Functional Safety Standards and Implications for Vehicle Power Electronics Design

Andrew Ellenson, John Deere Electronic Solutions

What is Functional Safety (FuSa)?

General Definition

The detection of a potentially dangerous condition resulting in the activation of a protective or corrective device or mechanism to prevent hazardous events arising or providing mitigation to reduce the consequences of the hazardous event.

[1] International Electrotechnical Commission, "About the IEC - Functional Safety," 2019. [Online]. Available: https://www.iec.ch/functionalsafety/explained/.

What is Functional Safety?

ISO 26262 Definition

The absence of unreasonable risk due to hazards caused by malfunctioning behavior of E/E systems.

[2] International Organization for Standardization, "Road Vehicles - Functional Safety - Part 1: Vocabulary," 2018. [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso:26262:-1:ed-2:v1:en. [Accessed 27 November 2019].

– Reduction of risk caused by potential malfunctions within the Electrical and Electronic (E/E) system

What is Functional Safety?

Risk

– Exposure
  - Probability of occurrence of harm
– Severity of harm

A Third Factor - Controllability

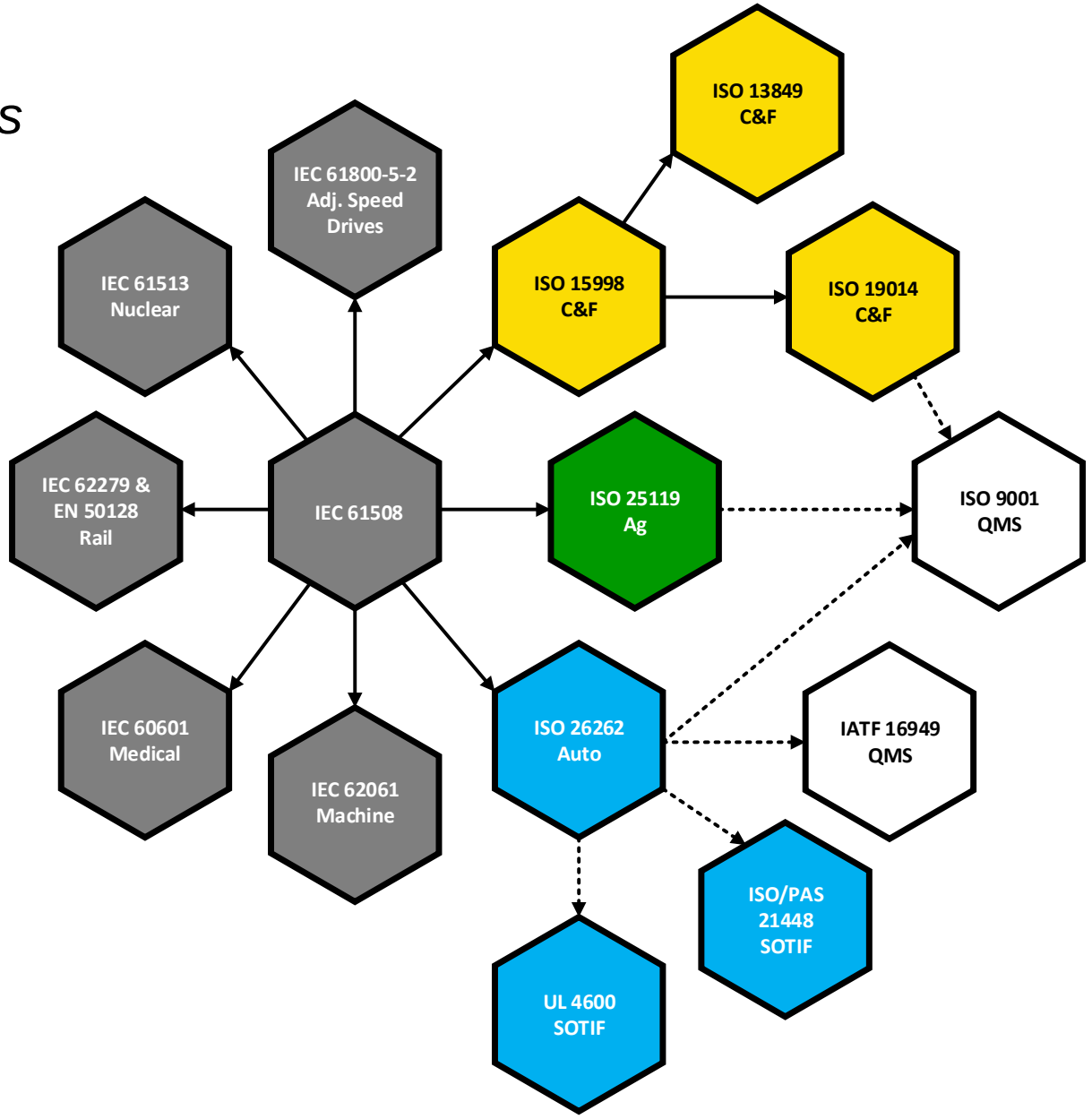
– The ability to avoid harm through timely reaction of the person(s) involved
  - Driver, other drivers, and/or pedestrians

What is Functional Safety?

