MAY 25, 2022

Functional Safety in Energy Storage

Layne Lueckemeyer

Business Manager, Functional Safety

About the Speakers

Layne Lueckemeyer, Global Functional Safety Business Manager for CSA Group is a leading global compliance professional with more than two decades of experience in consultative sales leadership, helping customers understand worldwide Functional Safety, EMC/EMI, Wireless, Environmental, Reliability, Product Safety, Machinery Safety, and Hazardous Locations testing and certification requirements.

Jody Leber, Global Energy Storage Business Manager for CSA Group is an International Compliance Professional with 30 years of experience in the industry. His specialties include Battery, Electromagnetic Interference, Electromagnetic Compatibility, Environmental Simulation, Product Safety, and Renewable Energy.

.

Agenda

- Introduction
- Functional Safety – What, Why, and How?
- Functional Safety Standards
- Functional Safety Evaluation

Introduction

As the Energy Storage market continues to grow, manufacturers struggle with the regulatory issues facing them every day. These hurdles can be time-consuming and expensive to overcome. Increased reliance on electronics and embedded software for safety monitoring and critical safety controls drive the need to consider Functional Safety in addition to Electrical Safety requirements.

INSERT DIAGRAM / PICTURE

Challenges for Manufacturers

- Safety Analysis can be complicated and time exhaustive
- Determining which standards are relevant for compliance
- Compliance with electrical safety requirements may not be enough

What is Functional Safety?

- Part of the overall safety concept that depends on a **system** or equipment operating correctly in response to inputs.
- Functional safety is achieved when all the specified safety functions are carried out and the level of performance required of each safety function has been met.
- Functional safety is undertaken by **active systems**.
- Safety achieved by **passive elements** is not considered functional safety.

INSERT DIAGRAM / PICTURE

Hazard & Risk

- A **hazard** is anything that may cause harm
  - "Something with the potential to cause harm"
  - Physical injury or damage to health

- A **risk** is the chance, high or low, that somebody could be harmed by a hazard, plus an indication of how serious the harm could be.

INSERT DIAGRAM / PICTURE

Why is Functional Safety Important?

Example - Battery Management System (BMS)

The BMS monitors

- Voltage
- Current
- Temperature

INSERT PICTURE – Batteries

What happens if the BMS fails?

- Thermal runaway
- Fire
- *Potential for catastrophic consequences*

UL 1973 Batteries for Use in Stationary and Motive Auxiliary Power Applications

Section 7.8 System Safety Analysis

- Hazard Identification
- Risk Analysis
- Risk Evaluation

INSERT DIAGRAM / PICTURE

Analysis Documents

- IEC 60812
- IEC 61025
- MIL-STD 1629A
- IEC 61508
- **Other**

UL 1973 Batteries for Use in Stationary and Motive Auxiliary Power Applications

Minimum Requirements

- Cell Over-Voltage
- Cell Under-Voltage
- Battery Over-Temperature
- Battery Under-Temperature
- Battery Over-Current (Charge)
- Battery Over-Current (Discharge)

General Requirements

- Reliability of Monitoring Components and Systems
- Communications that Affect Safety
- Single Fault Conditions

INSERT DIAGRAM / PICTURE

UL 1973 Batteries for Use in Stationary and Motive Auxiliary Power Applications

Section 7.9 Protective Circuit and Controls

Active protective devices may not be relied upon for critical safety unless they comply with the following:

- IEC 61508 (SIL Level 2 or better)
- ISO 13849 (PL c)
- ISO 26262 (ASIL C)

INSERT DIAGRAM / PICTURE

UL 9540 Energy Storage Systems and Equipment

Section 15 System Safety Analysis

- Hazard Identification
- Risk Analysis
- Risk Evaluation
- Consider Compatibility of System Components

Analysis Documents

- IEC 60812
- IEC 61025
- MIL-STD 882E
- **Other**

INSERT DIAGRAM / PICTURE

UL 9540 Energy Storage Systems and Equipment

Active protective devices may not be relied upon for critical safety unless they comply with the following:

- IEC 61508 (SIL Level 2 or better)
- ISO 13849 (PL c)
- ISO 26262 (ASIL C)

INSERT DIAGRAM / PICTURE

IEC 62619 Secondary cells and batteries containing alkaline or other non-acid electrolytes - Safety requirements for secondary lithium cells and batteries, for use in industrial applications

Section 8 Battery system safety (considering functional safety)

