

University of Luxembourg

SnT - CritiX

Towards sustainable safety and security in autonomous vehicles

Marcus Völp

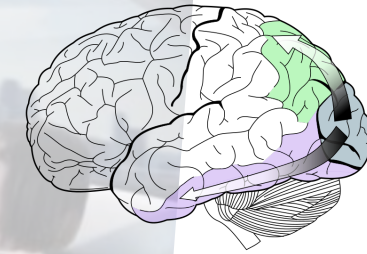
marcus.voelp@uni.lu

Autonomous driving – the next complexity milestone

Acceptance and Reputation

1957
Level 4 autonomy => Level 5

Brain areas involved in human visual perception



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

Recognition not only of regular traffic



Source: Autobild

Implicit Communication



ELECTRICITY MAY BE THE DRIVER. One day your car may speed along an electric super-highway, its speed and steering automatically controlled by electronic devices embedded in the road. Highways will be made safe — by electricity! No traffic jams . . . no collisions . . . no driver fatigue.

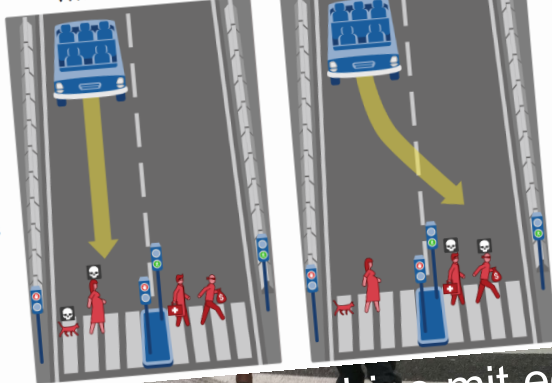
Source: <http://paleofuture.com/blog/2010/12/9/driverless-car-of-the-future-1957.html>

Self-driving Uber car hits, kills pedestrian in Arizona



Ethics

What should the self-driving car do?



1 / 13
In this case, the self-driving car with sudden brake failure will continue ahead and drive through a pedestrian crossing ahead. This will result in ...
Dead:
• 1 cat
• 1 pregnant woman
Note that the affected pedestrians are flouting the law by crossing on the red signal.

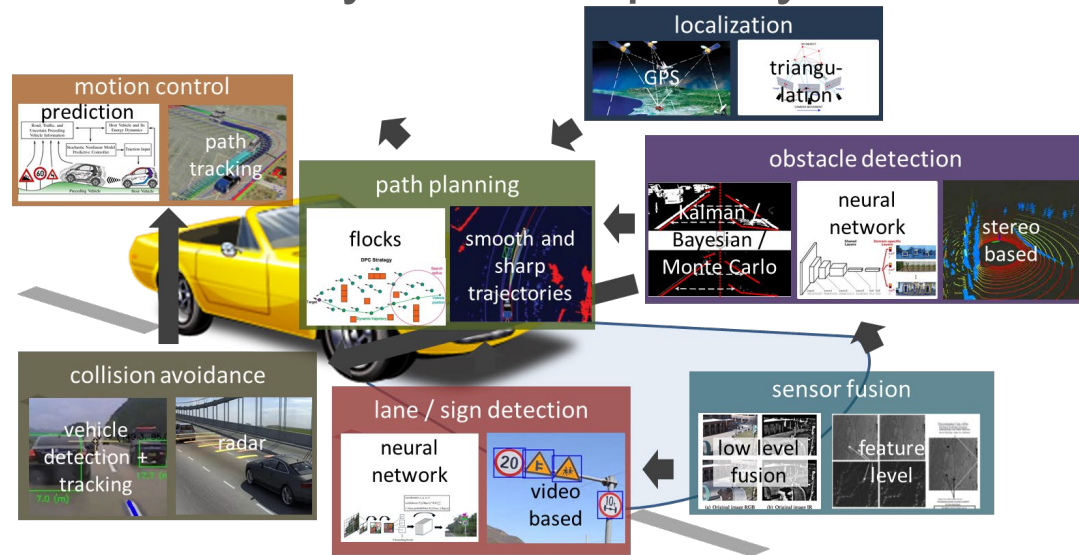
Note that the affected pedestrians are abiding by the law by crossing on the green signal.

<http://moralmachine.mit.edu/>



Autonomous driving – the next complexity milestone

Functionality vs. Complexity



- Components associated with physical control of the vehicle
- Components associated with safety
- Components associated with entertainment and convenience

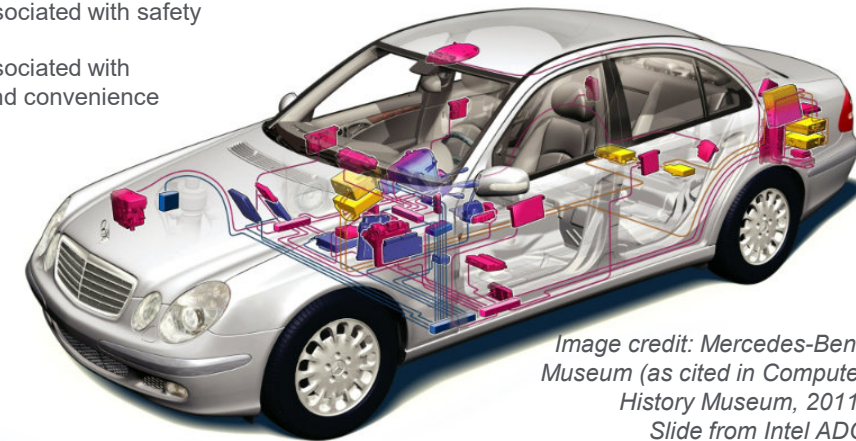


Image credit: Mercedes-Benz Museum (as cited in Computer History Museum, 2011) Slide from Intel ADG

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

Functionality vs. Complexity

WIRED

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

ANDY GREENBERG SECURITY 07.21.15 06:00 AM

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT

SHARE 208403

TWEET

COMMENT

EMAIL

through a port in its dashboard.

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

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/>

Current

• ~ 100

• ~ 100

processors

Autonomous driving – the next complexity milestone

Functionality vs. Complexity

Components associated with physical control of the vehicle

Safety Certification?

We need:

