What is Your SIS Doing When You're Not Watching

Anand Makhija

PAS, Global

Safety Case Symposium 2018 Singapore

Agenda

- Introduction to Process Safety
- Functional Safety Standards
- Independent Protection Layer Assurance
- SIS and Risk Management

Process Safety

- Situation
  - Managing Process Functional Safety and associated Safety Instrumented Systems (SIS) in an industrial hazardous process environment, is typically an intensive manual task consuming valuable skilled resources and providing more value to operations than mere compliance.

- Opportunity
  - Productivity tools are now available to automate, to a large extent, compliance requirements necessary for analysis, reporting, proof testing and verification of plant safety functions.
  - Automating these activities helps with plant availability and reliability whilst minimizing the operational disturbance and resource requirements necessary to perform these tasks
  - Analysis of safety performance information is now possible, enabling improvement actions to be taken.
  - Safety performance information can now be extracted directly into Process Safety Management dashboards

Consequences

2005 BP Texas City Refinery Explosion
1B$ economic loss, 15 people killed

1994 Texaco Milford Haven Refinery Explosion
£ 400M economic loss

- 275 alarms in the 11 minutes before the explosion
- "... warnings of the developing problem were lost in the plethora of instrument alarms triggered in the control room, many of which were unnecessary and registering with increasing frequency, so operators were unable to appreciate what was actually happening ..."

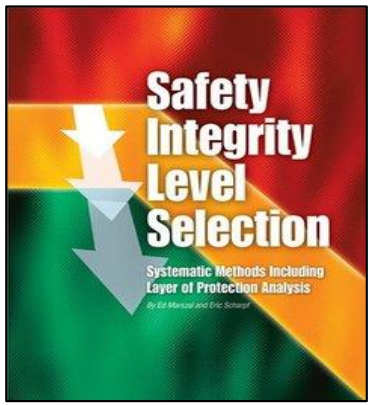
1984 Union Carbide Bhopal Isocynate Plant
Over 3800 people killed

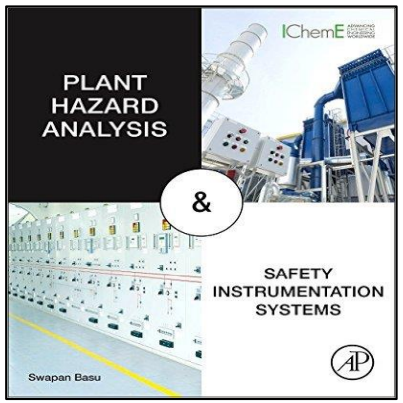
- Few alarms or interlocks in critical locations that might have warned operators of abnormal conditions
- Alarms sounded so many times a week (20 to 30) that no way to know what the siren signified
- Emergency signal was identical to that used for other purposes, including practice drills.
- Alarm at flare tower was non-operational

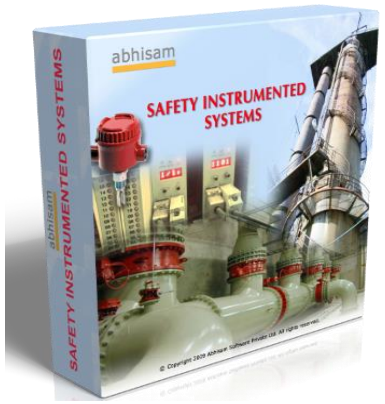
2010 BP Deepwater Horizon Oil Spill:
40B$ in economic loss, 11 people killed

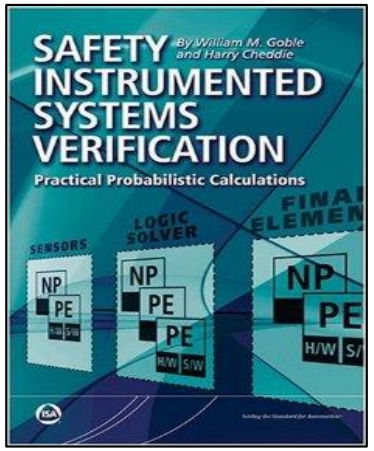
- Vital warning systems on the Deepwater Horizon oil rig were switched off at the time of the explosion in order to spare workers being woken by false alarms, a federal investigation has heard.
- The revelation that alarm systems on the rig at the centre of the disaster were disabled came in testimony by a chief technician working for Transocean, the drilling company that owned the rig