- Hazard Analysis
- Risk Assessment
- Safety Integrity Level (SIL)

INSERT DIAGRAM / PICTURE

Analysis Documents

- IEC 60812
- IEC 61025
- **Other**

IEC 62619 Secondary cells and batteries containing alkaline or other non-acid electrolytes - Safety requirements for secondary lithium cells and batteries, for use in industrial applications

Battery management system (or battery management unit)

Considers Key Factors

- Voltage
- Temperature
- Current

INSERT DIAGRAM / PICTURE

Tests

- Overcharge control of voltage (battery system)
- Overcharge control of current (battery system)
- Overheating control (battery system)

IEC 62933-5-2 Electrical energy storage (EES) systems - Part 5-2: Safety requirements for grid-integrated EES systems - Electrochemical-based systems

Section 6 BESS system risk assessment

Subsystems to consider

- Management (System Controller)
- Communication (Operation Panel)
- Protection (Relays)
- Auxiliary (Fire, Heat, Smoke Detectors)
- Auxiliary Connection (Terminals and Cable)
- Electrochemical Accumulation (Battery)
- Power Conversion (Inverter)
- Primary Connection (Terminals and Cable)
- Others (Building and Infrastructure)

INSERT DIAGRAM / PICTURE

The Need for Functional Safety Standards

Conduct Safety Analysis → Electronics and/or software are used for safety functions → **Requires Functional Safety Evaluation**

- **UL 1973 Stationary Batteries**
  - UL 991
  - UL 1998
  - CSA C22.2 No. 0.8
  - IEC 60730
  - IEC 61508
  - ISO 13849
  - ISO 26262
- **UL 9540 Energy Storage**
  - UL 991
  - UL 1998
  - CSA C22.2 No. 0.8
  - IEC 60730
  - IEC 61508
  - ISO 13849
- **UL 1741 Inverters**
  - UL 991
  - UL 1998
  - CSA C22.2 No. 0.8
  - IEC 60730
  - IEC 61508
  - ISO 13849
- **IEC 62619 Cells & Batteries**
  - IEC 60730
  - IEC 61508
- **IEC 62933-5-2 Grid Integrated EES Systems**
  - IEC 61511
  - IEC 61508

Functional Safety Standards Principles

- **Hazard and Risk Management** – What risks are present in the system?
- **Quality Management** – Are there procedures for managing the lifecycle of the product?
- **Measures to Address Random Failures** – Does the architecture of the control have redundancy? How reliable are the components?
- **Measures to Address Systematic Failures** – Are software procedures in place to eliminate bugs? Can the product withstand EMI and Environmental stresses?

Systematic Faults vs. Random Faults

- **Systematic Faults**
  - Design faults, human error
  - Specification errors
  - Software-related failures, bugs
  - Faults due to environmental stress and EMC/EMI

- **Random Faults**
  - Related to hardware, usage, and wear of components
  - Occurrence is random in nature
  - Average failure rates are usually known or predictable

INSERT DIAGRAM / PICTURE

Comparison of Functional Safety Standards

Systematic vs. Random Faults

	IEC 61508	IEC/UL/CSA 60730-1 Annex H	UL 991 / UL 1998
Functional Safety Rating	Safety Integrity Level (SIL)	Control Class A, B, C	Software Class 1, 2
Systematic Integrity (Addressing Systematic Faults)	Processes, methods, techniques required depending on SIL	Processes, methods, techniques required	Processes, methods, techniques required
Architectural Requirements (Addressing Random Faults)	Hardware fault tolerance (HFT)	Single or dual channel depending on Control Class	Single or dual channel depending on Software Class
Fault Detection Requirements (Addressing Random Faults)	Measures and techniques provide diagnostic coverage (Safe Failure Fraction)	Periodic self-test or functional test can be used depending on Control Class	Periodic self-test or functional test can be used depending on Software Class
Reliability (Addressing Random Faults)	SIL achieved by leveraging component failure rates, HFT, and SFF	Qualitative analysis only	Computational or Demonstrated method

Failures Addressed by Functional Safety

- Failure rate of embedded systems over time
- Early failures typically addressed by systematic faults, or faults inherent to the system design
- Random faults of the hardware and microelectronics
- Functional Safety requirements are focused on avoiding/detecting both systematic and random faults

INSERT DIAGRAM / PICTURE

Safety Analysis

Safety Analysis

Hazard and risk assessment conducted by the manufacturer to identify hazards and how they have been mitigated by the design elements. Some common hazard and risk assessment techniques are:

- Failure Mode and Effects Analysis (FMEA)
- Fault Tree Analysis (FTA)
- Guidance for FMEA and FTA methods can be found in IEC 60812, IEC 61025, and MIL-STD 1629A

- Typical Process:
  - Hazard analysis
  - Risk assessment
  - Safety integrity level (SIL) or Performance Level (PL) target

- Examples of hazards that could be identified: EMC, overcharge, over-discharge, overcurrent, overvoltage, over-temperature, etc.

