SAFETY & DEPENDABILITY

Use of probabilistic studies in TOTAL E&P
OUR MAIN ACTIVITIES

- Assist the affiliates and project groups in their studies:
  - General probabilistic studies
  - Production availability studies on production systems
  - SIL studies on safety instrumented systems (HIPS)

- Develop and disseminate the methodology and tools for dependability studies

- Ensure access to reliability data and produce reference data for RAM and HIPS studies
DEFINITION OF “RISK”

Frequency

2 Dimensions

Consequences

Safety

Dependability

Several kinds of Probabilistic studies
SAFETY VERSUS DEPENDABILITY

Safety
- Rare Event
- Big Consequences (Fatalities)
- Safety Authority
- Conservative Estimates

Dependability
- Frequent Events
- Small Consequences (Economical)
- Decision Aid
- Best Estimates
A WHOLE CORPUS OF METHODS AND TOOLS

- FUNCTIONAL ANALYSIS
- PRELIMINARY HAZARD ANALYSIS
- FME(C)A
- HAZOP

Qualitative Analysis
- Understanding how it works
- Risks Identification
- Rough analyses

Static Models
- Structural point of view
- Failure Combinations

Dynamic Models
- In depth Analysis
- Behavioural point of view

- RELIABILITY BLOCK DIAGRAMS
- FAULT TREES
- RELIABILITY NETWORKS

- MARKOVIAN APPROACH
- PETRI NETS & Monte Carlo simulation
- FORMAL LANGUAGES

Safety & Dependability
HIPS
INTRODUCTION

- When inherently safe design or mechanical protection is not possible, additional instrumented protection layers or safeguards must be provided **HIPS**

- **High Integrity Protection System (HIPS):**

  “a Safety Instrumented System (SIS) of high Safety Integrity Level (SIL), implemented as an alternative to industry standards and practices for the protection of production installations.”

- The function of the HIPS is to replace (or reinforce) the ultimate protection barrier
WHAT IS A HIPS?

“Spec Break + non conventional Safety System”:
- Upstream design to the worst possible conditions which may occur
- Downstream de-rating and installation of a Safety system not designed in accordance with conventional E&P Industry Standards → HIPS

First barrier: PT’s activating (E)SDV’s through PSS
Second barrier: PSV’s designed for most hazard scenario’s (at least Blocked Outlet)
Ultimate barrier: 2oo3 PT’s activating HIPS valves through dedicated HIPS logic
SIL PRINCIPLE: IDENTIFICATION OF RISK REDUCTION NEEDED

- Risk Reduction Factor: F1/F2
- HIPS
- Safety Integrity Level: SIL
- 1st Protection layer
- 2nd Protection layer
- 3rd Protection layer
- Risk Without HIPS
- Process Risk
- Dangerous Event Frequencies
- Dangerous Events Consequences
- RRF = 10 to 100
- RRF = 100 to 1000
- RRF = 1000 to 10 000
- RRF > 10 000

Tolerable Risk (target)
SIL CALCULATION: TYPICAL RESULTS

PFDavg over 30 Years = 1.045E-3

<table>
<thead>
<tr>
<th>Required SIL</th>
<th>Calculated SIL</th>
<th>Required RRF</th>
<th>Calculated RRF</th>
<th>Max reachable SIL for sensors (architectural constraints)</th>
<th>Max reachable SIL for actuators (architectural constraints)</th>
<th>Achieved for the SIF</th>
<th>SIL</th>
<th>Conclusion of SIL for the SIF</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>2</td>
<td>500</td>
<td>956</td>
<td>Undefined</td>
<td>Undefined</td>
<td>2</td>
<td>2</td>
<td>Compliant</td>
</tr>
</tbody>
</table>

Remark

Comments

<table>
<thead>
<tr>
<th></th>
<th>PFD Avg</th>
<th>RRF</th>
<th>SIL Computed</th>
<th>Contribution (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sensor(s) Part</td>
<td>3.56E-5</td>
<td>28097.33</td>
<td>4</td>
<td>3.41%</td>
</tr>
<tr>
<td>Solver Part</td>
<td>5.00E-4</td>
<td>2000.00</td>
<td>3</td>
<td>47.85%</td>
</tr>
<tr>
<td>Actuator(s) Part</td>
<td>5.10E-4</td>
<td>1962.13</td>
<td>3</td>
<td>48.77%</td>
</tr>
<tr>
<td>SIF</td>
<td>1.04E-3</td>
<td>956.95</td>
<td>2</td>
<td>100%</td>
</tr>
</tbody>
</table>
**DEFINITION**

*Production availability* is the ratio (expressed as a percentage) of actual production over the production forecast for a given period of time.
BENEFITS

- Quantify the performance (production, injection, flaring,...) of a system over its entire life cycle taking into account all planned and unplanned events,

- Optimize design by comparing the production availability of different architectural options,

- Identify weak points, i.e. those that contribute the most to production shortfalls.

