## **EMC For Functional Safety**

Ed Nakauchi Consultant Emulex Corporation

## What is "Functional Safety"

- The correct functioning of an electrical or electronic technology device that provides one or more functions having a direct impact on safety
- Errors or malfunctions could have implications for safety where appropriate EMC engineering is required to control safety risks
- All electrical or electronic technology devices are prone to errors or malfunctions due to EMI

# Why is "Functional Safety" Needed

- Electrical/Electronic devices are increasingly being used in applications where reliable functionality is required
- At the same time, the electromagnetic environment is increasing to higher levels of ambient noise

## **Functional Safety**

- EMI is controlled by the EMC Directive
  - Does not address safety
  - EMC engineers generally do not have a detailed knowledge of safety
- Low Voltage Directive do not address EMC very well if at all
  - Safety engineers generally do not have a detailed knowledge of EMC

## **Standards**

- There are no EMC standards that are suited for achieving functional safety
- There are no safety standards that are suited for EMC functional safety
- IEC 61508
  - Covers EMI functional safety, but offers no specifics
  - Is not a listed under any EU directive
  - IEC 61511 / IEC 62061
- IEC TS 61000-1-2
  - Offers practical recommendations

# **Shortcomings of Existing Immunity**

- Faults and misuse are not addressed
- Real environments are not addressed
- No EMI risk assessment is done
- Physical environment is not considered
- Complex interactions are not considered
- Shortcomings of "Performance Criteria"
- Process applies to entire lifecycle

## **Examples**

- Functional EMC is a system issue and cannot be fashioned by simply combining the reliable items
  - Example
    - Closed loop speed sensor
      - Analog sensor with a magnetic coil sensing a magnetic
      - Comparator to convert "analog" to digital
      - Microprocessor to control speed
      - For high speed, higher rates of pulses and less impact from noise
      - For low speed, lower rate of pulses and more impact from noise
      - Unreliability could be very high at low speeds
    - Pacemaker

## **Examples**

#### - Example of environment change

 In the 1990's analog cellphones were being replaced by digital cellphones. The digital cellphones operated at the same carrier frequency (around 900 MHz) as the analog cellphone, and operated at about the same power level. However, where the analog cellphones did not cause interference to hearing aids, the digital ones did. The difference, and what caused the interference, was the change to digital modulation.

### The Consultant's Oath

If you're not a part of the solution, there's good money to be made in prolonging the problem.

## **EMC Functional Safety Process**

#### • Planning

- Management Responsibilities
  - Procedures
  - Department interfaces and responsibilities
  - Authority
  - Supplier responsibilities
  - Budget and schedule
- Develop an EMC Safety Plan
  - Location / environment / lifecycle
  - What standards or specifications
  - Design guides / training / consulting / testing / documentation

# **Step 1: Determine the environment**

- Determine the worst-case electromagnetic environment that the device could reasonably be exposed to over its expected lifecycle
  - Mobile and portable devices
  - Future technology trends
  - Take into account "uncertainties"
  - EM threats caused by foreseeable misuse
  - Simultaneous threats
  - Effects of transport and storage
  - Use of existing IEC standards (61000-2-5)
  - If unknown, then make an "educated" guess

### Step 1: Determine the environment (cont)

#### - Physical environment

- Could affect filtering, shielding, etc.
- Liquids, molding, sand, dust, cleaning
- Maintenance
  - Opening / closing panels and doors
  - Extended operations of controls
- Perform a site survey

## Step 2: Determine intrasystem environment

- Determine the worst-case electromagnetic environment that the device could reasonably be exposed from other parts of itself
  - Drifting of parameters
  - Aging of components or materials
  - Effect of external environment such as vibration, temperature, humidity, etc.
  - Corrosion
  - Take into account "uncertainties"
  - Effects of transport and storage