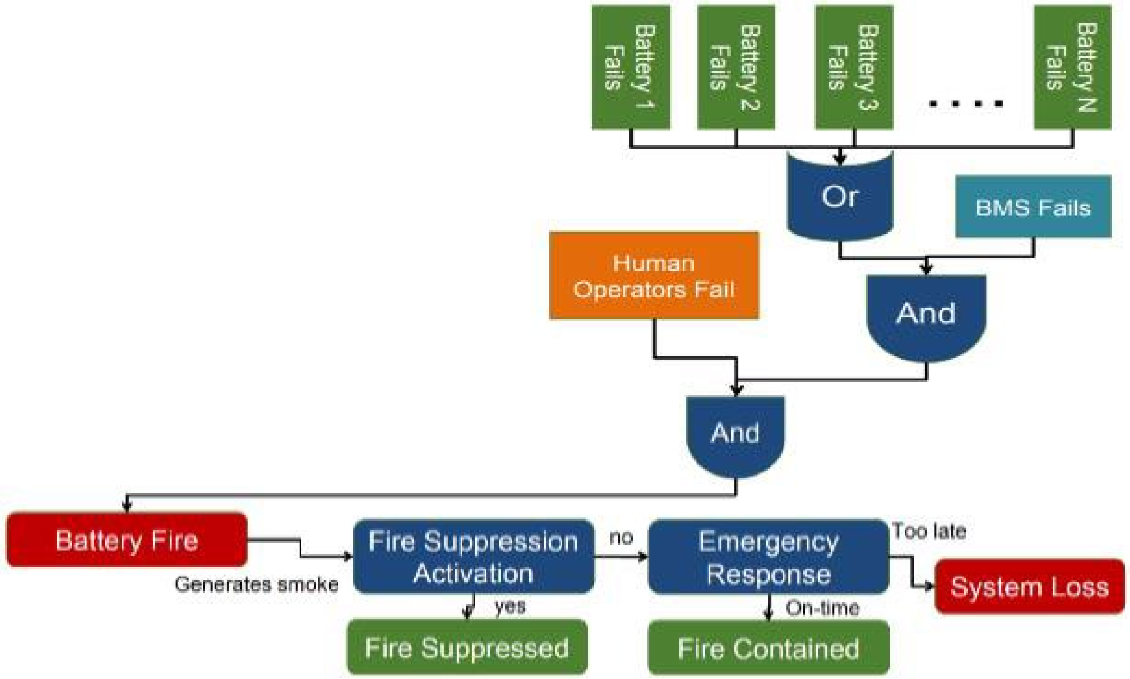
Failure Mode and Effects Analysis (FMEA)

- “Bottom up” approach
- Each component and its failure modes are noted along with the corrective action used in the safety design. Software failure conditions are also listed.
- Note that the FMEA analysis reflects the system view and includes potential failures in any component, safety-related device, or software component.

