University of Luxembourg

SnT - CritiX

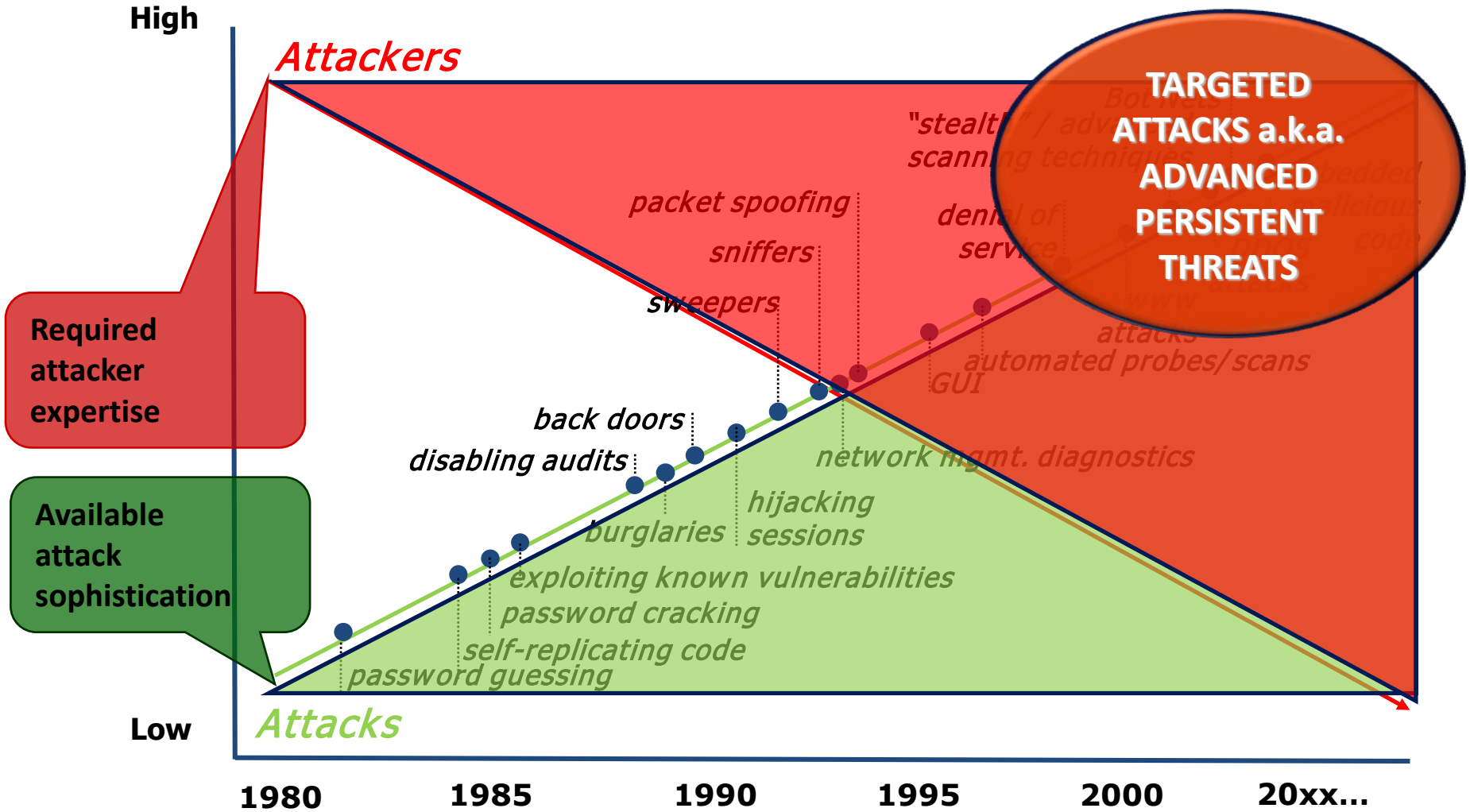
# Sustainable Security & Safety: Challenges and Opportunities

Andrew Paverd, Marcus Völp, Ferdinand Brasser, Matthias Schunter, N. Asokan, Ahmad-Reza Sadeghi, Paulo Esteves-Veríssimo, Andreas Steininger, Thorsten Holz

Intel Collaborative Research Center – Collaborative Autonomous Resilient Systems

marcus.voelp@uni.lu

# Attack sophistication vs. attacker expertise




(Source: Adapted from Lipson, H. F., Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues, Special Report CMS/SEI-2002-SR-009, November 2002. (CERT)

# Autonomous driving – the next complexity milestone

securityandtrust.lu

UNIVERSITÉ DU LUXEMBOURG

CRITIX

## Acceptance and Reputation

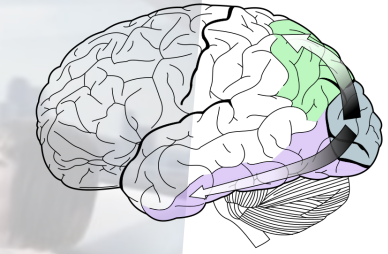


## Ethics


## 1957
## Level 4 autonomy => Level 5


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

## Brain areas involved in human visual perception



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

## Recognition not only of regular traffic

Source: Autobild

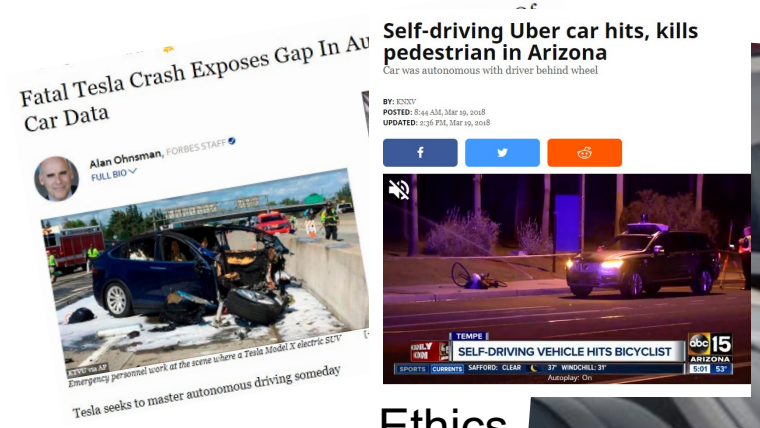
# Autonomous driving – the next complexity milestone

securityandtrust.lu

UNIVERSITÉ DU LUXEMBOURG

CRITIX

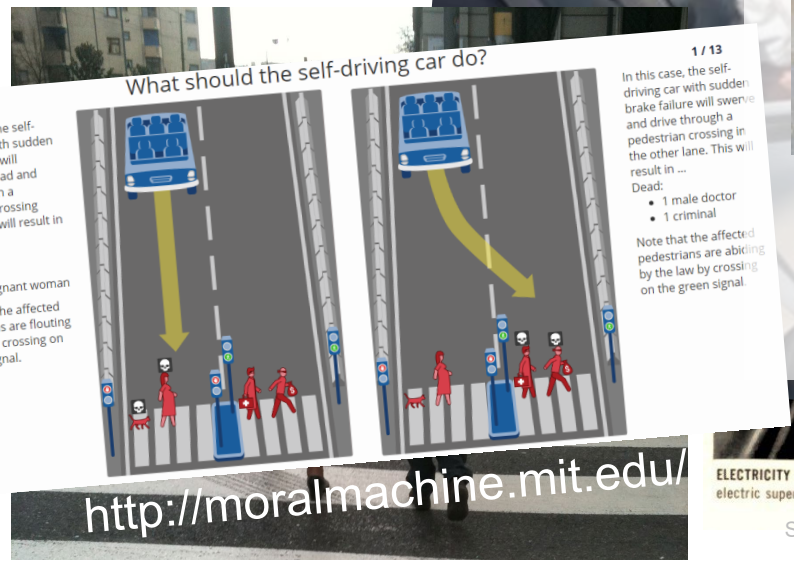
## Acceptance and Reputation







## Ethics




## 1957
## Level 4 autonomy => Level 5

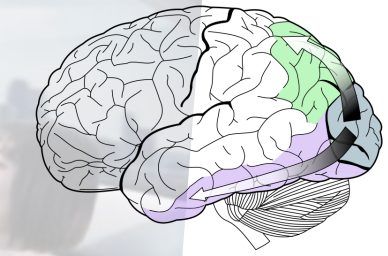

Source: http://paleofuture.com/blog/2010/12/9/driverless-car-of-the-future-1957.html