1. *fault and 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*

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

• ~ 100

• ~ 100



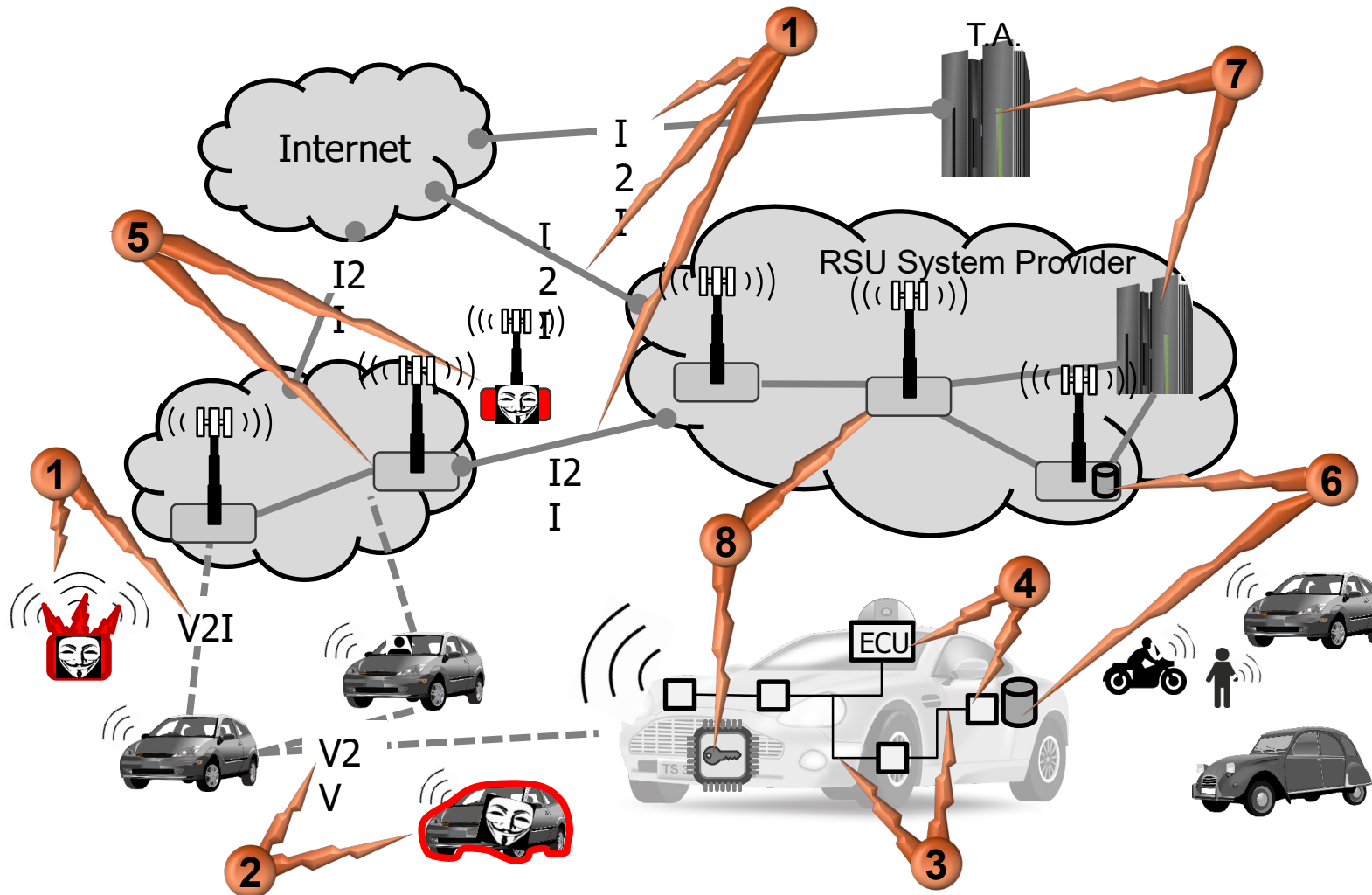
<https://arstechnica.com/cars/2017/07/gm-to-offer-ota-software-updates-before-2020-but-only-for-a-new-infotainment-platform/>

processors



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

Threat Vectors on autonomous and cooperative vehicle ecosystems



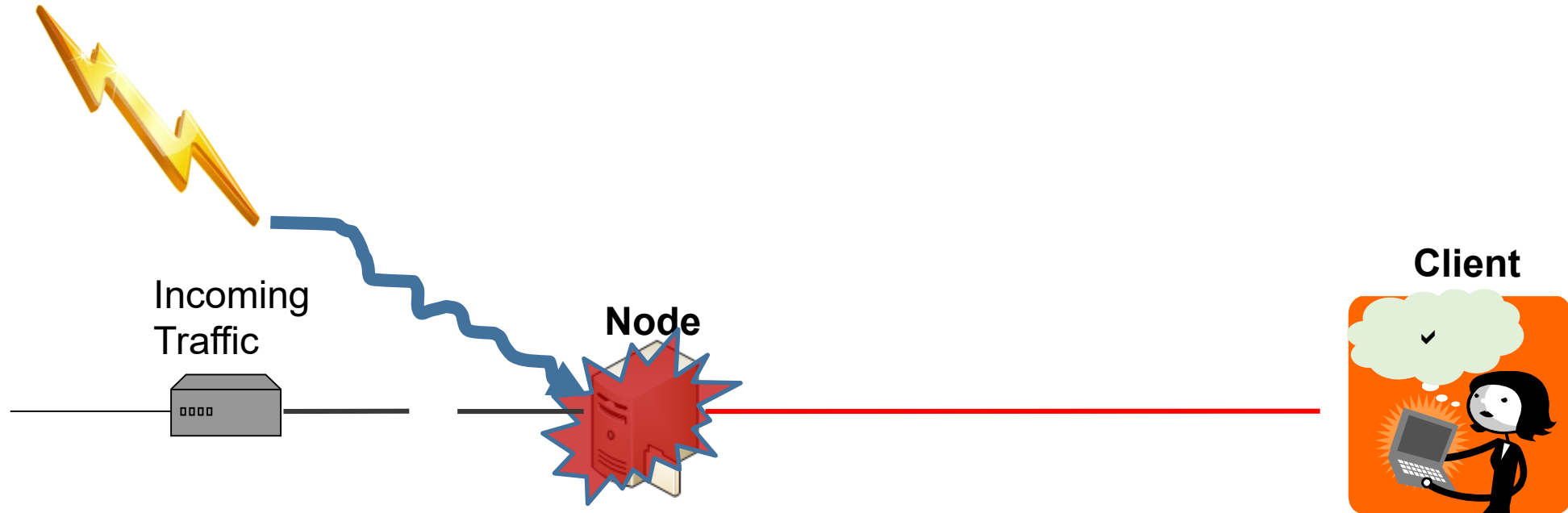
Threat Vectors:

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

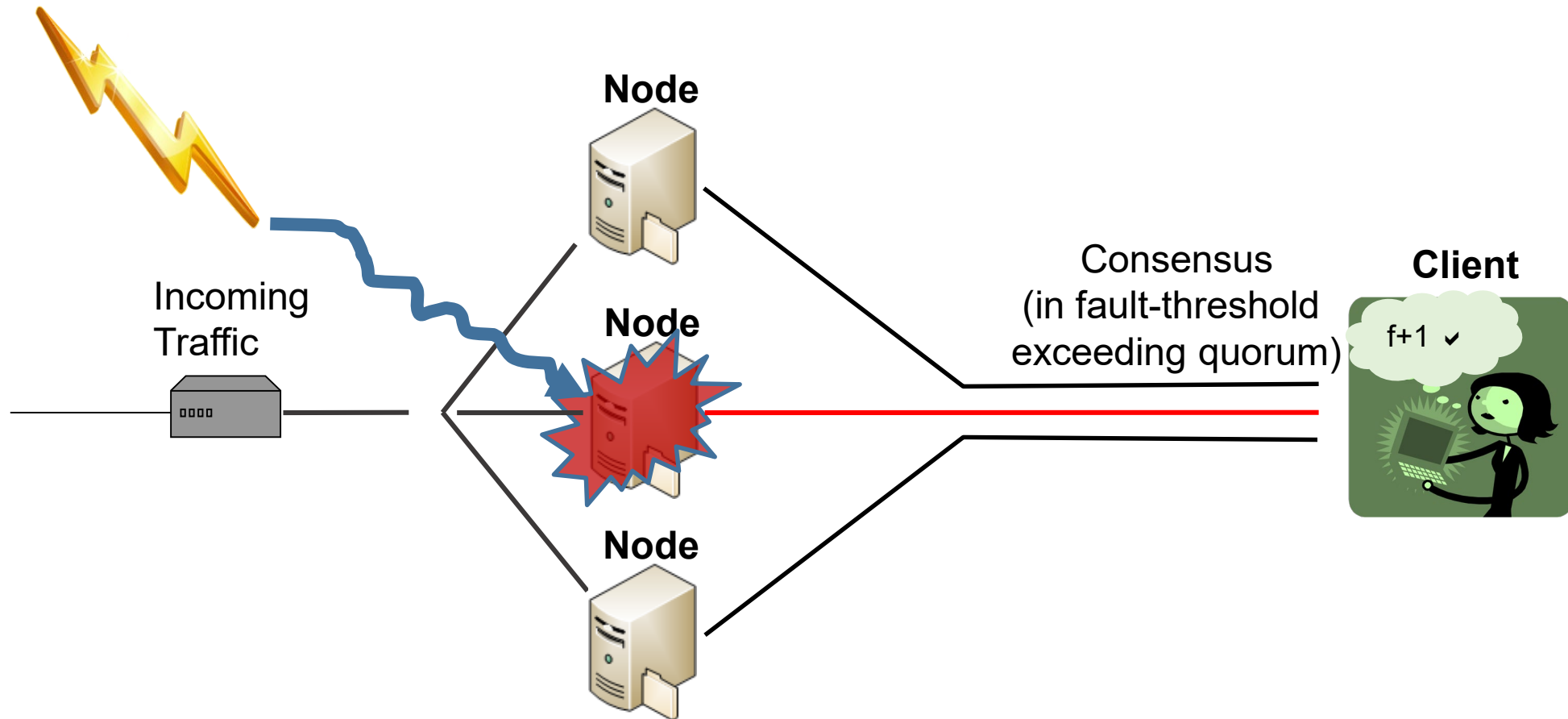
[Lima et al. "Towards Safe and Secure Autonomous and Cooperative Vehicle Ecosystems", CPS-SPC 2016]