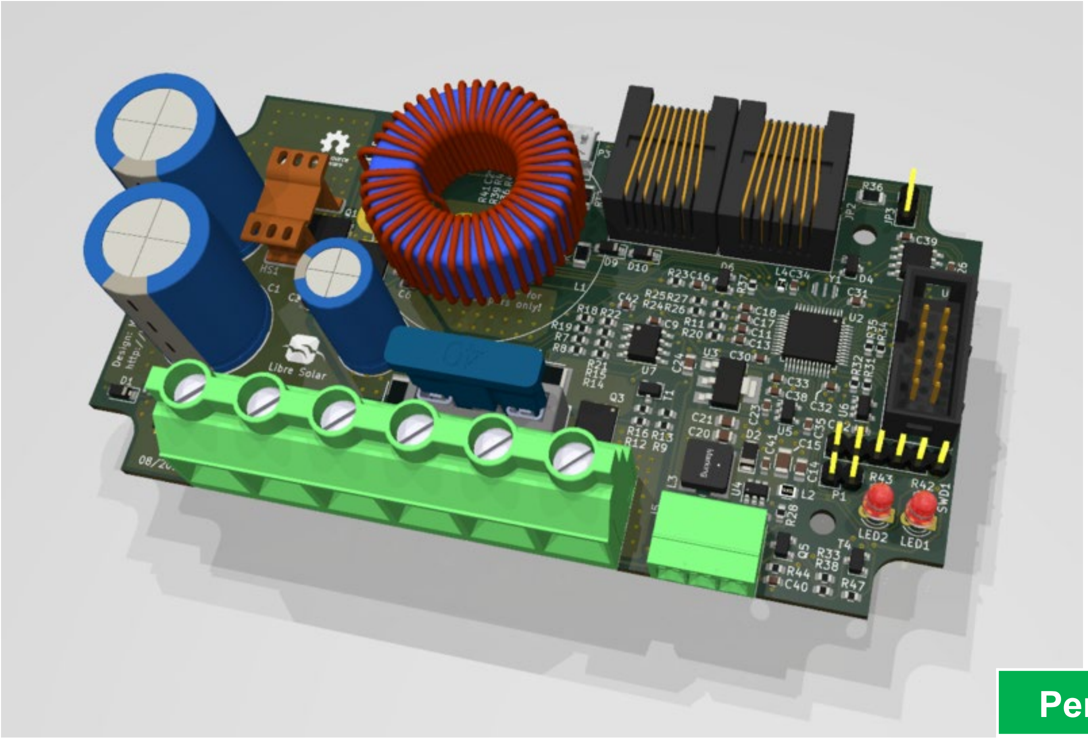
Failure Mode and Effects Analysis				
System	Potential Failure Mode	Potential Effect	Risk Level	Control Mechanism
Battery	Overdischarge	Thermal Runaway	High	BMS Voltage Sensing
Battery	Overcharge	Thermal Runaway	High	BMS Voltage Sensing

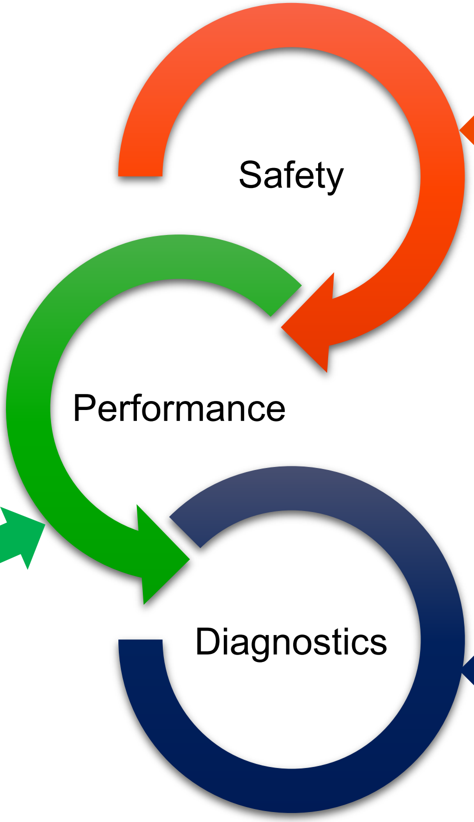
Fault Tree Analysis – (FTA)

- "Top-down" approach where the identified hazard is shown at the top, and where the bottom failure events or "basic events" can no longer be subdivided.
- Technique for reliability and safety analysis that uses logic blocks in a diagram to show graphically the relationship between an identified hazard and each of the potential fault events that could result in that hazard.