Partial map of common FuSa standards

IEC 61508

- The “grandfather” of safety standards
- ISO 26262 derived from IEC 61508



What is Functional Safety?

There are several standards currently in publication

- IEC 61508: Functional safety of E/E safety-related systems
- **ISO 26262: Road Vehicles – Functional Safety**
- ISO 25119: Tractors and machinery for agriculture and forestry – Safety-related parts of control systems
- ISO 13849: Safety of machinery – Safety-related parts of control systems *{being replaced by ISO 19014}*
- ISO 19014: Earth-moving machinery – Functional safety
- Several in aviation
- …

What is ISO 26262?

On highway vehicle Functional Safety

- First edition released in 2011, Parts 1-9
- Second edition released in 2018, Parts 1-12

Covers

- Automobiles
- Trucks and Buses – as of Ed. 2
- Motorcycles – as of Ed. 2
  - Excludes mopeds as defined in ISO 3833 (speed < 50kph)
- Semiconductor Guidance – as of Ed. 2

What is ISO 26262?

12 Parts

Part 1: Vocabulary

Part 2: Management of Functional Safety

Part 3: Concept Phase

Part 4: Product Development at the System Level

Part 5: Product Development at the Hardware Level

Part 6: Product Development at the Software Level

Part 7: Production, Operation, Service and Decommissioning

Part 8: Supporting Processes

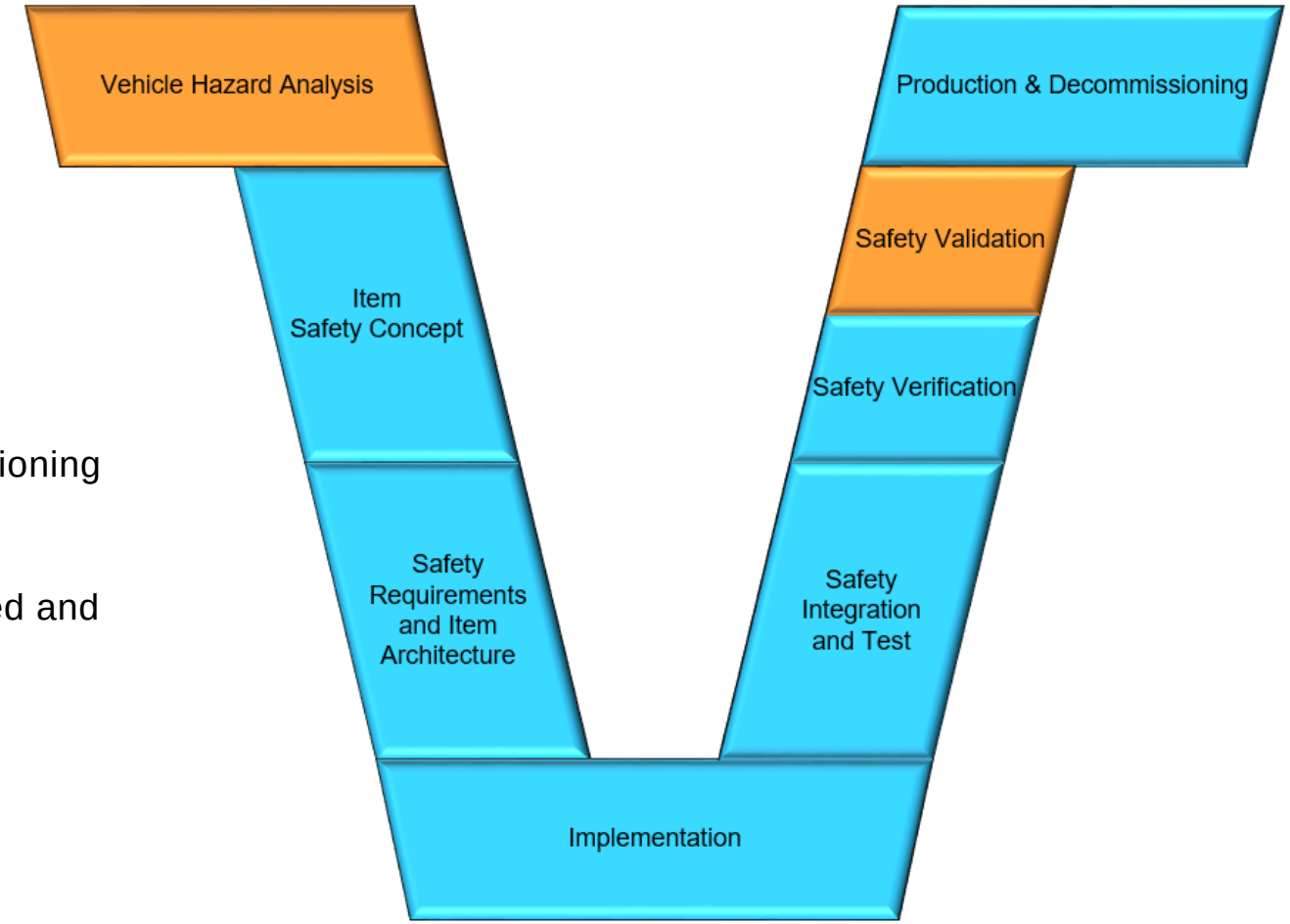
Part 9: Automotive Safety Integrity Level (ASIL)-oriented and Safety-Oriented Analyses