- 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

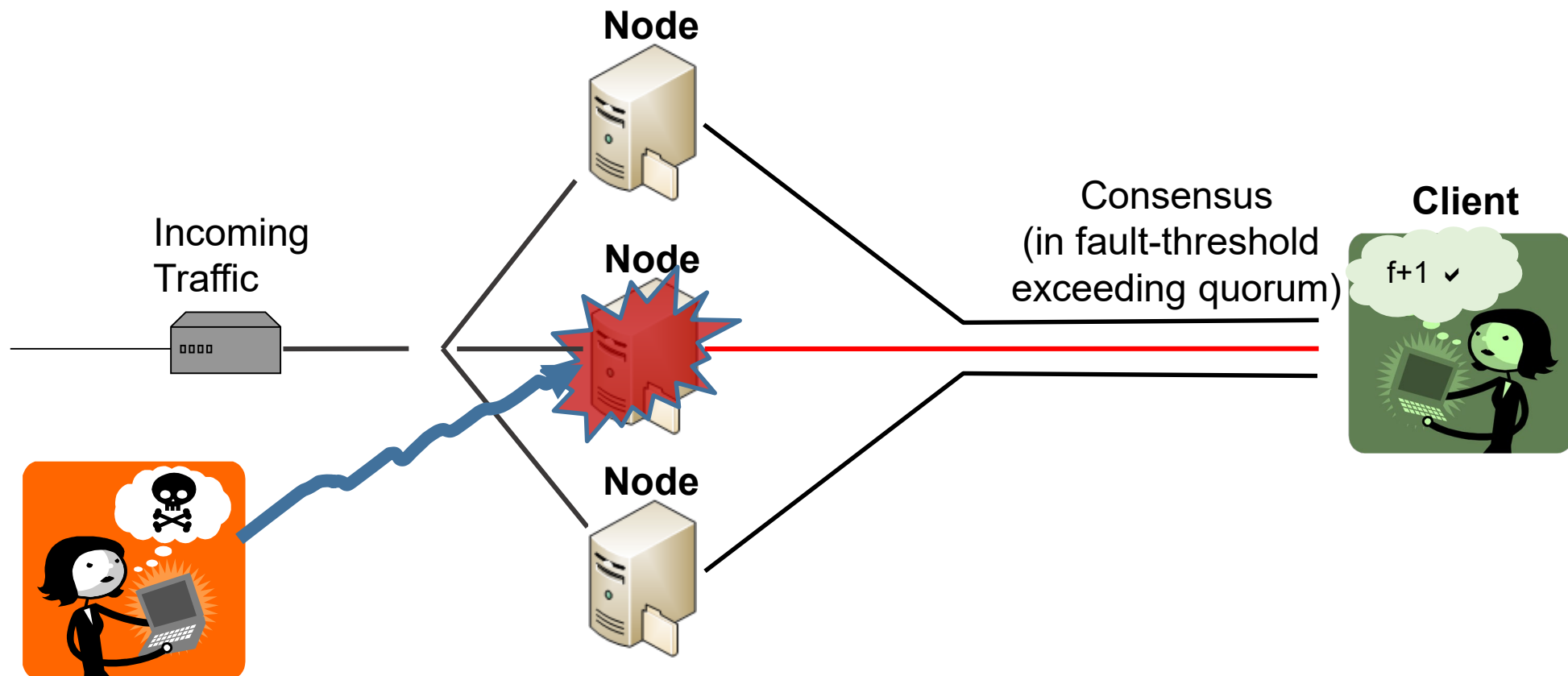
Fault and Intrusion Tolerance



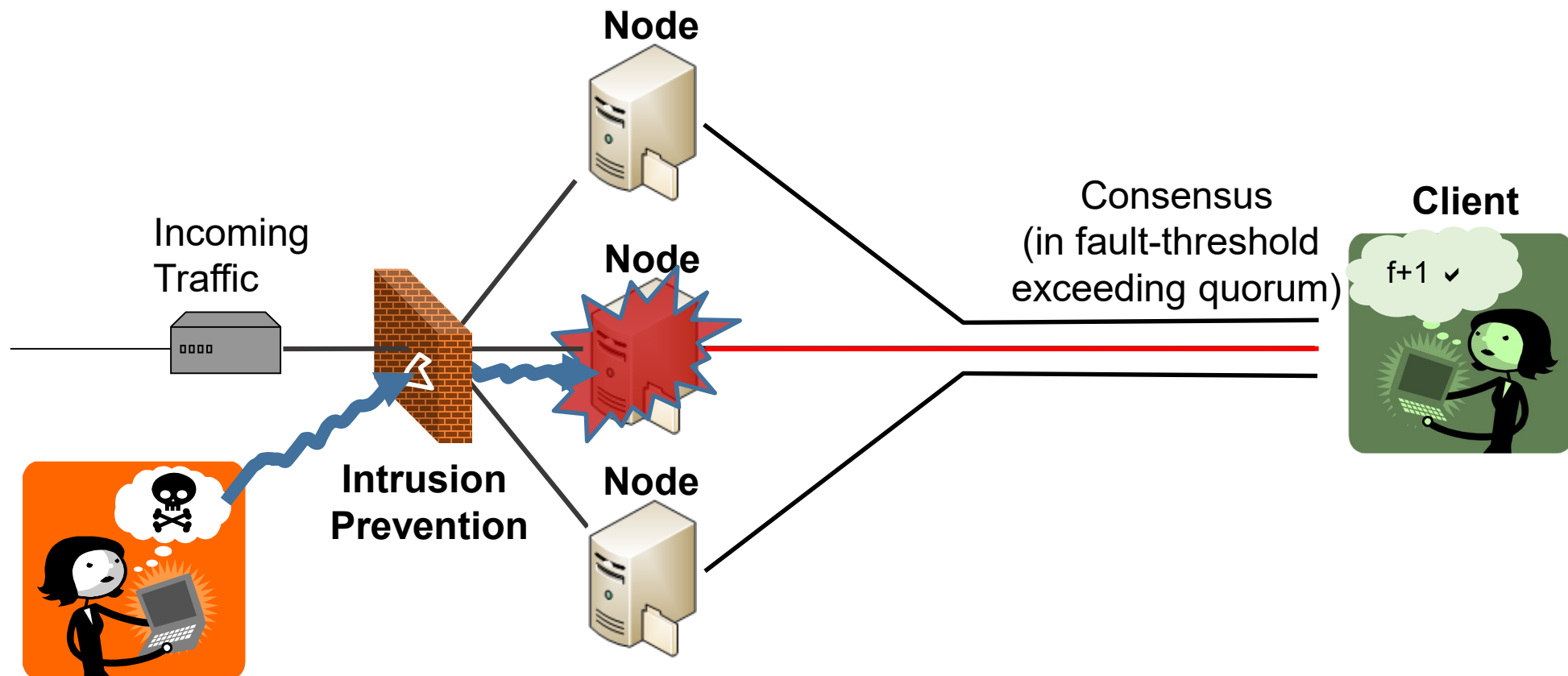
Fault and Intrusion Tolerance



