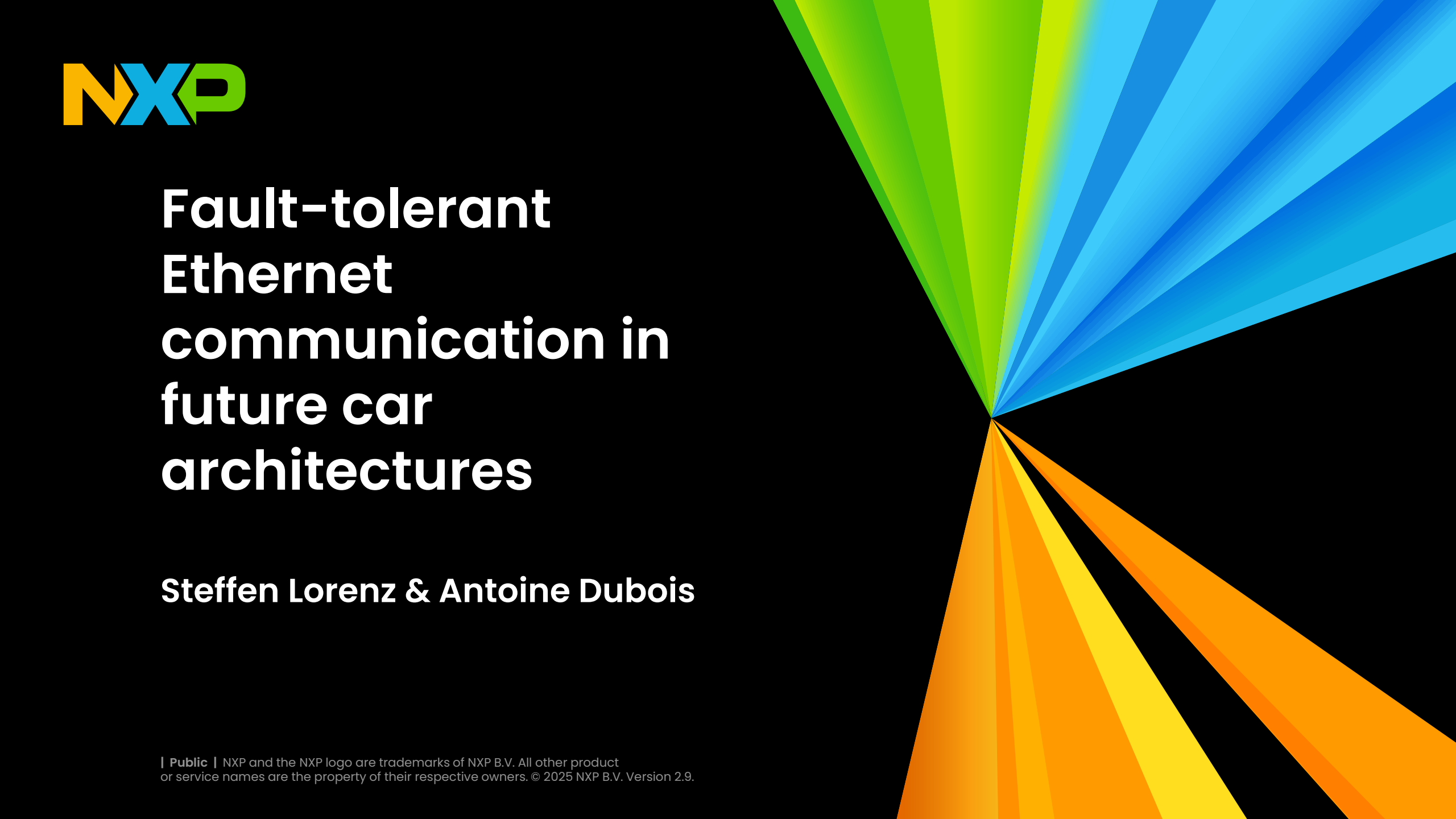


Fault-tolerant Ethernet communication in future car architectures

Steffen Lorenz & Antoine Dubois


TRAVEL AT
YOUR OWN RISK
BEYOND
POINT
Not for self-driving cars

Agenda

System context

Cascading faults

Fault containment regions

Conclusion

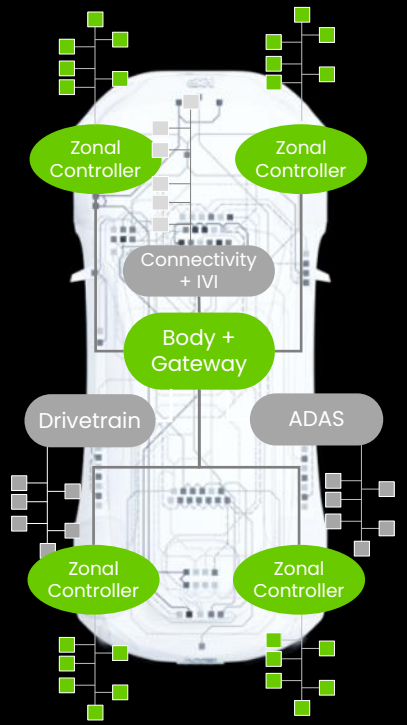
System context

Vehicle architectures go zonal & software defined

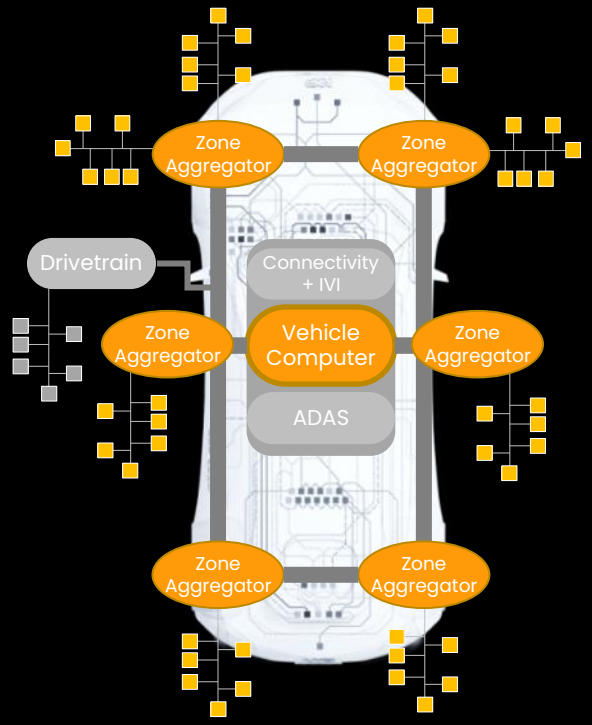
Distributed safety functions

Aggregated & mixed criticality data over Ethernet

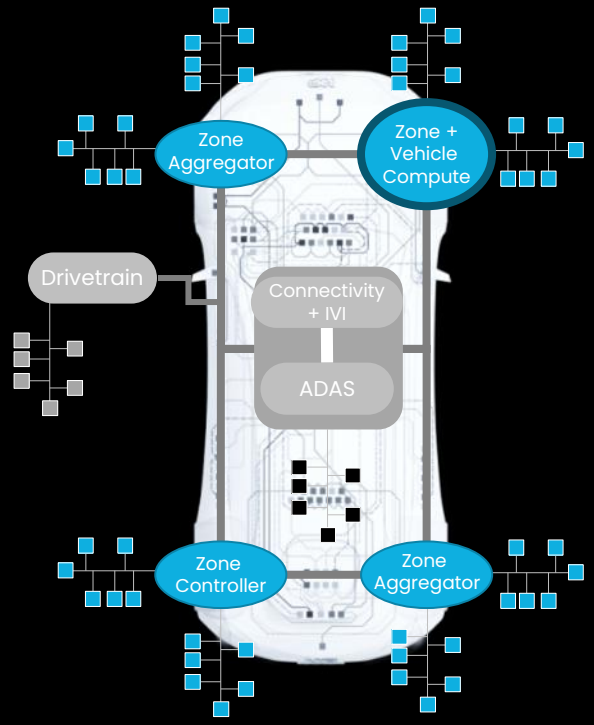
Used for L3+ autonomous driving



distributed compute



central compute



HP zonal compute

Availability requirement for (semi-)autonomous driving

- Fail-safe operation is not sufficient anymore

- In case of faults, the car must continue to securely operate until
  a) the driver is able to take-over control or
  b) the car is stopped in a controlled way

- Requires the system to be fail-operational
  - at least for a certain time to allow for Minimum Risk Maneuver
  - potentially with a certain degraded set of functions

- Requires the network to be fault-tolerant
  -ability to deliver a specified functionality in the presence of specified faults

Availability

