

Experiences in applying IEC 61508 for power plants

**SIPI61508 - Workshops on Safety in the Process Industry -
Tampere, Finland
10th ... 11th June 2003**

**Tapio Nordbo
Enprima Engineering Oy**

Enprima Engineering

New independent engineering and consulting company

A merger of Fortum Engineering and Empower Engineering



Resent SRS projects by Enprima Engineering

- **Tricon V9 of Triconex:**

- Edenderry, Ireland, TMR logic, peat burning CFB boiler
- Braila, Romania, TMR logic, coal, oil, gas burning boiler, 200 MWe
- Esti Power Pant, Estonia, TMR logic, 200 MWe
- Bucharest South, Romania, TMR logic, two oil and gas burning boilers, 2 * 100MWe
- Tychy, Poland, TMR logic, coal fired CHP plant, 70 MWe

- **PLU of Metso Automation :**

- Olomouch, Czech Republic, 1oo2 with HW signals, coal fired CHP, 41MWe
- Kotka, Finland, 1oo2 with HW signals, CCGT CHP plant
- Vanaja, Finland, 1oo2 with HW signals, BFB boiler
- (PLU = 8 input, 4 output rack card with hardwired signals and a non-volatile program)

Resent SIS project by Enprima Engineering Oy

- **HIMA of Paul Hildebradt GmbH:**
 - Vaasan Sähkö, Finland, 1oo1 failsafe logic, oil burning steam boiler
 - Tolkkinen, Finland, 1oo2 failsafe logic, BFB boiler, 16MWe
 - Deva, Romania, 2oo2 failsafe logic (HRS), two coal fired boilers, 210 MWe
 - Härnösand, Sweden, 1oo2 failsafe logic
 - Hammeln, Germany , 1oo2 failsafe logic, BFB boiler, 40 MWe, gas, oil,bio
 - Herbrechtingen, Germany , 1oo2 failsafe logic
 - Kispest, Hungary , 1oo2 failsafe logic with 2* CPU, CCGT plant
 - SCA Edet, Sweden, 1oo2 failsafe logic with 2* CPU

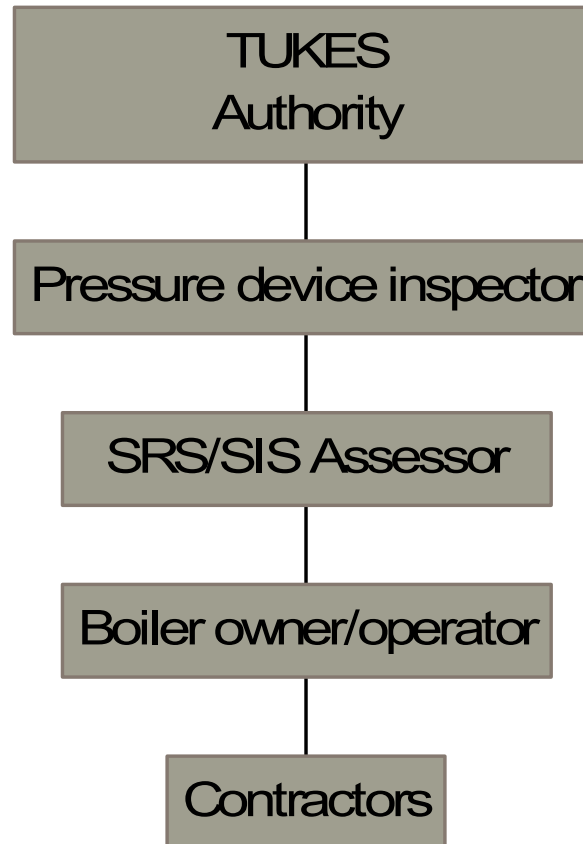
Authority procedures in Finland in boiler area

Assessment of Safety related programmable/electronic controls are obligatory since 1994, professional assessment service provided Inspecta Oy. Harmonized standards (OJ) are accepted by law. IEC 61508/11 is accepted in practise.

Assessment has to be done before the first startup of the boiler or the assessment is included in the CE compatibility assessment. Assessment has to cover both the SRS logic system (product) and the application in question.

Risk estimation of boiler risks has been obligatory since 2001, guideline book 4/2000 of TUKES. The used method is not IEC compatible and will not give the needed SIL number. Method gives the residual risk of an existing boiler while SRS system "ON-LINE". Situation is very confusing.