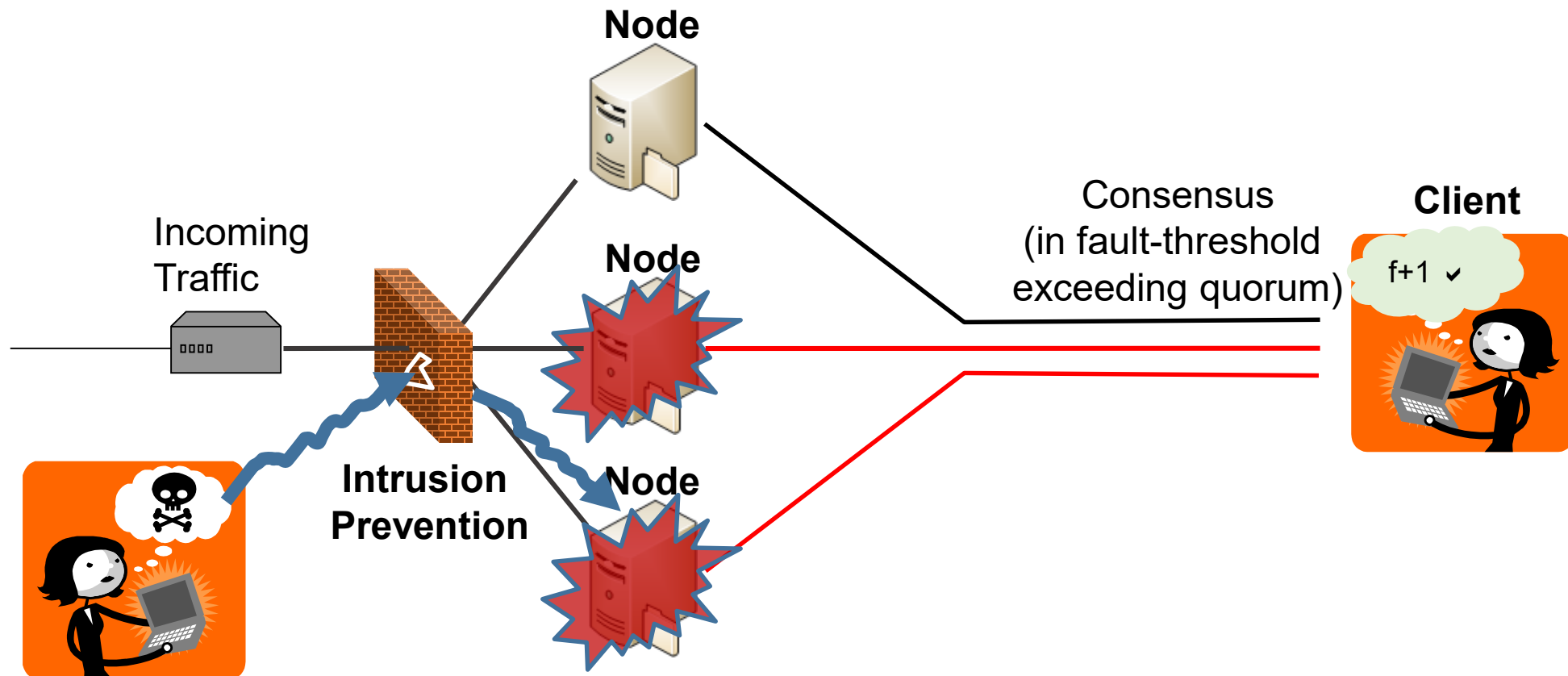
Fault and Intrusion Tolerance



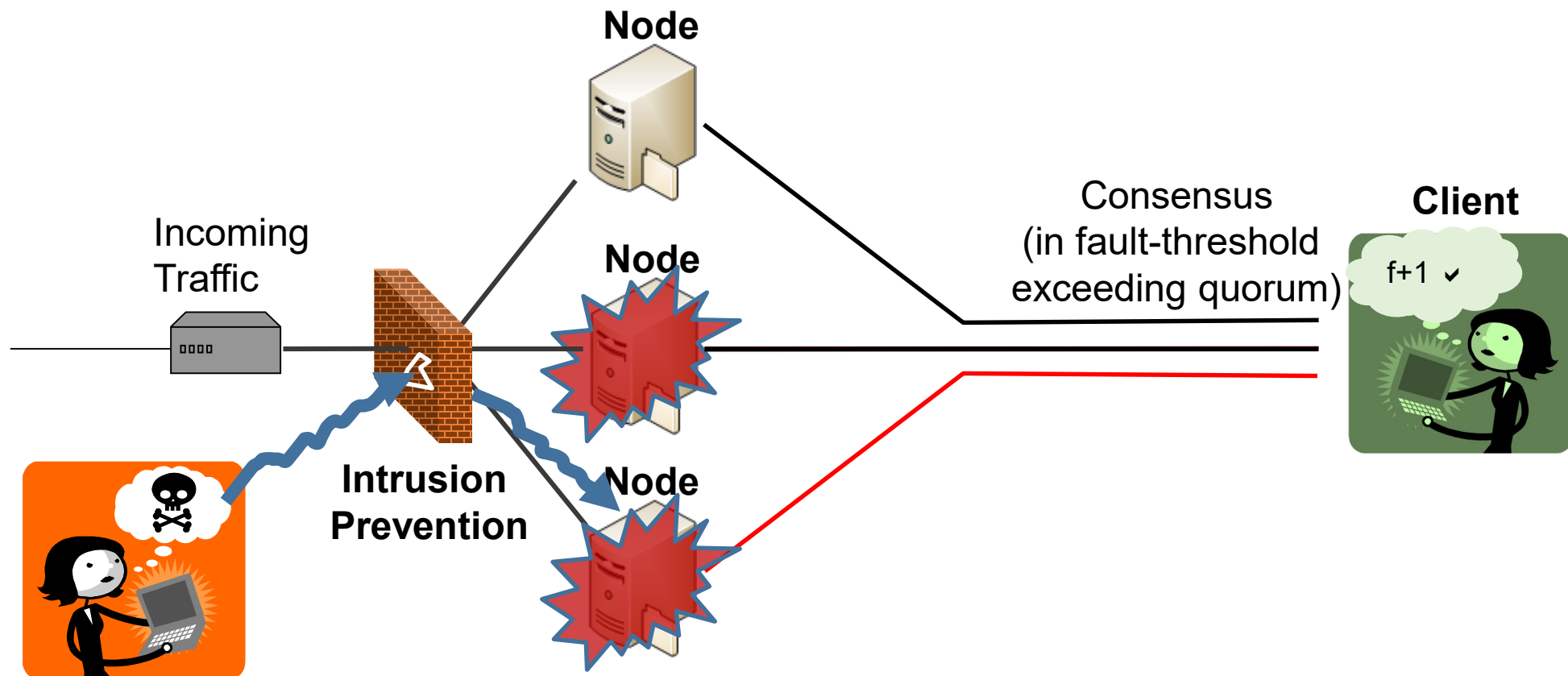
Fault and Intrusion Tolerance



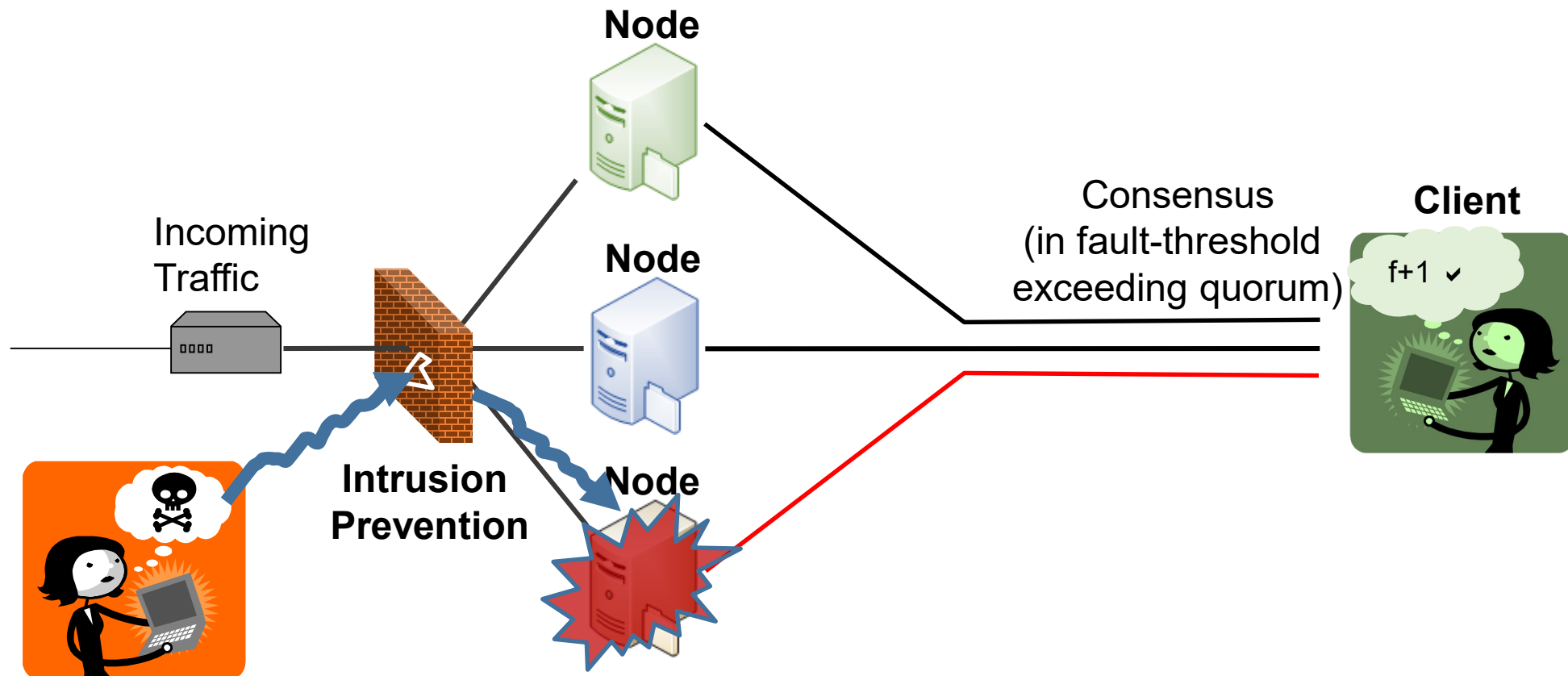