Part 10: Guideline on ISO 26262

Part 11: Guidelines on the Application of ISO 26262 to Semiconductors

Part 12: Adaptation of ISO 26262 for Motorcycles

V-Model Development Cycle



What is ISO 26262?

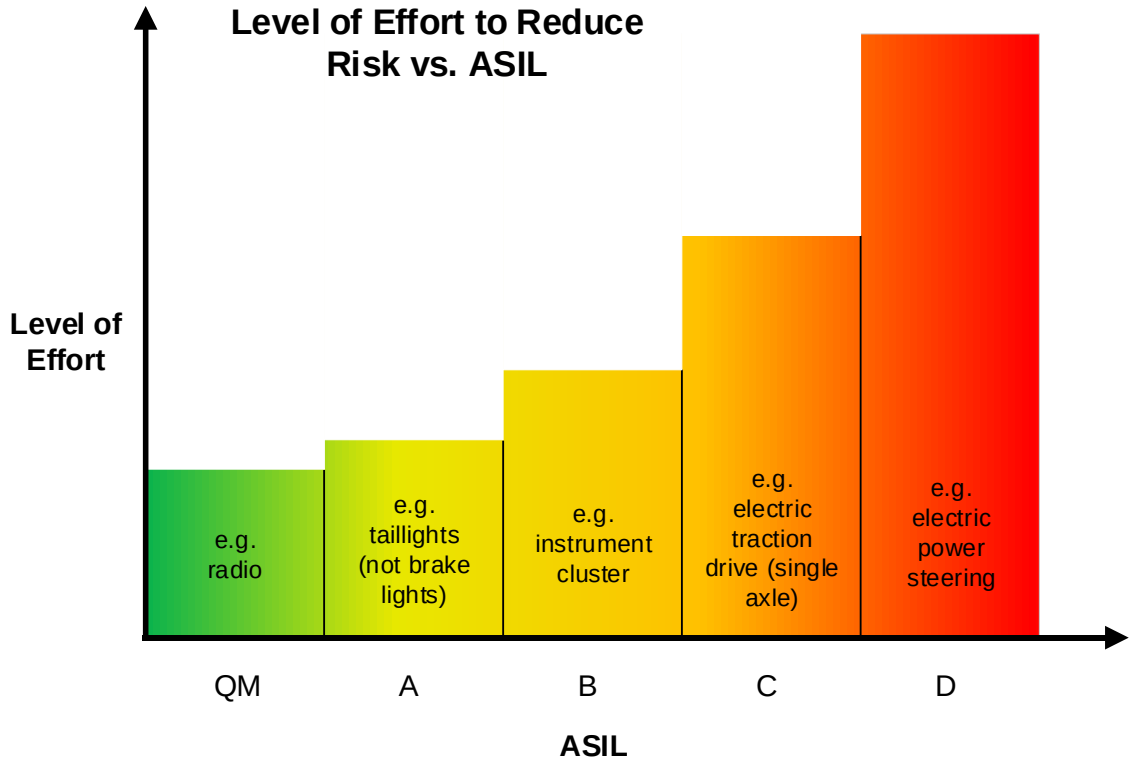
Avoidance and Control of Systematic and Random Failures

- Avoid and Control Systematic Failures
  - Functional Safety Management
  - Product development processes & supporting processes
  - Production & Operation
- Control Random Hardware Failures
  - System architecture
  - Hardware (HW) reliability – probabilistic analysis
    - Mean Time To Failure (MTTF), Failures In Time (FIT)
  - Software (SW) diagnostics

What is ISO 26262?