## 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

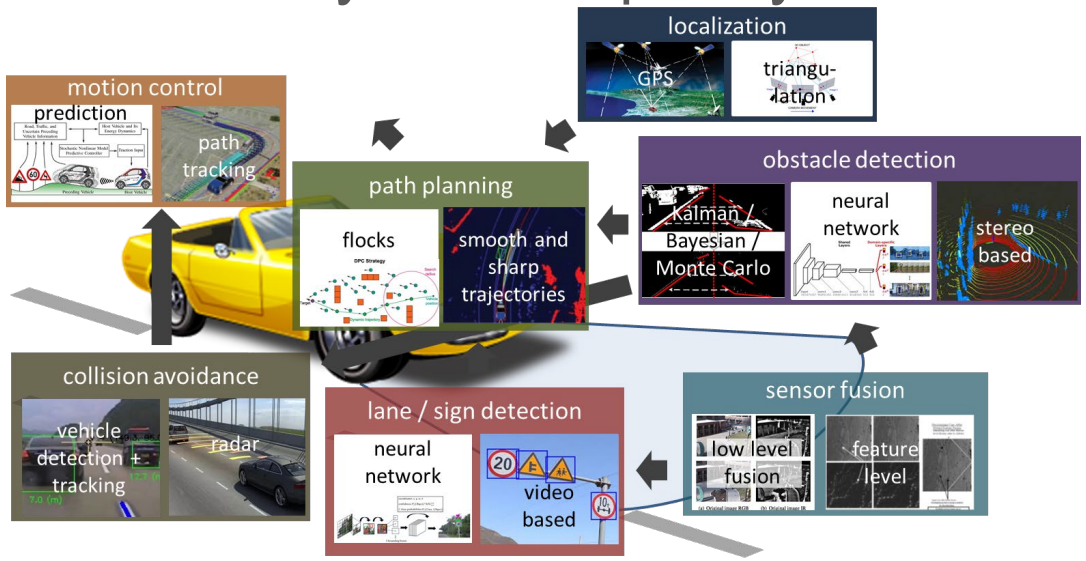
# Autonomous driving – the next complexity milestone

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

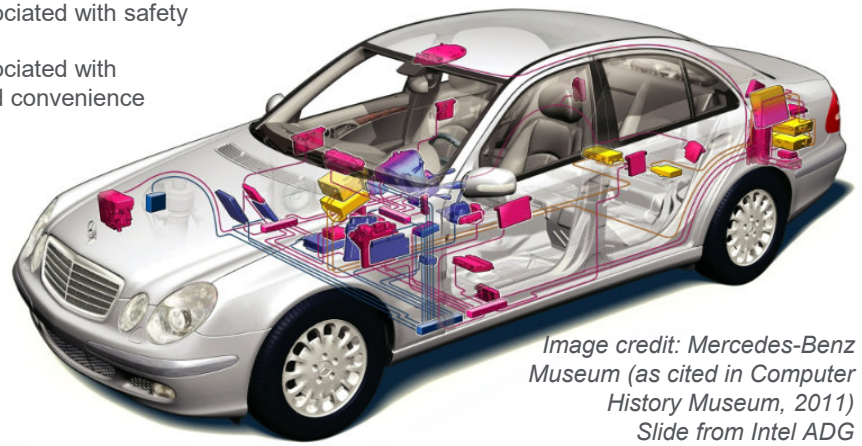


*Image credit: Mercedes-Benz Museum (as cited in Computer History Museum, 2011) Slide from Intel ADG*

## 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?

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

**We need systems to survive faults and intrusions throughout their lifetime!**

*(for cars: avg. lifetime of 11.6 year on US roads)*
*[IHS Markit Report '18]*

WIRED

Hackers Remotely Kill a Jeep on the Highway—With Me in It

ANDY GREENBERG SECURITY 07.21.15 06:00 AM

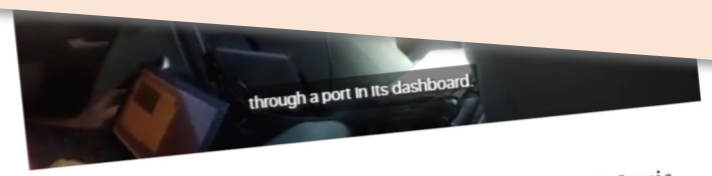
SHARE

SHARE 208403

TWEET

COMMENT

EMAIL




I WAS DRIVING 70 mph on the edge of downtown St. Louis when the exploit began to take hold.

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/

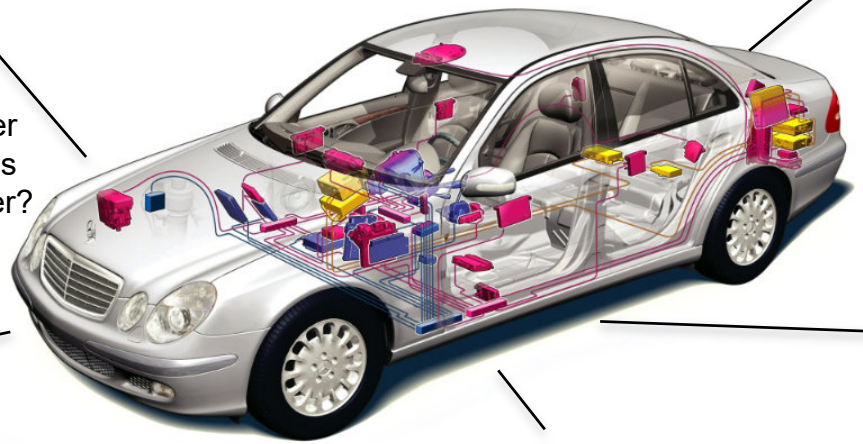
# Challenges

## ownership changes

- How to securely inform the system about the change in ownership, without opening a potential attack vector?
- How to erase sensitive data during transfer of ownership, without allowing the previous owner to later erase data of the new owner?

## maintainer changes

- How can a system decide that it is no longer maintained?
- How should an unmaintained system behave?



## subsystem failures

- How can we assert the sustainability of emerging material circuits, without at the same time giving adversaries the tools to stress and ultimately break these circuits?
- How to prevent the leakage of sensitive information from a compromised subsystem?
- How to securely re-provision a subsystem after all secrets have been leaked?

## requirement changes

- How to retroactively change the designed security, privacy, and/or safety guarantees of a system?
- How can a system be extended and adapted to meet new expectations after deployment?
- Howto determine whether a deployed system will retain its safety and security guarantees for an even longer lifetime?

## environmental changes

- How to tolerate failure of subsystems due to unforeseeable threats?

# Lifecycle


Safety (i.e., no harm despite accidental faults) ✓

Security (malicious faults, e.g., targeted attacks) ?

Security incidents affecting safety -

# Cyber Resilient Architectures

securityandtrust.lu

UNIVERSITÉ DU LUXEMBOURG

CRITIX

Prevent Intrusions

… but intrusions will occur

Detect Intrusions, Limit Damage

… but some attacks will succeed (attacks may be stealthy)