P. Sousa et al. – Exhaustion Failure



P. Sousa et al. – Exhaustion Failure

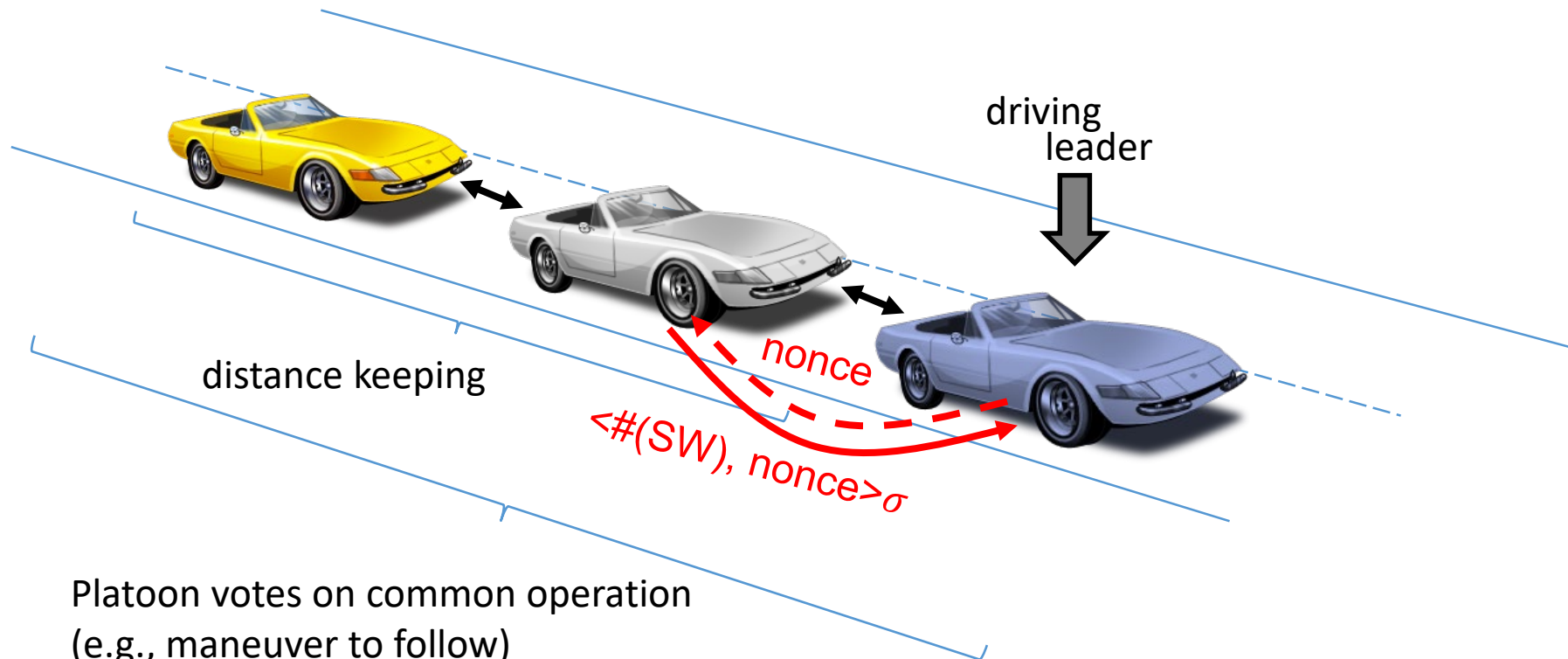


P. Sousa et al. – Exhaustion Failure



Full compromise of swarm individuals is intolerable