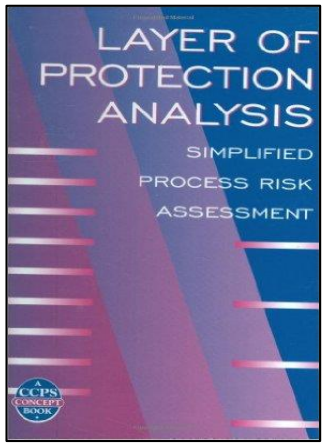
IPL – SIS - SIF – A COMPLEX BODY OF KNOWLEDGE

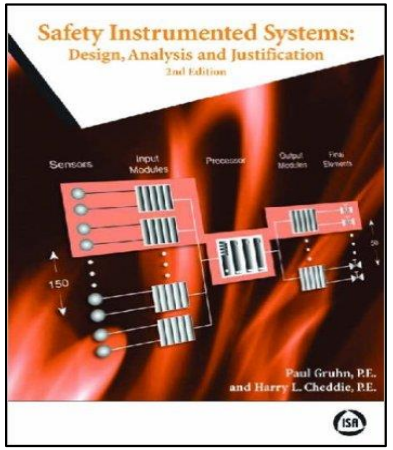


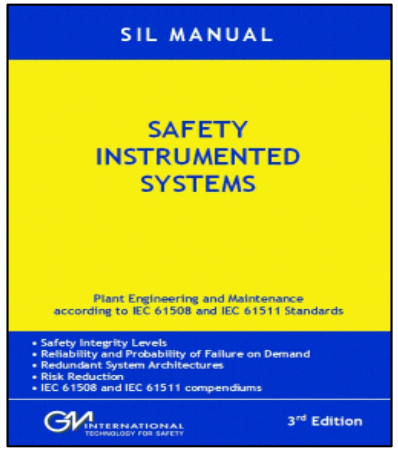












Standards

The Specification, Design, Implementation, Operation, and Maintenance of

- Safety Instrumented Systems **(SISs),** containing
- Safety Instrumented Functions **(SIFs),** as
- Independent Protection Layers **(IPLs)**

are governed by ISA and IEC standards known as the

ANSI-ISA-84.00.01-2004-IEC 61511-1 Functional Safety Series – containing multiple parts.

This is a comprehensive and complex body of knowledge.

Keeping track of a variety of issues mandated by these standards has long been an arduous and error-prone task.

Definitions

Relevant Definitions

Process Safety Event: What SIS-SIL-SIF-IPL is there to prevent!

Safety Instrumented System (SIS):

Hardware and software safety controls on critical process systems

Safety Integrity Level (SIL):

The relative level of risk-reduction needed to mitigate a hazard: SIL-1, 2, 3, and 4, each level requiring different design methods.

Safety Instrumented Function (SIF):

A specific control function used to achieve a SIL. An Emergency Shutdown (ESD) is an example of an SIF.

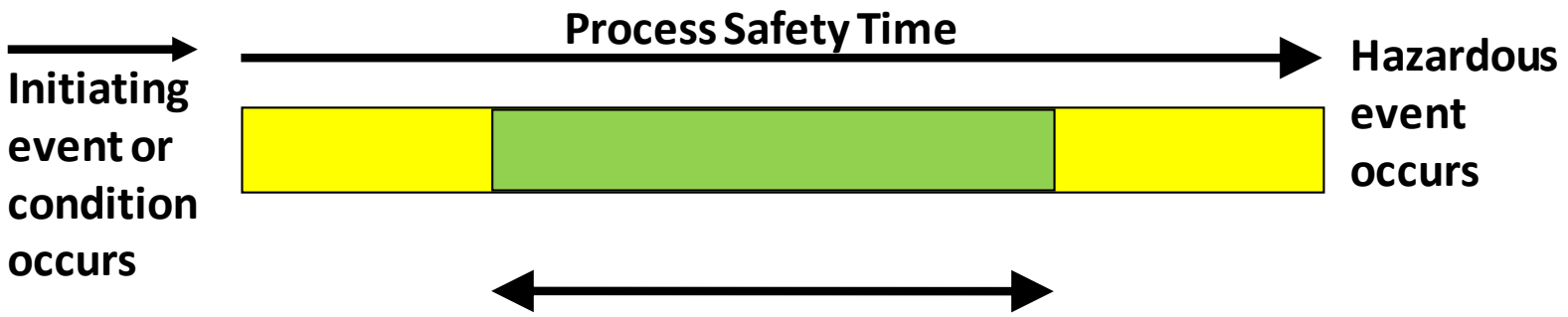
Independent Protection Layer (IPL): A prevention method that is independent of any other such method.

