Design Patterns for Highly Autonomous Vehicles – Achieving Fail Operational and High Level of safety and Security

Richard Messnarz, ISCN GmbH, Georg Macher, TU Graz, Jakub Stolfa, Svatopluk Stolfa, VSB TUO

EuroAsiaSPI 2019

"Always design a thing by considering it in its next larger context. A SW architecture on an electronic control unit, a connected service function in a central car computer, a connected vehicle function in the cloud, the cloud supporting artificial intelligence, a cloud intelligence on a planet, a planet connected with planets" – Eero Saarinen – "Extended".

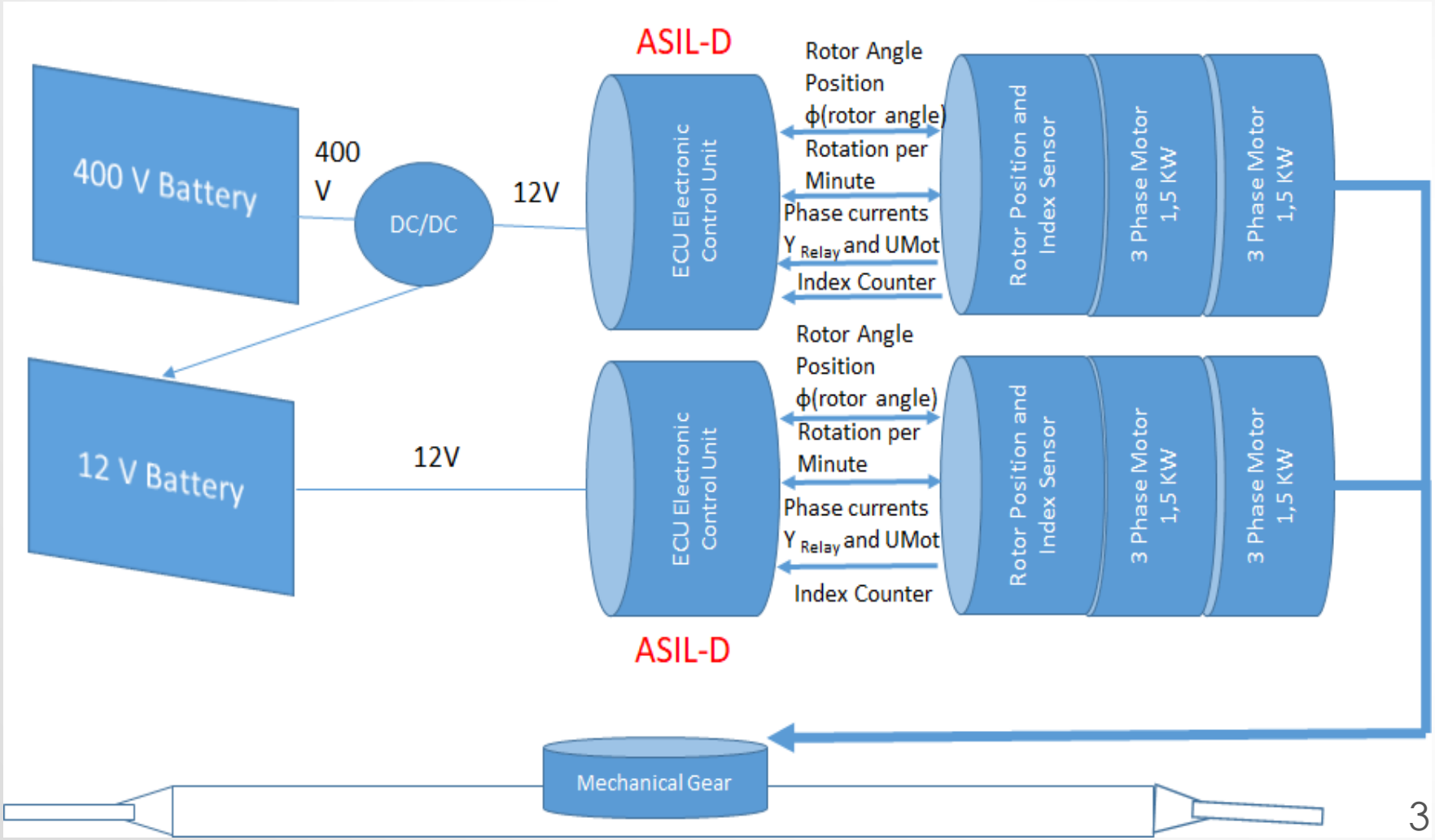
The whole is more than the sum of the items, Aistoteles

