Functional Safety of Electronics and Software

Jason R. Smith, Principal Engineer – Functional Safety

March 7, 2019 | Protection Engineers Conference

Empowering Trust™

Agenda

I. **What** is Functional Safety?

II. **Why** Functional Safety?

III. **How** is Functional Safety assessed?

What is Functional Safety?

“Part of the overall safety of a system, which depends on the correct execution of specific functions.”

— Functional Safety

Example – Circuit Breaker

Circuit breaker with an Electronic Trip Unit (ETU); includes:

- Sensors to detect current
- Hardware circuits to condition input signals
- Software to calculate values and make decisions
- Hardware circuits to trip circuit breaker

ETU must **function** correctly to ensure **safe** operation of the system; i.e. detect overload condition to prevent fire

Similar applications: GFCIs, AFCIs, EVSEs, etc.

Example – Photovoltaic (Solar) Inverter

Converts DC power (from the PV panels) to AC power, which is then put onto the electrical grid; inverter must:

- Measure voltage and frequency of the electrical grid
- If voltage and frequency are not within acceptable limits, indicating that the electrical grid is not operating properly, service personnel may be repairing parts of the electrical grid (e.g. electrical cables down, etc.)
- If this is the case, inverter shall turn off and disconnect its output from the electrical grid

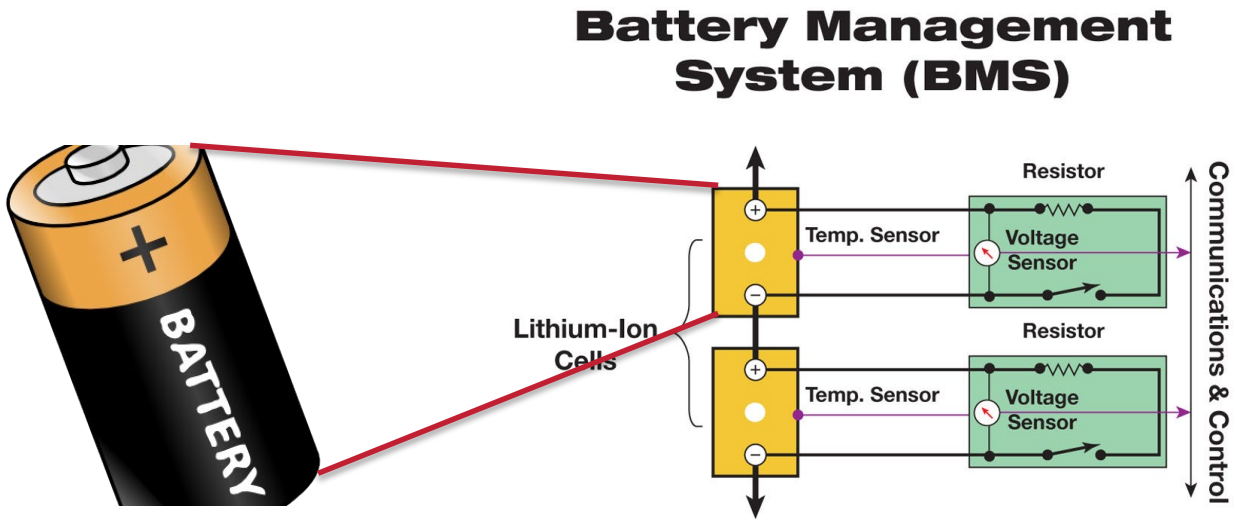
Inverter must **function** correctly to ensure **safe** operation of the system; i.e. prevent electric shock of service personnel

Example – Battery-Based Energy Storage System

Battery stores electrical energy, e.g. for back-up power; system includes a Battery Management System (BMS), which must:

- Measure voltage, temperature, and current of the battery to ensure that battery cells are operating within appropriate ratings, and if not, disconnect battery (disable charge/discharge)

BMS must **function** correctly to ensure **safe** operation of the system; i.e. prevent battery fire



Functional Safety is Everywhere

Why Functional Safety?

Why Functional Safety?