Safety Alarm: an alarm used as an IPL, with a 10% risk reduction credit. Such alarms must have periodic operator training, defined responses, suppression control, and several other administrative and depiction requirements.

Definitions

Relevant Definitions

- **Process Safety Time:**
  The amount of time between an initiating event in the process and a hazardous result, if a mitigating safety function is not performed.
- **SIF Design Time:**
  The amount of time within which a SIF is designed to successfully complete its mitigating action. The Design Time must always be shorter than the Process Safety Time. This is sometimes called the "response time" of the SIF.

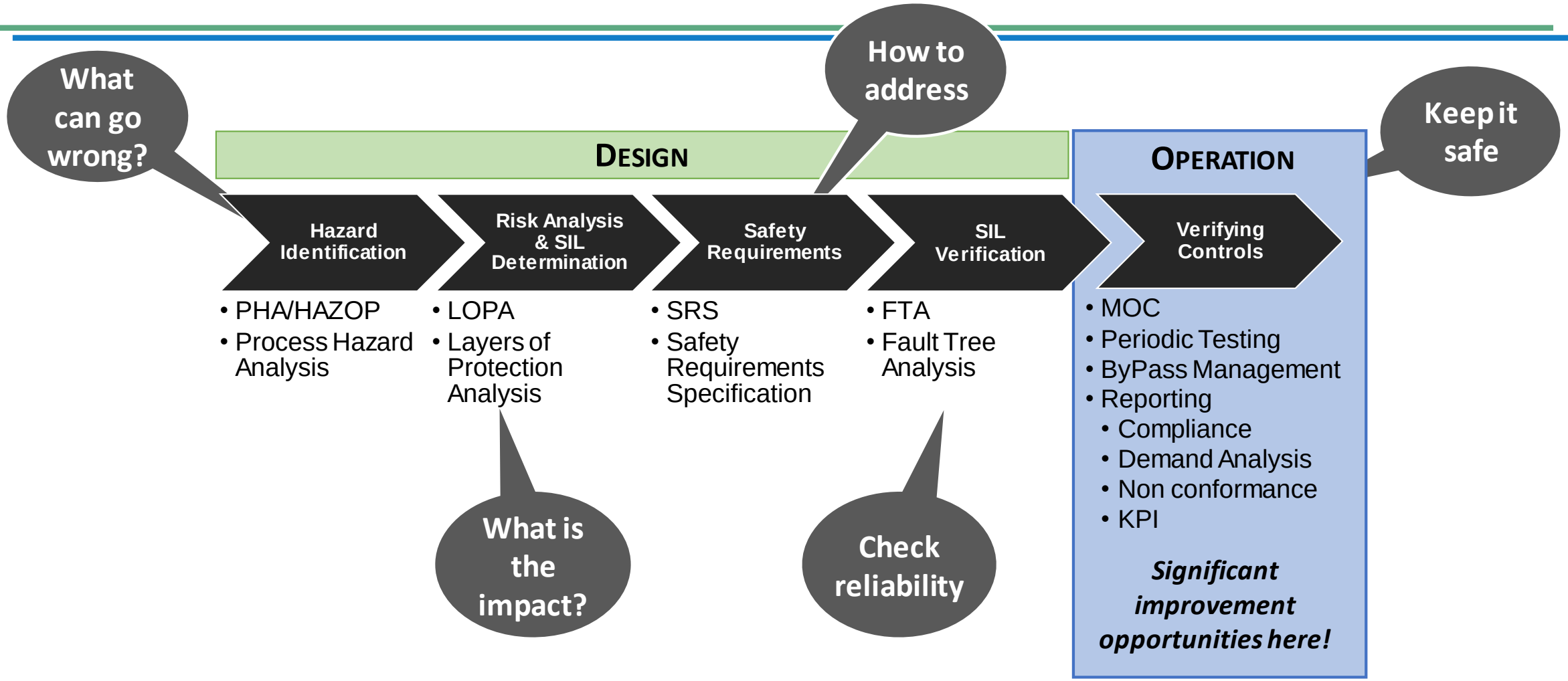


Standards

- ISA and IEC standard: ANSI-ISA-84.00.01-2004-IEC 61511-1 Functional Safety Series
- Covers the Specification, Design, Implementation, Operation, and Maintenance of