Tolerate Attacks

… but we loose resources

Restore System

## 1st Generation: Protection


Access Control & Physical Security


Cryptography


Multiple Security Levels

Trusted Computing Base

## 2nd Generation: Detection


Firewalls


Boundary Controllers


Intrusion Detection Systems


VPNs


PKI

## 3rd Generation: Tolerance


Intrusion Tolerance


Big Board View of Attacks Real-Time Situation Awareness & Response


Graceful Degradation


Hardened Operating System

## 4th Generation: Regeneration


Self-Aware


Diagnosis


Learning


Reconfiguration

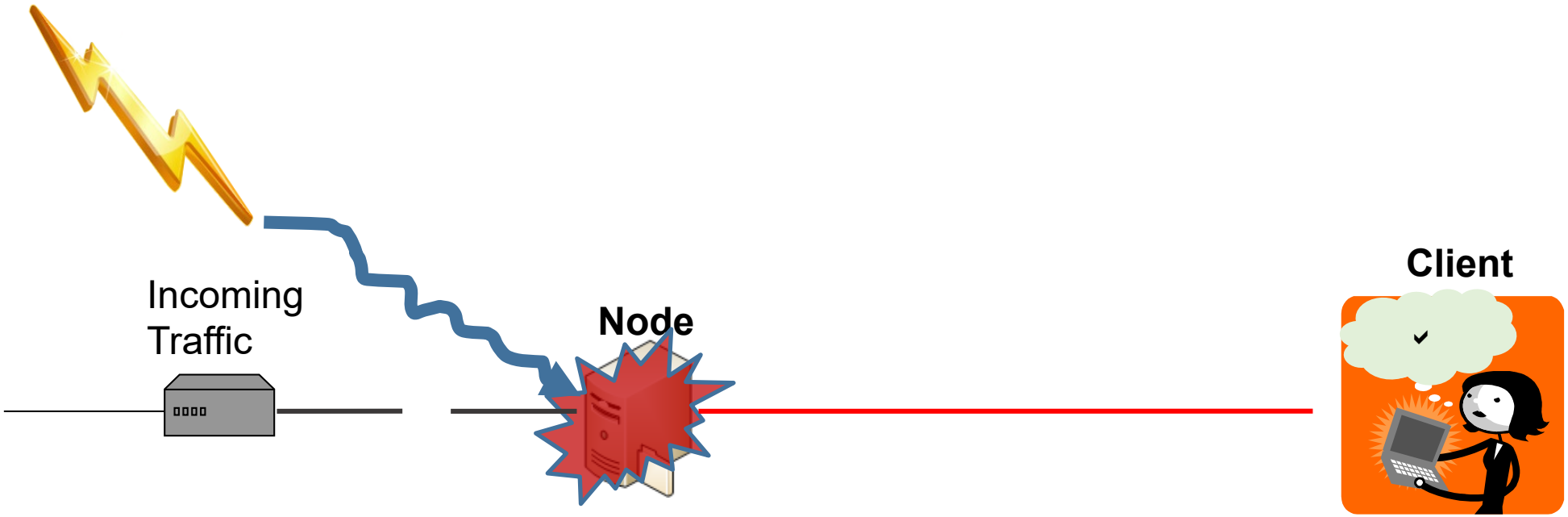

Reflection


Rejuvenation

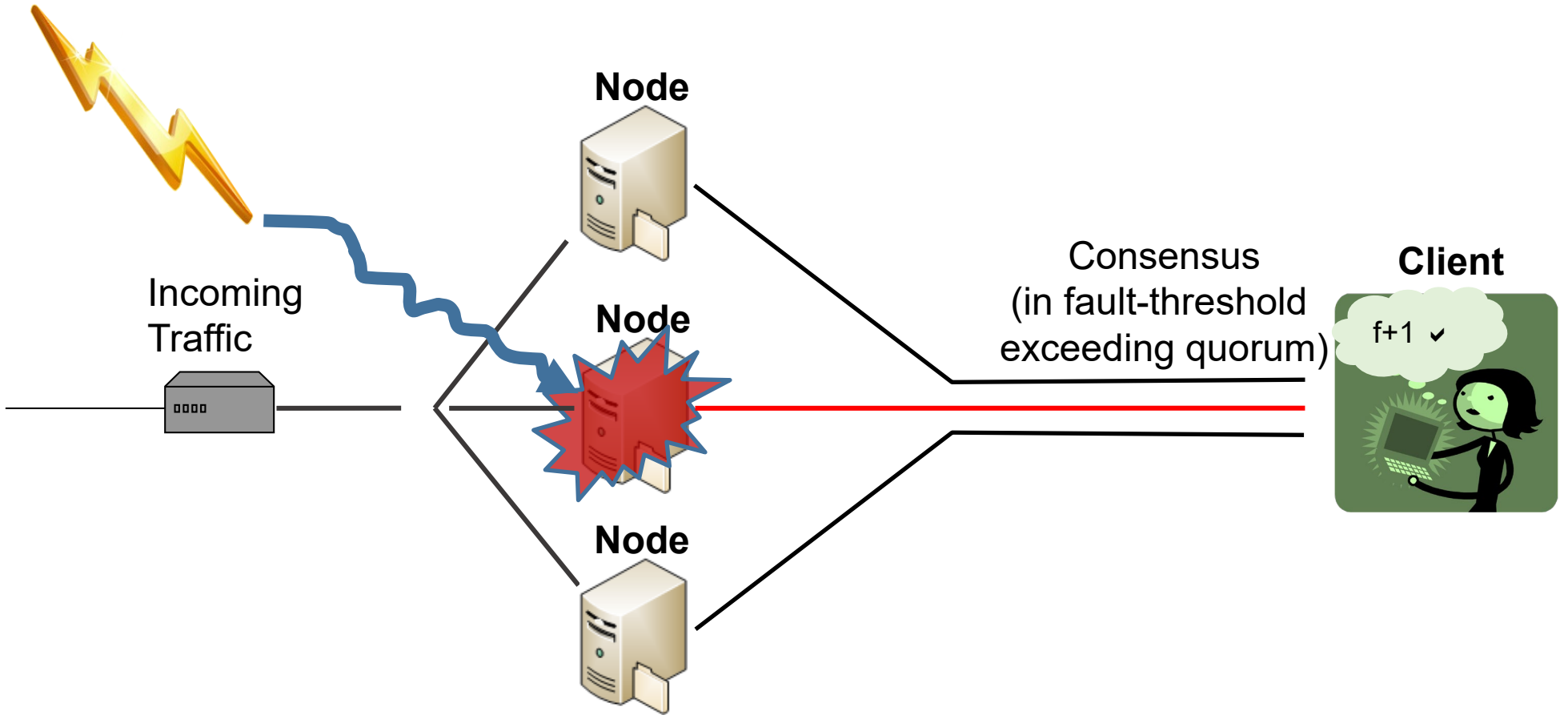
***Real Time***

(Source: Jay Lala – Autonomous Panel DSN'19)