Hierarchy of boiler SRS/SIS approval



Safety management with Enprima

The company has integrated QEHS system based on ISO9001. The quality system is regularly audited by both internal team and an external body. **Identified items that need improvement are :**

- the focus of HS sector is on site occupational safety (working safety) because the problems are there; more focus on risk estimation and design phases is needed
- with SRS design the frequency of internal audits is not high enough, deviations/improvements are not coming from audits, members of auditing team need more guidance
- identification of components/drawings related to safety is not systematic enough, problems are with the electrical and mechanical (piping, process) sector
- competence of persons are not exactly defined, however it is considered in the assessment procedure

Hazard and risk analysis

Projects teams are now doing the analysis with satisfactory results, scope includes also the balance of plant of the power plant process.

Used method is "analysis of potential problems" with risk classification using "risk graphs". The allocation of functions to systems and layers is done by the same risk estimation team.

Problems found during resent projects:

- **calibration criteria for boiler risks are not accurate, analysis teams have got different SIL levels with same process configuration**
- **understanding of "P" factor (possibility to avoid) has been failed sometimes, "independence" is not understood**
- **identification of safety related alarms has sometimes failed (lack of understanding)**
- **sometimes problems with DCS/SRS allocation or with the shared components**

SIS safety requirement specifications

Functional safety requirements are documented with logic diagrams (boiler protection, boiler purge, burner control)

Integrity requirements are stated as written text

- requirements from the safety manual of SRS logic
- requirements from the IEC 61508/11
- feedback from previous projects, assessors
- also SW requirements stated

No major problems anymore.

SIS design, conceptual

With SIL levels 1 and 2 no actual methods assumed for avoiding "Common cause errors", full 10% beta factor is assumed later in the calculations of PFD

- separation of DCS/SRS required
- some functional diversity, separation and protection with measurements
- diagnostic alarms via DCS (for maintenance)

With SIL level 3, methods to avoid common cause must be used:

- separation in card/rack level, cabling, transmitters
- technology diversity / manufacturing diversity of transmitters
- functional diversity in measurement principles
- separation of safety layers (DCS/SRS/Manual) using IEC61508 method
- protection of equipment / separation of I&C from electrical cables
- beta factor is calculated per safety function

Problems with conceptual design

Not afford for separate rooms/cabinets for logic solvers/separate voting gates (2004 concept with improved safety during maintenance operations)

Customers do not like technology/manufacturing diversity

Safety related alarms

- needed if the manual trip is the only one
- independent methods of alarming operators when SRS failed and DCS is the root cause

Manual backup if SRS fails

- operators can ensure manual local operations within 5 minutes (law in Finland), time is sometimes a problem if location of control room is not "centrally located"

SIS design, HW

Effective in-house tools for IO/cabinet/field cabling developed for SRS HW design => automatic design minimizes human-origin random errors.

Reference material/model documents essential for good results.

Verification: compatibility with requirements can be easily checked, random errors are found with FAT tests.

"Design is successful if the risk estimation and authority procedure is successful."

SIS design, SW

FB-programming with limited variability language happens very fast, most of the blocks come from our SW library.

But verification of the design output takes more time.

- **creating the verification plan (test cases and tables)**
- **testing of library functions with emulator using truth tables**
- **testing of diagnostic measures together with the actual safety function**
- **checking the architecture of the software**
- **checking the references to the functional safety requirements**
- **checking the usage of variables**
- **reading the code by experienced person**
- **testing the software integration using emulator**
- **testing the software with the ON-LINE system with HW IOs (FAT tests)**

Typical SW findings

Human origin:

- Connection from IO to program variable not correct
- Unused variable found
- Inverted measurement range not noted
- Alarm at DCS side not done or understood

Product origin:

- emulator test passed but ON-LINE code could not be translated
- emulator test passed but ON-LINE code caused error
- SRS logic internal diagnostic variable could not be tested/simulate
- application out of available memory

Verification of SIL levels

Verification is used to check that SRS/SIS system will fulfill the integrity requirements. Calculations are done after conceptual design and updated if deviations/new information found during the project.

Method A:

- **Identify all possible faults in SIS system, analyze if covered by diagnostic, make list for proof tests.**
- **Identify all process events that are covered by the SIS system functionality.**
- **make failure logic for the process cause**
- **calculate PFD averages using total failure rates, assume 50% dangerous, assume reasonable DC and beta**
- **sum measurement, logic and actuator PFD values and check against the SIL requirement**
- **check also the failure tolerance of the function**

SIL verification (cont.)

