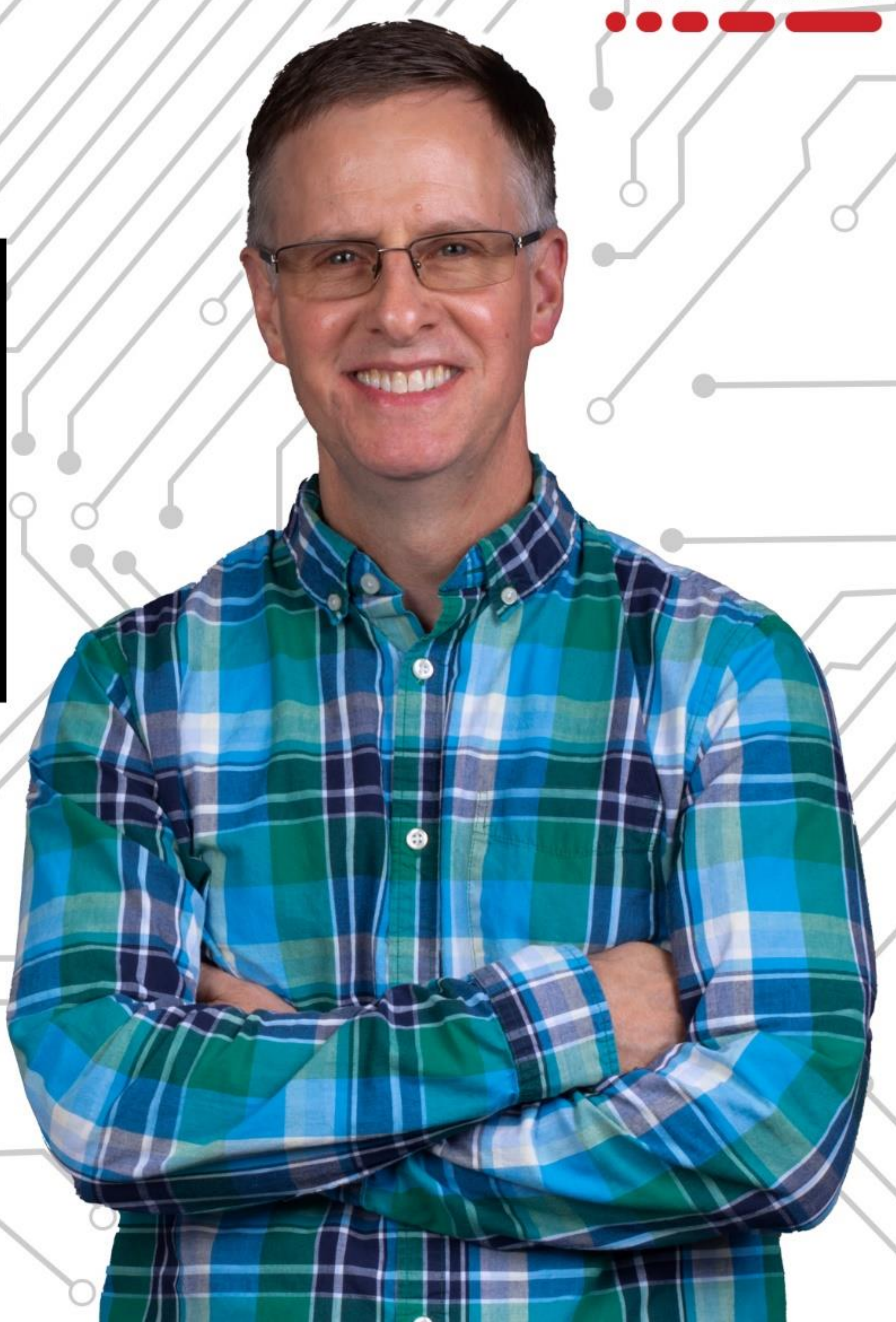
TEXAS INSTRUMENTS

TI POWER

TI *Live!* BATTERY MANAGEMENT SYSTEMS SEMINAR

TERRY SCULLEY

IMPLEMENTING FUNCTIONAL SAFETY SYSTEMS WITH TI'S INDUSTRIAL BATTERY MONITORS AND PROTECTORS



Agenda

- Overview
- Functional safety versus traditional product safety within TI
- TI battery protectors in functional safety systems
- TI industrial battery monitors in functional safety systems

Overview

Implementing functional safety systems with TI’s industrial battery monitors and protectors

- Many industrial battery management products require compliance to functional safety standards.
- Standards compliance often drives the battery management implementation architecture.