“Functional Safety” as a property has always existed

It is not specific to any one technology

But it has evolved into a technical term and engineering discipline

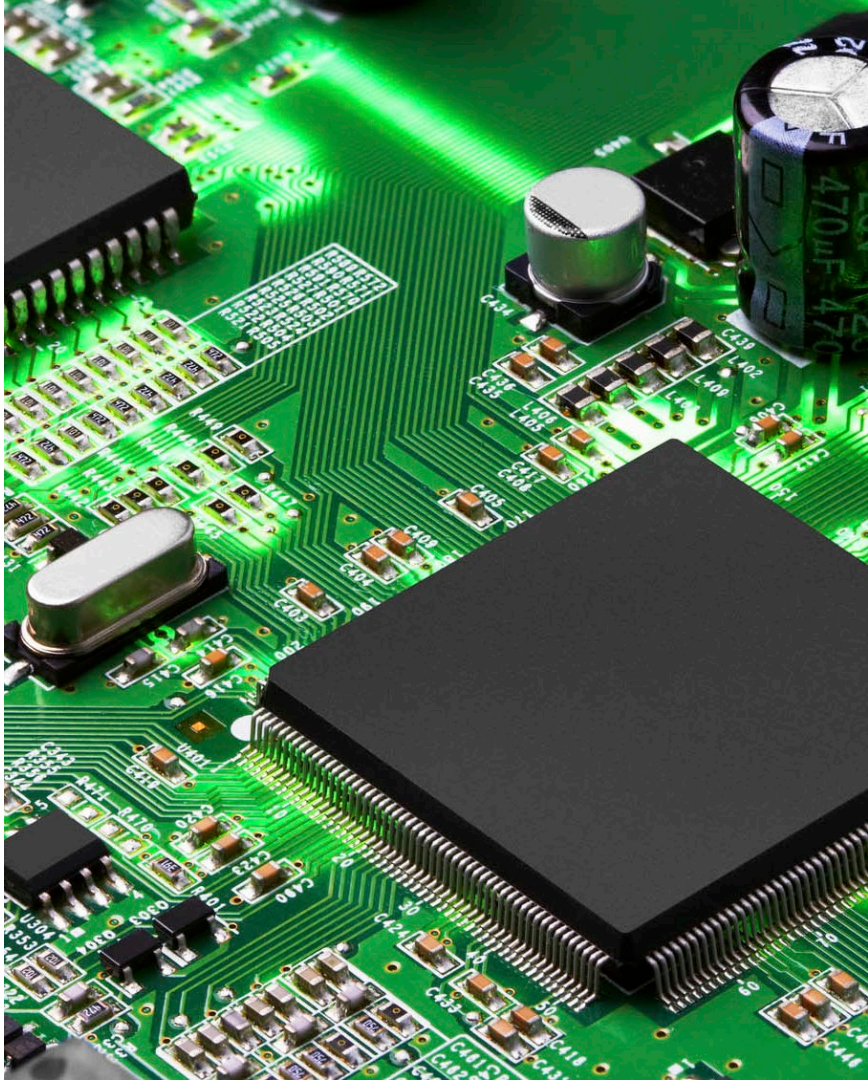
Standards have been developed

WHY??

Use of Electronics and Software

Emergence of Functional Safety is linked to the increased use of electronics and software, which are being used more often because:

- Lower costs
- Design flexibility
- Ease of reuse
- Less space
- Improved efficiency
- Greater functionality