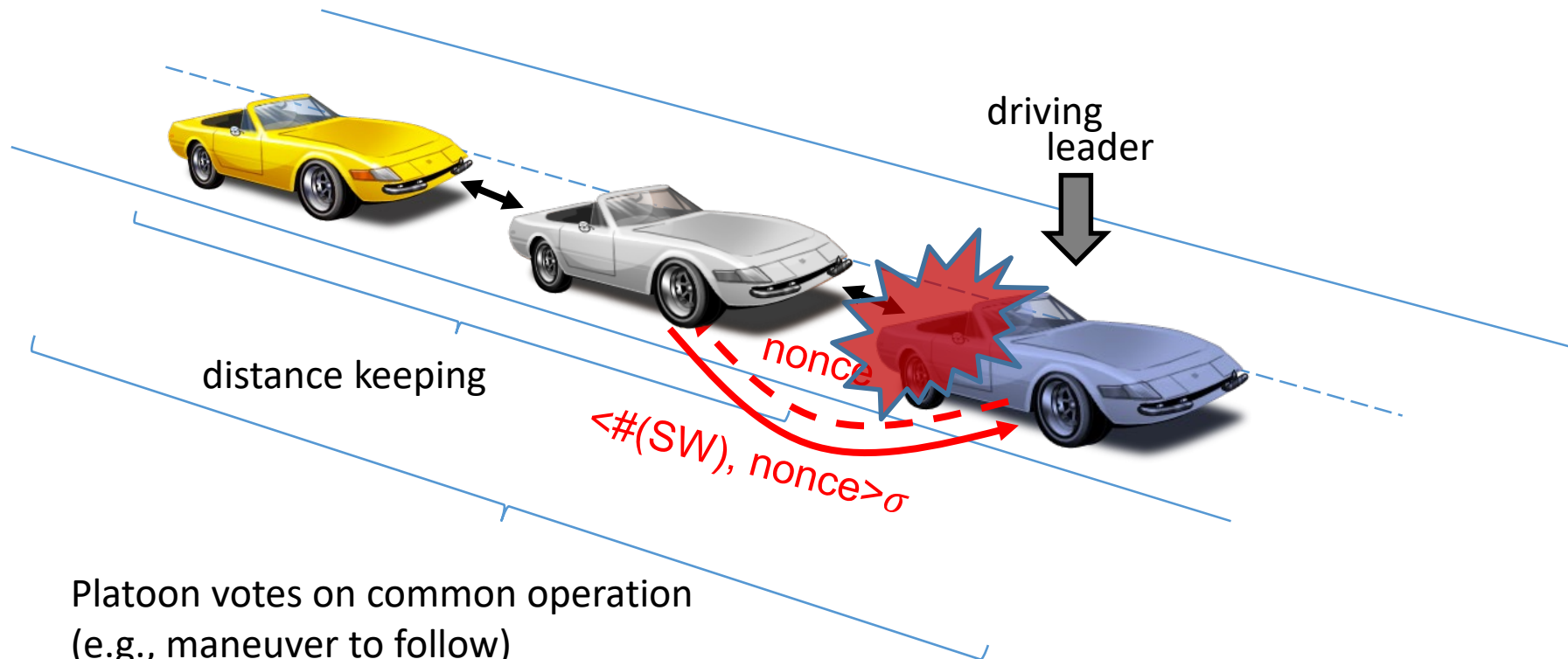
■ Platoon of Cars



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

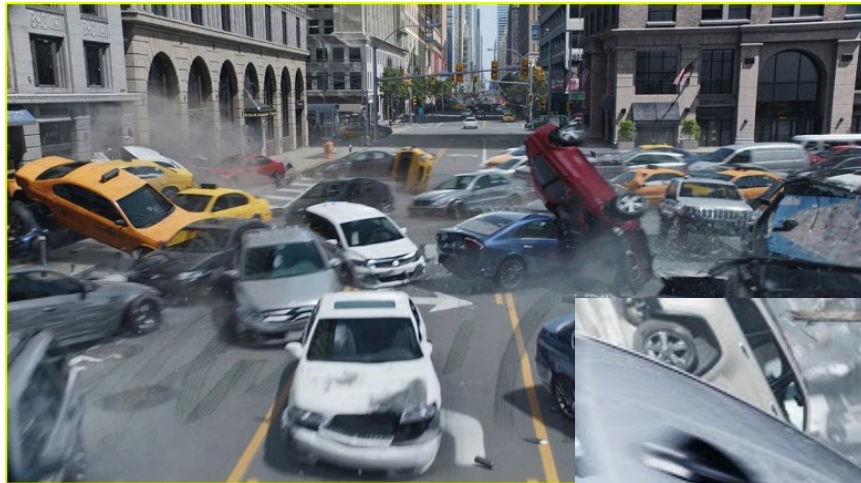
Full compromise of swarm individuals is intolerable