HAD Design Patterns

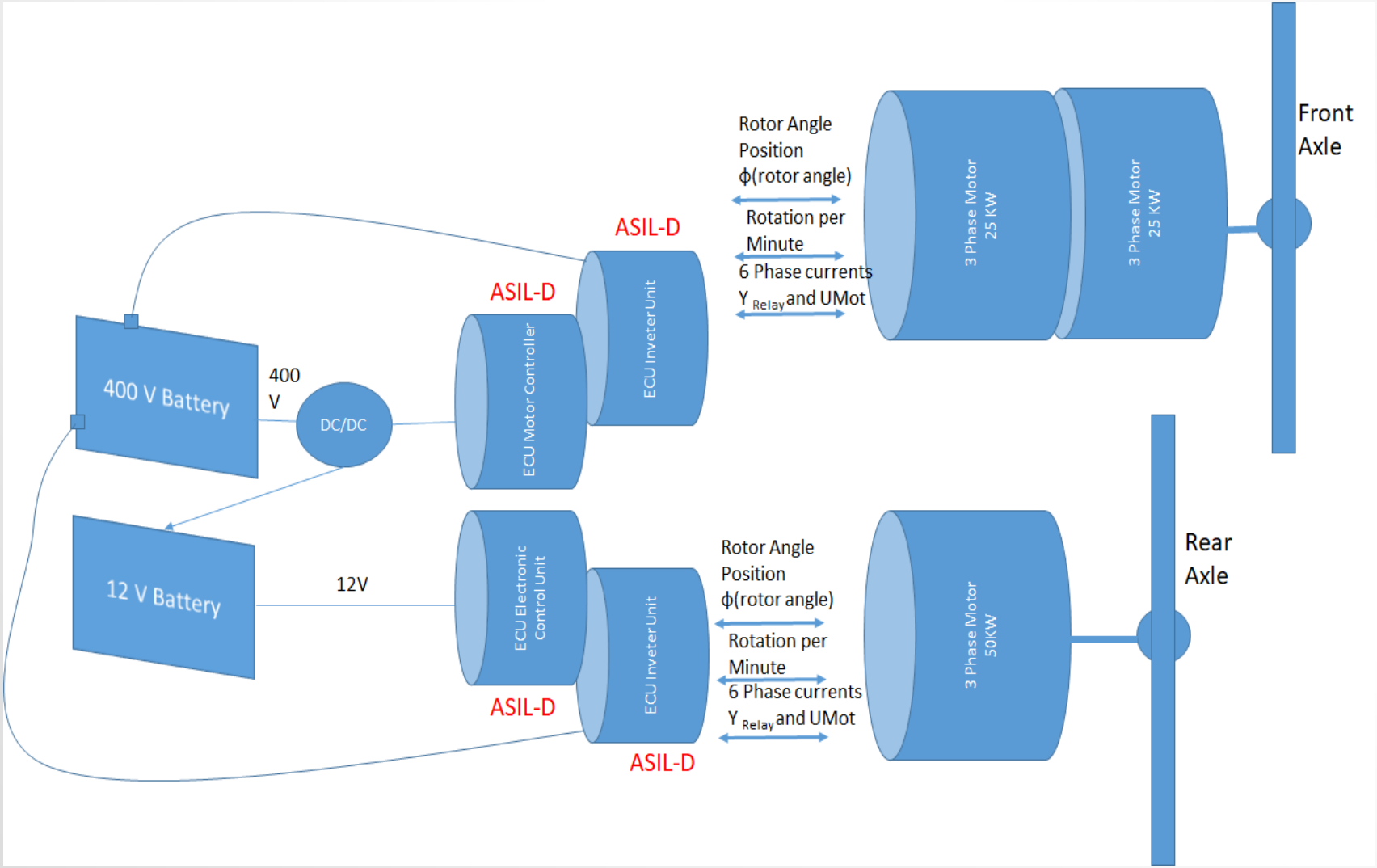
Fail Operational Concepts

- Fail-operational. Fail-operational systems continue to operate when their control systems fail.
- Fail safe. Fail-safe systems become safe when they cannot operate.
- Fail Operational Architectural Design
  - 3 Design Examples
  - Design Patterns

