Modeling of Digital I&C and Software Common Cause Failures: Lessons Learned from PSAs of TELEPERM® XS-Based Protection System Applications

Robert S. Enzinna, AREVA Inc. (USA)
Dr. Mariana Jockenhövel-Barttfeld, AREVA GmbH (Germany)
Yousef Abusharkhb, AREVA GmbH (Germany)
Hervé Bruneliere, AREVA SAS (France)

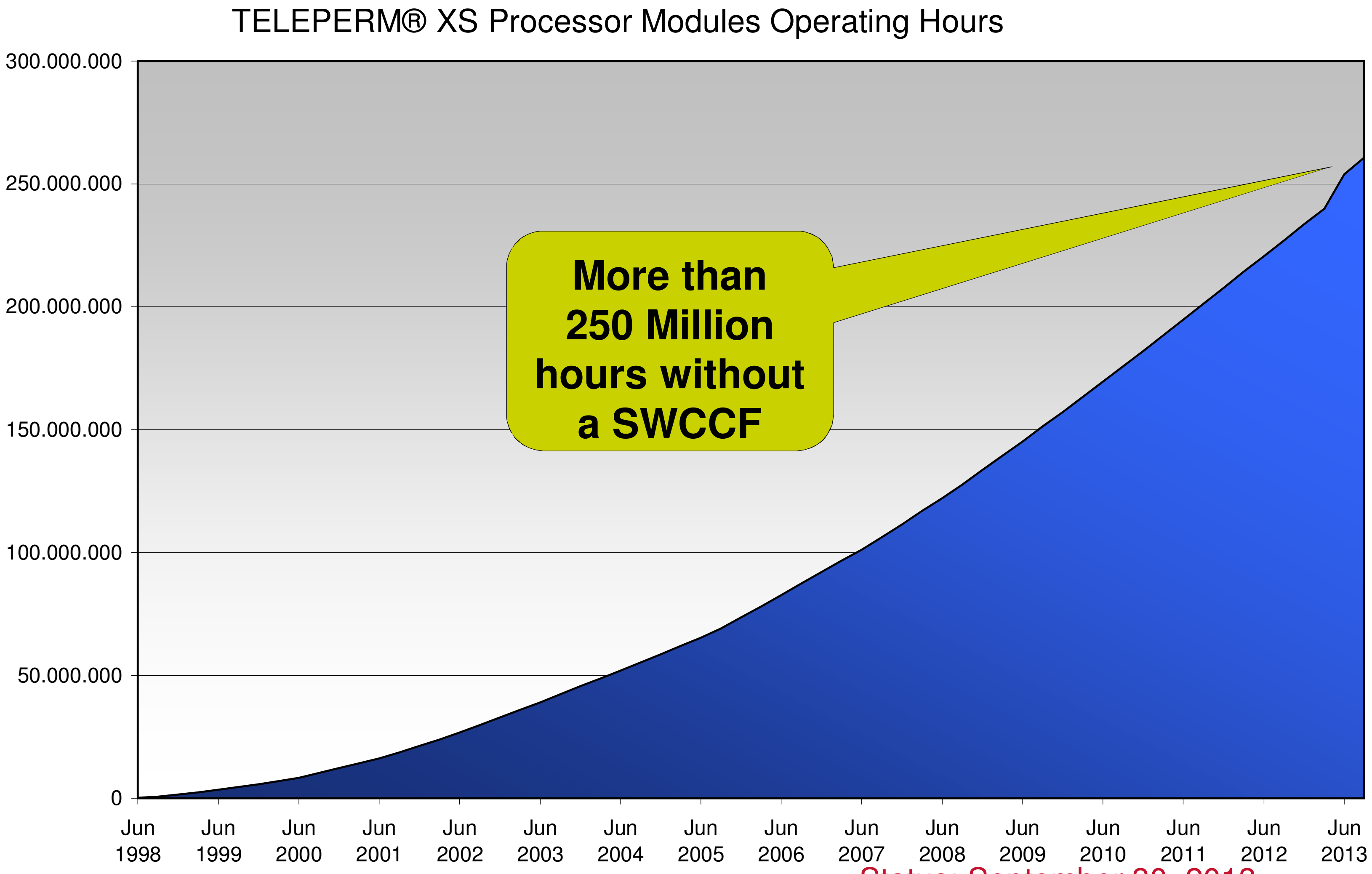
PSAM 12, Honolulu, Hawaii – June 2014

AREVA
forward-looking energy

Basis for Lessons Learned on PSA of Digital I&C

- TELEPERM® XS Operating Experience: 20 years, 60 plants, 11 countries, 10 different reactor designs
- Recent PSA's include new reactor builds in: USA, China, Finland, Brazil, France, UK
- Digital I&C PSA model for digital RPS/ESFAS upgrade in an operating US nuclear plant (Oconee, 2008)
- Extensive library of in-house analyses supporting reliability of the TELEPERM® XS platform (including hardware and software)
- Complete database of TELEPERM® XS field experience
- Involved with various industry groups exploring digital I&C PSA methodology

