safeguard safety through trusted trustworthy components



Platoon votes on common operation
(e.g., maneuver to follow)

Towards Sustainable Safety and Security

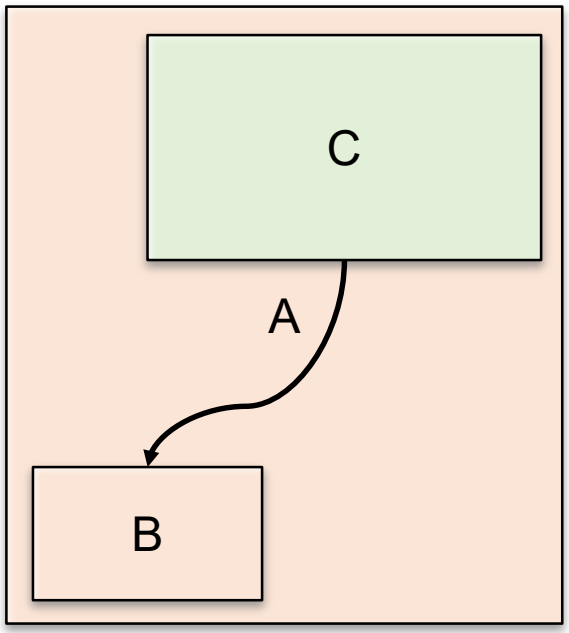
securityandtrust.lu

UNIVERSITÉ DU LUXEMBOURG

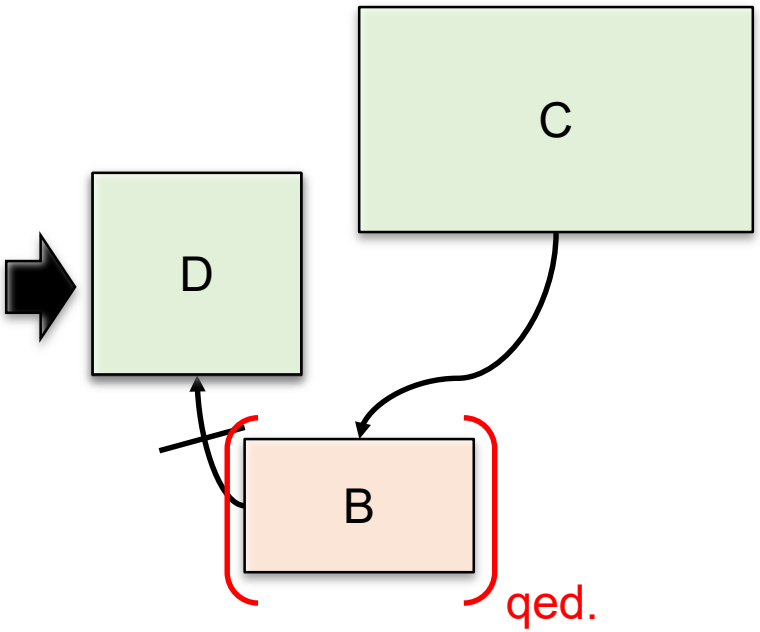
CRITIX

- Known Strategies for TCB Reduction

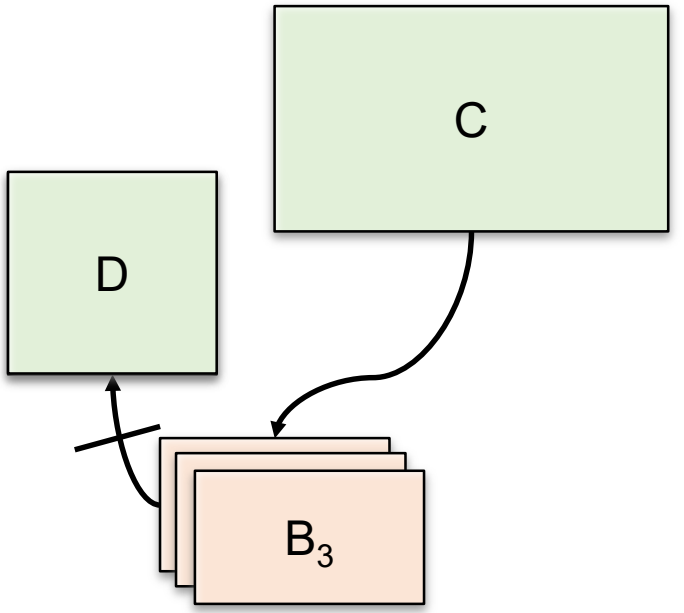
split applications: trusted / untrusted



reuse untrusted



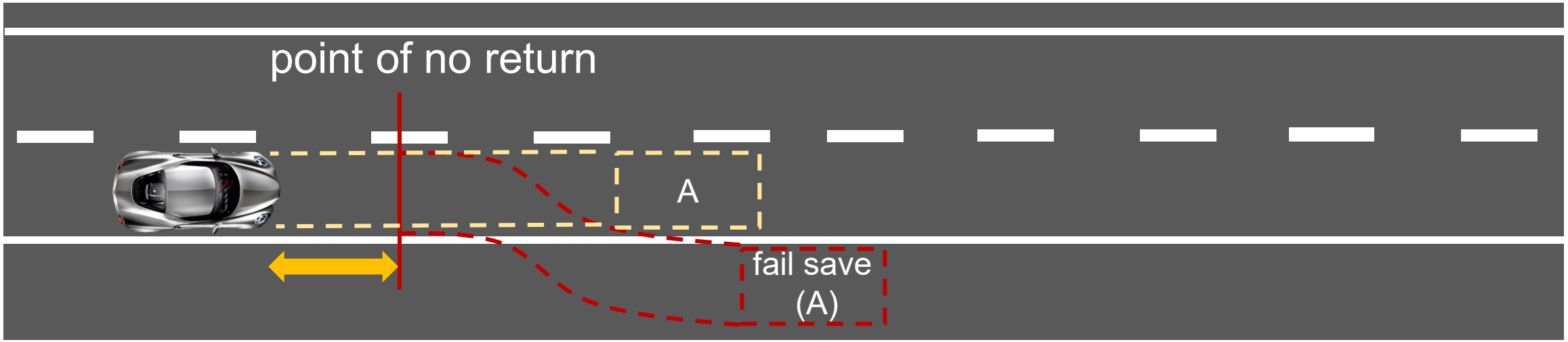
replication (trust majority; not individual)



e.g., C. Weinhold: JVPFS
(also Inktag, SGX)