## **Step 3: Specify EM vs functional performance**

- Hazard identification
- Uncertainties
- Risk Analysis = Severity \* Probability
  - Initial / Final
  - FMEA (MIL-STD-1629)
  - Criticality Analysis (FMECA)
  - MIL-HDBK-217 Reliability Standard
  - Event Tree
  - Fault Tree
  - Worst-case Analysis

# **Step 4: Study and Design**

- Designing the device to achieve the required level of safety risk or risk reduction
  - Chose suitable hardware and software
  - Communication techniques
    - Detection techniques
    - Correction techniques
    - Optical
  - Use of appropriate design guides and techniques
    - Shielding / separation
    - Filtering
    - PCB design
    - Power distribution
    - Simulation tools

# Step 4: Study and Design (cont.)

- Use of appropriate design guides and techniques
  - Physical techniques (e.g. ventilation, sealing, vibration, thermal, oxidation, etc.)
  - Safety engineering techniques
    - Fuses
    - Effects of component short/open
    - Overvoltage / overcurrent protection
  - Control of suppliers and subcontractors
  - Ensure correct operation, maintenance, repair, and refurbishment
  - Good instructions

# Step 4: Study and Design (cont.)

- Overcome lack of useful product data
  - Protective enclosure
  - Clever design
  - Additional product testing
  - Use a custom product

# Step 4: Study and Design (cont.)

- This is an iterative process since any new design or marketing changes should be reassessed (i.e. it's a living document)
- Do not consider only single fault
  - 10 independent faults that each occurs every 100 years for a particular hazard, so this hazard could occur in 10 years – may still unacceptable!

### Step 5: Create a Verification/Validation Plan

- EMC Testing
- Expert Review
  - Checklists
  - Inspections
  - Reviews
  - Audits
- Non-standardized testing
- Modelling / analysis
- HALT / HAAS

#### FIRST EXAMPLE HAZARD RISK ASSESSMENT MATRIX

HAZARD CATEGORY	(1) (2 CATASTROPHIC CRITICAL		(3) MARGINAL	(4) NEGLIGIBLE	
FREQUENCY					
(A) FREQUENT ( $X > 10^{-1}$ )*	1A	2A	3A	44	
(B) PROBABLE $(10^{-1} > X > 10^{-2})^{\circ}$	18	2B	3B	<b>4</b> B	
(C) OCCASIONAL $(10^{-2} > X > 10^{-3})^4$	10	2C	3C	4C	
(D) REMOTE $(10^{-3} > X > 10^{-6})^{\circ}$	1D	2D	3D	4D	
(E) IMPROBABLE $(10^{-6} > X)^{+}$	1E	2E	ЗE	4E	

\* Example of quantitative criteria

Hazard Risk Index 1A, 1B, 1C, 2A, 2B, 3A 1D, 2C, 2D, 3B, 3C 1E,2E,3D,3E,4A,4B 4C, 4D, 4E

Suggested Criteria Unacceptable Undesirable (MA decision required) Acceptable with review by MA Acceptable without review

#### EXAMPLE DECISION AUTHORITY MATRIX FOR RESIDUAL RISK

HAZARD CATEGORY	CATASTROPHIC	CRITICAL	MARGINAL	NEGLIGIBLE	
FREQUENCY					
FREQUENT	HIGH	нісн	HIGH	MEDIUM	
PROBABLE	PROBABLE HIGH		MEDIUM	LOW	
OCCASIONAL	OCCASIONAL HIGH		MEDIUM	LOW	
REMOTE HIGH		MEDIUM	LOW	LOW	
IMPROBABLE	MEDIUM	LOW	LOW	LOW	

Hazard Risk Level HIGH MEDIUM LOW Decision Authority Service Acquisition Executive Program Executive Officer Program Manager

<b>Probability</b>	Severity						
	e	d	С	b	а		
E	4	4	4	3	3		
D	4	4	3	3	2		
C	4	4	3	2	1		
B	3	4	2	1	1		
A	3	2	1	1 1	1		