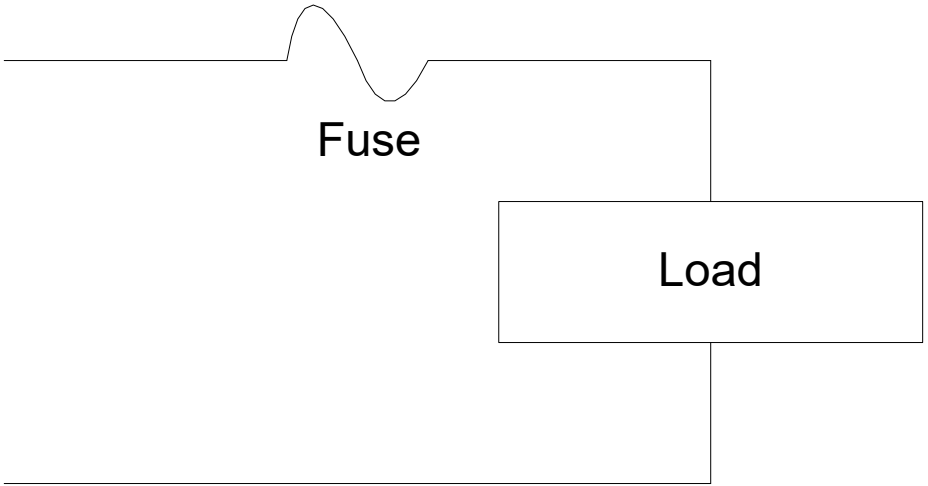
In the Past…

Example:

Overcurrent protection

In the past:

- Provided by electromechanical device, e.g. fuse
- Reliability of device could be sufficiently determined through a prescriptive test program (e.g. UL 248 for fuses)



…Now and in the Future

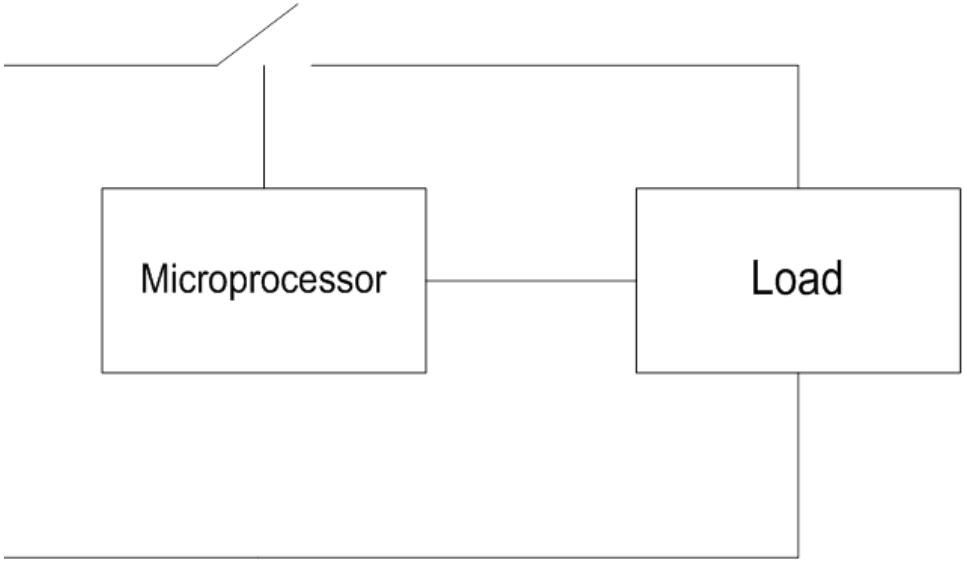
Example:

Overcurrent protection

Now and in the future:

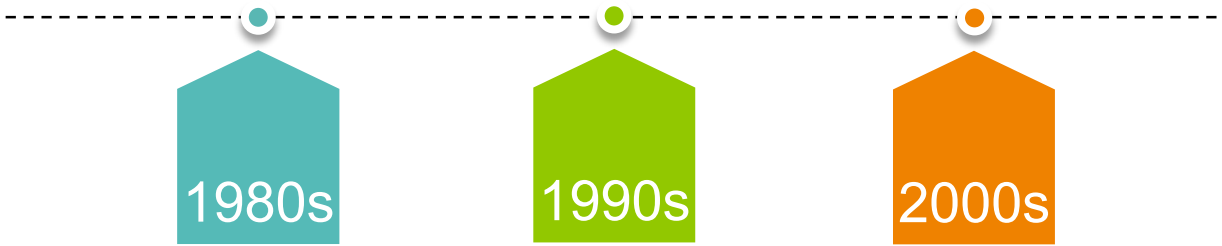
- Provided by complex electronics and/or software
- The question then becomes:

  How do you determine if electronics and/or software are reliable?