Method B, almost like FMEA:

- itemize all faults of a measurement channel
- analyze possibility of dangerous/non dangerous
- analyze diagnostic coverage for each failure
- analyze common cause possibility for each failure/cause
- combine one channel to single lamda, beta and DC so that the total lamda and beta are reasonable (dangerous/non dangerous ratio may not be 50%)
- calculate the voting gate/failure logic
- rest as with method A

Method B is better for SIL 3 tasks because it covers better the common cause and dangerous/non dangerous analysis.

Analyzing faults of measurement arrangement

Drum pressure measurement													
2003 trip of high pressure													
Appendix 1, page 6													
Failure	Signal	Value	Line signal validation	Median value validation	Weight	Failure rate	Detected	Trip if detected	Fails to safe	Detected with trip	Detected no trip	Undetected	Safe fault
Rootvalve closed	< 4 mA	Low pressure	Detected	Detected	0,1	0,71	100 %	100 %	0 %	0,71	0,00	0,00	0,00
Instr.tube not condensating /leakage	normal	Normal to low	Undetected	Undetected	0,1	0,71	0 %	0 %	100 %	0,00	0,00	0,00	0,71
Tube partial boggage	normal	Delay	Undetected	Possibly	0,2	1,43	40 %	0 %	0 %	0,00	0,57	0,86	0,00
Loop supply voltage is missing	< 4 mA	Low pressure	Detected	Detected	0,1	0,71	100 %	100 %	0 %	0,71	0,00	0,00	0,00
Frozen of instr tube	< 4 mA	Low pressure	Detected	Detected	0,1	0,71	100 %	100 %	0 %	0,71	0,00	0,00	0,00
Loop wire shortcut	> 20 mA	High pressure	Detected	Detected	0,1	0,71	100 %	100 %	100 %	0,00	0,00	0,00	0,71
Loop wire break	< 4 mA	Low pressure	Detected	Detected	0,1	0,71	100 %	100 %	0 %	0,71	0,00	0,00	0,00
Isolator DCS side open circuit	normal	normal	normal	normal	0,05	0,36	100 %	0 %	100 %	0,00	0,00	0,00	0,36
Isolator DCS side short circuit	normal	normal	normal	normal	0,05	0,36	100 %	0 %	100 %	0,00	0,00	0,00	0,36
Isolator voltage missing	< 4 mA	High level	Detected	Detected	0,05	0,36	100 %	100 %	100 %	0,00	0,00	0,00	0,36
Isolator internal mA to normal	normal	normal	Undetected	Possibly	0,05	0,36	40 %	0 %	0 %	0,00	0,14	0,21	0,00
Isolator internal mA out of range	out of mA	out of range	Detected	Detected	0,05	0,36	40 %	0 %	0 %	0,00	0,14	0,21	0,00
Internal transmitter failure to high mA	> 20 mA	High pressure	Detected	Detected	0,07	0,50	100 %	100 %	100 %	0,00	0,00	0,00	0,50
Internal transmitter failure to low mA	< 4 mA	Low pressure	Detected	Detected	0,07	0,50	100 %	100 %	0 %	0,50	0,00	0,00	0,00
Internal transmitter failure to normal mA	normal	normal	Undetected	Possibly	0,07	0,50	42 %	0 %	0 %	0,00	0,21	0,29	0,00
Common mode failure for 2-signals	out of mA	out of range	Detected	Possibly	0,090	0,64	100 %	100 %	50 %	0,32	0,00	0,00	0,32
Common mode failure for 2-signals	normal	normal	Undetected	Possibly	0,049	0,35	50 %	0 %	0 %	0,00	0,18	0,18	0,00
						1,399	10,00						

Calculating PFD average of the measurement arrangement

		Detected with trip	Detected no trip	Undetected	Safe	TOTAL
	Single	3,36	1,07	1,58	3,00	9,01
	Common	0,32	0,18	0,18	0,32	0,99
	TOTAL	3,68	1,24	1,75	3,32	10,00
Beta detected		0,10		Tce	2570,14	
Beta (undetected)		0,10		Tge	1716,1	
L _{DU}		1,75				
L _{DD}		1,24				
L _D		2,99				
MTTR		8				
T1		8760				
PFD _{average} 2003		9,62E-04		Reference: IEC 61508, annex B		
SFF		0,82				
DC		0,74				

Calculating the SRS logic part's PFD

For SRS logic	PFD
Analog input F6217	2,87E-05
V-BG F7553	9,78E-06
CPU	2,94E-05
Binary output F3330	8,18E-06
SUM of PFD	7,61E-05
Value used for further calc.	1,50E-04