Automotive Safety Integrity Level (ASIL)

- Quality Management (QM), and A through D
- Determined from vehicle-level analysis
- Increasing level of effort to reduce risk to a generally acceptable level
  - More stringent HW metrics
  - More analysis, reviews, and testing required
- Applied to the Safety Goals for the system



What is ISO 26262?

Safety Goals (SG)

- Determined from vehicle-level analysis
- Each SG may have a different ASIL
- Only applied to ASIL A through D, not QM
- Each SG has a corresponding Safe State(s)
  - Fail Safe or Fail Operational

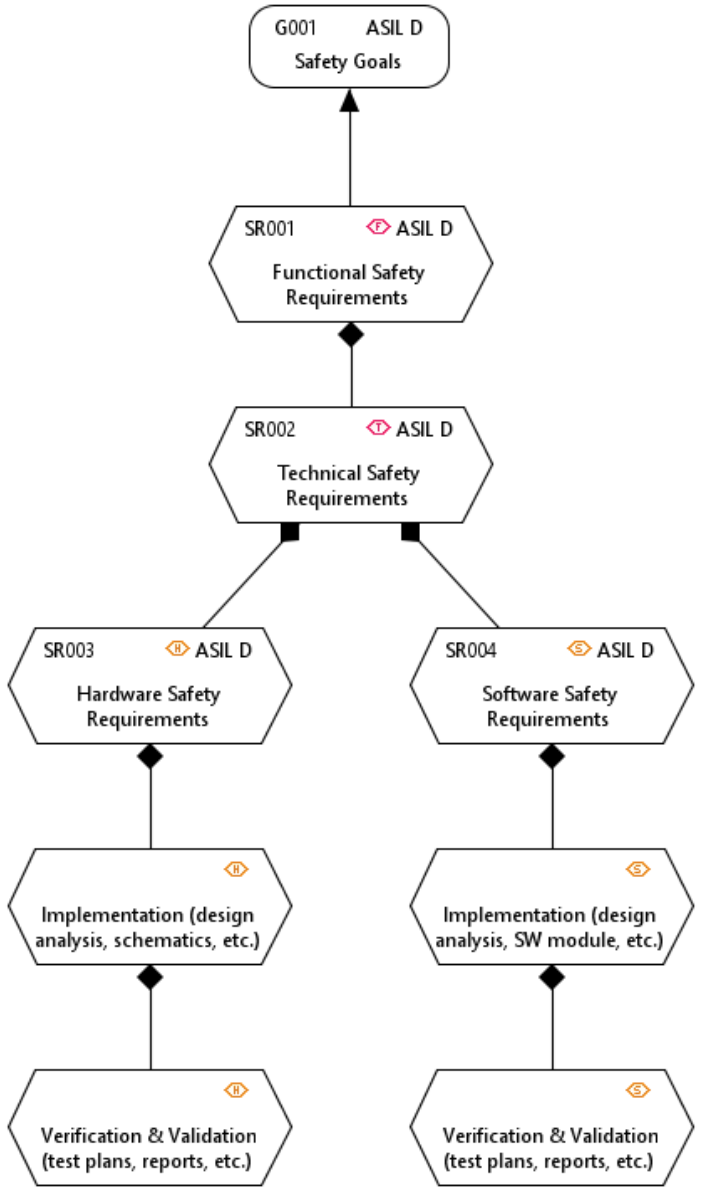
Example Safety Goals and Safe States for a Single Axle, Electric Traction Drive, Three Phase Inverter

Safety Goal	Safe State
Prevent un-commanded torque from standstill (ASIL C)	Six switch open
Prevent excessive torque in opposite direction from commanded torque (ASIL C)	Three phase short
Prevent excessive torque in the same direction as commanded torque (ASIL B)	Three phase short

What is ISO 26262?

