ETHERNOVIA

TRANSFORMING HOW CARS OF THE FUTURE ARE BUILT

IEEE802.1DG – REDUNDANCY CLASSES | **2020-12-01**

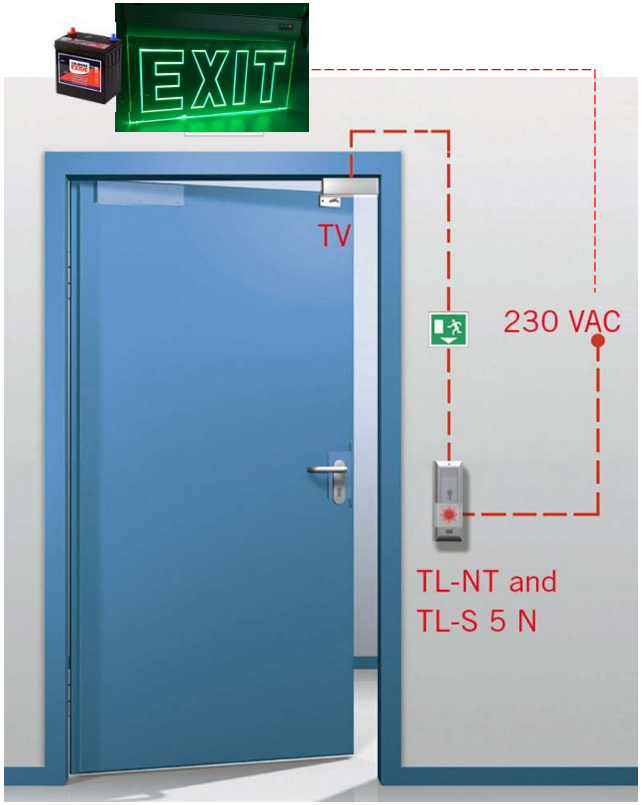
IEEE contribution

ETHERNOVIA
TRANSFORMING HOW CARS OF THE FUTURE ARE BUILT

Fail-Safe vs. Fail-Operational

A **System** relies on an **Input** for executing its **Mission**.

- Fail-Safe
  - After an **Initial Error** to the **Input**, the **System fails**, but assumes some **Final Safe State**, that will not cause further harm, but it can **no longer perform its Mission**.
  - A **Secondary Error** is not considered.
- Fail-Operational
  - After an **Initial Error** to the **Input**, the **System** has some **Alternate Input** enabling it to **continue its Mission** for a **Limited Time**.
  - After some **Time** or **Secondary Error** the **System** may
    - **fail** or
    - go into a **Final Safe State**.
  - A **Ternary Error** is (usually) not considered.



A personal view, based on experience, not deemed normative nor complete (yet)!

ETHERNOVIA
TRANSFORMING HOW CARS OF THE FUTURE ARE BUILT

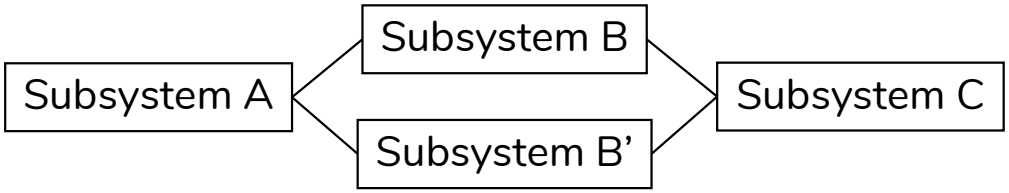
Redundancy Classes proposal

- **No Redundancy:** Fail safe – after loss immediate transition to a local safe state
- **Extended ~~wear-out~~:** Ignore initial failure, second failure will loose system functionality (temporal, intermittent, FEC)
- **Aging:** … Extend lifetime …
- **Fail gracefully:** Redundant data after initial failure used to mitigate transition to a system safe state within limited time to avoid secondary failure
- **Limp home:** Continue mission for extended period, maybe with reduced performance, but no reduction of safety level (secondary failure must at least be handled gracefully)