  - Safety Instrumented Systems (SISs), containing
  - Safety Instrumented Functions (SIFs), taken as
  - Independent Protection Layers (IPLs)
- Comprehensive and Complex body of knowledge

Keeping track of a variety of issues mandated by these standards has long been an arduous and error-prone task.

Functional Safety Lifecycle

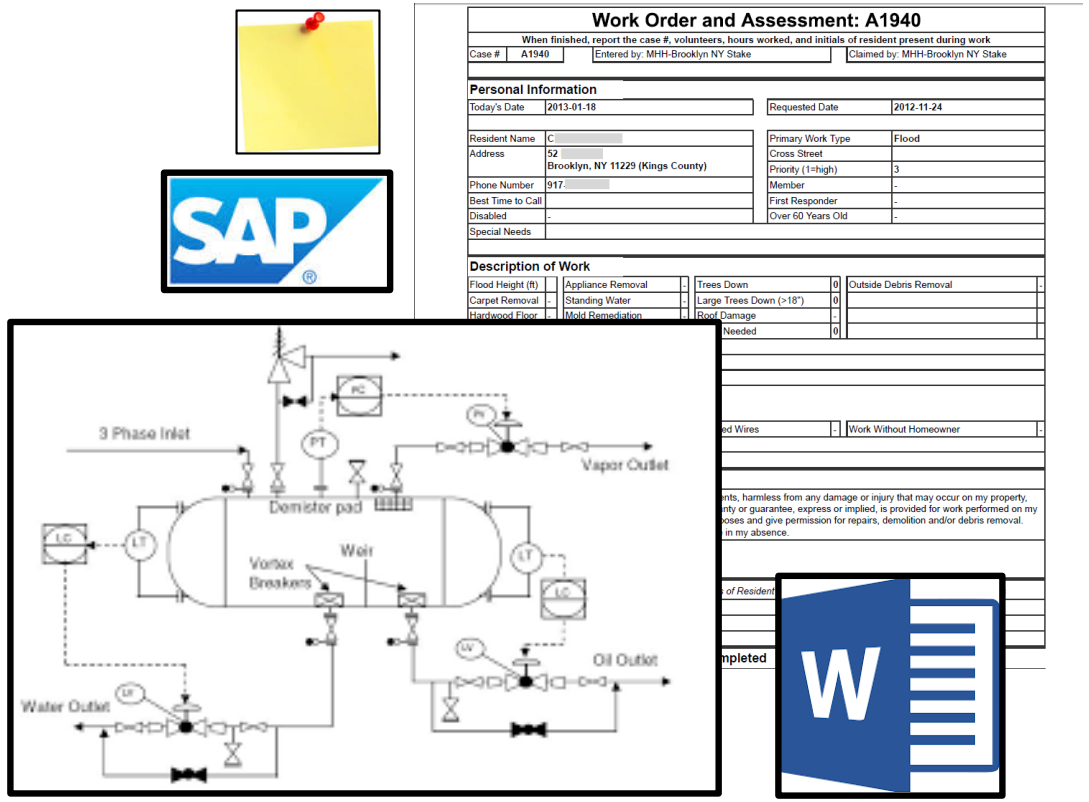


IPL, SIS and Risk Management

- Taking IPL Credit for Risk Reduction
  - SIF must be defined and communicated
  - Engineered implementation of SIF to achieve a SIL
  - Regular verification (testing) mandated by regulations
  - Bypass system a must for operations
    - Required to startup a plant
    - Required for SIS testing
    - Must be carefully managed
    - Must understand increased risk while in bypass
      - Supplemental Procedures are common to mitigate abnormal risk when in bypass

How are IPLs managed today?