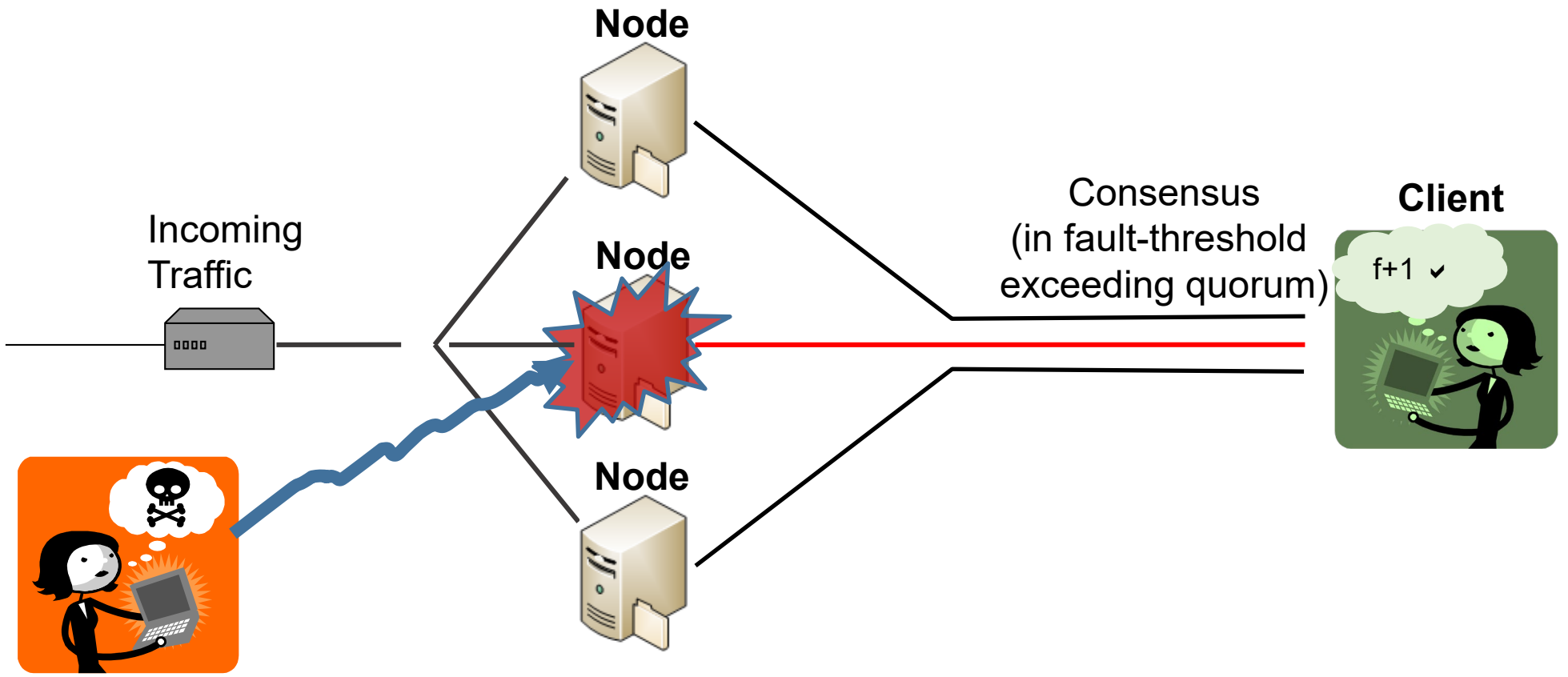
# Fault and Intrusion Tolerance



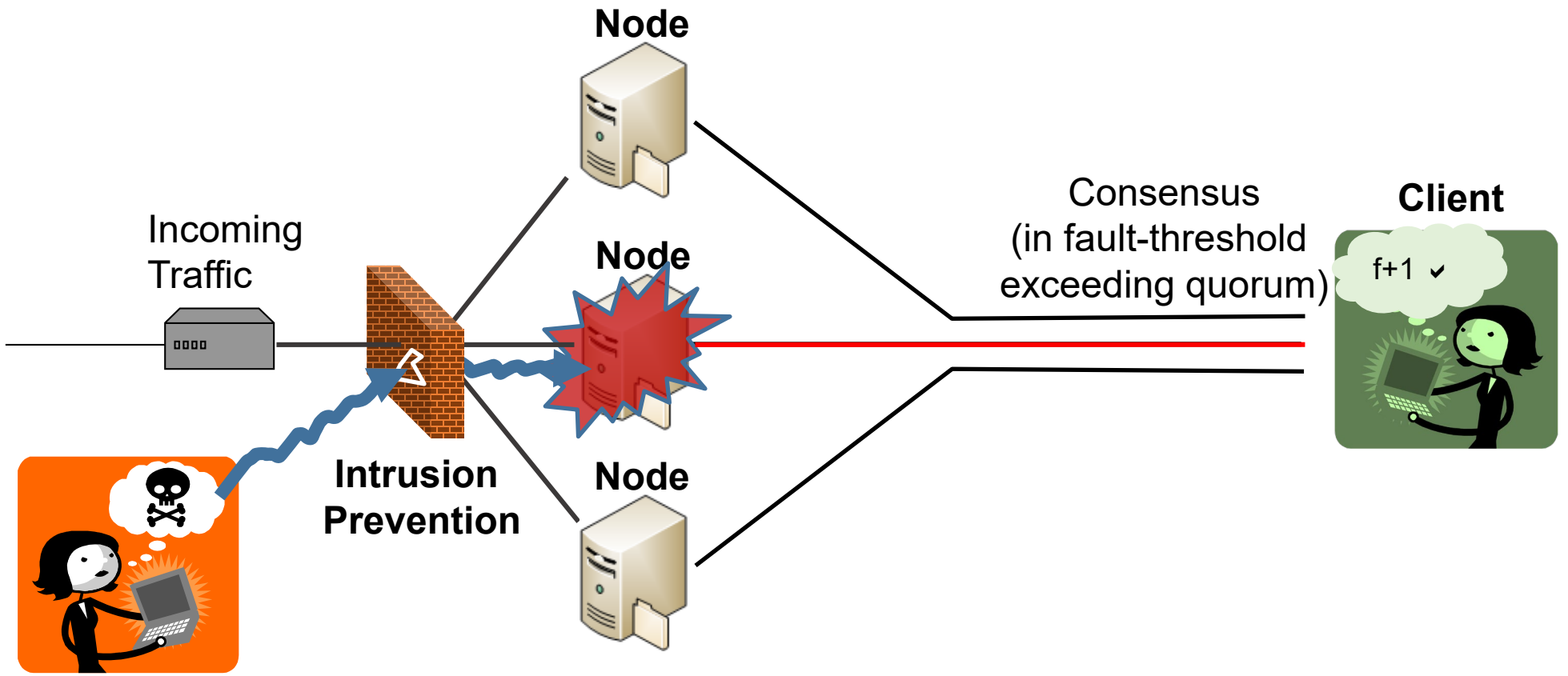
# Fault and Intrusion Tolerance



# Fault and Intrusion Tolerance

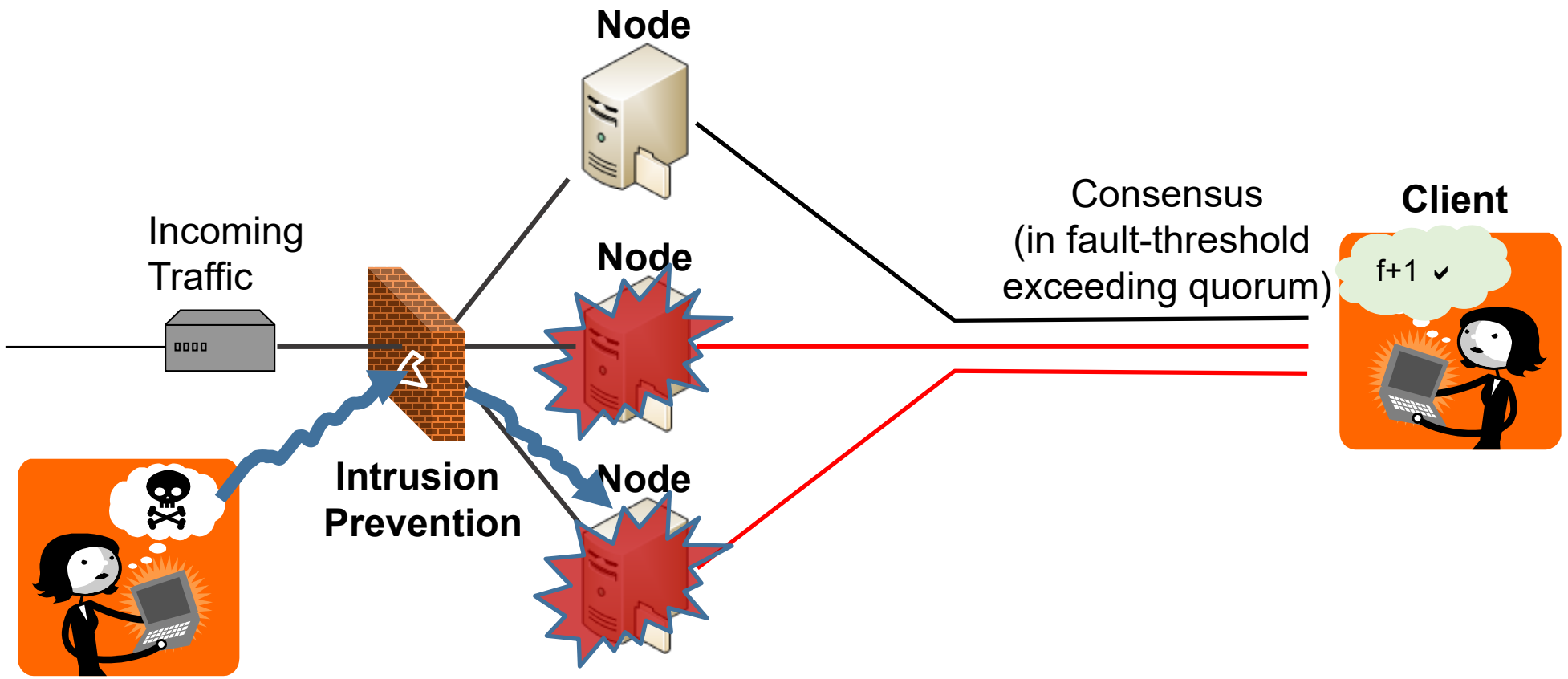


# Fault and Intrusion Tolerance



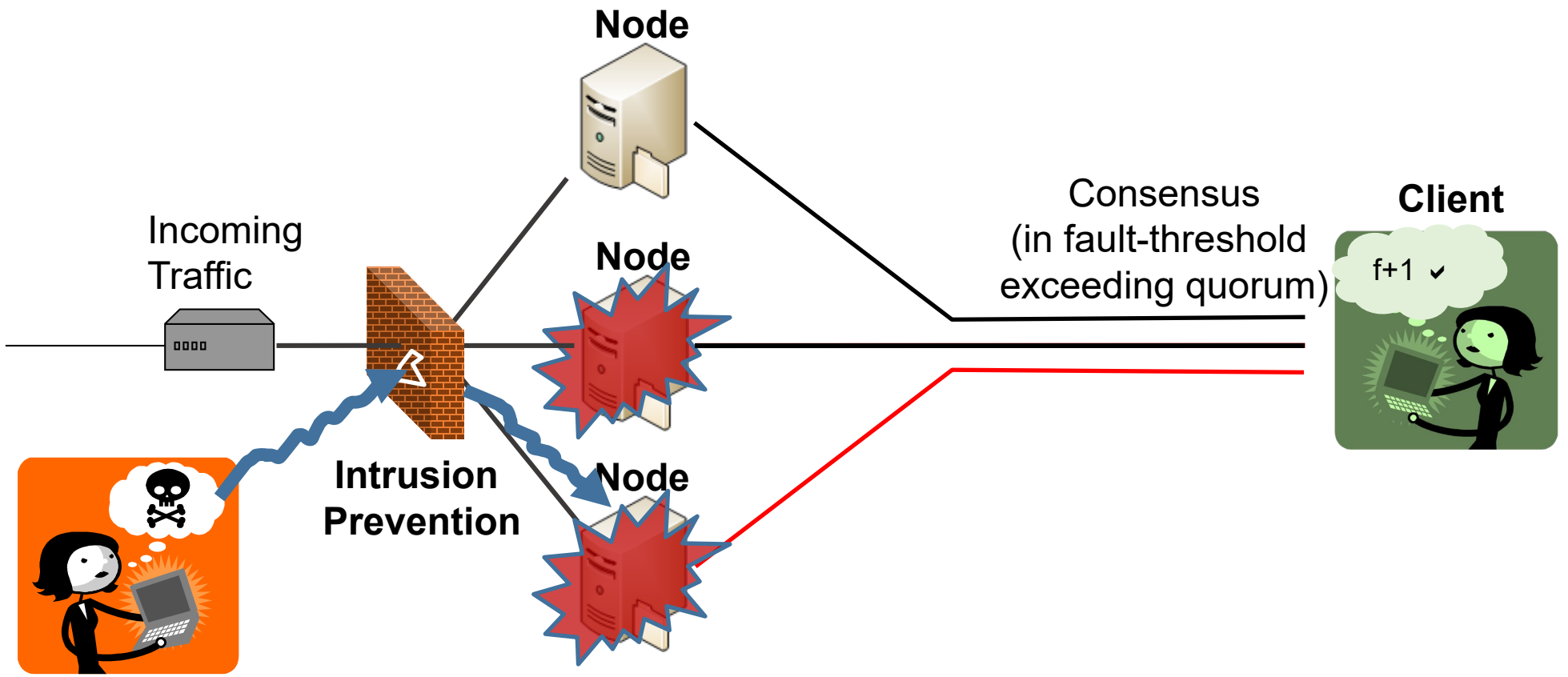
# Fault and Intrusion Tolerance

P. Sousa et al. – Exhaustion Failure



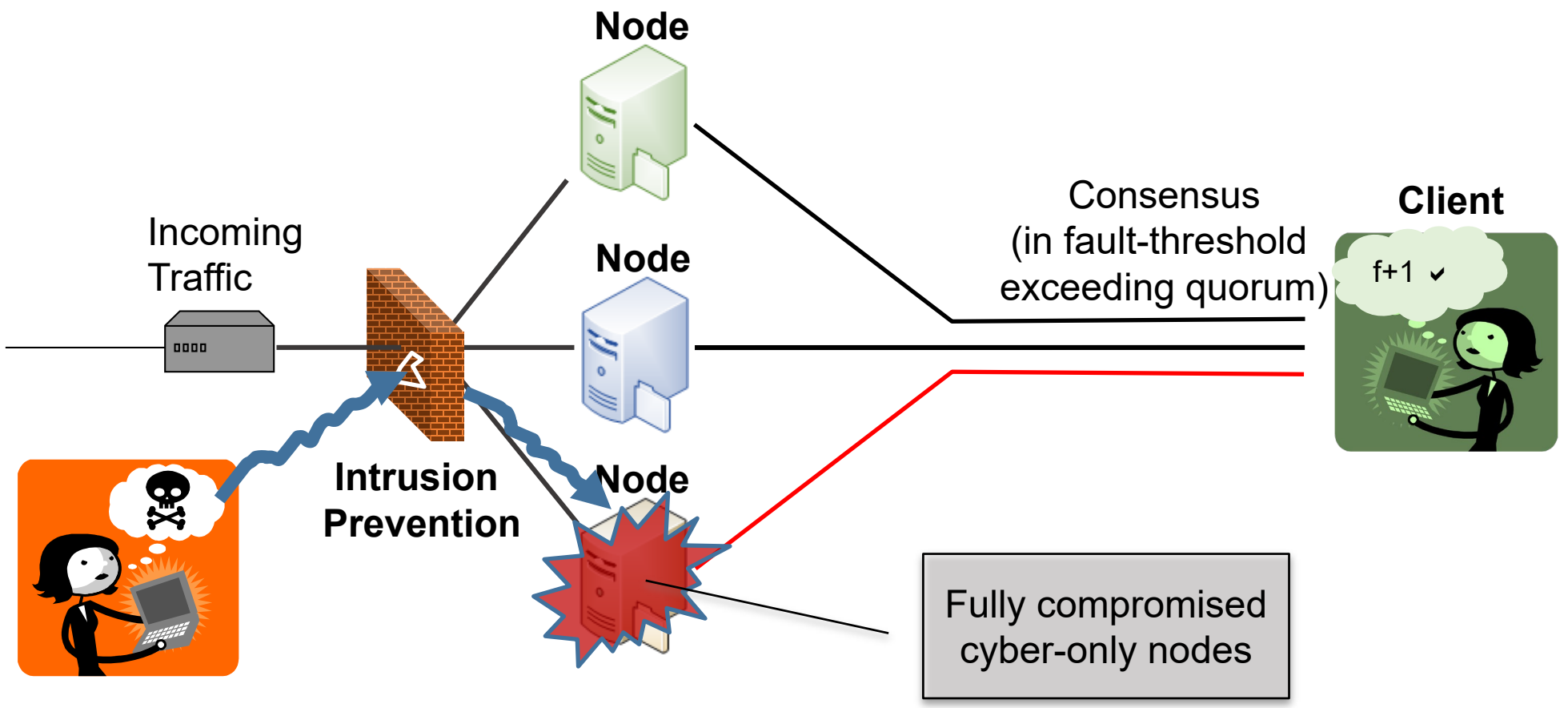