Prevent loss of function!

Faults

- **Systematic fault**

Fault whose failure is manifested in a deterministic way that can only be prevented by applying process or design measures

- **Random HW fault (RHF)**

Hardware fault with a probabilistic distribution; can occur unpredictably during lifetime

Fault-tolerant network

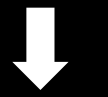
ISO26262-1:2018, 3.54:

fault

- *abnormal condition that can cause an element (3.41) or an item (3.84) to fail*
- *Note 1 to entry: Permanent, intermittent, and transient faults (3.173) (especially soft errors) are considered.*

Stays until removed or repaired resp. occurs from time to time.

Disappears autonomously or can be corrected.

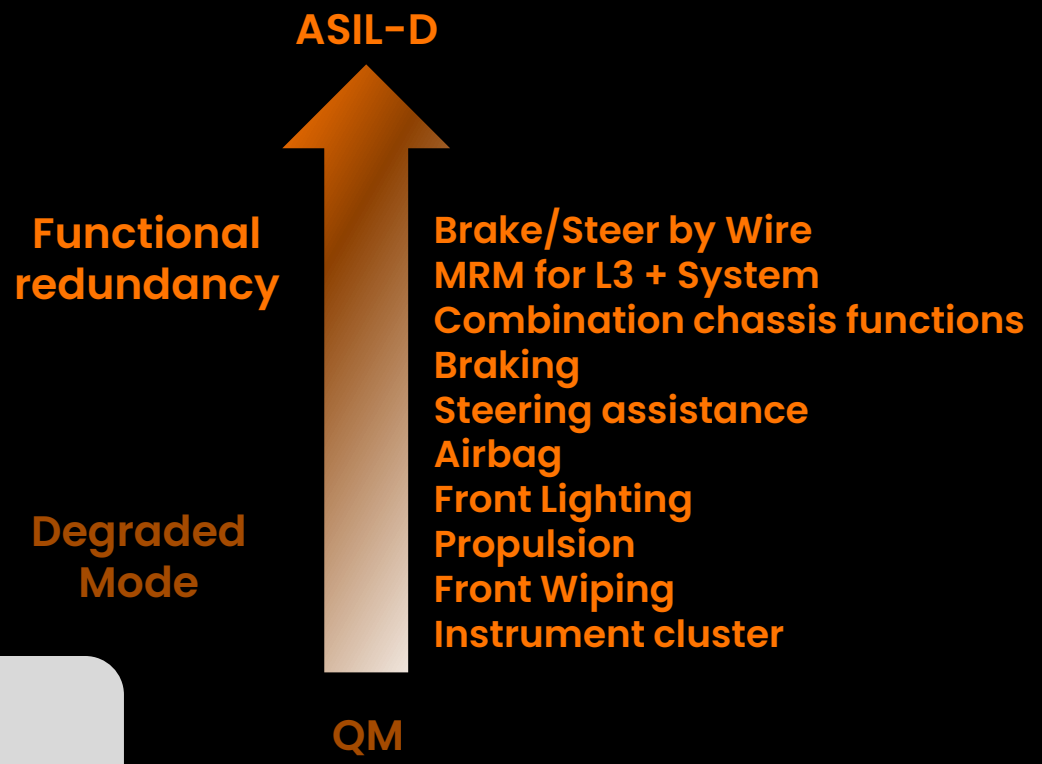


Needs to get mitigated

Should get recovered

Vehicle Function with Safety Availability

- Faults of shared resources
- Systematic capability
- Cascading failure



Prevent HW/SW Dependent failure

Faults of shared resources

Avoid SPF of shared HW resources leading to loss of Primary and secondary path. (ASIL-D)

SPFM >99%, PMHF <1FIT

Solutions:
HW redundancy

Systematic capability

Prevent loss of primary and secondary functions due to systematic failure (bugs).