SWCCF is Rare in a Well-Designed System

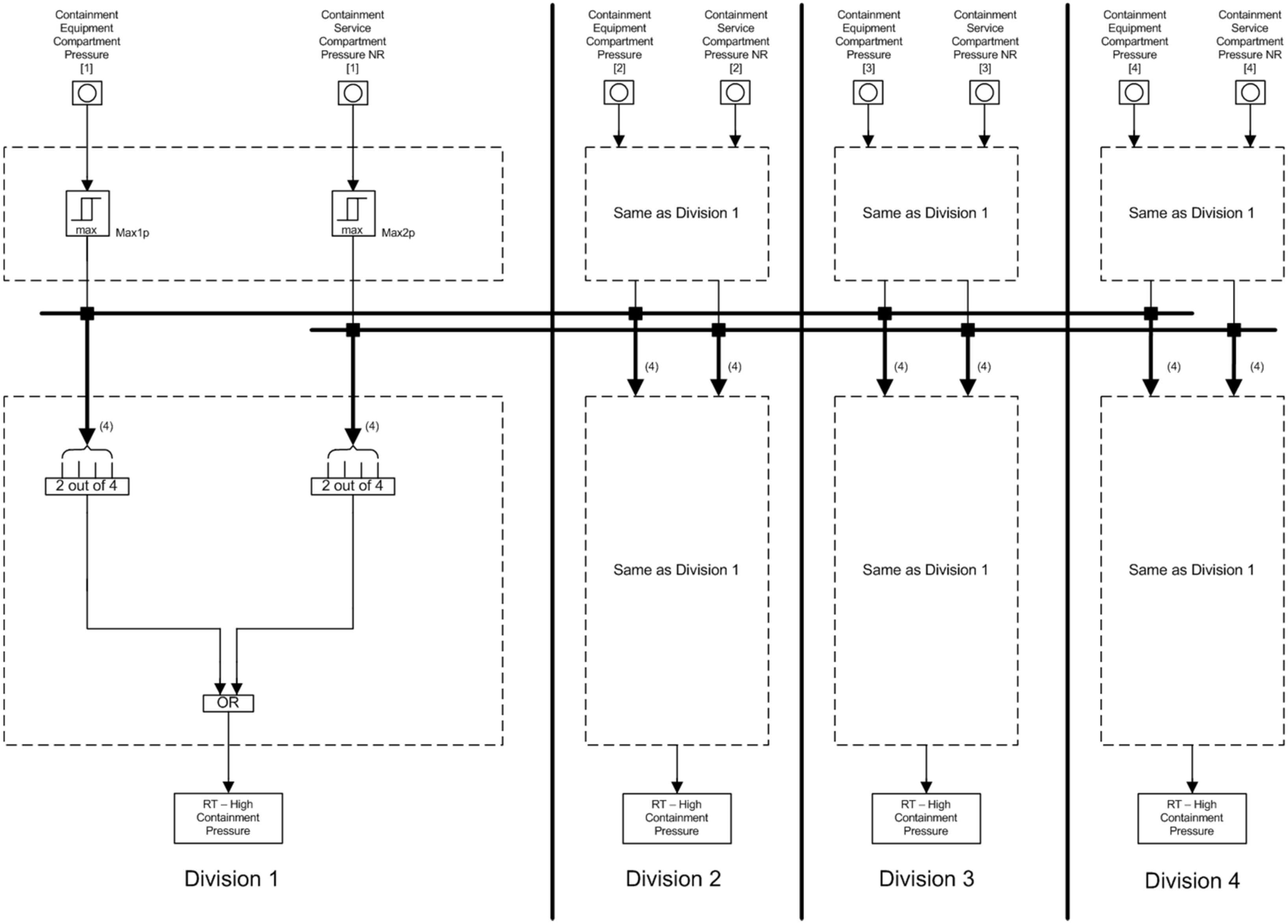


Status: September 30, 2013