The Emergence of Functional Safety Standards

As a result, many functional safety standards have emerged over the past several decades



How is Functional Safety assessed?

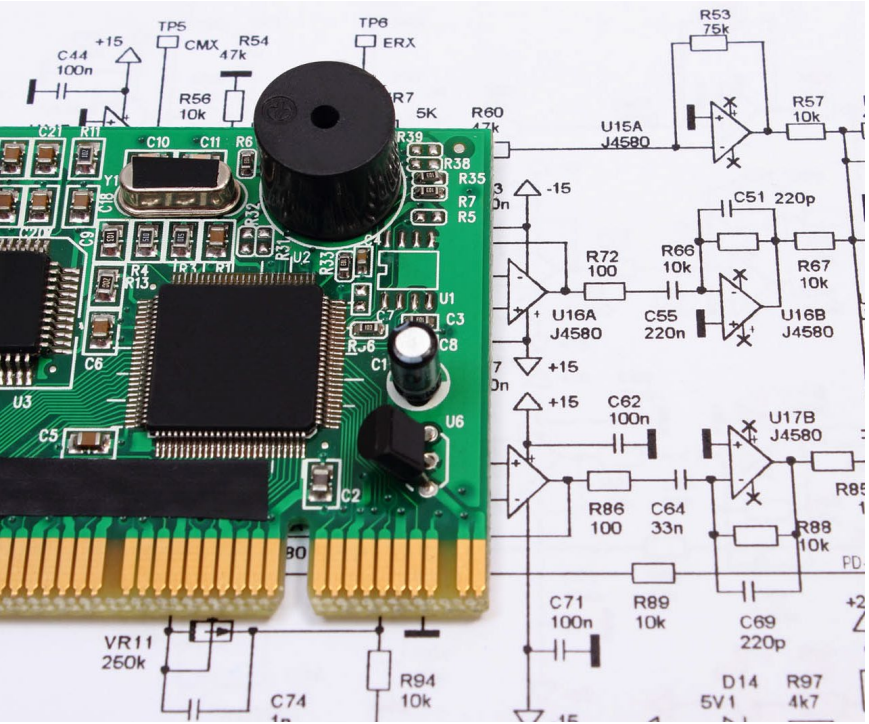
Hazard and risk assessment

Hazard and risk assessment conducted by manufacturer to identify hazards and how they have been addressed by various design elements of the system including by Functional Safety; typical types of hazard and risk assessments include:

- Failure Mode and Effects Analysis (FMEA)
- Fault Tree Analysis (FTA)

Item/Function / Failure Mode	Potential Effects of Failure	Severity	Potential Causes/ Mechanisms of Failure	Occurrenc	Current Design Controls	Detectior	RPN (Note3)	Recommended Actions
Battery cell - overcharge	Thermal overload, venting, leakage	10	Imbalance, charger fault, abuse from customerUnbalanced SOC between cells or charger fault, customer abuse	7	Internal cell protection	7	490	Add overvoltage protection in BMS
Battery cell - overdischarge	Thermal overload, venting, leakage	10	Faulty load, abuse from customer	4	Internal cell protection	7	280	Add undervoltage protection in BMS, overload/short circuit protection in BMS

Hardware assessment



With respect to the safety functions identified in the hazard and risk assessment, the hardware is assessed to ensure that it has a sufficient combination of:

- Redundancies
- Fail-safe techniques (built-in self-tests, diagnostics, etc.)
- Reliable components

This ensures that the safety functions will work when needed the most, and that random hardware failures will not cause a risk of a hazard occurring

Environmental stress tests

Electronics undergo a series of environmental stress tests (UL 991 test program shown to the left as an example)

Safety functions are verified for correct operation before, during, and after each of the environmental stresses

Only if the safety function still works correctly, or the product has transitioned to a safe state, are the test results considered to be compliant