Solutions:
- Decomposed ASIL-B(D)
- Systematic capability

Cascading Failure

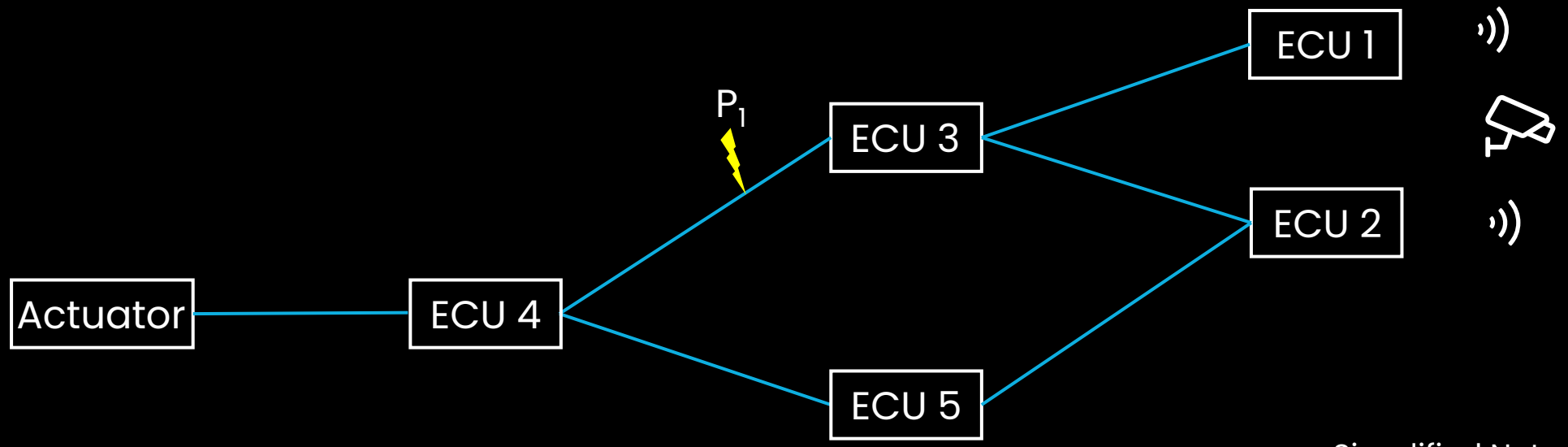
Prevent failure from one channel to impact functionality of another channel (ASIL-D)

Solutions:
Fault containment regions

Cascading faults

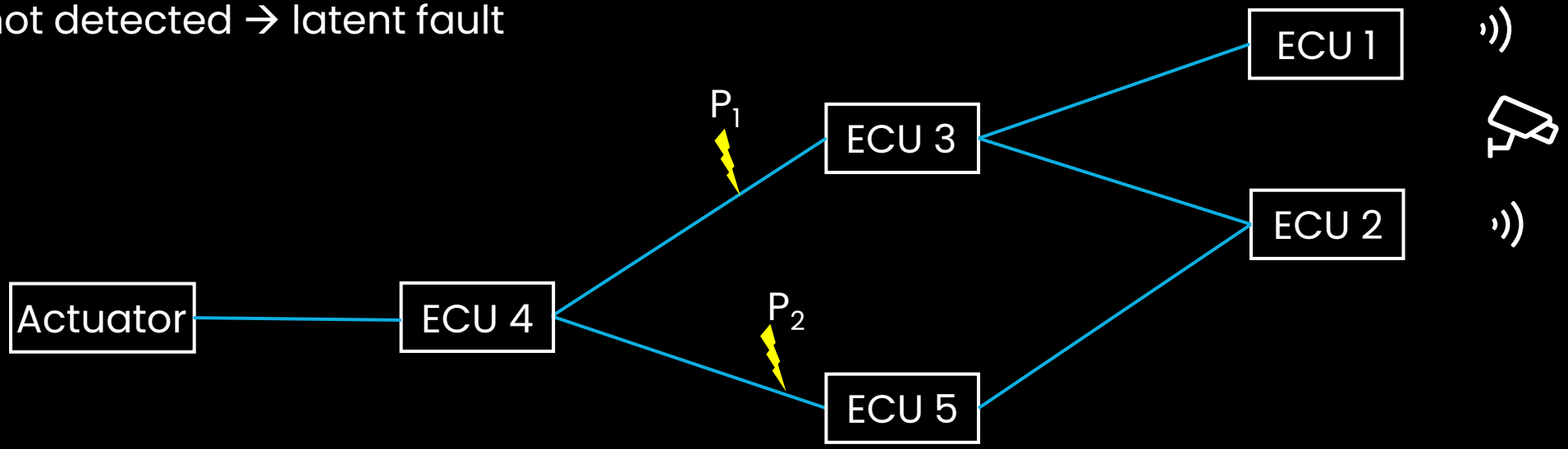
Fault-tolerant network (RHF)

- Random HW faults are typically covered by redundancy to allow for fail-operational
  - 802.1CB or VLAN redundancy
  - HW redundancy
- Should be static redundancy due to system timing requirements



Fault-tolerant network (unconstraint faults)

- Faults may happen in both channels
- Multiple-point fault, with low probability
  - unless not detected → latent fault

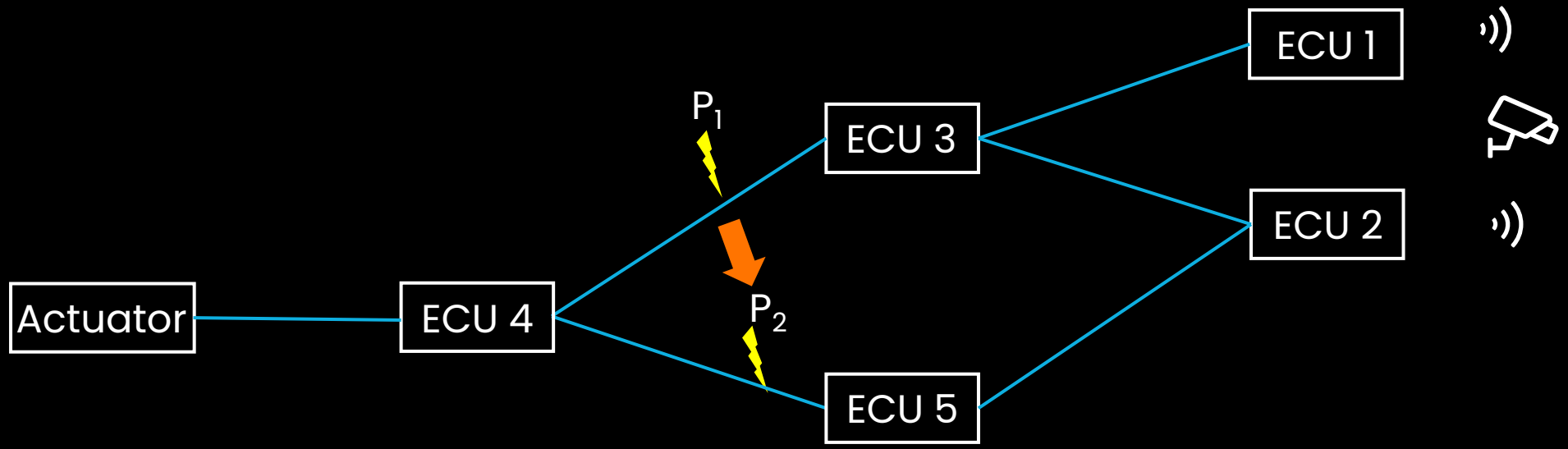


Random HW faults

$P = P_1 \times P_2$

Fault-tolerant network (cascaded fault)