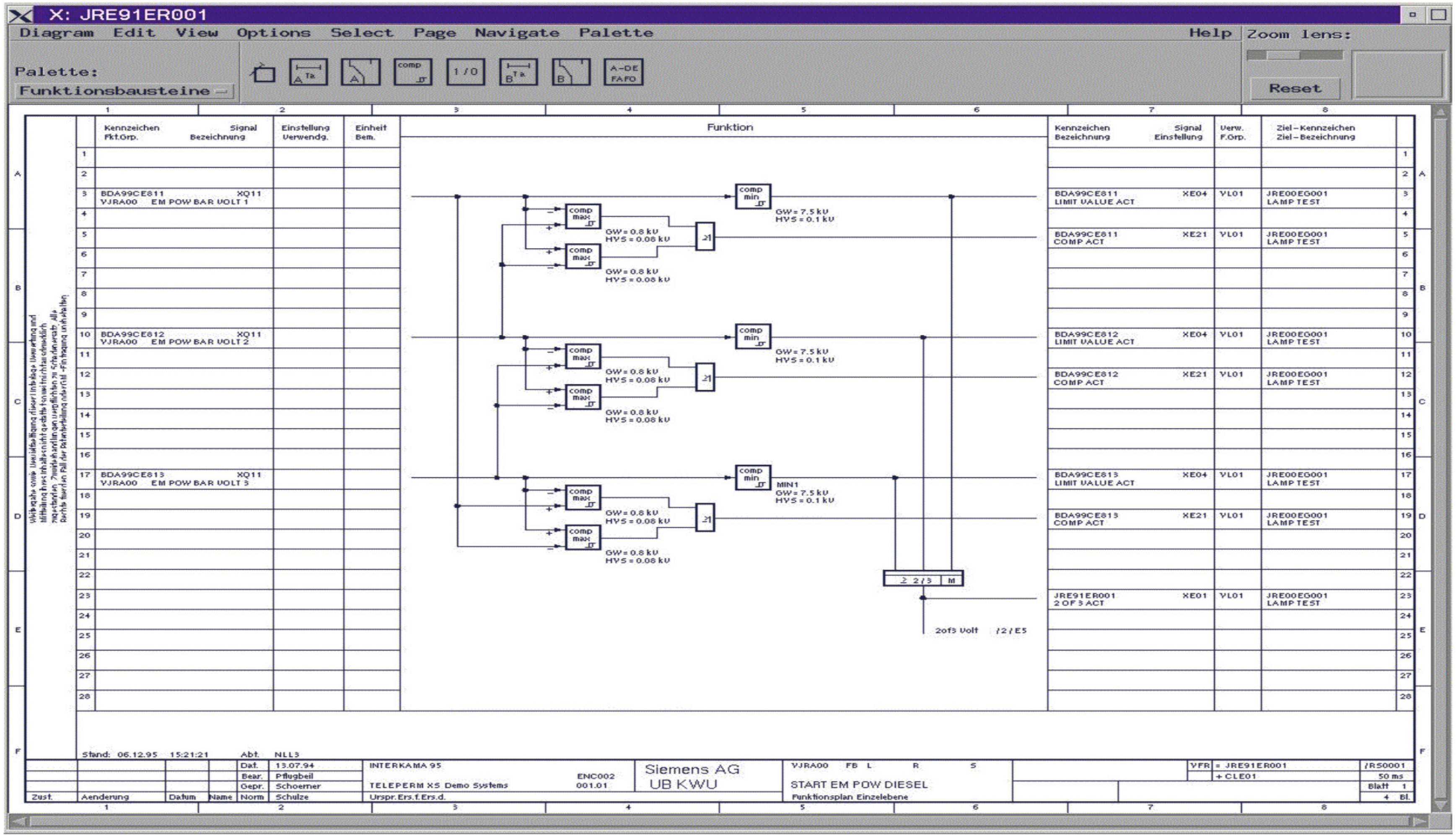
For SWCCF Prevention the Platform/Operating System Design is just as Important as the SW Development

