Partial Stroke Testing

A.F.M. Prins
Partial Stroke Testing

• PST in a safety related system.

As a supplier we have a responsibility to our clients.

What do they want,
and what do they really need?

I like to explain the concept based on a simple example:

HIPPS
• What is a HIPPS?

HIPPS stands for **High Integrity Pressure Protection System**

A HIPPS is a protection device.

It acts like a fuse;

if the current is too high, the fuse blows.

If the pressure is too high;
the valves close.

The system behind is safe!
A HIPPS is that something NEW?

HIPPS are used for more than 30 years.

And HIPPS are still used, all around the world.

In all kind of applications.
Why a HIPPS?

A HIPPS is, or can be a protection against…

- Human casualties
- Environmental damage
- Damage to your Investments
- Penalties due to emissions (no flaring policy)
- Too high investments….?
When Availability & Integrity Really Count

OCTOBER 16 1997

KINGFISHER ON STREAM EARLY

BY IAIN ESAU

Shell Explo’s innovative North Sea field weeks ahead of schedule and 10% under budget.

KINGFISHER, a high-pressure, high-temperature (HPHT) field lying in block 16/8a with a small extension in 16/6c, has been developed as a subsea tie-back to Marathon’s Bree B platform by an alliance of Shell, McDermott Marine Construction and Kværner FSSL.

To protect the flowlines from high wellhead pressures in the Heather reservoir during the first two or three years of production, Kingfisher incorporates the world’s first subsea high integrity pressure protection system.

Another novel aspect of the project is an intelligent pig developed by RI Services.

Global lines up H&W yard for drillships

To protect the flowlines from high wellhead pressures in the Heather reservoir during the first two or three years of production, Kingfisher incorporates the world’s first subsea high integrity pressure protection system.

Another novel aspect of the project is an intelligent pig developed by RI Services.

Copyright © Yokogawa System Center Europe 2010
SAFETY

A.F.M. Prins
process risk

Residual risk level

Tolerable risk level

Risk inherent in process

SIS

Other

External

Risk reduction

Process

Risk
risk graph

- Extent of damage (S)
  - \(S_1\): Minor injury/damage
  - \(S_2\): Serious injury, death of one person
  - \(S_3\): Death to several persons
  - \(S_4\): Catastrophic consequences

- Frequency of exposure (A)
  - \(A_1\): Seldom
  - \(A_2\): Quite often to permanent

- Avoiding of hazard (G)
  - \(G_1\): Possible
  - \(G_2\): Almost impossible

- Probability of event (W)
  - \(W_1\): High
  - \(W_2\): Low
  - \(W_3\): Very low
From the risk graph a Target SIL for the SIS will result.

The target SIL indicates the maximum average Probability of failure on demand (PFD) the safety system may have.

<table>
<thead>
<tr>
<th>Safety Integrity Level</th>
<th>Average Probability of failure on demand</th>
<th>Safety Availability</th>
<th>Risk Reduction Factor</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>$\geq 10^{-5}$ to $&lt; 10^{-4}$</td>
<td>$&gt; 99.99%$</td>
<td>$&gt; 10,000$</td>
</tr>
<tr>
<td>3</td>
<td>$\geq 10^{-4}$ to $&lt; 10^{-3}$</td>
<td>99.9 - 99.99%</td>
<td>1 000 - 10 000</td>
</tr>
<tr>
<td>2</td>
<td>$\geq 10^{-3}$ to $&lt; 10^{-2}$</td>
<td>99 - 99.9%</td>
<td>100 - 1 000</td>
</tr>
<tr>
<td>1</td>
<td>$\geq 10^{-2}$ to $&lt; 10^{-1}$</td>
<td>90 - 99%</td>
<td>10 - 100</td>
</tr>
<tr>
<td>0</td>
<td>(Control NA)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Industrial standards for safety

- **IEC 61508**
  - Functional safety of electrical/electronic/programmable electronic safety-related systems (E/E/PE)
  - Can be applied to all electro-mechanical systems across a wide range of industries.