- Spreadsheets
- Written Procedures
  - Operating
  - Bypass
- Manual Testing
  - Maintenance
    - Online
    - Offline
    - Full/Partial stroke
    - Etc.
- Process Drawings
- Work order systems
- Handwritten notes
- Homegrown applications
- Verification of Design Demand Rate



Disparate solutions with no input controls, no interoperability, limited change tracking, and limited functionality

IPL Management Challenges

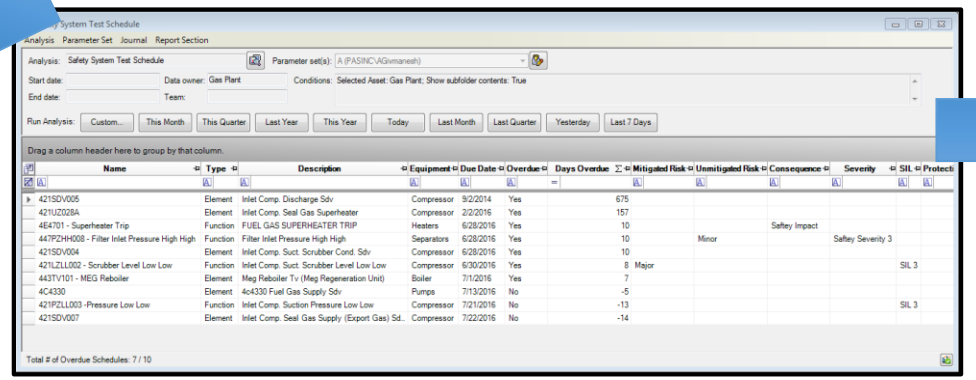
- Visibility of current risk
  - Many ways to disable IPLs
  - Manual effort to aggregate and contextualize data
- IPL/SIS/SIF lifecycle challenges
  - Safety system must be highly reliable
  - Testing and validation is highly inefficient and creates risks
    - Consumes Technical and Maintenance resources during turnarounds
    - On-line testing introduces reliability risk and potential lost production
  - SIS demand rate and failure rate are difficult to track, but are required in the standards to track for verification of proper design
  - SIL validation is based on difficult to collect demand and failure data

Consequence of a failure on demand of an IPL/SIF
is a SAFETY CRITICAL EVENT

IPL Analytics – Better way to manage IPL's

Configuration and Design Data for Each SIF

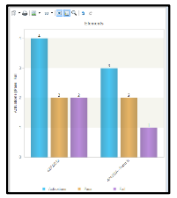
Design Time, Process Safety Time, Testing Interval, Risk, Consequence, Severity, SIL Level, etc.



Process and Event Data from the control system

SIF Activation, Success or Failure Verification, Bypass, Un-Bypass, Test, etc.

Safety System Performance Analysis and Reports



IPL Assurance Analytics

Benefits

- **Assures the Safety System is Functional**
  - Automated notification of failures to appropriate personnel
  - Bypass management, SIS availability, and risk assessment
- **Reduced production interruptions**
  - Use DOSS event as SIS test
  - Reduction in on-line testing
- **Improved Turnaround Efficiency**
  - Reduction in validation testing during turnarounds
- **Accurate SIL determination**
  - Process demands and failures are documented every activation
  - Improved accuracy of validation testing; “proof test” at process conditions
  - demand rate for verifying design
- **Complete documentation of all safety functions and testing**
  - Maintenance forecasting for testing plans
  - Audit evidence as required by IEC 61508 and IEC 61511