# Fault and Intrusion Tolerance

P. Sousa et al. – Exhaustion Failure



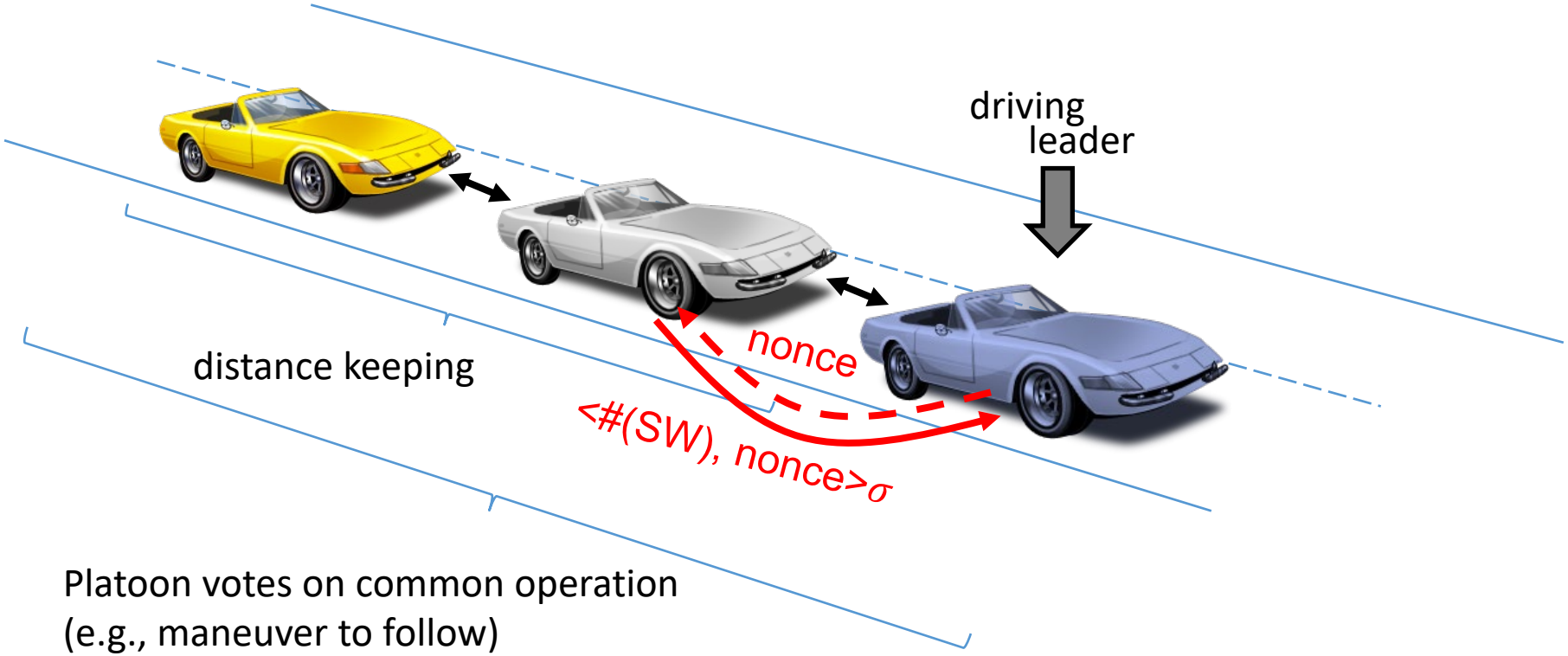
# Fault and Intrusion Tolerance

P. Sousa et al. – Exhaustion Failure



# Full compromise of swarm individuals is intolerable

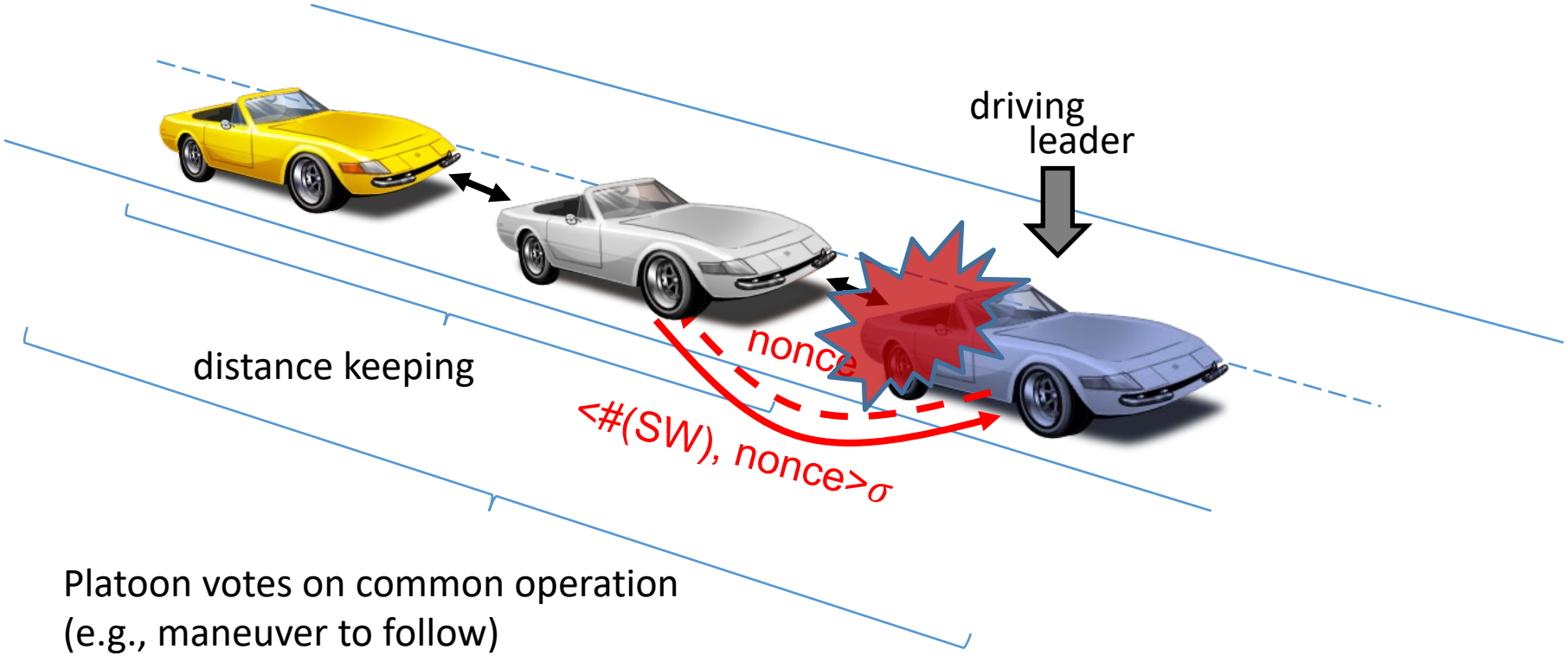
- Platoon of Cars




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