Other Important Concepts

- Enforces a “culture of safety”
  - Processes and personnel in place across the organization
  - Training – from senior management to entry level
- Focuses heavily on processes
  - Ensure no missed steps and correct order of development
- Traceability is crucial
  - Traceability from requirements to implementation to verification
- Reviews
  - Design reviews and confirmation reviews (process audits)
  - Several require independence



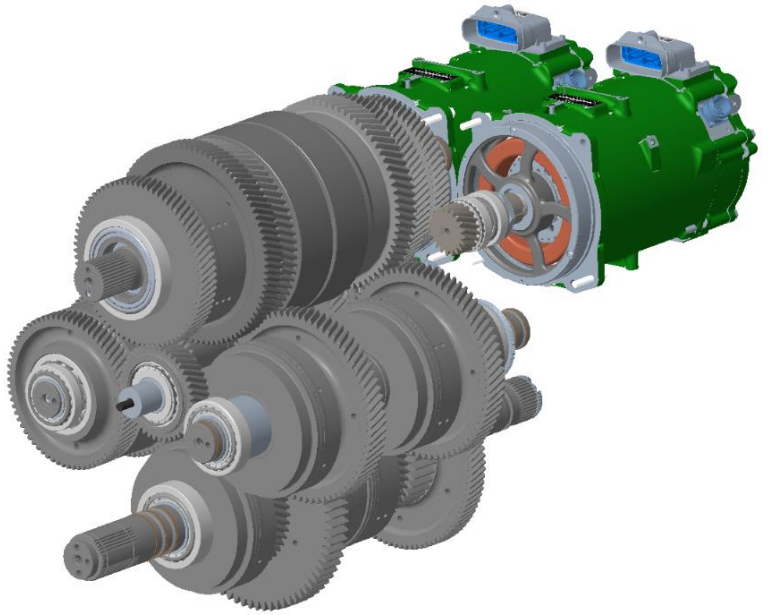
What ISO 26262 is Not?

- Not a reliability standard
  - Failures are allowed as long as they result in a safe state
- Not concerned with shock, fire, flammability, etc.
  - ***Unless…*** they are a direct result of a malfunction of a safety-related E/E system
- Not concerned with nominal system performance
  - ISO 26262 will not address issues with autonomous operation
  - ISO/PAS 21448: Road Vehicles – Safety of the Intended Functionality (SOTIF), was developed to address this *{currently being updated}*
- Not concerned with cybersecurity (CS)
  - ISO 26262 Part 2 references effective communication between FuSa and CS
  - ISO/SAE 21434: Road Vehicles – Cybersecurity Engineering, is under development to address this

Driving Forces in Power Electronics (PE) Design

Why should the PE community be concerned with FuSa?

- EU and global OEMs requiring compliance
  - ISO 26262 considered state-of-the-art
  - Liable to follow and show compliance to state-of-the-art design practices
  - Expansion into Commercial – Truck and Bus
- **PE components used in many safety-related systems**
  - **Steering, braking, traction drives, etc.**
- Increasing SW complexity
  - Today's vehicles can have >100 million lines of code
- Not just automotive
  - ISO 25119 for Agriculture, ISO 19014 for Construction Machinery, etc.



John Deere eAutoPowr Transmission

Effects on PE Design and Processes

What does this mean for PE design?

- Safety starts before you design anything
  - Have processes, tools, and FuSa personnel in place first
- Process tools – text documents and spreadsheets are not the way forward
  - Automated traceability
  - Records of work products and reviews
  - Track development progress against the standard – checklists, etc.
- ISO 26262 qualified development tools
  - Compilers, configuration management, Model-based Software Design (MBSD) toolsets, etc.

Effects on PE Design and Processes

What does this mean for PE design?

- System architecture design
  - Safety Goals and ASIL drive system architecture
    - Provisions for monitoring, testing, redundancy, etc.
  - System safety analysis
    - FuSa analysis methods (FMEDA, FTA, Markov Chains, etc.)
    - Analysis and reduction of Single-Point Faults (SPF) and Multi-Point Faults (MPF)
    - ASIL-dependent HW metrics (FIT rates)
  - Analysis and implementation of Safety Mechanisms (SM)
    - Maintain intended functionality or achieve safe state

Effects on PE Design and Processes

What does this mean for PE design?

- Component and supplier selection
  - “ASIL X capable” components
    - Typically complex ICs – Micros, PMICs, Gate Drivers, etc.
  - Qualified embedded operating systems
- Testing
  - ASIL dependent
  - Fault injection
  - Traceability to safety requirement(s)

Effects on PE Design and Processes

What does this mean for PE design?

– Production, Service, and Decommissioning

- Consider effects of production and service processes on safety
- Warning and degradation strategy
- Field monitoring
- Lessons learned from field application
- Emergency and rescue considerations
- Instructions for safe decommissioning

Conclusion

Closing Remarks

- ISO 26262 is considered state-of-the-art for on-highway Functional Safety
  - Power Electronics are increasingly used in on-highway applications
- Safety Goals will dictate the system architecture
  - Define them as early as possible
- Process compliance and safety culture are vital
- Significant impacts to product design and processes
- Drives improved design processes and documentation

Q&A

JOHN DEERE