The Problem of Availability

Reliability Block Diagrams

During Operation

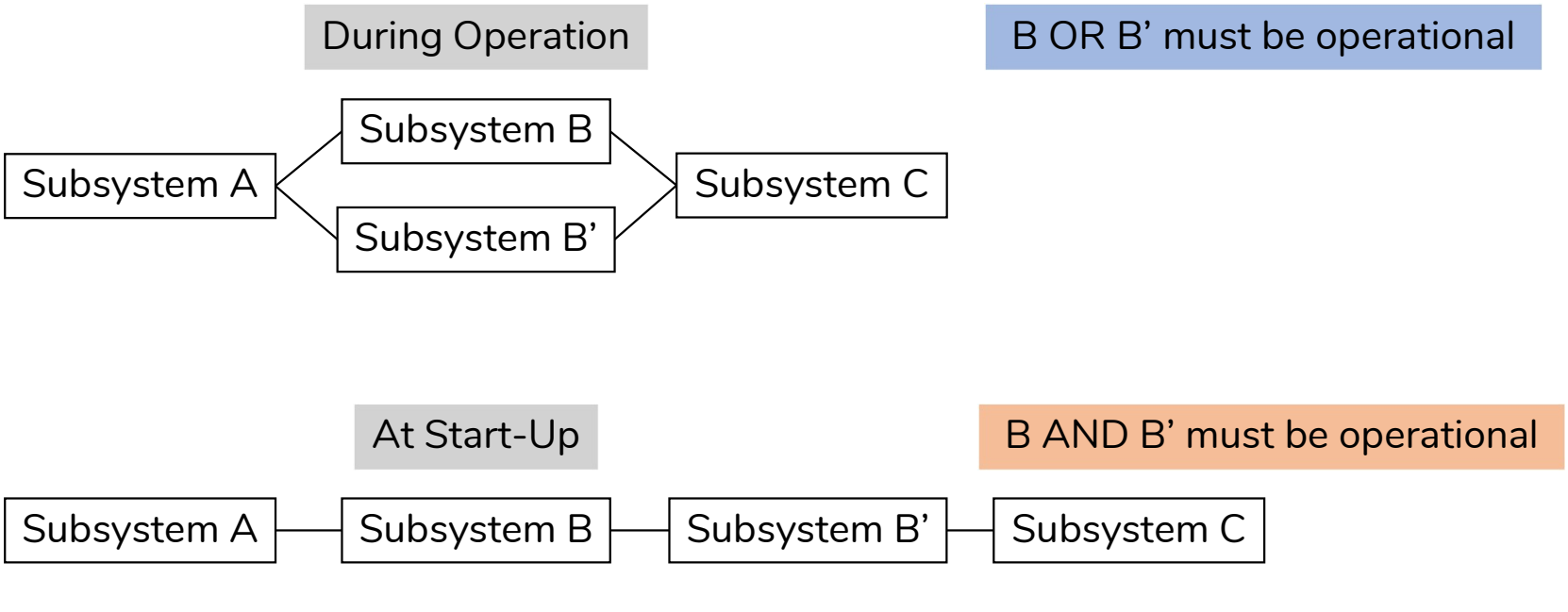


B OR B' must be operational

All elements are of the same "Quality".

The Problem of Availability - Start-Up

Reliability Block Diagrams



All elements are of the same "Quality".

The Problem of Availability - Operation

Reliability Block Diagrams

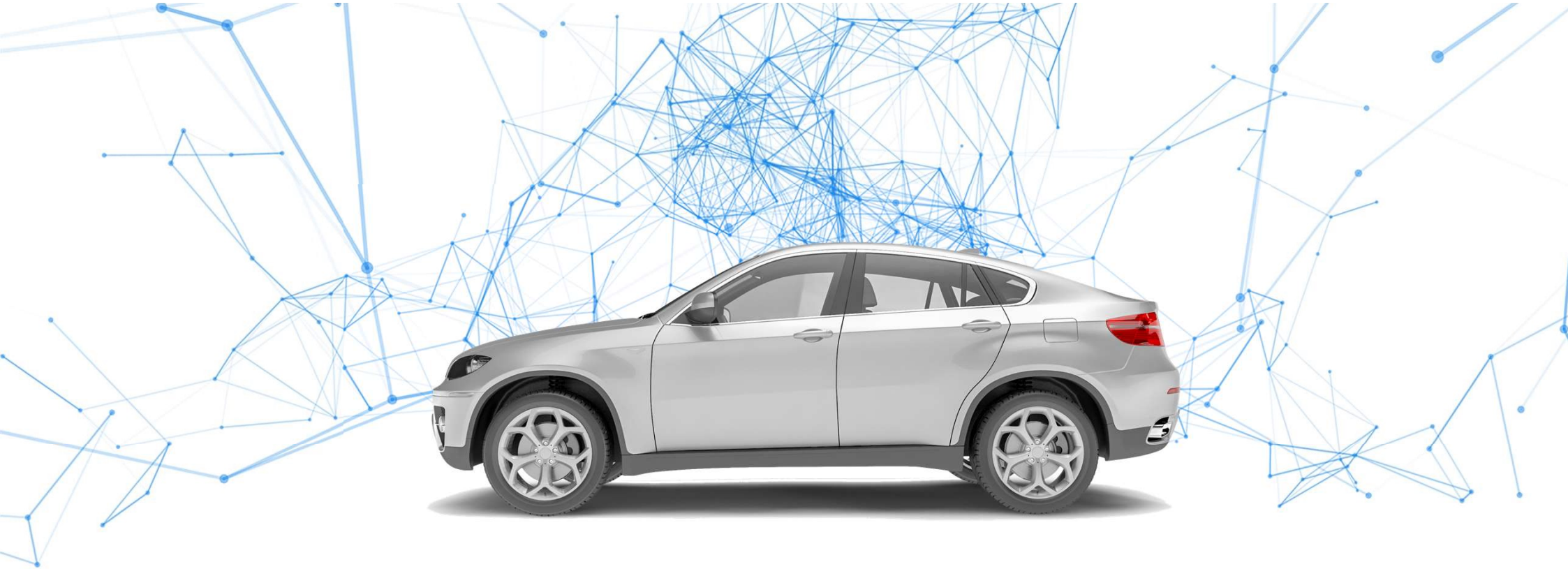
During Operation and Stat-Up

B AND B' must be operational and agree

IMHO: This is different from IT/Telecom!

Still "better" than this!

All elements are of the same "Quality".



THANK YOU

ETHERNOVIA | max.turner@ethernovia.com