- Conduct sensitivity studies on redundancy (rotating machinery,...), maintenance and inspection policies, the environment (logistics, human resources, flaring restrictions, etc.),

- Provide economic figures for estimating operational costs.
DATA GATHERING
Poor reporting

Gaps Censored Mixed Sparse ...

Without data of good quality, no good results to anticipate

Increasing needs for reliable data

DATA GATHERING

OREDA 1982
Reliability data collected from different worldwide installations

OSTRA 2007
Forum for exchange and development of reliability methods and know-how

WellMaster 1997

Safety & Dependability
Field observations

1. \( \delta_1^1 \), \( \theta_1^1 \), \( \delta_2^1 \), \( \theta_2^1 \), \( \delta_3^1 \)
2. \( \delta_1^2 \), \( \theta_1^2 \), \( \delta_2^2 \), \( \theta_2^2 \), \( \delta_3^2 \)
3. \( \delta_1^3 \), \( \theta_1^3 \), \( \delta_2^3 \), \( \theta_2^3 \)
4. \( \delta_1^n \), \( \theta_1^4 \), \( \delta_2^n \), \( \theta_2^4 \), \( \delta_3^n \)

UPPA – Total study on failure rates estimating procedures in OREDA in case of heterogeneous data

Parameters Estimation \((\lambda, \mu, \ldots)\)
**What is GRIF?**

A systems analysis software for determining the key indicators of dependability: **Reliability – Availability – Performance – Safety.**
Enables to choose the most suitable modelling technique

Includes pre-configured architectures, making modeling all the easier.
<table>
<thead>
<tr>
<th>What is GRIF?</th>
<th>Composition</th>
<th>GRIF in the Total environment</th>
<th>Strong points</th>
<th>Boolean Package</th>
<th>Simulation Package</th>
</tr>
</thead>
</table>

**HIPS (High Integrity Protection System) reliability studies**
- To check that reliability of HIPS (ultimate safety barrier) meets SIL requirements.
- To ensure that the architecture selected and the associated maintenance policy offer an efficient response when faced with the unwanted event.

**PAS (Production Availability Studies)**
- To model the architecture, behavior (failures, interactions, etc) and operating conditions (logistics support, maintenance policies, etc).
- To forecast system’s production level throughout its entire lifecycle.
- To act as a decision-making tool.
What is GRIF?

Composition

GRIF in the Total environment

Strong points

Boolean Package

Simulation Package

Variety and relevance of the methods

High-performance computation engines

Versatility of the models
Availability - Safety
Boolean function assessment and SIL calculations

ALBIZIA
- Exact calculation (instantaneous / average) with BDD
- PFD, PFH, SIL, interval distribution
- Minimal cut sets, Importance Factors
- Automatic Generation of calculation points
- Parameters uncertainties (mean, quantiles)
What is GRIF?

Composition

GRIF in the Total environment

Strong points

Boolean Package

Simulation Package

---

**Fault Tree**

- Fall to close index on LSFI
- Or16
  - And14
    - CCP ESDV3
    - CCP ESDV3 ps
  - Or15
    - Fail to close ESDV3
    - Fail to close ESDV4
  - Or17
    - Fail to close ESDV3
    - Fail to close ESDV4

**Block Diagram**

- OPF1
  - OPF2

---

**Pros**

- Easy to use
- Fast computation and exacts results (analytical approach)

**Cons**

- Hypothesis of independency (Static Model)
- Work/not Work (Boolean States only)
- Limitation of one observation point
Reliability- Availability- Performance

Behavior simulation of dynamic complex systems based on Petri Net

- Prototypes creation
- Interactive simulation

MOCA-RP

- Ultra fast Monte Carlo Simulation
- Temporal, average or time range assessment of any user created indicator
- Statistical estimators (90% CI, standard deviation...)
What is GRIF?

Composition

GRIF in the Total environment

Strong points

Boolean Package

Simulation Package

Enhance Petri Nets

Stochastic Block Diagram

MOCA RP

Pros

- Dynamic Model
- Can handle (almost) every behavior
- Self approximating
- Can manage uncertainty on data

Cons

- Difficulties to cope with low probability events
- Computation time
Any questions?

The end