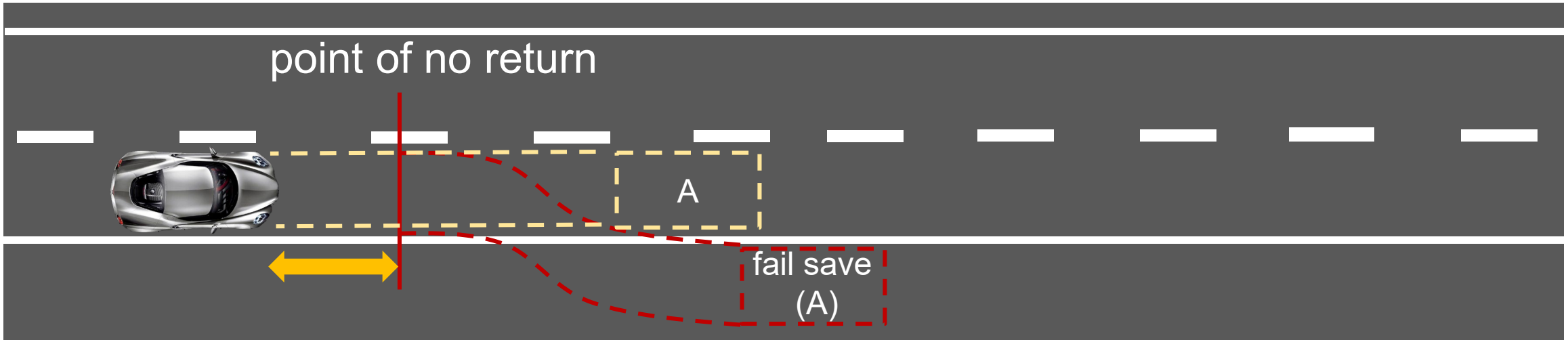
Towards Sustainable Safety and Security

- Reusing potentially unavailable maneuver planning



Towards Sustainable Safety and Security

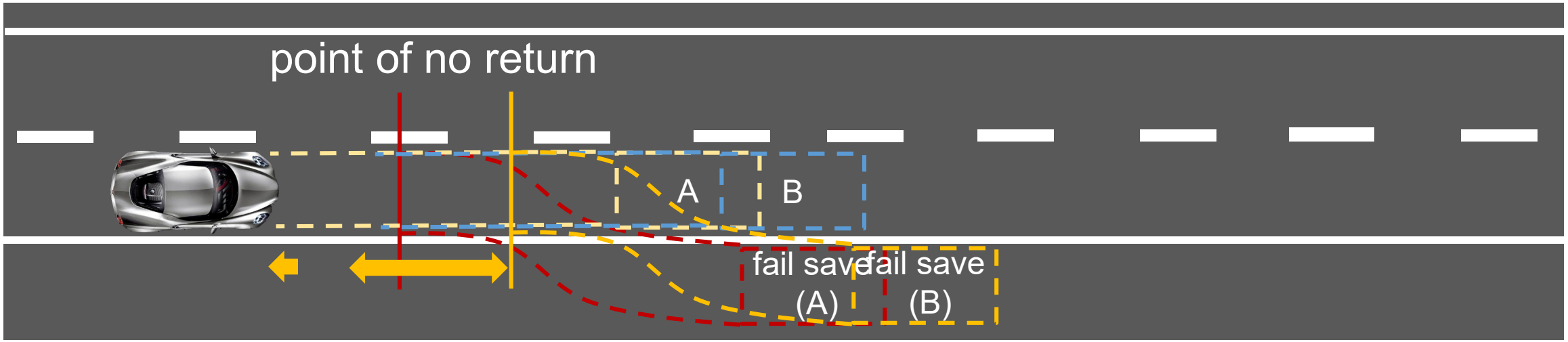
- Reusing potentially unavailable maneuver planning