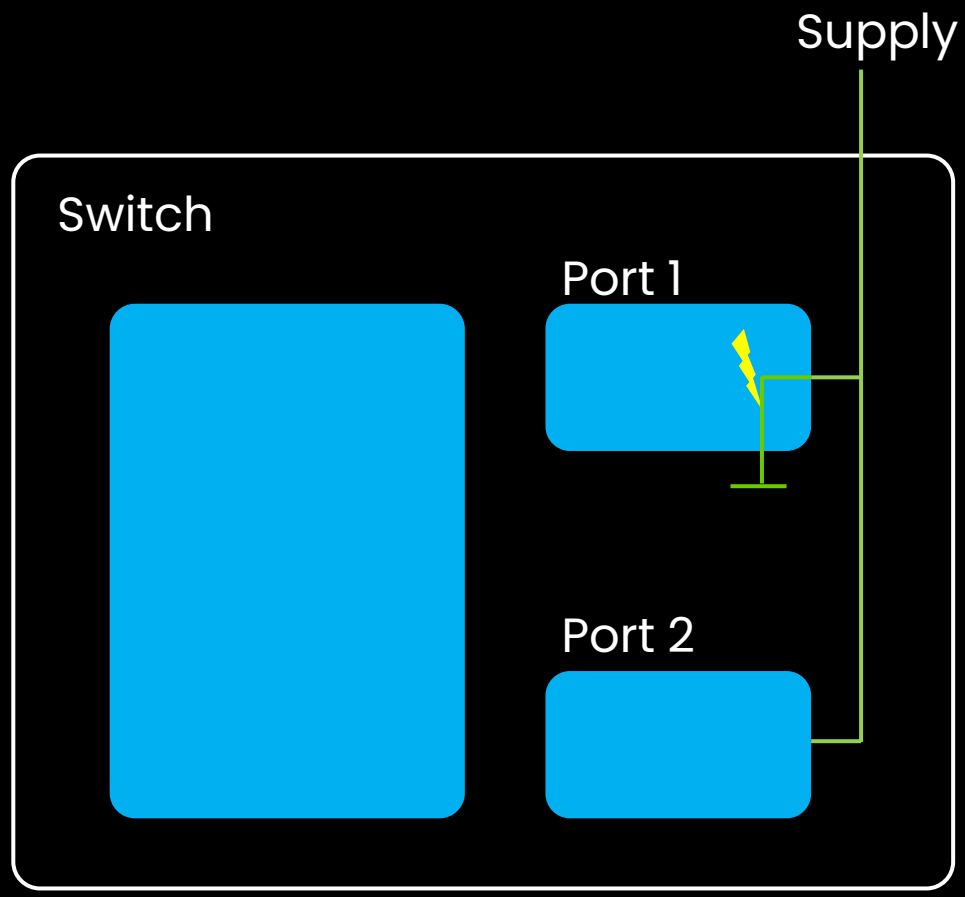
- Cascaded, when one fault is causing another fault
- Chain reaction of failures