- Today we will discuss
  - Functional safety versus traditional product safety within TI
  - TI industrial battery protectors in functional safety systems
  - TI industrial battery monitors in functional safety systems

Functional safety versus traditional product safety within TI

How TI defines types of safety

Comprehensive product safety

Traditional product safety

Relates to electrical shock, fire, mechanical and similar hazards.

Functional safety

Relates to the absence or freedom from unacceptable risk due to hazards caused by malfunctioning behavior of electrical/electric systems; refers to the correct function of a safety-related product.

Functional safety and battery management

- Functional safety in battery management systems is often mandated for compliance to required standards.
- Commonly required standards include:
  - UL 2595 – General requirements for battery-powered appliances
  - IEC 60335 – Household and similar electrical appliances
  - IEC 62841 – Electric motor-operated hand-held tools, transportable tools and lawn and garden machinery
  - ISO 13849 – Safety of machinery

- These standards often cite many others, including IEC 61508 – functional safety of electrical/electronic/programmable electronic safety-related systems.

Functional safety and battery management

- Many facets of system design focus on safety and risk reduction, including physical items such as keyed connectors to avoid incorrect connections, covers or barriers to prevent unintended touching, etc.
- As applied to semiconductor components and software, ***functional safety*** relates to the role these elements play in the correct function of our customers' safety-related systems and end equipment.
- Who is responsible for ***functional safety***?
  - The companies that design and build functional safety systems and applications.
  - However, especially for selected products, TI seeks to help the OEMs and systems developers meet their safety objectives.

Functional safety and TI

- TI has developed collateral for selected products to support customer's compliance to functional safety standards

		Functional Safety-Capable	Functional Safety Quality-Managed*	Functional Safety-Compliant*
Development process	TI quality-managed process	✔	✔	✔
	TI functional safety process			✔
Analysis report	Functional safety FIT rate calculation	✔	✔	✔
	Failure mode distribution (FMD) and/or pin FMA**	✔	included in FMEDA	included in FMEDA
	FMEDA		✔	✔
	Fault-tree analysis (FTA)**			✔
Diagnostics description	Functional safety manual		✔	✔
Certification	Functional safety product certificate***			✔

** We are phasing out the "SafeTI" terminology in favor of the three categories outlined in the table above. For products previously labeled SafeTI-26262 or SafeTI-61508, see the Functional Safety-Compliant category. For SafeTI-60730 or SafeTI-QM products, see Functional Safety Quality-Managed.*

*** May only be available for analog power and signal chain products.*

**** Available for select products.*

- See https://www.ti.com/technologies/functional-safety/overview.html

Functional safety and TI

Three categories:

- **Functional Safety - Capable**
  - Low complexity products marketed for functional safety which do not meet all applicable requirements of a functional safety standard. Functional safety information is supplied to help customers evaluate the products for use in functionally safe systems.
- **Functional Safety Quality Managed**
  - Already released products which now have auto/industrial functional safety market opportunities, or new products focusing on other functional safety standards.
- **Functional Safety - Compliant**
  - Products designed and developed to be compliant to key functional safety standards (automotive ISO 26262 and/or industrial IEC 61508) with a targeted safety integrity level (SIL).

Functional safety and battery management

- Most standards have defined levels, such as:
  - Safety integrity level (SIL) level
  - Class
  - Performance level (PL)
  - Category

With each level having specific requirements.

- A common requirement among safety standards is to detect unsafe faults within a system and then mitigate or tolerate the faults to maintain safe operation.

Functional safety and battery management

- For a functional safety system, a set of safety goal assumptions are defined, which could be:
  - Avoiding overcharging any cell beyond the manufacturer’s specification
  - Avoiding charging any cell at a current and temperature exceeding the manufacturer’s specification
  - Avoiding the pack reaching an excessive temperature when used in the expected manner
  - Avoiding fire or explosion when exposed terminals are shorted

Functional safety and battery management

- The system is designed to handle ***abnormal events*** that may occur in practice, such as the shorting of exposed terminals or being placed into an excessive ambient temperature environment.
- When an ***abnormal event*** occurs, this should be detected and the system placed into a ***risk addressed state*** before the system fails in a dangerous manner. Maintaining normal operation is generally not required.
- The ***safety critical functions*** are then identified within the system that facilitate this procedure.
- Functional safety focuses on the malfunctioning of system components (faults or failures) and how they affect the operation of the ***safety critical functions***.