■ Platoon of Cars

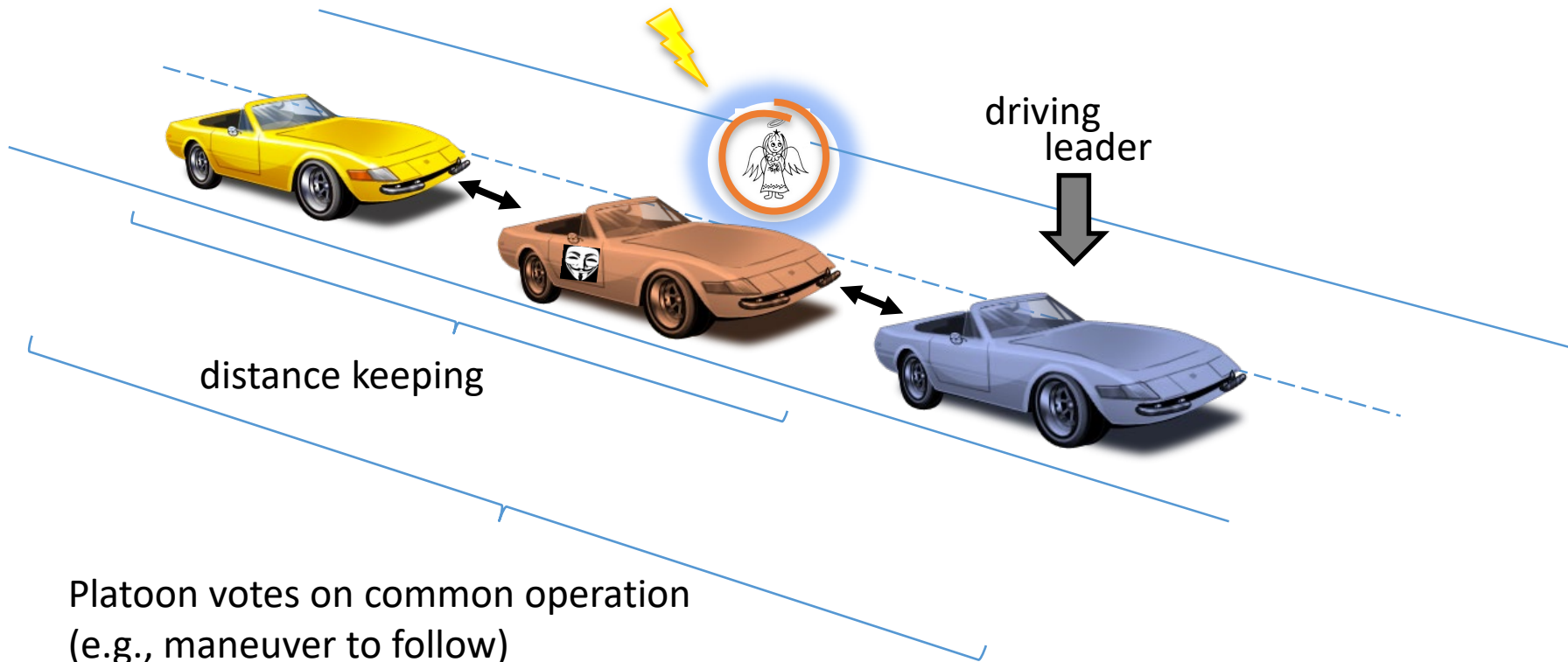


Platoon votes on common operation
(e.g., maneuver to follow)

Full compromise of swarm individuals is intolerable

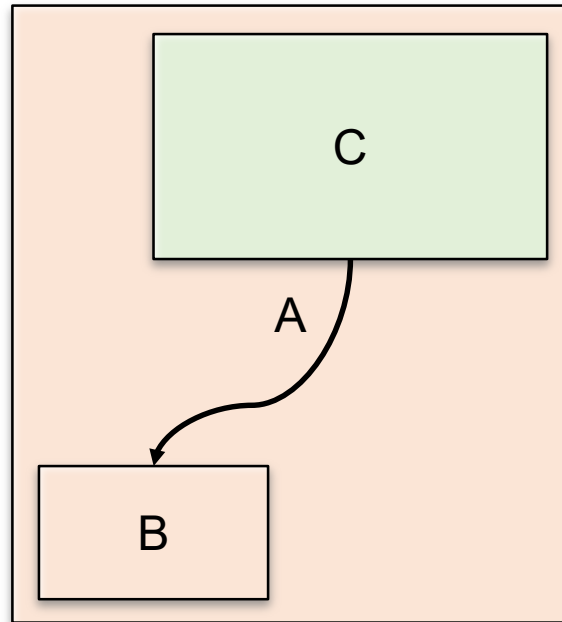


- Safeguard safety through trusted trustworthy components

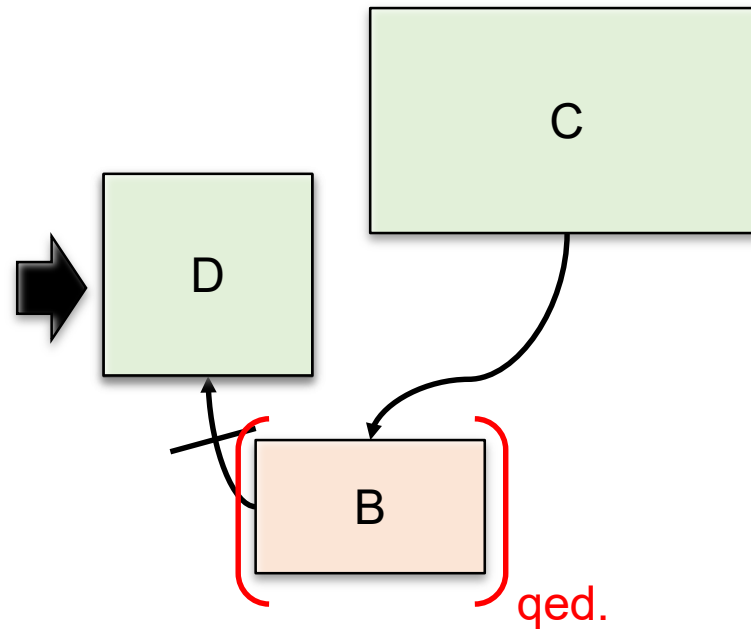


Known Strategies for TCB Reduction

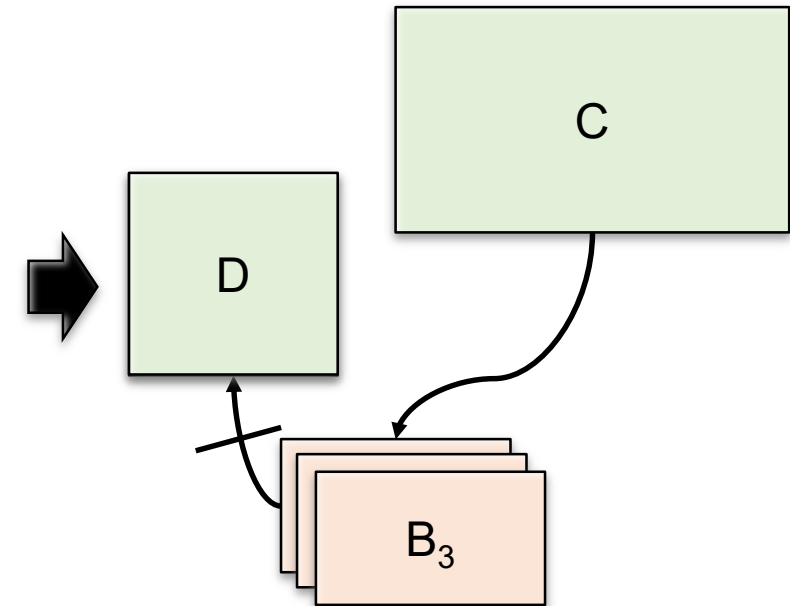
split applications: trusted / untrusted



reuse untrusted

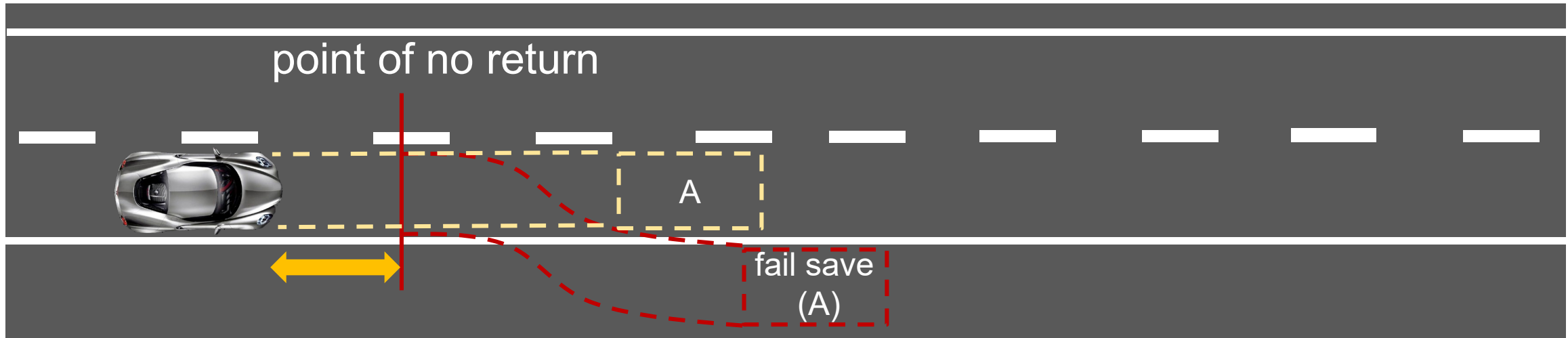


replication (trust majority; not individual)