Cascading faults
$P = P_1$

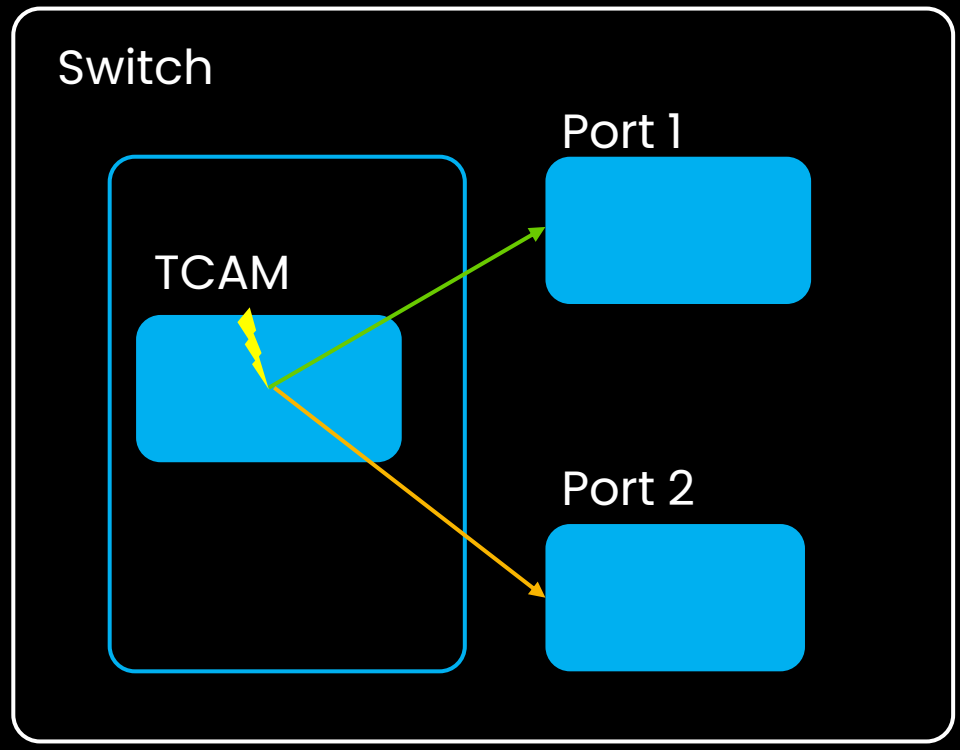
Example fault- short circuit

- Fault creates short to GND
- Port 2 affected due to voltage drop



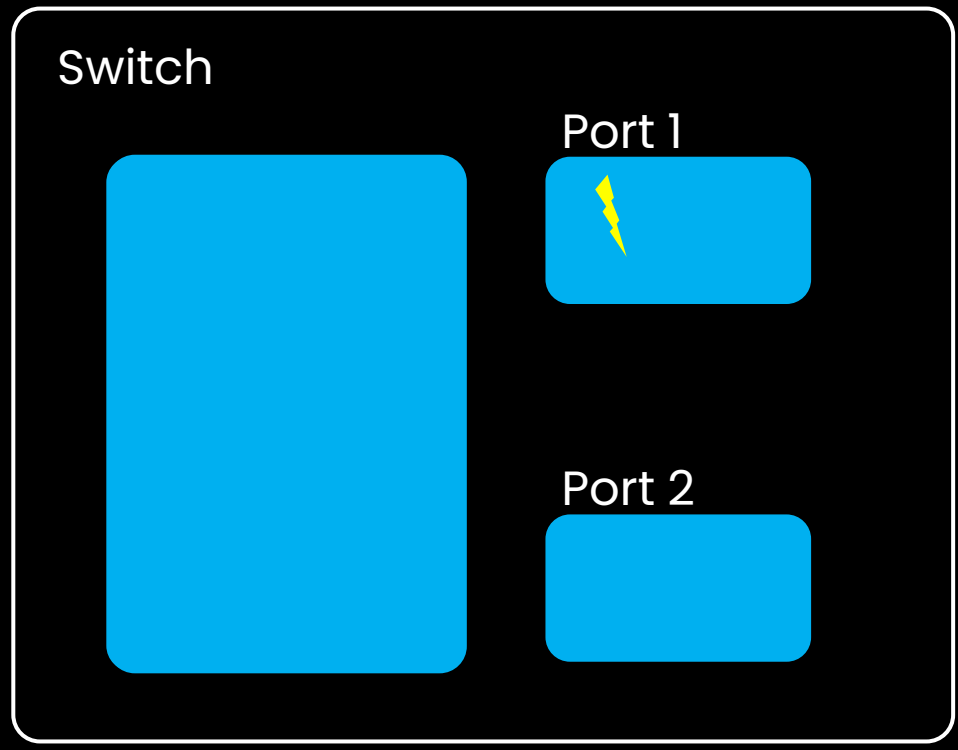
Example fault - TCAM

- Fault in TCAM lookup table
  - Pointer to another port
- Potential traffic congestion



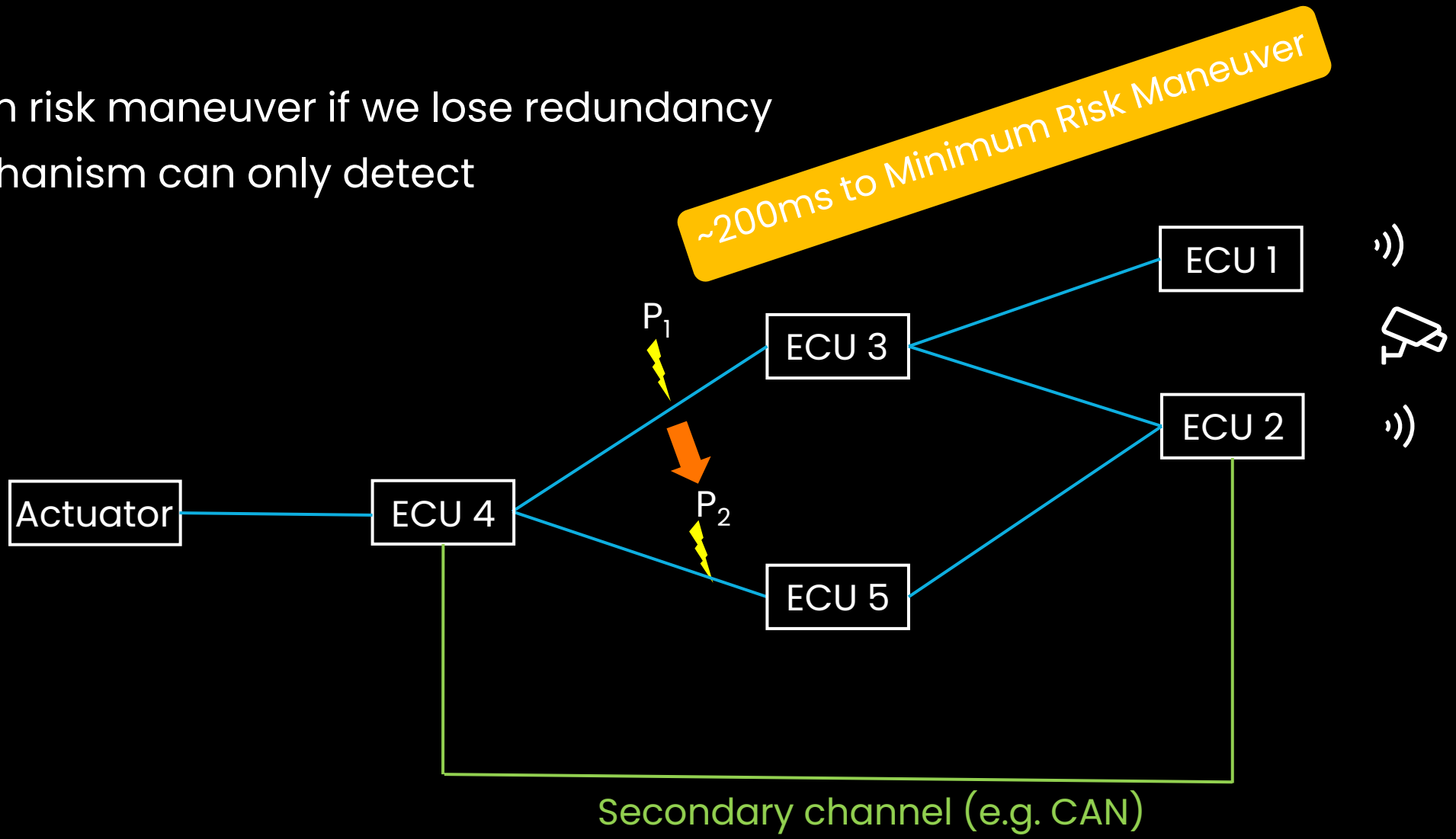
Example fault – soft error

- Corrupted configuration of one port
- Re-configuration/reset affects other ports
  - Resetting the whole communication takes longer than 200ms



Why do we need to take action?