Types of failures in functional safety components

Failures

Random

- Result from random defects inherent to process or usage condition.
- ***All random failures cannot be eliminated;*** focus must be on the detection and handling of random failures in the application.

Systematic

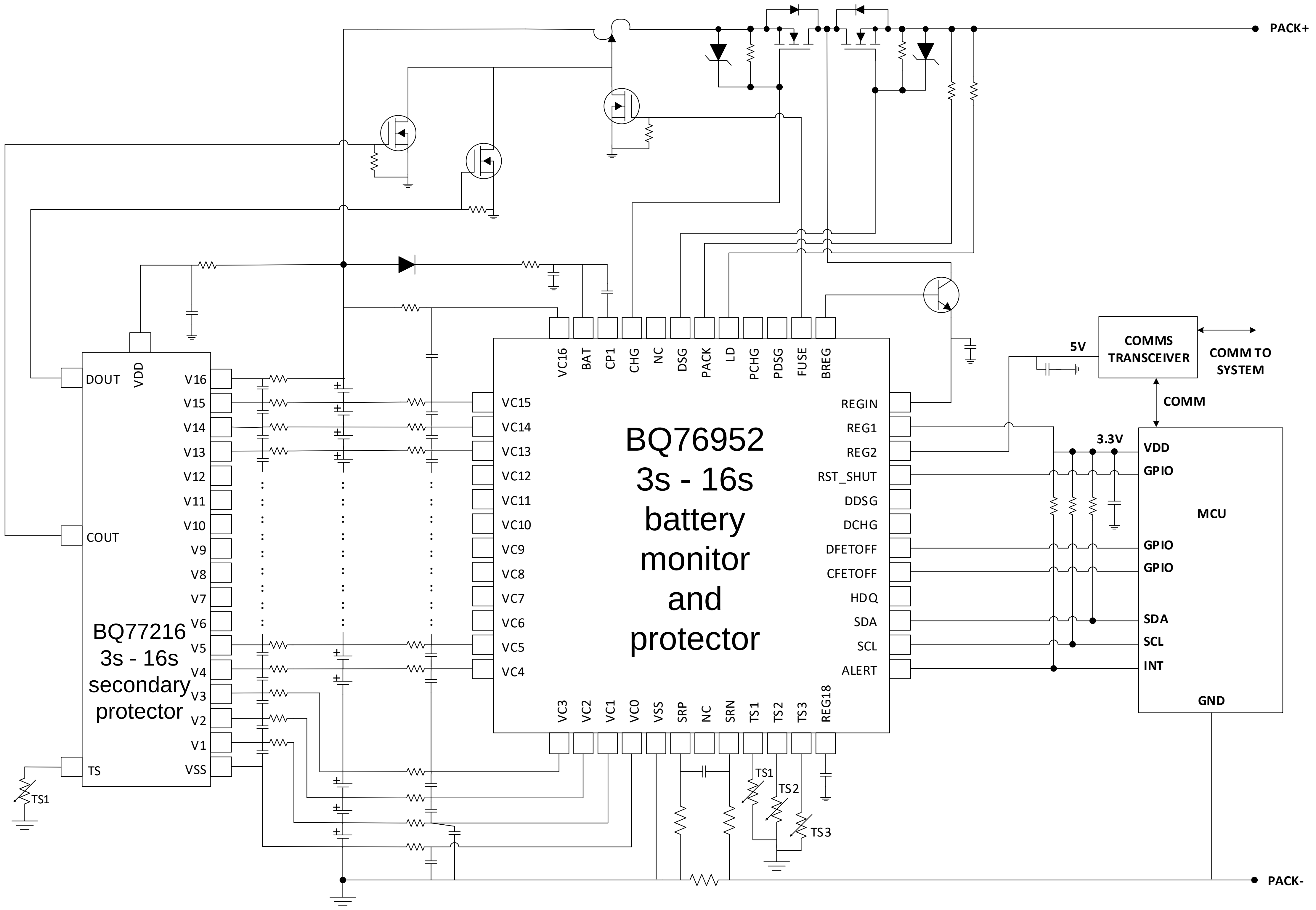
- Result from an inadequacy in the design or manufacturing processes.
- Often due to gaps in the current process & best practices.
- Rate of systematic failures can be reduced through continual and rigorous process improvement.