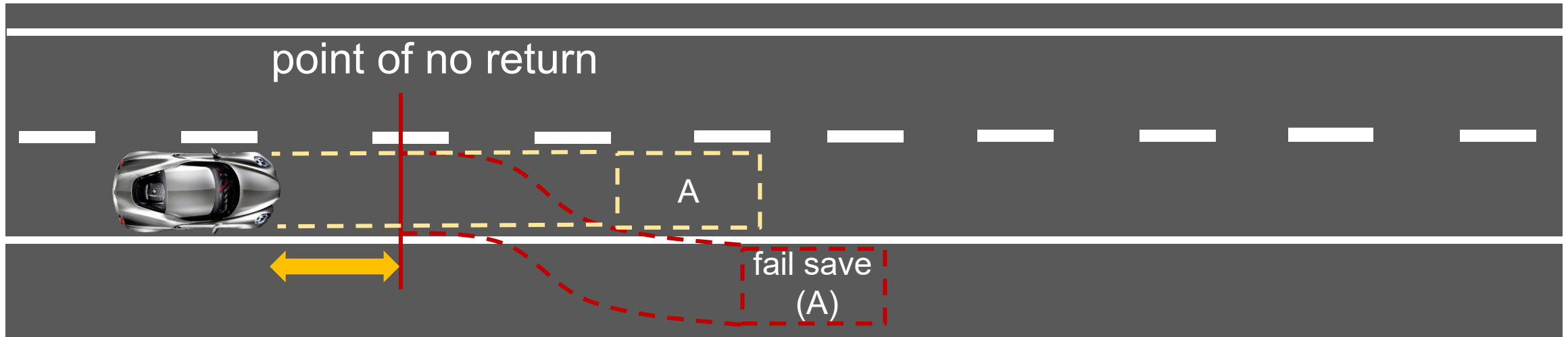


e.g., C. Weinhold: JVPFS
(also Inktag, SGX)

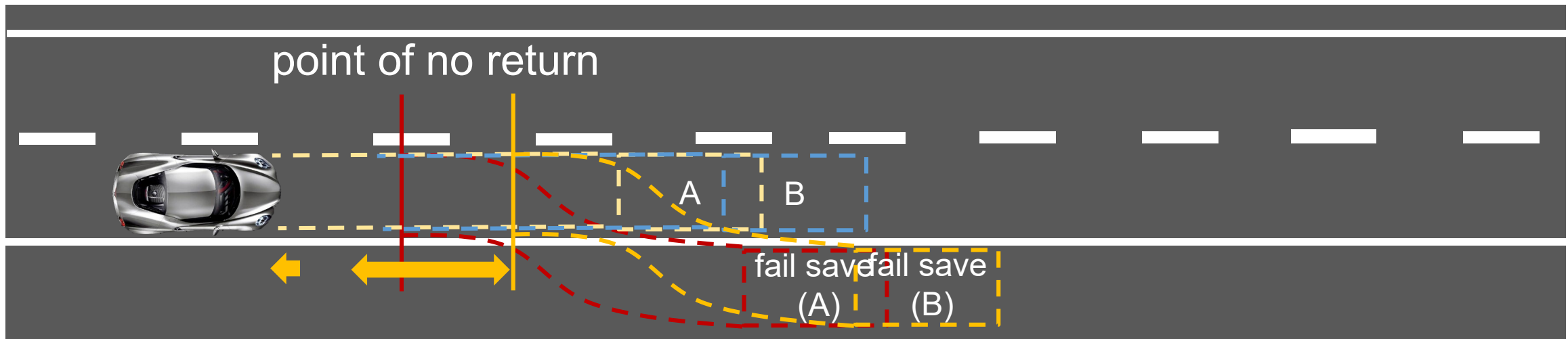
- Reusing potentially unavailable maneuver planning



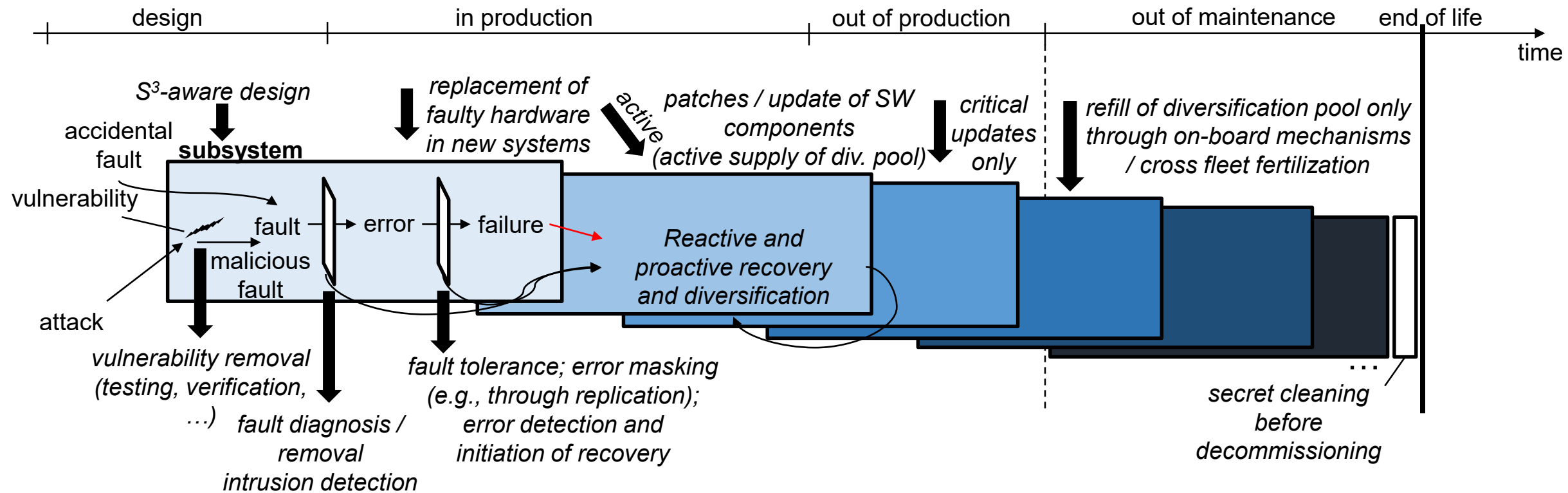
- Reusing potentially unavailable maneuver planning



- Reusing potentially unavailable maneuver planning



■ Lifecycle for safeguarding safety and security



Autonomous driving – the next complexity milestone

Full compromise of swarm individuals is intolerable

Towards Sustainable Safety and Security

Towards Sustainable Safety and Security

- Reusing
- Lifecycle for safeguarding safety and security

design | in production | out of production | out of maintenance | end of life | time

accidental fault, S³-aware design, vulnerability, malicious fault, attack, vulnerability removal (testing, verification, ...), fault diagnosis/removal, intrusion detection, subsystem, fault, error, failure, replacement of faulty hardware in new systems, active patches/ update of SW components (active supply of div. pool), critical updates only, Reactive and proactive recovery and diversification, refill of diversification pool only through on-board mechanisms / cross fleet fertilization, secret cleaning before decommissioning, fault tolerance; error masking (e.g., through replication); error detection and initiation of recovery

Marcus Völp - Towards sustainable safety and security in autonomous vehicles - 75th IFIP WG 10.4 on Dependable Computing and Fault Tolerance - 2019 23

We are hiring bright PhD students and postdocs!