- Dominant causes of application SW failure are latent defects from:
  - Faults in requirements specification
  - Faults introduced in maintenance and update
- Leading causes OS failure in standard computer systems are related to interference from application software:
  - Memory conflicts
  - Special loading (aka Data Storm)
  - OS Complexity
- Primary objectives of TELEPERM ® XS platform design
  - Eliminate known OS failure causes by design
  - Forbid application software failures from interrupting the OS and thus propagating to diverse functions
  - Minimize application SW error with automated code generation

Functional Specification


Containment Equipment Compartment Pressure [1]
Containment Service Compartment Pressure NR [1]
max
Max1p
max
Max2p
(4)
(4)
2 out of 4
2 out of 4
OR
RT – High Containment Pressure
Division 1
Containment Equipment Compartment Pressure [2]
Containment Service Compartment Pressure NR [2]
Same as Division 1
(4)
(4)
Same as Division 1
RT – High Containment Pressure
Division 2
Containment Equipment Compartment Pressure [3]
Containment Service Compartment Pressure NR [3]
Same as Division 1
(4)
(4)
Same as Division 1
RT – High Containment Pressure
Division 3
Containment Equipment Compartment Pressure [4]
Containment Service Compartment Pressure NR [4]
Same as Division 1
(4)
(4)
Same as Division 1
RT – High Containment Pressure
Division 4

Space Diagram



Weitergabe sowie Vervielfältigung dieser Unterlage, Verwertung und Mitteilung ihres Inhalts nicht gestattet, soweit nicht ausdrücklich zugestanden. Zuwiderhandlungen verpflichten zu Schadenersatz. Alle Rechte fuer den Fall der Patenterteilung oder GM-Eintragung vorbehalten.

	Kennzeichen Fkt.Grp.	Signal Bezeichnung	Einstellung Verwendg.	Einheit Bem.
1				
2				
3	BDA99CE811 VJRA00	XQ11 EM POW BAR VOLT 1		
4				
5				
6				
7				
8				
9				
10	BDA99CE812 VJRA00	XQ11 EM POW BAR VOLT 2		
11				
12				
13				
14				
15				
16				
17	BDA99CE813 VJRA00	XQ11 EM POW BAR VOLT 3		
18				
19				
20				
21				
22				
23				
24				
25				
26				
27				
28				