# Full compromise of swarm individuals is intolerable

- Platoon of Cars

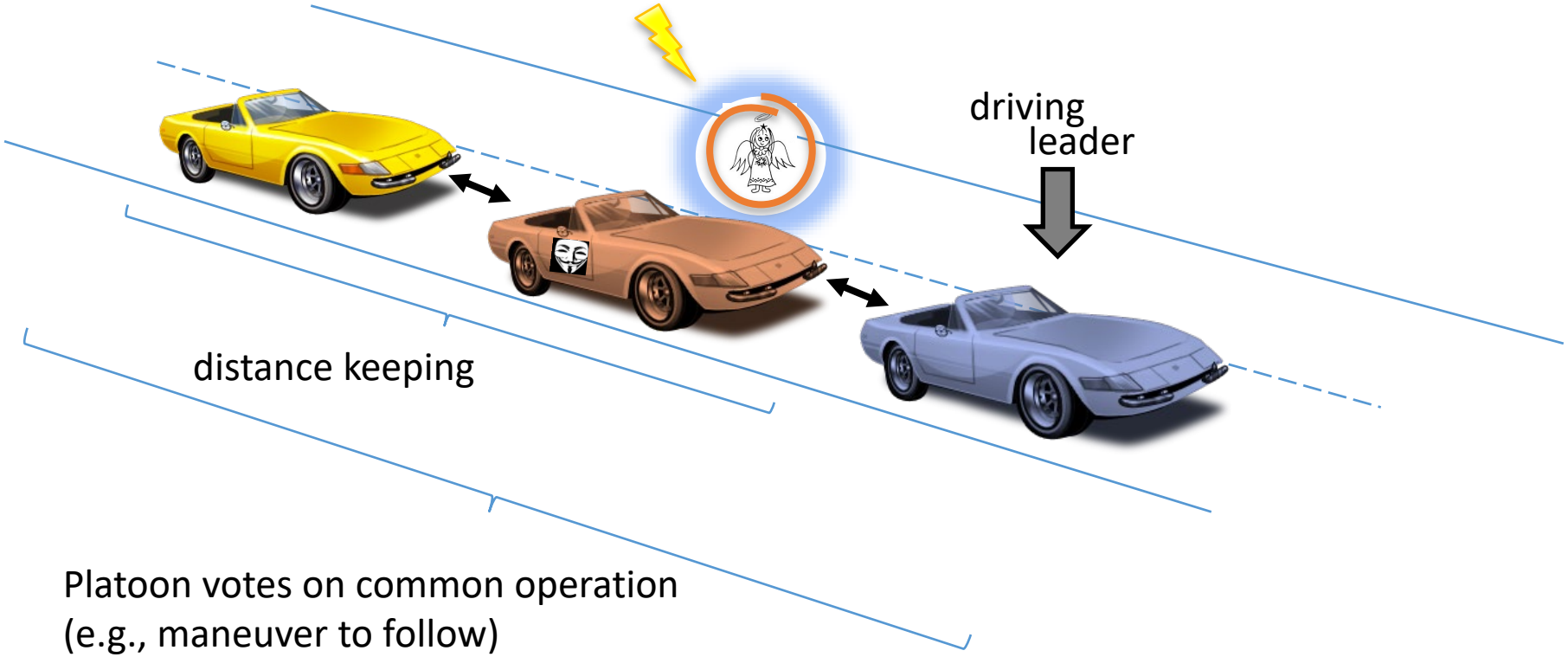



Platoon votes on common operation
(e.g., maneuver to follow)

# Full compromise of swarm individuals is intolerable

# Towards Sustainable Safety and Security

- Safeguard safety through trusted trustworthy components

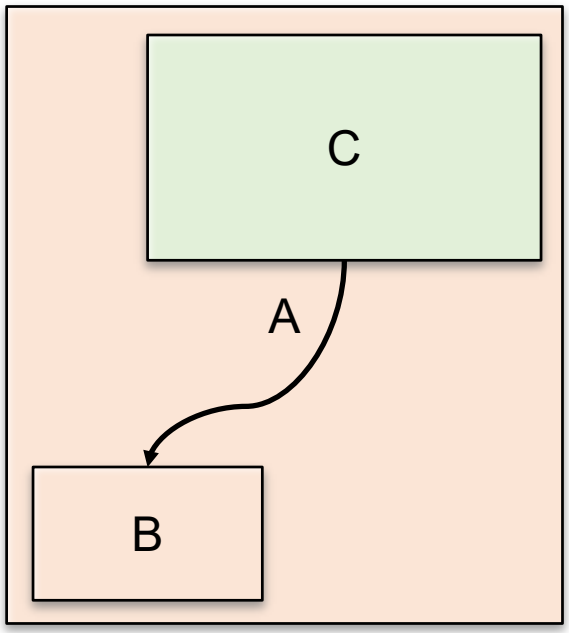



Platoon votes on common operation
(e.g., maneuver to follow)