Functional safety and battery management

- Metrics are defined for failures which consider important factors such as severity and ability to detect their occurrence, as well as a required threshold to help meet the safety goals.
- A common requirement is tolerance of a single point failure, so that a single occurrence or incident of component malfunction does not result in the system failing in a dangerous manner.
- This may lead to needing redundancy in the system implementation, such as needing two separate devices (a primary protector and a secondary protector) checking for cell overvoltage with both independently capable of disabling further charging when the condition is detected.
- Cross-monitoring of redundant subsystems may also be required, so a second failure later in time does not result in a dangerous situation.

Example of redundancy in battery management

- The primary protector in the monitor controls high-side series NFETs, which can take action when an ***abnormal event*** is detected.
- If the primary protector fails to function, the secondary protector can blow the fuse and disable the pack.



TI battery protectors in functional safety systems

Functional safety-capable battery protectors

TI provides the following battery protectors as functional safety-capable:

- BQ7718: 2- to 5-series overvoltage protector family with internal delay timer
- BQ29209-Q1: Automotive voltage protection with automatic cell balance for 2-cell Li-ion batteries
- BQ77904: 3- to 4-series low-power battery protector
- BQ77905: 3- to 5-series Li-ion and Li-phosphate ultra-low-power stackable battery protector
- BQ77915: 3- to 5-series Li-ion and Li-phosphate ultra-low-power stackable battery protector with autonomous cell balancing

Functional safety-capable battery protectors

2 Functional Safety Failure In Time (FIT) Rates

2.1 DPJ Package

This section provides Functional Safety Failure In Time (FIT) rates for the DPJ package of BQ7718 based on two different industry-wide used reliability standards:

- Table 1 provides FIT rates based on IEC TR 62380 / ISO 26262 part 11.
- Table 2 provides FIT rates based on the Siemens Norm SN 29500-2.

Table 1. Component Failure Rates per IEC TR 62380 / ISO 26262 Part 11

FIT IEC TR 62380 / ISO 26262	FIT (Failures Per 10^9 Hours)
Total Component FIT Rate	8
Die FIT Rate	3
Package FIT Rate	5

The failure rate and mission profile information in Table 1 comes from the Reliability data handbook IEC TR 62380 / ISO 26262 part 11:

- Mission Profile: Motor Control from Table 11
- Power dissipation: TBD mW
- Climate type: World-wide Table 8
- Package factor lambda 3 Table 17b
- Substrate Material: FR4
- EOS FIT rate assumed: 0 FIT

Table 2. Component Failure Rates per Siemens Norm SN 29500-2

Table	Category	Reference FIT Rate	Reference Virtual T_J
5	Digital, analog / mixed	25 FIT	55°C

The Reference FIT Rate and Reference Virtual T_J (junction temperature) in Table 2 come from the Siemens Norm SN 29500-2 tables 1 through 5. Failure rates under operating conditions are calculated from the reference failure rate and virtual junction temperature using conversion information in SN 29500-2 section 4.

- TI provides functional safety FIT rate, failure mode distribution information, and pin FMA on these products to assist customers in their system development.

3 Failure Mode Distribution (FMD)

The failure mode distribution estimation for BQ7718 in Table 5 comes from the combination of common failure modes listed in standards such as IEC 61508 and ISO 26262, the ratio of sub-circuit function size and complexity and from best engineering judgment.

The failure modes listed in this section reflect random failure events and do not include failures due to misuse or overstress.