- **IEC 61511**
  - Functional safety / Safety Instrumented Systems for the process industry
  - Targeted at end users implementing SIS for the process industry, it has with more emphases towards PROVEN IN USE
# Fault tolerance

## Table 2 — Hardware safety integrity: architectural constraints on type A safety-related subsystems

<table>
<thead>
<tr>
<th>Safe failure fraction</th>
<th>Hardware fault tolerance</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0</td>
</tr>
<tr>
<td>&lt; 60 %</td>
<td>SIL1</td>
</tr>
<tr>
<td>60 % - &lt; 90 %</td>
<td>SIL2</td>
</tr>
<tr>
<td>90 % - &lt; 99 %</td>
<td>SIL3</td>
</tr>
<tr>
<td>&gt; 99 %</td>
<td>SIL3</td>
</tr>
</tbody>
</table>

## Table 3 — Hardware safety integrity: architectural constraints on type B safety-related subsystems

<table>
<thead>
<tr>
<th>Safe failure fraction</th>
<th>Hardware fault tolerance</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0</td>
</tr>
<tr>
<td>&lt; 60 %</td>
<td>not allowed</td>
</tr>
<tr>
<td>60 % - &lt; 90 %</td>
<td>SIL1</td>
</tr>
<tr>
<td>90 % - &lt; 99 %</td>
<td>SIL2</td>
</tr>
<tr>
<td>&gt; 99 %</td>
<td>SIL3</td>
</tr>
</tbody>
</table>

## Table 5 — Minimum hardware fault tolerance of PE logic solvers

<table>
<thead>
<tr>
<th>SIL</th>
<th>Minimum Hardware Fault Tolerance</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>SFF &lt; 60%</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>Special requirements apply - See IEC 61508</td>
</tr>
</tbody>
</table>

## Table 6 — Minimum hardware fault tolerance of sensors and final elements and non-PE logic solvers

<table>
<thead>
<tr>
<th>SIL</th>
<th>Minimum Hardware Fault Tolerance (see clauses 11.4.3 and 11.4.4)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>Special requirements apply - See IEC 61508</td>
</tr>
</tbody>
</table>

**Note 1:** In case of prior use evidence the required hardware fault tolerance as per Table 6 may be decreased by one.

**Note 2:** If wanted Table 2 and 3 of IEC 61508 may be used instead of Table 6
three most significant aspects of IEC 61508

◆ The Safety Lifecycle
◆ The “Pipe-to-Pipe” approach
◆ The quantitative safety assessment
Periodic proof test interval

- Required SIL
  - Periodic proof test interval
    - PFD
      - $10^{-5}$
      - $10^{-4}$
      - $10^{-3}$
      - $10^{-2}$
      - $10^{-1}$
    - Time
      - $T_0$
      - $T_1$
      - $T_2$
      - $T_3$
      - $T_4$
      - Required SIL

Copyright © Yokogawa System Center Europe 2010

A Yokogawa Commitment to Industry

vigilance.
Quantitative Assessment

◆ **Total Loop**
  
The safety requirements concern *(as a minimum)* a complete safety loop and are expressed in Safety Integrity Levels (SIL).

◆ **PFD**
  
The SIL levels correspond to the average Probability of failure on demand (PFD target) of a complete safety loop.

◆ **Quantification**
  
Calculations need to be performed to show that a specific safety loop meets its required SIL level.
Probabilities / Safety Integrity Level

\[ P_{fd_{\text{loop}}} = \text{SIL} = P_{fd_{\text{target}}} \]

\[ P_{fd_{\text{sensors}}} + P_{fd_{\text{logic solver}}} + P_{fd_{\text{final elements}}} \]

SIF Failure Rate Distribution

- Sensors: 30% to 45%
- Logic Solver: 5% to 15%
- Final Elements: 40% to 55%
HIPPS Functionality

A.F.M. Prins
Process parameter range

- **Safety**
  - **Normal Condition**
  - **Alarm Condition**
  - **Unsafe Condition**

- **Control**
  - **Process value**
  - **Operator takes action**
  - **ESD action**

- **Time**
  - **Low level**
  - **High level**
  - **High alarm level**
  - **Trip level**
  - **Mechanical safety level**

- **Boom?**

---

Copyright © Yokogawa System Center Europe 2010

YOKOGAWA
What is a HIPPS

◆ HIPPS, the last line of defense

ProSafe COM / Sequent of event / Alarm handling
Status information / Analogue values
Modbus RS-232, RS-485