Towards Sustainable Safety and Security

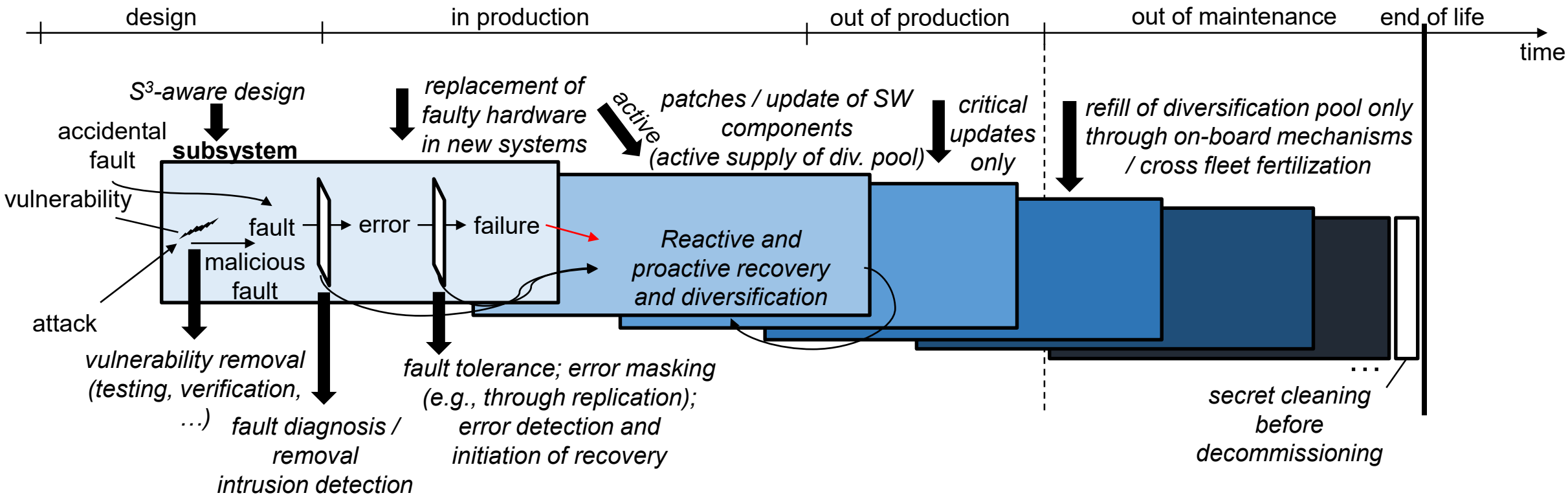
securityandtrust.lu

- Reusing potentially unavailable maneuver planning



Towards Sustainable Safety and Security