- Minimum risk maneuver if we lose redundancy
- E2E mechanism can only detect



Fault containment regions

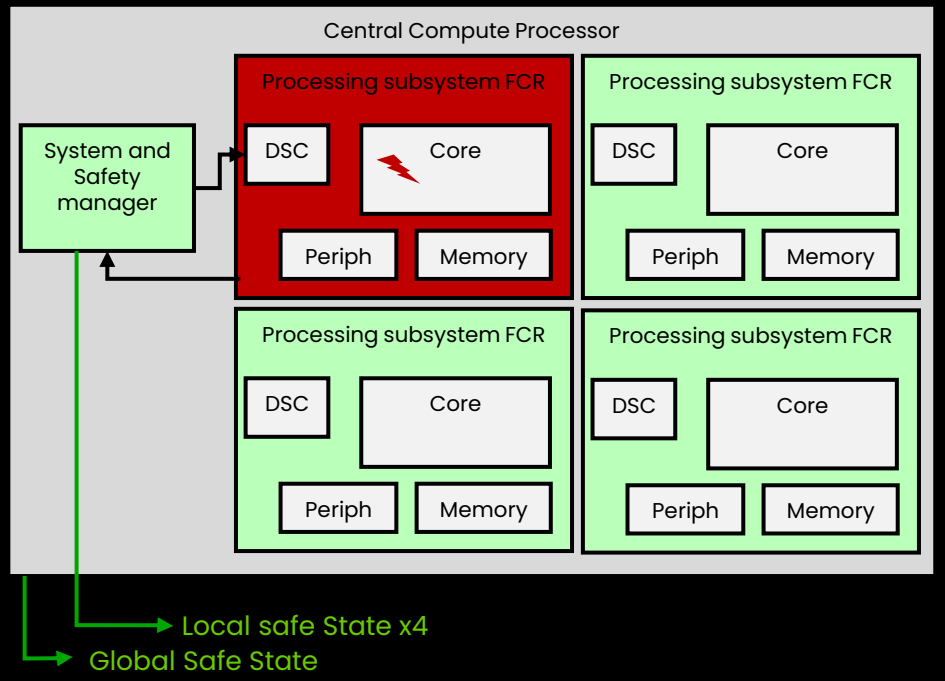
Fault containment region

Fault containment region (FCR)

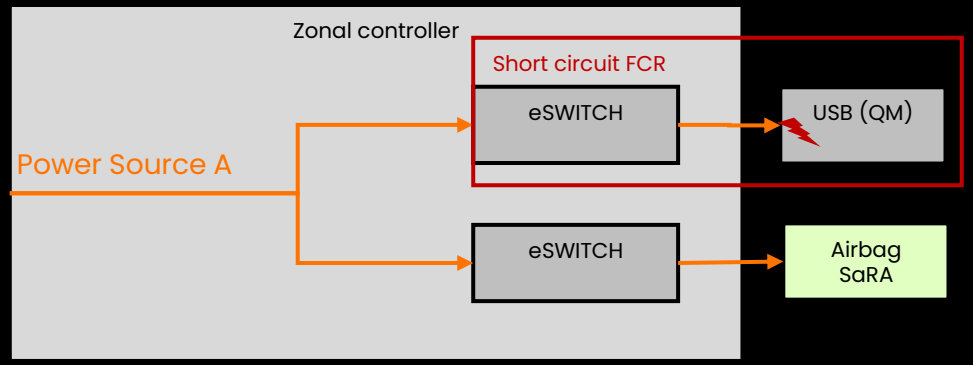
Prevent failure from one channel to impact functionality of another channel

Limit cascading effect of failure to least number of functions/systems.