Judgement of common cause factor Beta								
Method: IEC 61508-6 annex D								
				Max points		Scored points		
Method to avoid common causes				X	Y	X	Y	
Separate cable routes used			NO	1	2	0	0	
Separate IO cards used			YES	2,5	1,5	2,5	1,5	
Separate indoor cabinets			NO	2,5	0,5	0	0	
Separate measurement physical principles			NO	7,5		0	0	
Mesurement done by different technology/manufacturing			NO	5,5		0	0	
Multichannel MooN, N > M+2			NO	2	0,5	0	0	
Multichannel MooN, N = M+2			NO	1	0,5	0	0	
Channels tested by separate methods and people			NO	1	1	0	0	
Channel maintenance by different people at diff. times			NO	2,5		0	0	
Exchange of information between channels precluded			NO	0,5	0,5	0	0	
Field device types in use > 5 years			NO	1	1	0	0	
More than 5years Experience of same hardware in similiar environm			NO	1,5	1,5	0	0	
Are inputs and outputs protected by overvoltages/current			YES	1,5	0,5	1,5	0,5	
All devices/components conservatively rated			YES	2		2	0	
Has predetermined common causes analysed and eliminated			NO		3	0	0	
Were common causes considered in design review (with feedback			NO		3	0	0	
Are all field failures fully analyzed with feedback to design			YES	0,5	3,5	0,5	3,5	
Is there a written system of work for handling root causes of failures			NO	0,5	1,5	0	0	
Are there a procedure for allowing diagnostic to run before taking n			NO	2	1	0	0	
Relocation of devices forbidden in maintenance procedures			NO	0,5	0,5	0	0	
Are printed-circuit board maintenace at an off-site, qualified repair c			YES	0,5	1,5	0,5	1,5	
Does the system diagnostic report failures to field replaceable modu			NO	1	1	0	0	
Have designers been trained to understand common cause failures			YES	0,5	3	0,5	3	
Have maintainers been trained to understand common cause failures			NO	0,5	4,5	0	0	
Is personal access to fielddevices limited by locks etc.			NO	0,5	2,5	0	0	
Is the system likely to operate always within the tested environment			YES	3	1	3	1	
All all powercables and signal cables separated at all positions			YES	2	1	2	1	
Has the system been tested for immunity to all relevant environment			NO	10	10	0	0	
						12,5	12	
							Z	
							S	
							Sd	
							1	
							24,5	
							37	
					Judgement	Beta Detected	0,1	
					Judgement	Beta undetect.	0,1	

Problems with SIL verification

What is exactly the safety function?

- Risk analysis teams do not identify the functions with sufficient detail so that all failure-logic cases were covered.

Calculations are complicated

- Calculation of the PDF average makes things complicated, if the failure logic is non-trivial, calculation of the safety function at the last day of operational period would make calculations easier.
- manual enumeration of cases run out of human scale

Data availability is limited

- Data from OREDA does not exactly match the needs of SIL calculation
- Data from transmitter manufacturer covers only part of the failure rate (=random internal failure), "certificates" are misleading

Verification of architecture limitations

1) Separation

In Finland the local engineering practice has been that the boiler drum level measurements are analog 2003 measurements but are **shared between DCS and SRS**.

This is generally not allowed by IEC61511 without improving the safety by other methods.

Normally the task is SIL2, so the fault tolerance is fulfilled but the independence of DCS/SRS is not. What are the methods needed for improved safety, what is the criteria for approval?

- tripping of a measurement channel based on diagnostic coverage
- alarming from measurement deviations from median value
- increasing the total SIL from 2 to 3, shorter test period
- maintenance procedures immediate
- avoidance of common cause failures by separation/diversity of transm.

2) Common position needed on "single motor control contactor" at SIL2&3

O&M planning

Plant operators need training to understand SRS philosophy

Four kind of written instructions are needed:

- **administrative instruction**
 - management of safety, handling deviations and high fault rates
 - authorization, work orders, passwords. keys
 - testing periods
 - management of changes, maintaining documents, maintaining separation/diversity
 - life time management
- **test tables with right coverage and methods for periodic proof tests**
- **"how to do it in practise"- instruction for each test task**
- **SW modification and test procedures with test tables**

An Open End Item to be discussed:

A safety PLC is a failsafe 1oo1 logic with double CPUs. Safety is achieved by the internal self testing. Logic has SIL3 certificate if proof test period is 10 years.

What shall the end-user/operator do after 10 years:

- **try to proof test the diagnostic functions using own staff**
- **ask manufacturer to test the logic solver, is service available?**
- **change new hardware every 10 years, original replacements may not be available anymore, redesign needed**
- **if the highest task is SIL2, may the test period be extended to 20 years or 13 years**