Communication to PLC/DCS/SCADA
Modbus

Local SOE recorder

HIPPS

ESD

PSD

DCS

2oo3 manifold

MC-562
AI repeat

4-20 mA

4-20 mA

4-20 mA

Input
DI-511
8-channel

Prog.
Tripamp
AI-917

Prog.
Tripamp
AI-917

Prog.
Tripamp
AI-917

Prog.
Tripamp
AI-917

Analog value discrepancy

Proximity switches, other

Reset, valve test

Alarm Logic

Solenoid
Driver

DO-523
Lamp driver

4 * 5 W Solenoid driver

2oo3

HI PPCS Logic

P

T

4-20 mA

P

T

P

T

Flow direction

HI PPCS valve

HI PPCS valve

HI PPCS solenoid local reset

HI PPCS solenoid local reset

HI PPCS solenoid local reset

HI PPCS solenoid local reset

HI PPCS solenoid local reset
Pressure Transmitter

A.F.M. Prins
TÜV SIL 2 Approved

Certificate

The Certification Body RWTUV Systems GmbH of Product Safety and Medical Devices hereby certify

Yokogawa Electric Corporation
2-4-32 Nakaecho, Musashino-ku
Tokyo, 180-8590 Japan

that the product
Pressure Transmitter

EJX

meets the below mentioned requirement:

IEC 61508: 2000 Part 1 to Part 7
Functional safety of electrical/electronic/programmable
electronic safety-related systems:
Type B:
SIL 2 (single use)

Based on the report No. 701-0677020037 in the said version
This certificate entitles the holder to use the mark

RWTUV

Safety Approved
Transmitters; certified for use in a SIL 2 loop…

3 transmitters meeting SIL 3 … SIL 4 voting 2oo3 or 1oo2.

What is the influence of a common fault…
Triple Manifold
Locking Manifolds

Key controlled procedures in single manifolds.

- Double block and bleed
- Mechanical interlock
- Detection
- SIL approval
LOGIC SOLVER

A.F.M. Prins
Innovation and Continuity

1960
MagLog 3

1970
MagLog 14

1990
MagLog 24

1997
ProSafe-SLS

A PROVEN CONCEPT

COMFORTABLE IN SAFETY
**Magnetic Core**

Rectangular Hysteresis loop

Flat Hysteresis loop

Magnetic particle orientation

Anticlockwise magnetisation

Clockwise magnetisation
“AND” Function

output

“Write”

“Read”

X

&

Y

Z
AND function

X
\[ \text{B-pulse (Clock)} \]

Y
\[ \text{A} \]

\[ +20V \]

\[ 0 \]

B
\[ \text{A-pulse (Clock)} \]

A
\[ \text{Z} \]

Logical 0

Logical 1
HIPPS Valves

A.F.M. Prins
Control of the Valves

- Solenoids
- Actuator
- Valve

CLOSED
Solenoid valve = Normally closed
De-energized situation

OPEN
Solenoid valve = Normally closed
Energized situation
Testing of a Valve

Partial stroke testing

What are we testing?
What do we claim?
Is that safe?

Please note that Partial Stroke test can never replace a full stroke test!!!

Full stroke test
HIPPS Philosophy

Isolate the source of the problem rather than releasing to the atmosphere.

To do so;
High reliable equipment is required!

A failure in your HIPPS will result in damage of equipment or endanger the safety of personnel.
CERTIFICATION

A.F.M. Prins
Wherever you need safety expertise, whether in bid phase, early project involvement, or in project execution … contact a Safety Assurance & Consultancy.
Conclusion

A.F.M. Prins
Conclusion on PST

\[ SFF = \frac{\lambda^{SD} + \lambda^{SU} + \lambda^{DD}}{\lambda^{SD} + \lambda^{SU} + \lambda^{DD} + \lambda^{DU}} \]

Extending the full stroke testing to 3 years at turnaround, and implementing partial stroke testing every 3 months, the PFD\text{avg} is still lower than the original PFD\text{avg} at FST of 1 year without PST.
In general you can say:

A well designed HIPPS, not only saves money but

“makes the world a little safer after all”.
Thank you for your attention.

Commitment means building the future to last.