Battery Management System (BMS) Example





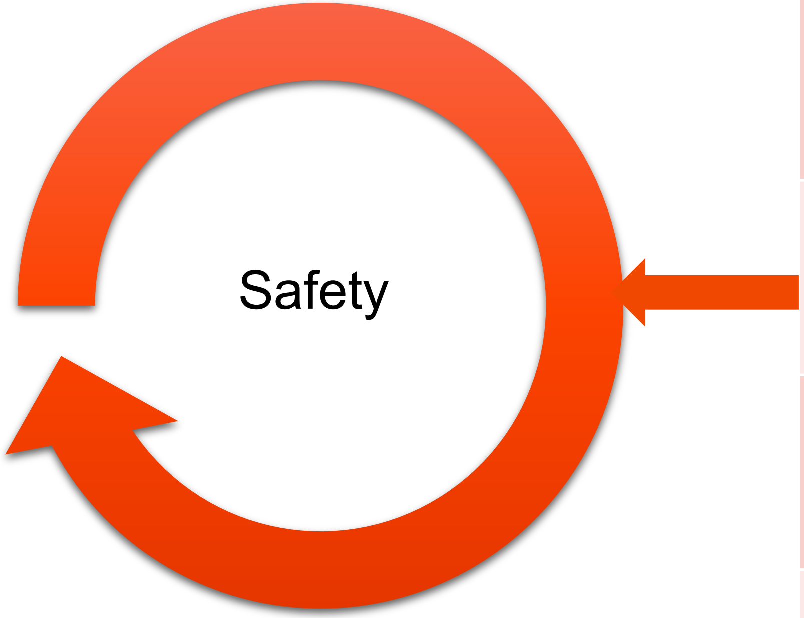
Safety
- Overcharge
- Overdischarge
- Temperature
- Overcurrent
- Short Circuit
- Voltage

Performance
- Current
- Voltage
- Temperature Monitoring
- Cell Balancing
- SOC
- Power Limits

Diagnostics
- Battery State of Health (SOH)

Battery Management System (BMS) Example

- Safety Analysis identifies safety functions reliant on the BMS
- Defines the scope of the Functional Safety evaluation



SAFETY
Overcharge: BMS shall transition battery to a safe state upon detection of a cell voltage > 4.0V
Overdischarge: BMS shall transition battery to a safe state upon detection of a cell voltage < 2.5V
Overtemperature: BMS shall transition battery to a safe state upon detection of a temperature > 60° C
Overcurrent: BMS shall transition battery to a safe state upon detection of a charge/discharge current > 12A

Functional Safety Evaluation

Functional Safety Documentation Requirements

Information Item	Details
Product & Operational description	• System configurations that apply to the certification • Description of all modes of operation
Safety Analysis	• List of 'identified' hazard(s) to be included in the safety design. • Result of Fault Tree analysis • Failure modes for any safety-critical I/O operation (FMEA)
Safety Requirements	• Safety Requirements that apply to the product (combined hardware and software) as derived from the safety functions and from the hazard analysis.
System Architecture and Safety Design	• Functional block diagram • All major equipment components. • Safety design • Fault reaction time(s) • Schematic and wiring diagrams
Software Safety Requirement and Software Design	• List of safety requirements that apply to the software • Details showing how the software design covers all software safety requirements and design requirements from the standard
System Testing	• Test results covering each of the main test areas • Test plan covering all software with test procedures and test cases
Software Development Procedures	• Procedures for software development
Software Tools	• List of software tools

Hardware Assessment

- With respect to the safety functions identified in the hazard and risk assessment, the hardware is assessed to ensure it has a sufficient combination of:
  - Redundancies
  - Fail-safe techniques (built-in self-test, diagnostics, etc.)
  - Reliable components
- This ensures that the safety functions will work when needed most, and random hardware failures will not cause a risk of a hazard occurring