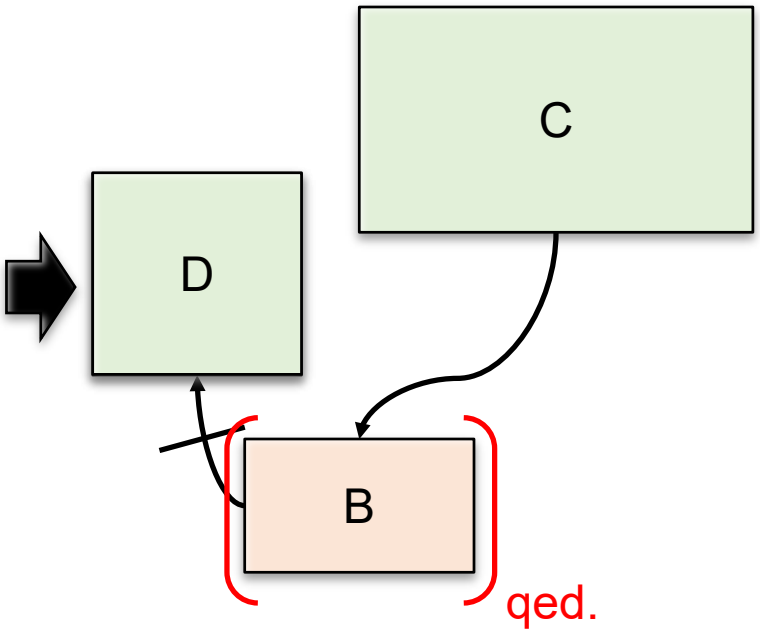
# Towards Sustainable Safety and Security

- Known Strategies for TCB Reduction

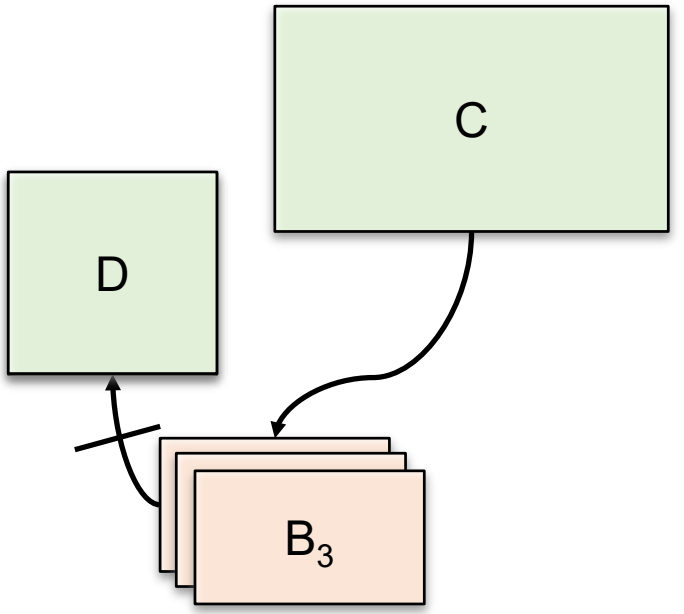
split applications: trusted / untrusted




reuse untrusted



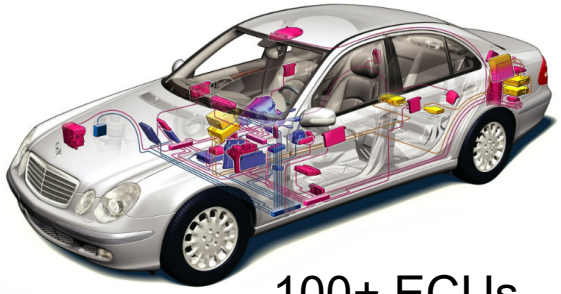

replication (trust majority; not individual)



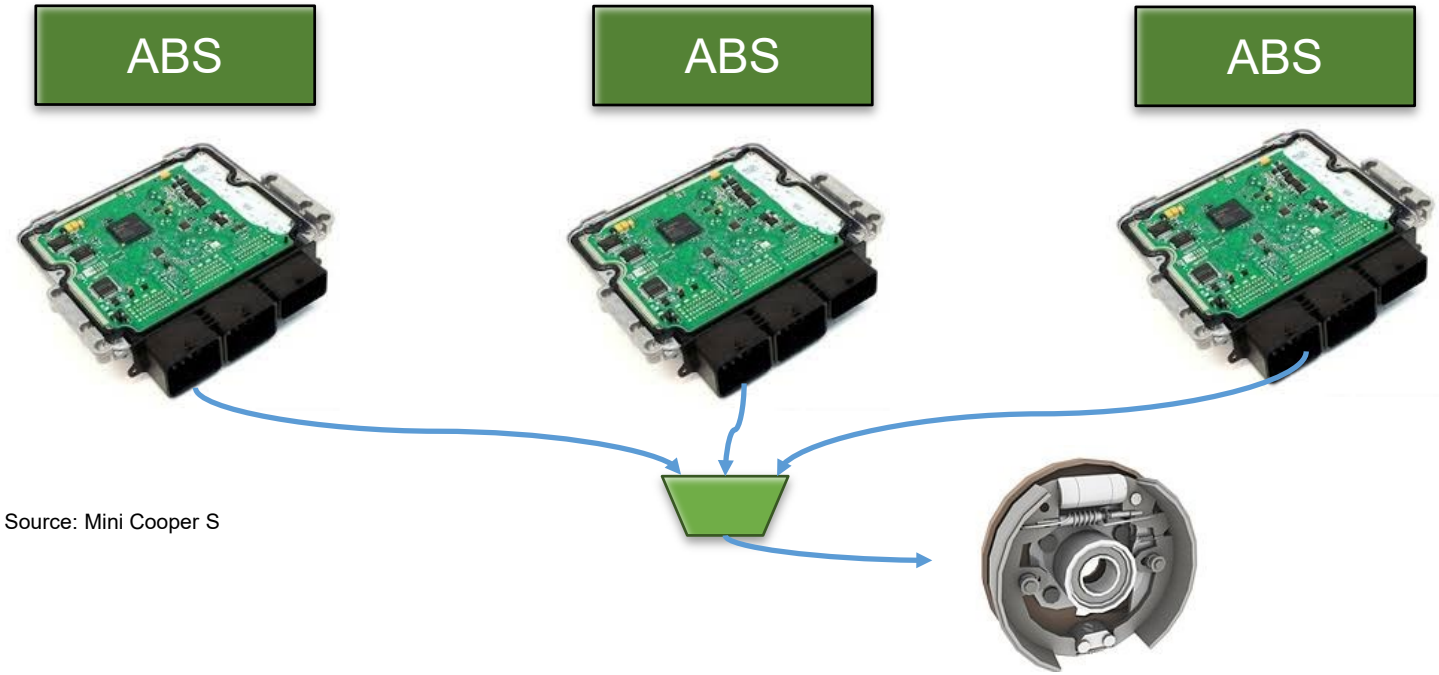

e.g., C. Weinhold: JVPFS
(also Inktag, SGX)