FCR within central / domain controller

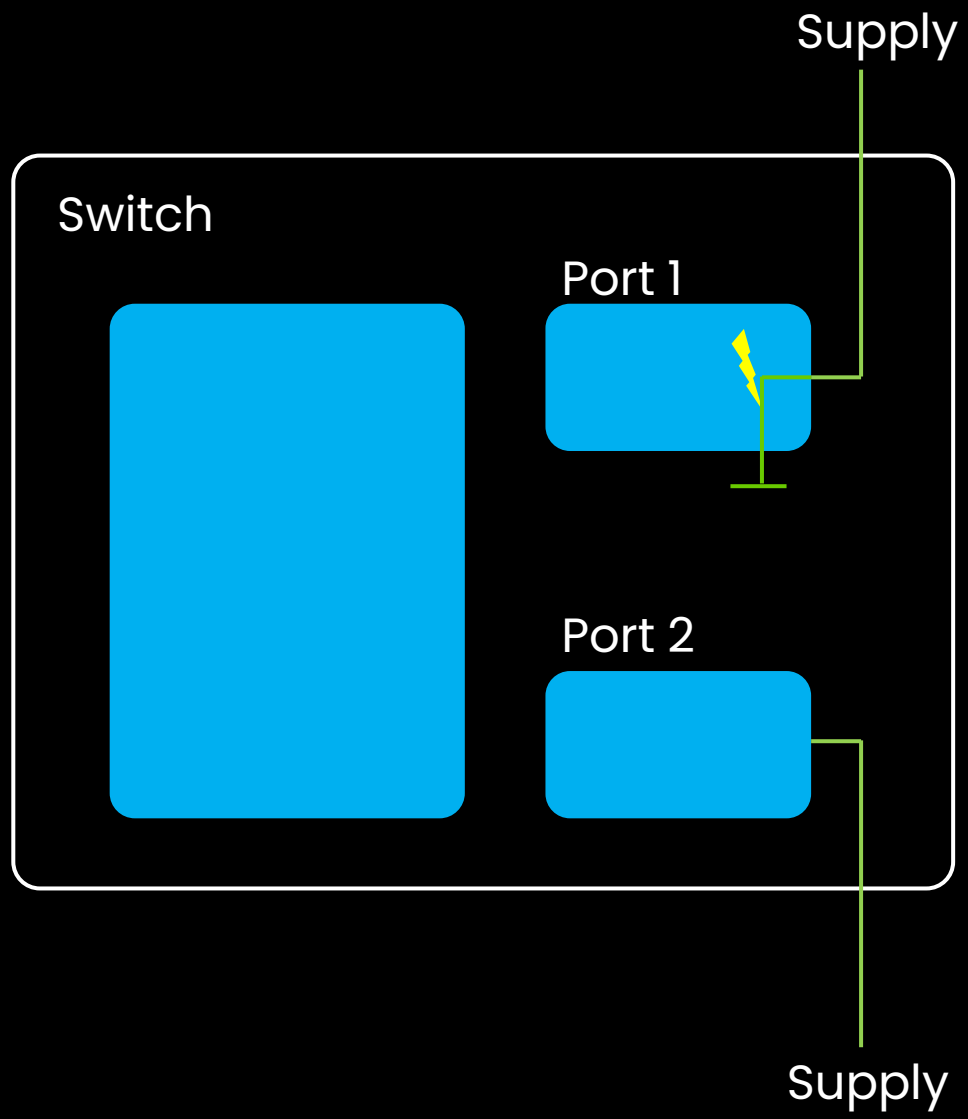


FCR Energy distribution



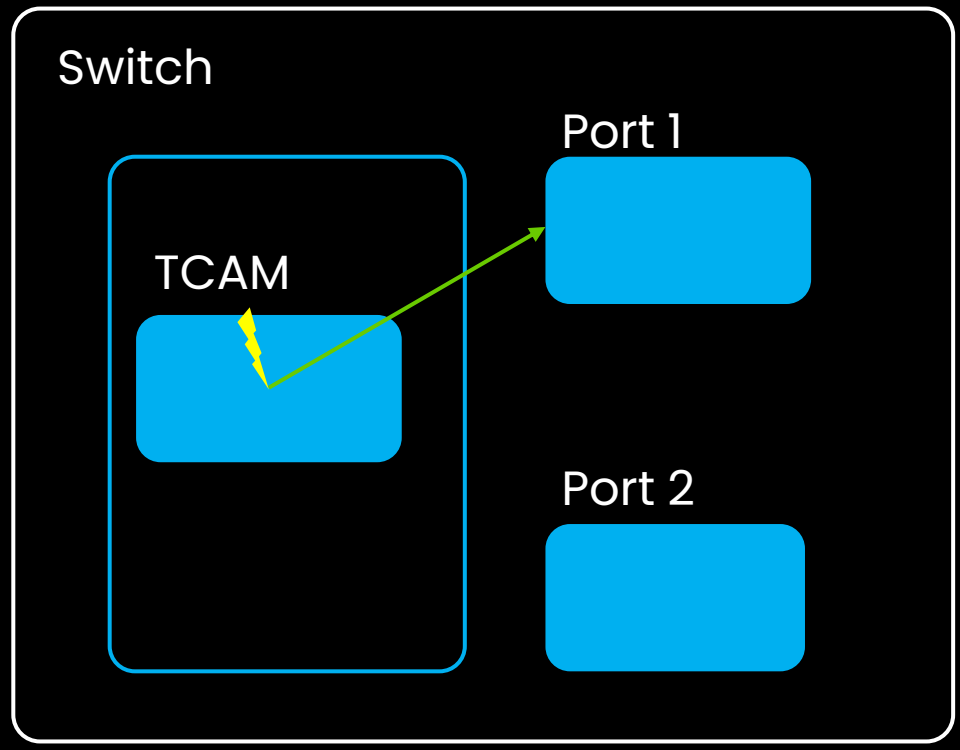
Example FCR for short circuit

- Separate power supply
- Current limitation of sub-blocks
- Ability to switch-off before over-heating (temp-detection)