#### Interpretation of Risk Index

free states and the second states and the se	
Risk Index	Interpretation
A INTER MILLER	Interpretation
Personal second se	

4	Acceptable only if approved by company management
3	Acceptable if approved by project management
2	Acceptable with design review
1	Acceptable as implemented

**Definitions of Probabilities:** 

- E: Frequent Likely to occur many times per year for each system (e.g., untrained operator errors)
- D: Probable Likely to occur only a few times per year for each system (e.g., trained operator errors)
- C: Occasional Likely to occur less than once every year for each system (e.g., failures of consumable accessories)
- B: Remote Likely to occur less than once in the life of the system (e.g., electromechanical failures)
- A: Extremely Unlikely Never expected to occur in the life of the system (e.g., semiconductor or passive electronics failures)

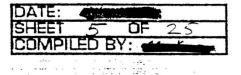
**Definitions of Severity:** 

- e: Catastrophic: May result in death to a typical operator or patient.
- d: Critical: May result in major injury (requiring physician intervention or therapy) to a typical patient or operator.
- c: Marginal: May result in minor injury a typical patient or operator (does not require physician intervention).
- b: Moderate: May result in damage to the system (placing the device out of service), but no injury to a typical patient or operator.
- a: Negligible: May cause minor nuisance to the operator or patient, but no injury or system damage.

SYSTEM:
SUBSYSTEM:
Ref. Dwg.:

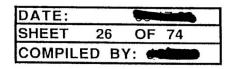
#### FMEA WORKSHEET

. . . . . .



SYSTEM FAILURE HAZARD FAILURE SUBSYSTEM DESIG ID # FUNCTION EFFECT DETECTION CATEGORY REMARKS MODE EFFECT 1031 OPEN 01-32 MTRAØ4 CAT II ERRATIC SA VOI 2U1300 =ØV MOTOR = 5V TEST 1032 01-33 SA: SELF CAT II SLIDECLAMP OPEN ERRONTOUS HIE= TEST FAIL TEST A DETECTION =øv SC SIGNAL TEST = 5V 1033 U1-34 CAT I MTRBØ3 FRRATIC OPEN OCCLUSION SA = ØV MOTOR = 51 01-35 MTRE 04 CATI SA 1034 OPEN DECLUSION ERRATIC = av MOTOR = 5V 01-36 1035 VSS OPEN PFE PS;AA WATCHDOG CAT II SUBSTRATE TEST POWER 01-37 1036 PROGRAM NONE? NOISE ? 2 OPEN MAY BE NONT TEST OPEN 1037 01-38 MTR BHGH CORRENT = ØV SA HULDING ONLY OCCLUSION = 5V NONE ? CURRENT RINTS WRISTED PWR on U1 - 391038 PO WER OFF OPEN POSSIBLE TURN OF PUMP OFF, AA HARDWARE-UZ CATI =ØV PAMO OFF, AA PUMP OFF HARDWARE-UZ CATI TEST PUMP CAN'T =5V CAT I TEST-Try OPERATOR TURN OFF TURN OFF

#### FMEA CRITICALITY



ID #	DESIG	FUNCTION	FAILURE MODE	SYSTEM EFFECT	FAILURE PROBABILITY	SEVERITY	FMEA CRITICALITY
100	NONE	POWER CORD	OPEN GROUND	NO GROUND	0.005	1	0.005
101	NONE	GROUND WIRE	OPEN SOLDER JOINT	NO GROUND	0.004	1	0.004
175	U2	EPROM	BIT ERROR	PROGRAM ERROR	6.00E-04	4	0.0024
185	LED 2	DISPLAY	MISSING SEGMENT	DISPLAY ERROR	0.001	3	0.003
							а.
1. T							

## Conclusion

- Functional safety requires much more than simply asking a test laboratory to perform some standardized tests
- Achieve a required level of confidence in functional safety performance over the anticipated lifetime