Table 5. Die Failure Modes and Distribution

Failure Modes	Failure Mode Distribution (%)
OUT fails to trip – stuck high	15%
OUT fails to trip – stuck low	15%
OUT open HIZ	5%
OUT functional out of specification timing or threshold	60%
Pin to Pin short any to pins	5%

TI industrial battery monitors in functional safety systems

TI industrial battery monitors

TI offers several battery monitors for industrial applications:

- BQ76925 – 3s to 6s analog output battery monitor.
- BQ769x0 – battery monitor and protector family with low-side NFET drivers.
  - BQ76920 – 3s to 5s
  - BQ76930 – 6s to 10s
  - BQ76940 – 9s to 15s
- BQ769x2 – battery monitor and protector family with high-side NFET drivers.
  - BQ76942 – 3s to 10s
  - BQ769142 – 3s to 14s
  - BQ76952 – 3s to 16s

BQ769x2 3s – 16s battery monitor and protector family

- The BQ769x2 family of battery monitors and protectors integrates a variety of protection features to identify ***abnormal events*** and take action, as well as diagnostics to assist system developers.
- Protection features include:
  - Cell over/undervoltage
  - Safety over/under voltage
  - Short circuit in discharge
  - Overcurrent in charge/discharge
  - Safety overcurrent in charge/discharge
  - Over/under cell temperature in charge/discharge
  - Over/under internal die temperature
  - Over temperature FETs
  - Safety over cell & FET temperature
  - Precharge timeout
  - Cu deposition check
  - Voltage imbalance during active / relax
  - Latching short circuit in discharge
  - Latching cell overvoltage

BQ769x2 3s – 16s battery monitor and protector family

- Diagnostic features are integrated to assist in identification of malfunctions within the device or in the system. These include:
- **Memory Checks**
  - One-time-programmable memory signature check
    - Checked at initial powerup and each full reset
  - Data ROM memory signature check
    - Checked at initial powerup, each full reset, and upon request
  - Instruction ROM memory signature check
    - Checked at initial powerup, each full reset, and upon request
  - Static RAM configuration check
    - Signature of static RAM information checked upon request
  - Saved RAM checksum check
    - A subset of RAM is checked periodically

BQ769x2 3s – 16s battery monitor and protector family

Diagnostic features (continued)

- **Block Checks**
  - Top of stack measurement check
    - Measurement of top-of-stack relative to gnd is measured periodically and compared to the sum of differential cell voltage measurements
  - Voltage reference check
    - Periodic check of one internal reference versus another internal reference.
  - VSS measurement check
    - Periodic check of ADC mux by measuring VSS voltage and comparing to expected result.
  - Protection comparator mux check
    - Periodic check of mux associated with protection comparator subsystem
  - Low frequency oscillator (LFO) check
    - Periodic check of LFO frequency versus a separate hardware detector

BQ769x2 3s – 16s battery monitor and protector family

Diagnostic features (continued)

- **Operational Checks**
  - Data conversion watchdog check
    - Periodic check that internal measurement loop is operating
  - Internal watchdog check
    - Periodic check to detect an internal processing error
  - Host watchdog check
    - Periodic check to detect an external host processor error
  - Serial communication CRC check
    - Check on serial communications to detect errors during communications
  - Second level protector check
    - Periodic check to detect if a secondary protector has triggered a fault

BQ769x2 3s – 16s battery monitor and protector family

- The device also includes capability to use up to 9 pins for either thermistor temperature measurement or as general purpose ADC inputs.
- These pins can be used to digitize other voltages within the system or to implement additional diagnostics, such as measurement of the reference voltage in a microcontroller.

BQ769x2 3s – 16s battery monitor and protector family

- While this product family is not listed under the TI functional safety categories, TI has additional collateral for the BQ76952 which can be provided on request:
  - detailed FMEDA (failure modes, effects, and diagnostic analysis)
  - pin FMEA (failure mode & effects analysis)
  - functional safety manual
  - functional safety analysis report

- Many of the features integrated within the BQ76942 and BQ769142 mirror those in the BQ76952.

TI automotive battery monitors and protectors

TI offers additional families of battery monitors specifically designed for automotive applications with ASIL D compliance to ISO 26262:

- BQ79606A-Q1 – 3s to 6s battery voltage and temperature monitor and protector
- BQ7961x – battery voltage and temperature monitor and protector family
  - BQ79612-Q1 – 6s to 12s
  - BQ76914-Q1 – 6s to 14s
  - BQ79616-Q1 – 6s to 16s
- BQ79656-Q1 – 6s to 16s battery voltage, temperature, and current monitor and protector

Summary

- Many TI products are utilized in functional safety systems implemented by customers.
- TI provides accompanying collateral and documentation on a selection of products, to assist system developers achieving compliance to functional safety standards.
- For more information, see https://www.ti.com/technologies/functional-safety/overview.html or contact TI.