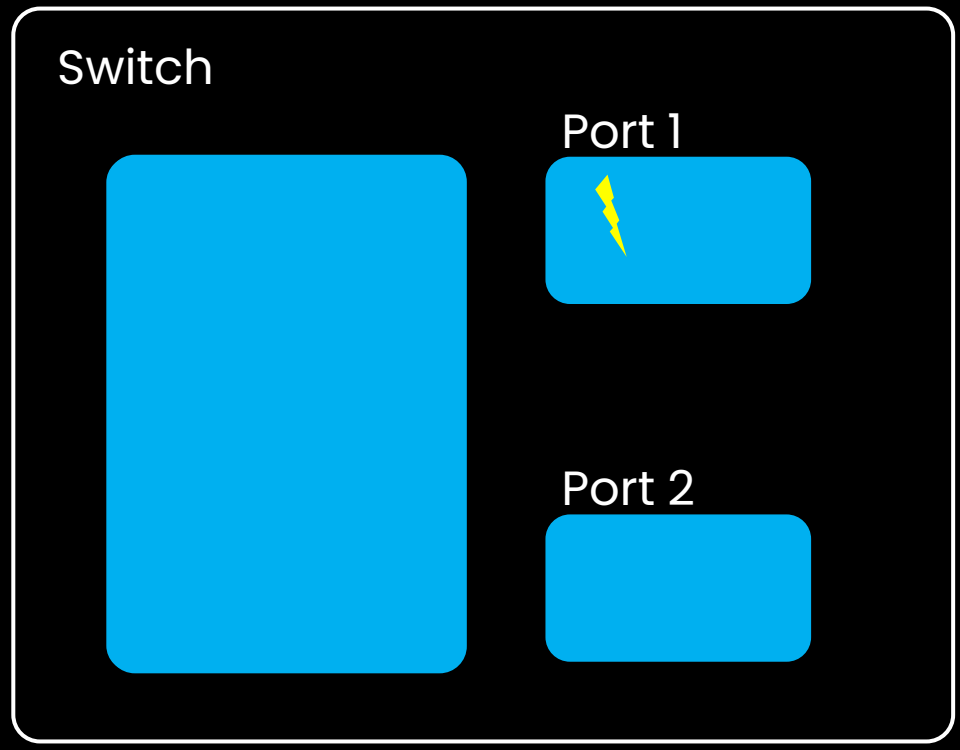
Example FCRs for TCAM

- Detect the fault (FHTI = 10ms)
- Prevent Pointer to another port

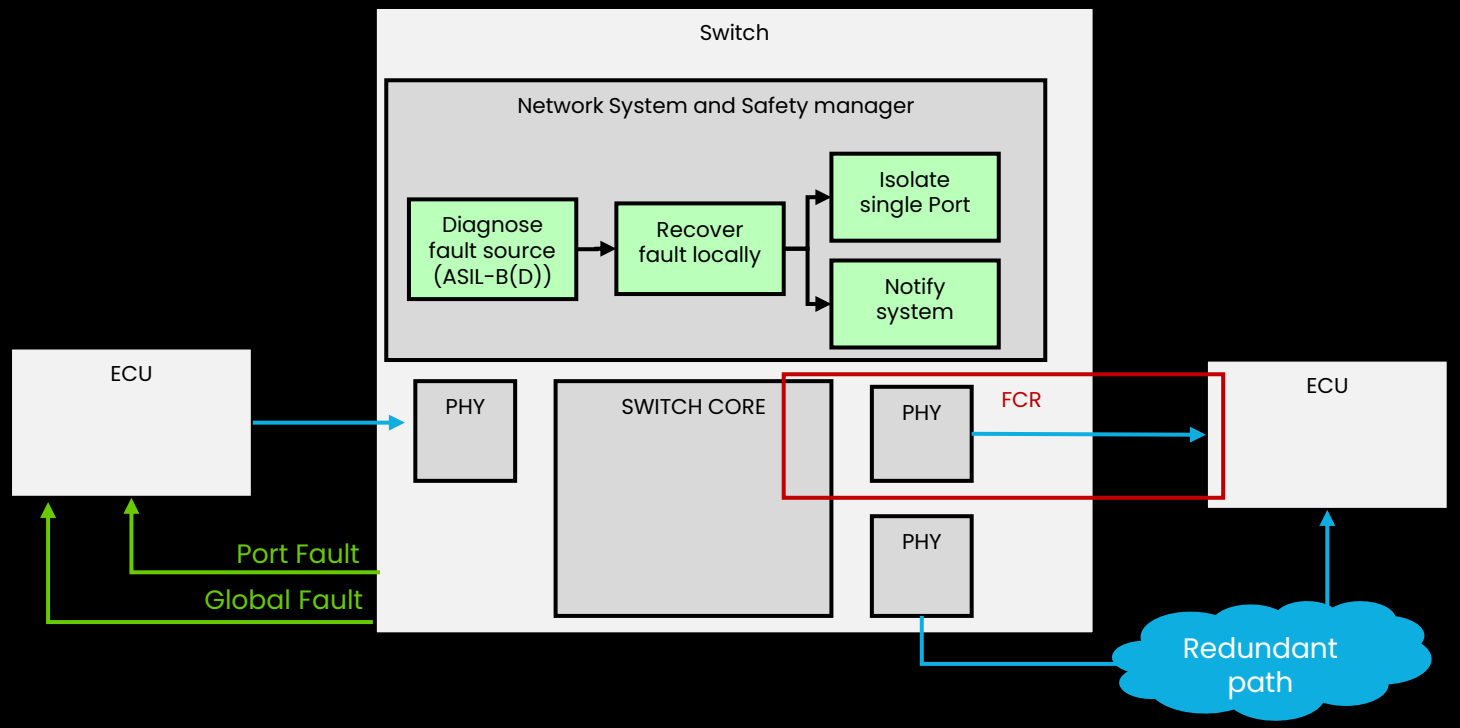


Example FCR for soft error

- Detect and fix the broken part only
  - Keep the link up to prevent link startup time
  - Keep other ports unaffected



Summarizing fault containment region on Ethernet



Detect/localize failure

Soft error

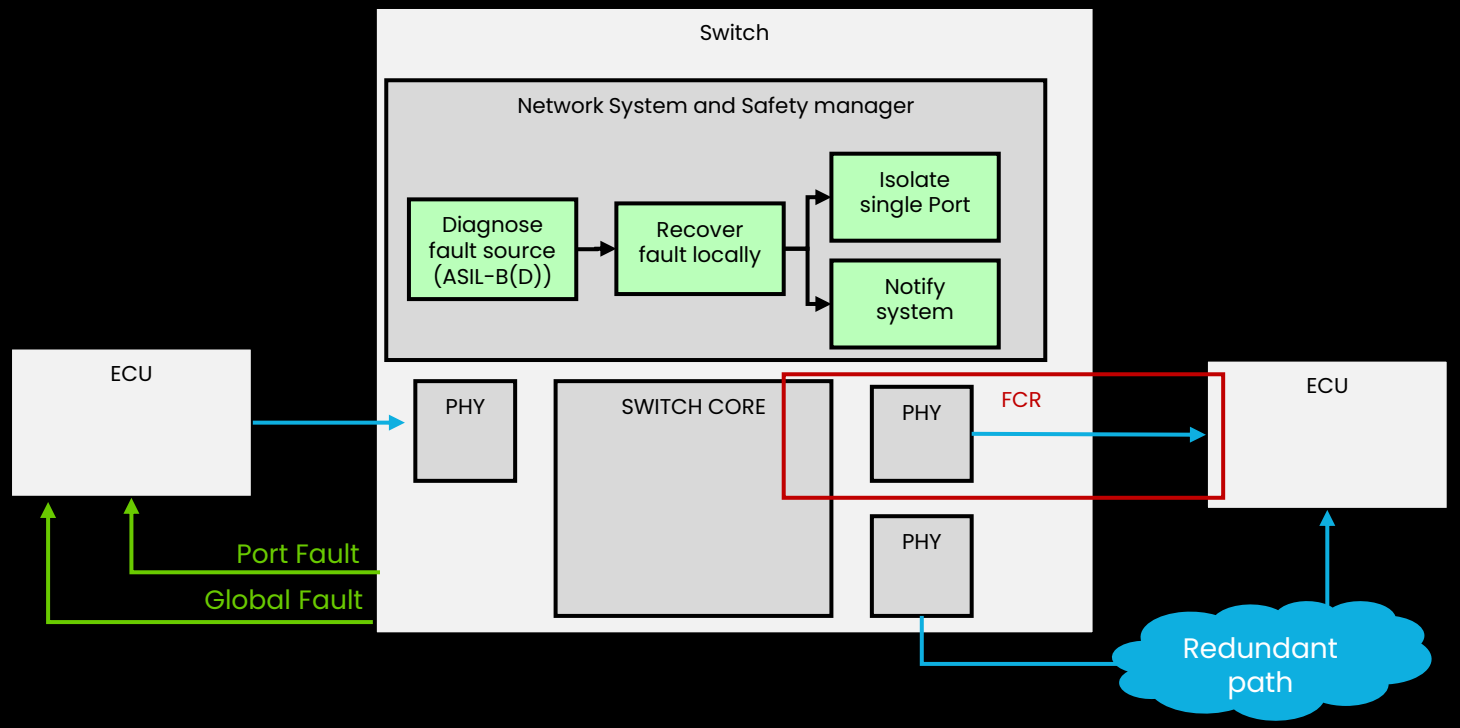
- Repair where possible
- Local recovery

Permanent error

- Enter port/function safe state
- Notify the system

Summarizing fault containment region on Ethernet

For this a switch must support:



Detect/localize failure

- error detection capability
- latent fault test

Soft error

- error correction
- independent reset/reconfiguration options

Permanent error

- independent safe state per port/function
- system safety concept

Conclusion

Summary & conclusion

Fail-operational systems require fault-tolerant communication networks

Summary & conclusion

Fault containment regions needed to prevent cascading faults

Summary & conclusion

Switch devices must be able to detect faults and allow for local recovery or degradation

Summary & conclusion

Prevent the End-2-End protection to kick-in, by keeping the communication available

nxp.com