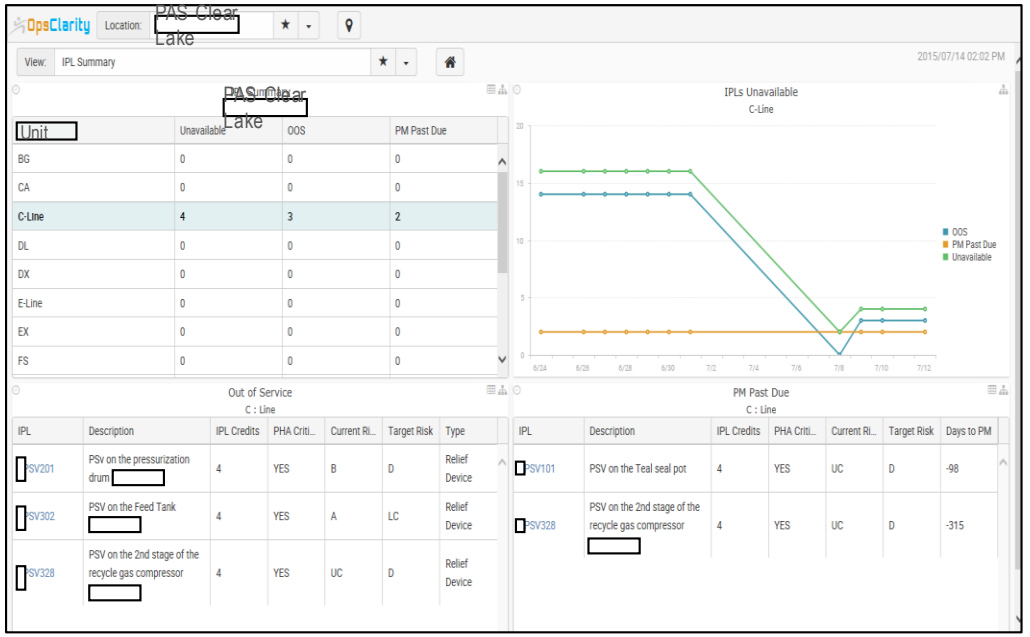
IPL Dashboard: Actionable Data Analytics

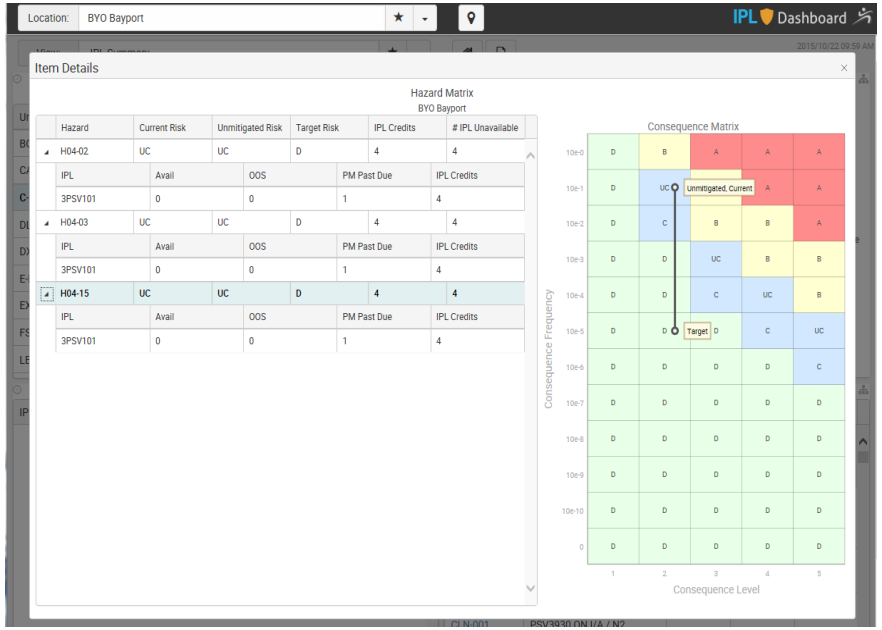
Safety System and Safety Device Assessment

Integration of Safety Functions and Risk

- PHA Risk Assessment
- IPL Service Status
- PM Maintenance

Unified view of safety critical devices





Safety Case Symposium 2018 Singapore

IPL Management: Critical Success Factors

- On demand, current visualization of risk
- Assures the safety system is functional
  - Automated notification of failures to appropriate personnel
  - Bypass management, SIS availability, and risk assessment
- Reduced production interruptions
  - Use DOSS event as SIS test
  - Reduction in on-line testing
- Improved turnaround efficiency
  - Reduction in validation testing during turnarounds
- Accurate SIL determination
  - Process demands and failures are documented every activation
  - Improved accuracy of validation testing; “proof test” at process conditions
  - Demand rate for verifying design
- Complete documentation of all safety functions and testing
  - Maintenance forecasting for testing plans
  - Audit evidence as required by IEC 61508 and IEC 61511

Questions

Anand Makhija

PAS, Global

Safety Case Symposium 2018 Singapore

www.SafetyCaseSymposium.com