- Lifecycle for safeguarding safety and security

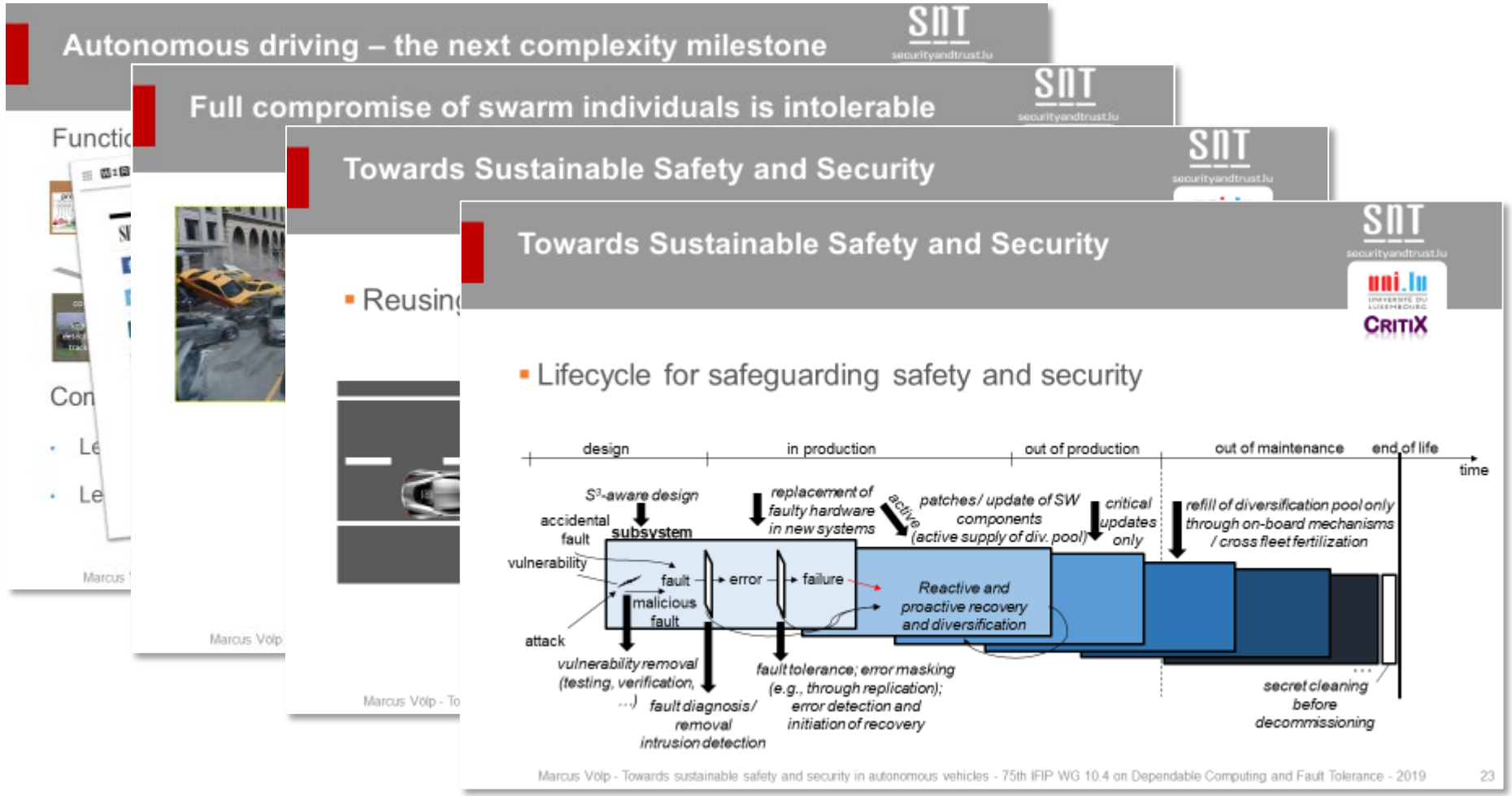


This Talk in one Slide

securityandtrust.lu

UNIVERSITÉ DU LUXEMBOURG

CRITIX



We are hiring bright PhD students and postdocs!