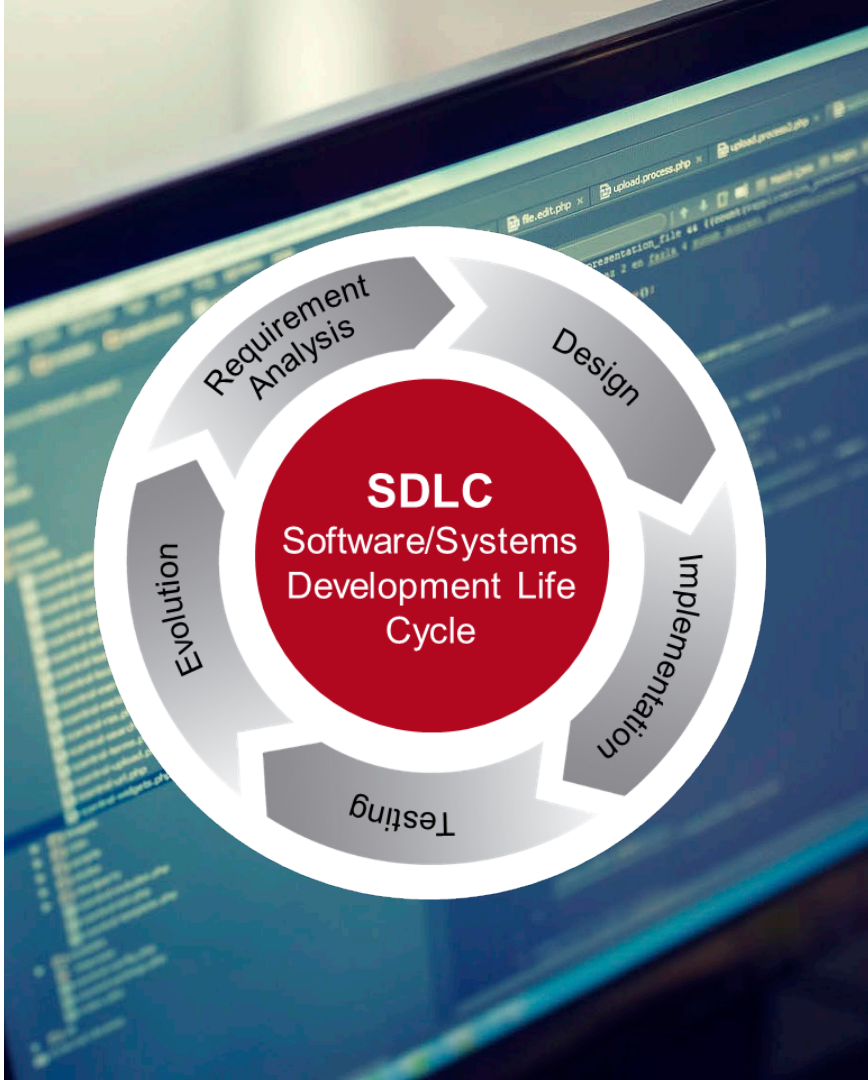
UL 991
Operational Verification (9)
Overvoltage and Undervoltage (10)
Power Supply Voltage Dips and Short Interruptions (11)
Transient Overvoltage Test (12)
Voltage Variation (13)
Electromagnetic Susceptibility (14)
Electrostatic Discharge Test (15)
Composite Operational and Thermal Cycling (16)
Effects of Shipping and Storage (17)
Thermal Cycling (18)
Humidity (19)
Dust (20)
Vibration (21)
Jarring (22)

Software assessment

To reduce/eliminate software bugs and defects, software developer shall follow documented, formal processes to develop their software, i.e. use a software development life cycle

Includes phases for:

- Software risk analysis
- Defining and documenting requirements
- Planning the software architecture and design
- Implementation, including use of coding standards
- Analyzing, debugging, and testing software
- Software release, and changes/maintenance to software



Functional Safety ensures:

- Hazards and risks of the product are identified and addressed
- Hardware is sufficiently reliable
- Electronics are not susceptible to adverse environmental conditions
- Software is free of bugs and defects

Functional Safety ensures that the product will operate safely

Questions?