Kennzeichen Bezeichnung	Signal Einstellung	Verw. F.Grp.	Ziel-Kennzeichen Ziel-Bezeichnung	
				1
				2
BDA99CE811 LIMIT VALUE ACT	XE04	VL01	JRE00EG001 LAMP TEST	3
				4
BDA99CE811 COMP ACT	XE21	VL01	JRE00EG001 LAMP TEST	5
				6
				7
				8
				9
BDA99CE812 LIMIT VALUE ACT	XE04	VL01	JRE00EG001 LAMP TEST	10
				11
BDA99CE812 COMP ACT	XE21	VL01	JRE00EG001 LAMP TEST	12
				13
				14
				15
				16
BDA99CE813 LIMIT VALUE ACT	XE04	VL01	JRE00EG001 LAMP TEST	17
				18
BDA99CE813 COMP ACT	XE21	VL01	JRE00EG001 LAMP TEST	19
				20
				21
				22
JRE91ER001 2 OF 3 ACT	XE01	VL01	JRE00EG001 LAMP TEST	23
				24
				25
				26
				27
				28

Stand: 06.12.95 15:21:21 Abt. NLL3

				Dat.	13.07.94	INTERKAMA 95	Siemens AG UB KWU	VJRA00 FB L R S	VFR = JRE91ER001 / RS0001
				Bear.	Pflugbeil	ENC002			+ CLE01 / 50 ms
				Gepr.	Schoerner	TELEPERM XS Demo Systems 001.01		START EM POW DIESEL	Blatt 1
Zust.	Aenderung	Datum	Name	Norm	Schulze	Urspr.Ers.f.Ers.d.		Funktionsplan Einzelebene	4 Bl.

Application SW (Function Block) Execution

- Each FB is executed individually, independently, with no coordination.
- Each and every FB is executed once per cycle. No branching (if, then, else).
- Same path through the application SW every time

- This is known as deterministic program execution

Recognize Features that Minimize CCF of Application SW

TELEPERM ® XS uses four-pronged approach:

1. Defects reduced with high quality software life cycle process
   - Simple Reusable software (function blocks)
   - No custom programing allowed
   - Configuration control (including post delivery)
   - Rigorous V&V, testing
   - Automated code generation tools
2. OS features that minimize failure triggers in signal trajectory
   - Deterministic program execution - one path thru program
   - Asynchronous operation
   - communication with minimal coordination
   - Constant bus loading
3. OS features that minimize failure consequence / propagation
   - Fault-tolerant design
   - Strict separation between system and application SW
   - System interference/interrupt by failed application SW or process is prohibited
   - Prevent application SW failures from propagating to diverse functions
4. Functional diversity
   - is defense for both data trajectory and errors in functional specs.

SWCCF Probability – Recommendation

- Use operating experience for SWCCF of OS/Platform SW
  - Because TELEPERM XS platform has a proven track record
- For application SW, operating experience is helpful to judge the track record of the SW development process.
  - But algorithmic logic and data trajectories are application specific
- PSA needs a SWCCF method that:
  - Considers the application-specific functions
  - And the quality of SW development process
  - Also recognizes the value of CCF defenses in platform design
  - Is realistic and practical to apply

IEC-61508: Functional Safety of Electrical / Electronic / Programmable Electronic Safety-Related Systems

- Hardware safety integrity
- Systemic safety integrity (i.e., software).
- Covers entire SW life cycle:

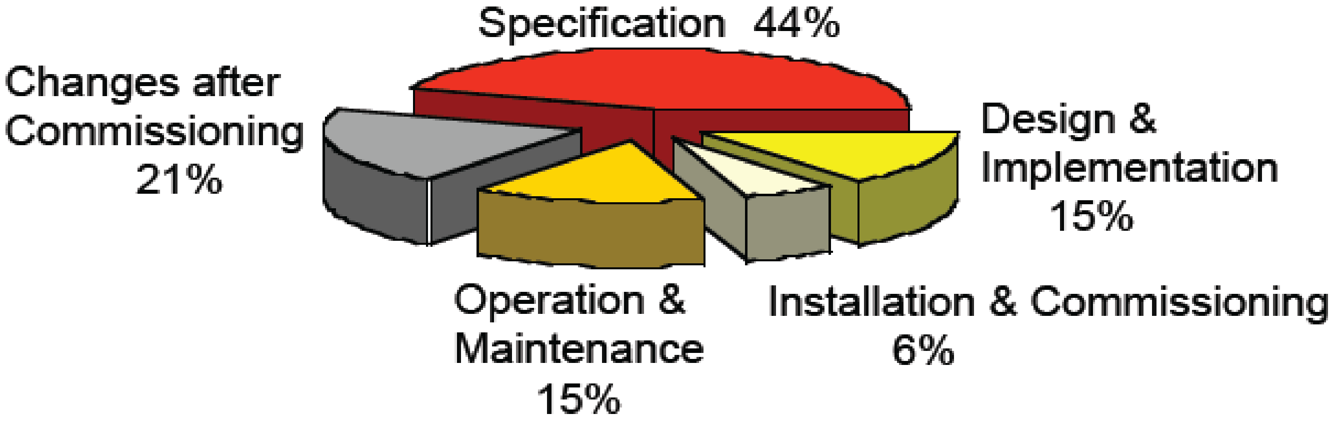


Figure from exida IEC 61508 Overview report 2006

IEC-61508 Allowable Failure Probability

Safety Integrity Level	Probability of Failure on Demand (low demand mode of operation)	Probability of Dangerous Failure per hour (continuous mode of operation)
SIL 4	≥ 10^{-5} to < 10^{-4}	≥ 10^{-9} to < 10^{-8}
SIL 3	≥ 10^{-4} to < 10^{-3}	≥ 10^{-8} to < 10^{-7}
SIL 2	≥ 10^{-3} to < 10^{-2}	≥ 10^{-7} to < 10^{-6}
SIL 1	≥ 10^{-2} to < 10^{-1}	≥ 10^{-6} to < 10^{-5}

- Modify target ranges with “performance shaping factors” such as
  - Complexity of the function
  - Operating experience
- Advantages
  - Relatively simple basis for SWCCF probability in PSA
  - Puts responsibility on design team rather than PSA team
  - Provides opportunity for PSA/design team interaction

Failure Mode Taxonomy is Important

- **Why Taxonomy is Important:**
  - **assess the extent of fault propagation (function, CPU, linked CPUs, subsystem, etc.)**
  - **the effectiveness of defenses**
- **Triggering mechanisms (initiators) of latent faults that have potential of causing a SWCCF:**
  - **Human actions**
  - **Communication faults**
  - **Signal trajectory**
  - **Temporal effects**
- **Examples**
  - **Communication faults affect computers that are linked**
  - **Failure triggered by Signal Trajectory may affect unconnected computers with identical application functions/process parameters**
- **Lack of understanding of the taxonomy – leads to a tendency to prescribe hypothetical failure modes with far reaching effects.**
  - **Masks realistic PSA contributors**
  - **De-values the efforts that design team has put into reducing CCF vulnerability.**

Failure rates for Digital Hardware

- **There is no Substitute for Vendor Failure Rate Data for I&C Modules**
  - New module failure rates derived from part-stress analysis
  - Failure rates for mature modules from operating experience and 95% Chi-squared
  - Cumulative operating experience for TELEPERM® XS modules:

	Processor Modules	I/O Modules	All Platform Modules
Components in Operation	2,672	9,323	47,464
Operating Hours	> 250 Million	> 720 Million	> 3.2 Billion

Final Lesson: Always Remember that the Objective is to Improve the Design

- **Engage the design team for improvement of reliability and SWCCF**
  - SIL
  - Complexity metric
  - Operating Experience / Corrective Action Programs
  - Decision making: Architecture, redundancy, diversity.
- **Fit PSA level of detail to design decision making**
  - Use to drive functional diversity (key attribute for IEC 62340 – Coping with CCF)
  - Architecture (e.g., degree of separation between diversities)
- **Avoid conservative bounding estimates for SWCCF, because this will mask the effect of design counter measures, and may drive the design in directions that are not productive.**