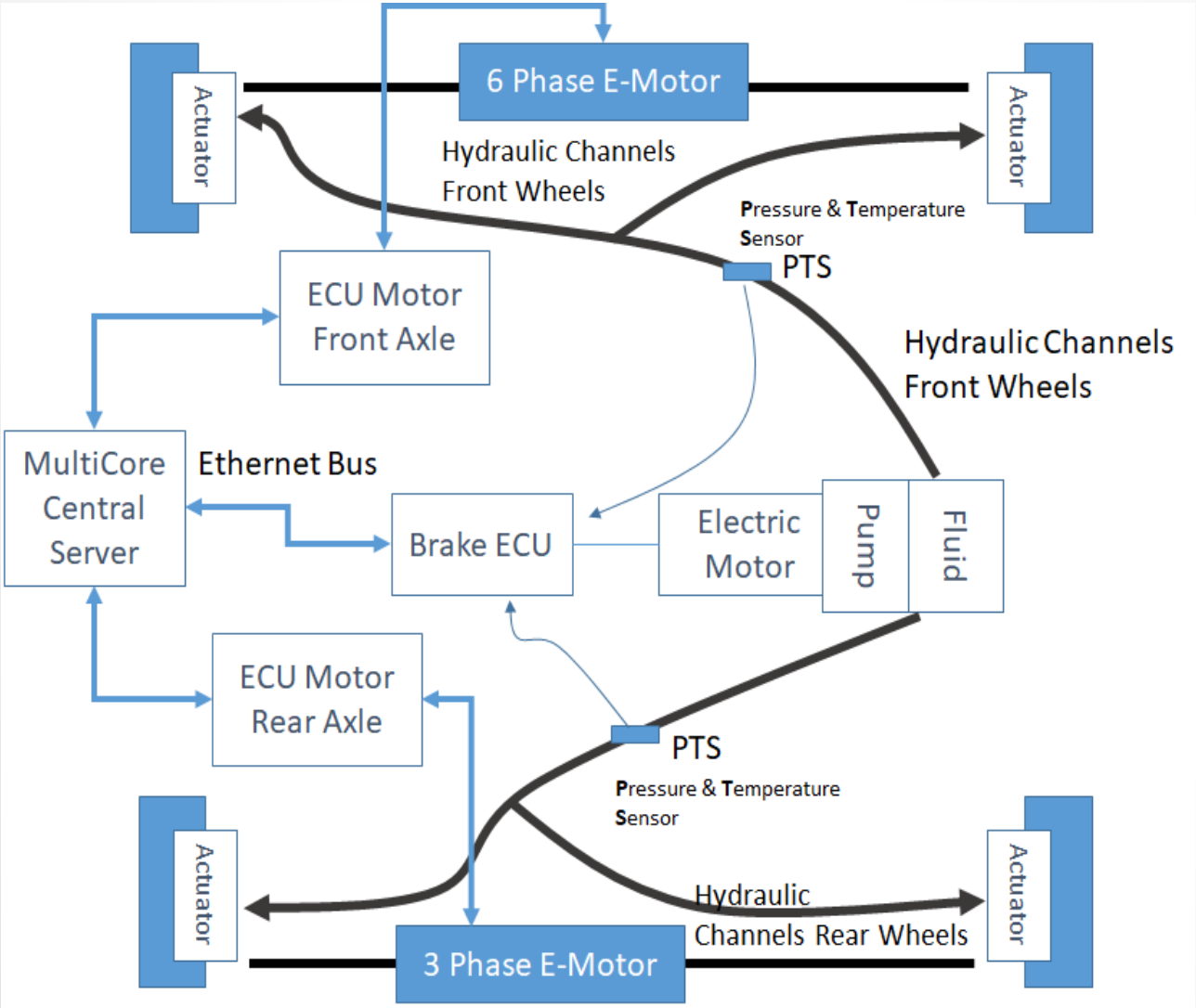
STEERING EXAMPLE



POWERTRAIN EXAMPLE



BRAKE EXAMPLE



HAD Design Patterns

What Patterns?

- **Two independent board nets.** All fail operational cars will have two board nets to prevent from common-cause power supply failures.
- **Two buses.** All fail operational cars will have two buses to also avoid a single cause failure cable breaking.
- **Two ASIL-D controllers** for each basic driving function. All fail operational cars will base on two independent diverse redundant ASIL-D components.
- **Four/Three and not any more dual fault strategy**. While in current cars a dual fault must happen before a hazard appears, in fail operational cars 3 to 4 faults must happen at the same time before a hazard appears.
- **New combination of systems** due to changes in signal paths: Since driver based information is not available any more (brake pedal, steering torque input, acceleration pedal, etc.) new combination of signals are needed to control the vehicle.
- **Multicore server** as a central computer in the car. Each component (brake, steering, motor, etc.) will need an App running on the central computer (Linux server) which communicated with the components of the vehicle and off-board networks (clouds) where driver inputs will be generated by the App based on environment information.

HAD Design Patterns

What Patterns?

- **Fail-operational HV battery system.** While in current cars failures in the HV battery system are prevented by deactivation and disconnection of the whole HV battery, future HV battery systems will have to support fail operational scenarios to further provided HV power supply in case of partial defects.

- **Separate HV battery output and smart fusing.** While in current cars fail operational powertrain can be ensured via the combustion engine or a loss of the HV power (resulting in loss of e-powertrain) can be handled by the driver, fail operational cars will have to have separate HV battery outputs and respective smart metering/fusing devices to also avoid a single cause failure via the HV battery system and enable partial deactivation and healing of the HV system.

Design Patterns for Highly Autonomous Vehicles

Richard Messnarz, Georg Macher, Jakub Stolfa, Svatopluk Stolfa

"Always design a thing by considering it in its next larger context. A SW architecture on an electronic control unit, a connected service function in a central car computer, a connected vehicle function in the cloud, the cloud supporting artificial intelligence, a cloud intelligence on a planet, a planet connected with planets" – Eero Saarinen – "Extended".

The whole is more than the sum of the items, Aistoteles

"Everything should be made as simple as possible, but not simpler." –Albert Einstein

"If you feel no resistance you have not done real research." –Richard Messnarz