# Towards Sustainable Safety and Security

- Local Replication



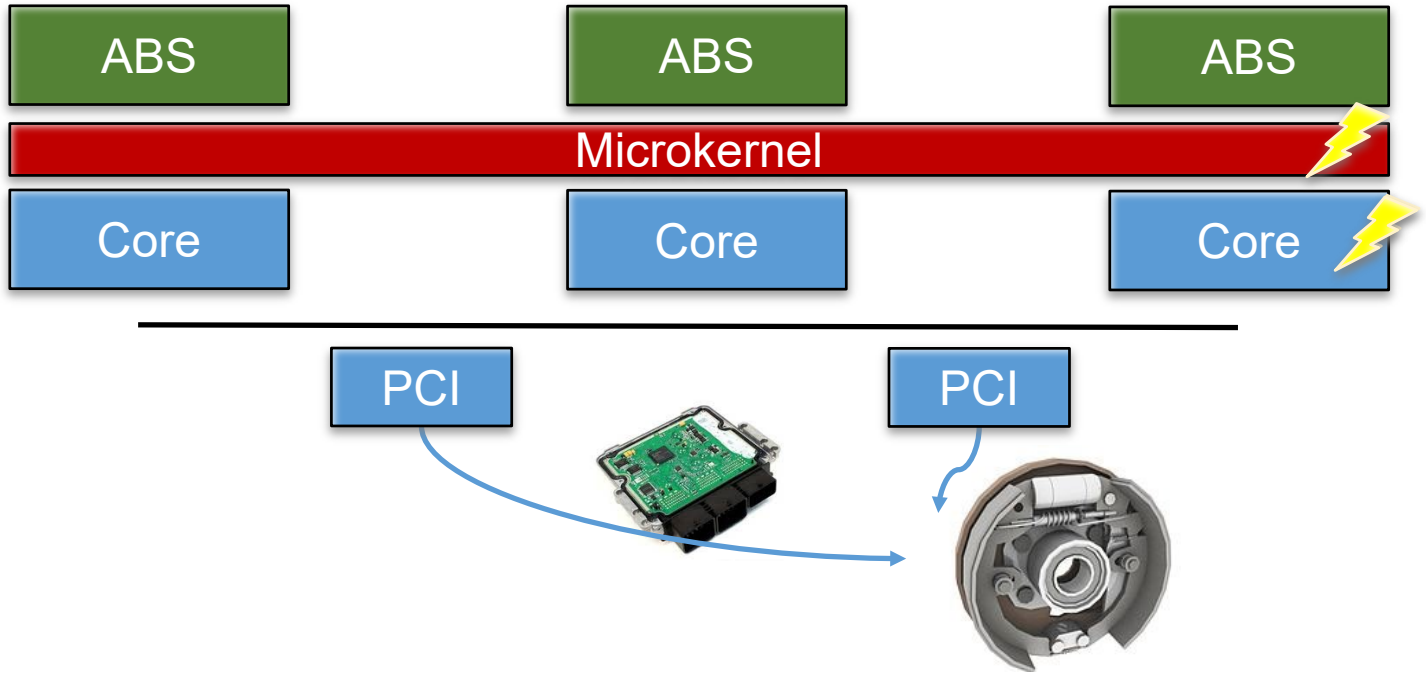
100+ ECUs

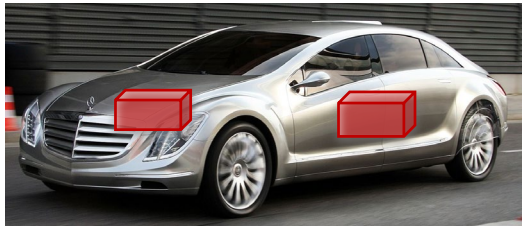



Source: Mini Cooper S

# Towards Sustainable Safety and Security

- Local Replication

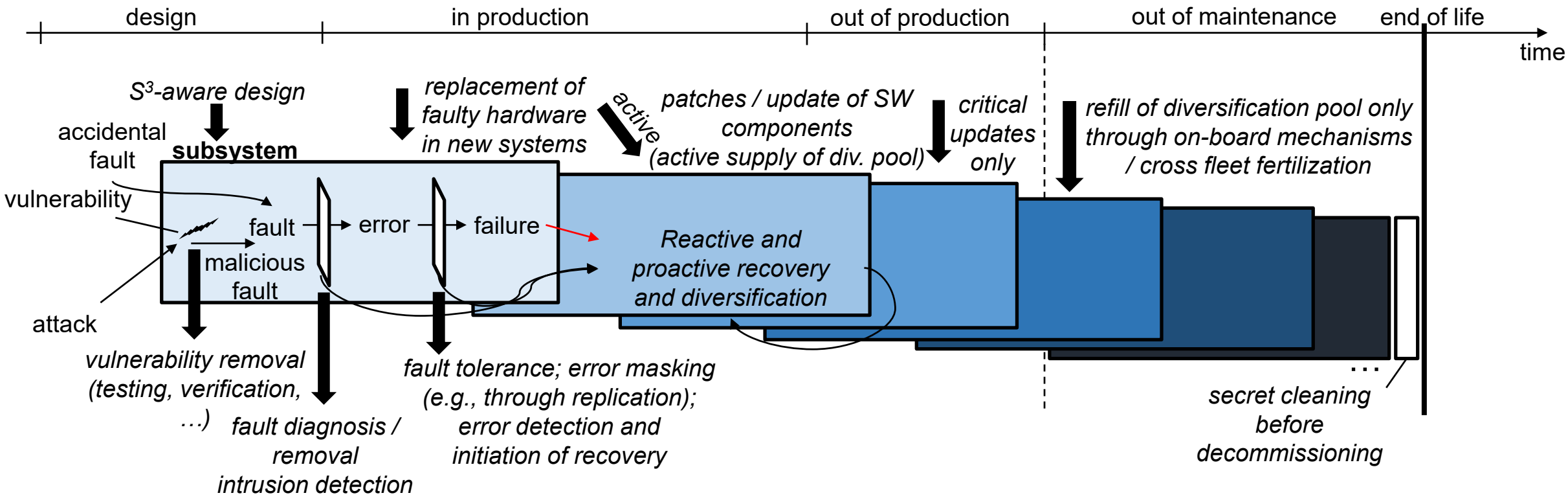


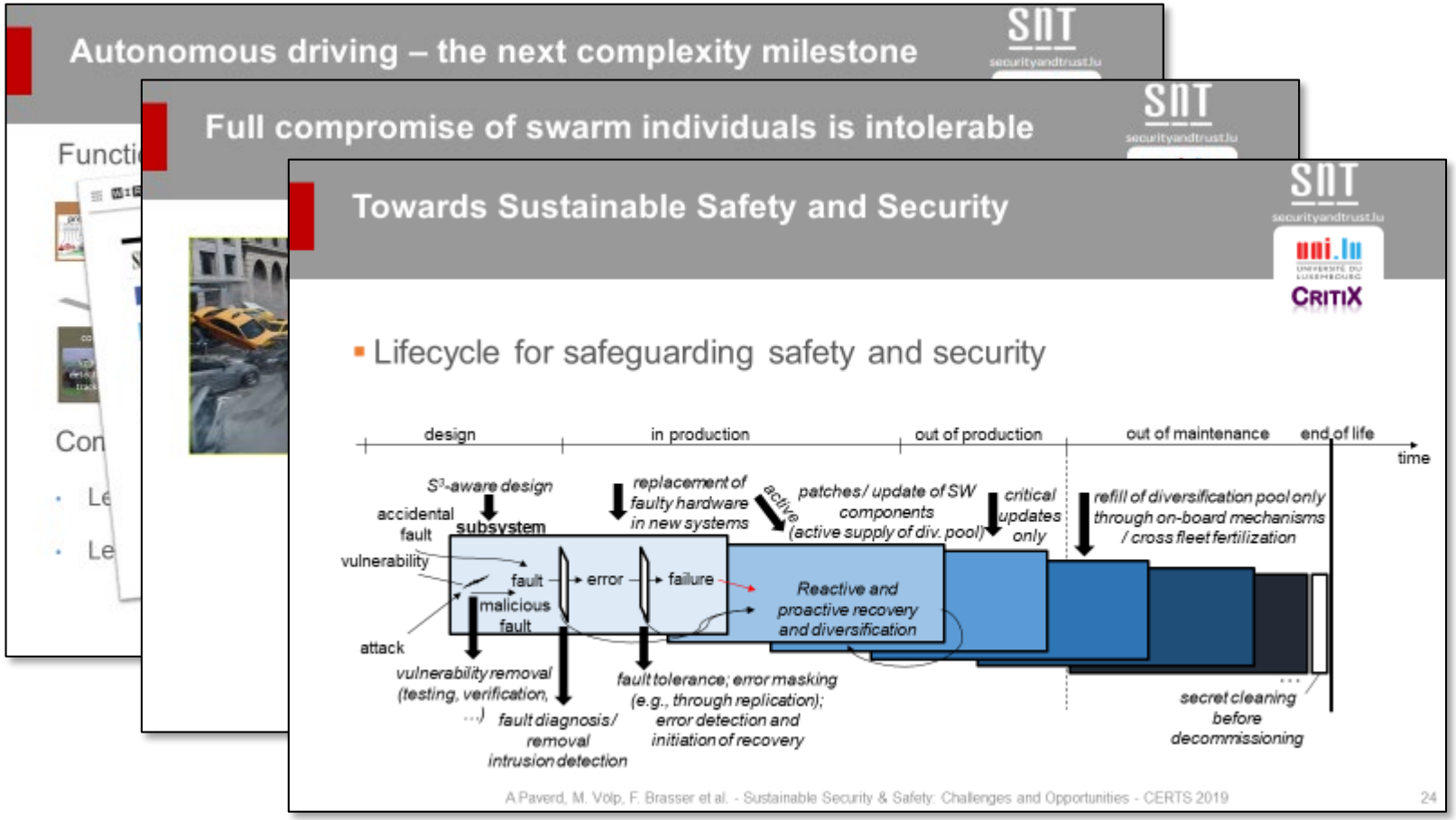
https://en.wikipedia.org/wiki/Mercedes-Benz_F700#/media/File:Mercedes-Benz_F700_amk.jpg

# Towards Sustainable Safety and Security

- Lifecycle for safeguarding safety and security



# This Talk in one Slide




*We are hiring bright PhD students and postdocs!*