INSERT DIAGRAM / PICTURE

Hardware Assessment

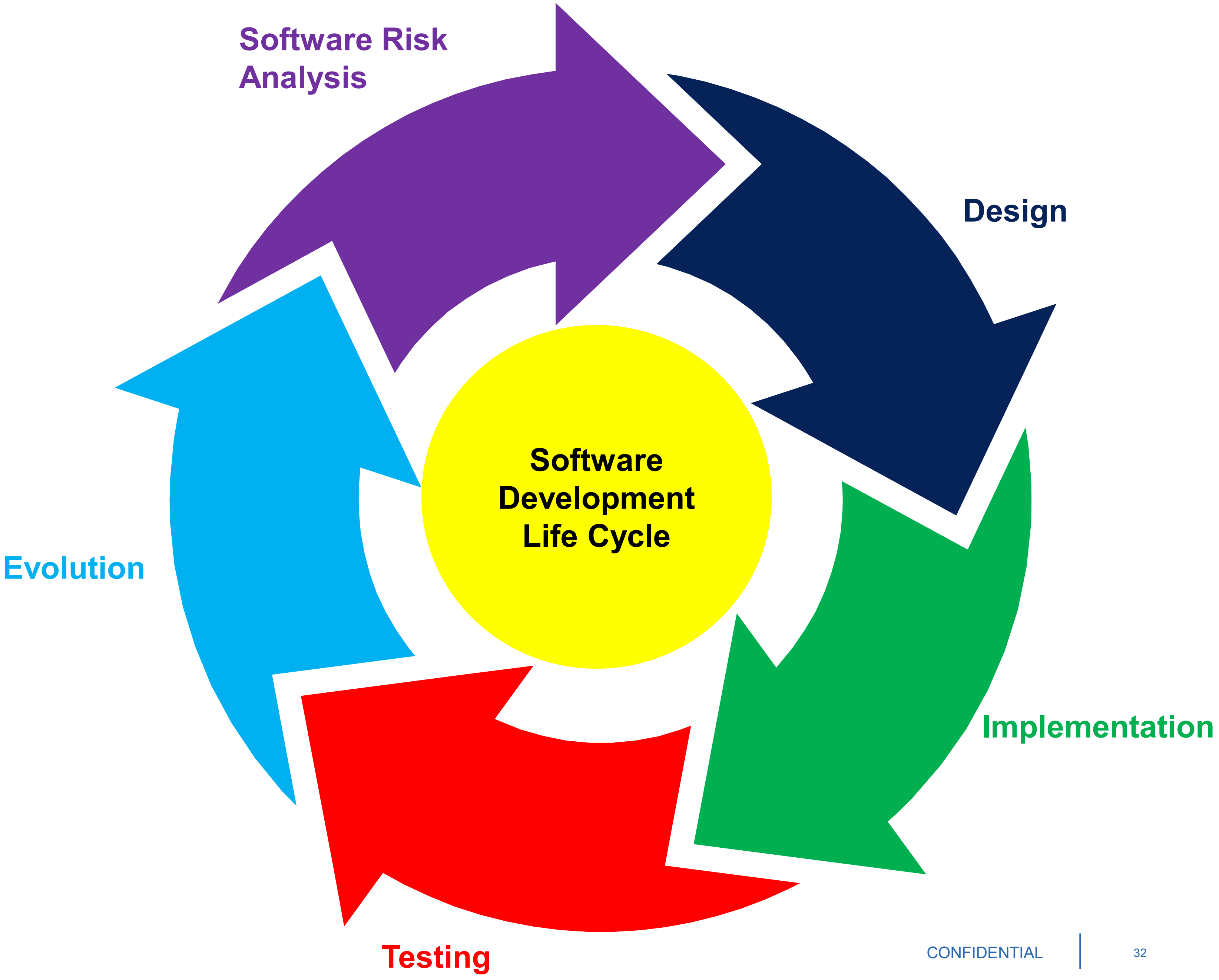
- Environmental Stress Tests
  - Electronics undergo a series of environmental stress tests
  - Safety functions are verified for correct operation before, during, and after each of the environmental stresses
  - Only if the safety function still works correctly, or the product transitions to a safe state, are the test results considered compliant

UL 991 Example Test Plan

Section	Requirement
7	Failure-Mode and Effect Analysis
8	Electrical Supervision
9	Operational Verification
10	Overvoltage and Undervoltage Tests
11	Power Supply Voltage Dips and Short Interruption Test
12	Transient Overvoltage Test
13	Voltage Variation Test
14.2-7	Electrical Fast Transient/Burst Test
14.8	Radiated EMI Test
14.10	Keying Interference Test
15.1-4	Electrostatic Discharge Test
15.5	Electric Field Test
15.6	Magnetic Field Test
16	Composite Operational and Thermal Cycling Test
18	Thermal Cycling Test
19	Humidity Test
20	Dust Test
21	Vibration Test
22	Jarring Test
24	Computational Investigation
26	Power Cycling Tests – General
27	Overload Test
28	Endurance Test

Software Assessment

- Reduce/eliminate software bugs and defects
- Documented formal processes
    - Risk Analysis
    - Defining and documenting requirements
    - Planning software architecture
    - Implementation
    - Analyzing, debugging, and testing
    - Software release, changes/maintenance to software



Product confidence

Functional Safety ensures:

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

Functional Safety ensures the product will operate safely

Summary

- Functional Safety – What, Why, and How?
- When is a Functional Safety evaluation required?
- Safety Analysis
- Hardware Assessment
- Software Assessment
- Remote Software Updates

Questions?

Thank you.

Layne Lueckemeyer
Business Manager, Functional Safety

+1 251 504 8098
Layne.Lueckemeyer@csagroup.org

Jody Leber
Business Manager, Energy Storage

+1 xxxxxx
Jody.Leber@csagroup.org