Managing critical operational Process Safety Performance Indicators (PSPI)

Prepared for the 10th European Chemical Engineering Congress, Nice, France – September 2015

Jon Keswick, CFSE
aeSolutions Inc.
250 Commonwealth Drive, Suite 200
Greenville, SC 29615, USA

Jon Keswick's Bio

Jon has amassed nearly thirty years of experience working with automation technology companies, with extensive specialization in the development and implementation of Safety Instrumented Systems (SIS) and associated safety lifecycle consulting. Since the inception of the functional safety standards around the turn of this century, Jon has been a practising consultant in the domain; leading Functional Safety Assessments, Safety Integrity Level (SIL) studies and working with end users on many SIS projects. As well as being accredited as a Certified Functional Safety Expert (CFSE) since 2004, Jon holds a HNC in Electronics from Leicester Polytechnic and a Certificate in Safety Critical Systems Engineering from University of York, UK.

Abstract

It has been suggested before that organizations operating major hazard facilities without effective Performance Indicators "are at best operating partially sighted"[i].

Following several major accidents in process facilities in the last few decades, various guidance documents have been produced around the need for Process Safety Performance Indicators (PSPI). Noteworthy documents are HSE[ii], API[iii] and OGP[iv]. Each guidance document suggests there is a need for senior management and safety professionals to have a much clearer picture of the health of the measures, systems, procedures and policies in place to manage risk in hazardous process plant.

Effective PSPI metrics are achievable with changes in leadership practices, maintenance procedures, training and audits. These may take time to implement, but as the measures are "management oriented" it is natural to expect some eventual successes.

Typically much less effectively implemented are those PSPI metrics that are closest to the operation of the actual process and its control and safety systems. This paper proposes that an enterprise-level safety lifecycle management[v] approach is required to integrate with existing process control and safety systems to capture, analyze and monitor leading and lagging operational PSPI metrics. This paper will show that as the data gets generated, it can deliver better quality process hazard and risk assessments, as well as keeping critical safety lifecycle data "evergreen".

Key Terms to be explained

Process Safety Performance Indicators (PSPI), leading and lagging indicators, PSPI priorities, Safety Lifecycle, tag-centric Enterprise Safety Lifecycle Management.

Process Safety Performance Indicator Priorities

Process Safety Performance Indicators (PSPI) are the safety-related metrics that companies who operate hazardous process facilities should both actively and reactively monitor. Aimed at senior management and safety professionals, well designed PSPI metrics should give warning of negative issues related to risk controls (so-called "lagging" indicators), as well as active monitoring of procedures and tasks for controlling risk (so-called "leading" indicators). The idea of well-designed PSPI's is to create an environment where there is early warning before catastrophic failure.

PSPI's can be classified broadly into 3 categories; the first we will call the "Procedural" category, the second the "General" category and the third "Operational". Each has their merits and challenges as described below.

Procedural Indicators

Within the context of the IEC 61511 (S84) safety lifecycle, procedural performance indicators would include active monitoring of aspects such as functional safety audits going to schedule. If audits are slipping or finding significant issues when conducted, then management should begin to see a long term pattern that possibly reflects a poor safety culture over time.

Other key metric opportunities are presented when Process Hazards Analysis (PHA) or Hazard and Operability (HAZOP) action close-out is monitored during a project, or at any time they are conducted for revalidation purposes. If a HAZOP is conducted and there are many recommendations for improvement, this can indicate poor initial design in a capital project, or poor ongoing maintenance / operability and risk control in an existing plant.

If implemented, these type of PSPI metrics will provide reassurance to management that appropriate safety culture is well embedded and that safety management systems are being actively followed.

General Indicators

General safety lifecycle PSPI opportunities include monitoring management of change such as percentage compliance with preventative or corrective maintenance plans. Operating under a permit to work (PTW) system, it should be possible to implement effective PSPI's that are both lagging and leading in nature, for example by monitoring "number of permit violations observed during local PTW Audits"[vi] or "number of PTW reviews per week by asset managers".

These kinds of indicators are valuable but do not require access to data embedded in documents that are created over the lifetime of critical equipment such as Independent Protection Layers (IPL) and Safety Instrumented Systems (SIS).

Operational Indicators

Operational metrics are much more closely aligned with the critical equipment that exists in all major accident hazard process facilities. Consider the following list as an example:

a. Critical equipment faults and failures (focused on independent protection layers).
b. Frequency of alarms arising in the basic process control system but within the normal operating envelope.
c. Frequency of safety instrumented system demands (trip occurring when operating outside the normal envelope of level, pressure, temperature etc.).
d. Defeated safety equipment.
e. Time in bypass.
f. Availability of dedicated proof test procedures for every Safety Instrumented Function (SIF).
g. Percentage of SIF proof tests which occurred as planned without equipment failure.

Some of the above metrics are leading, some lagging. Without getting hung up on which is which, it is clearly possible to recognize that the operational metrics are closely linked to critical layers of protection, are the closest indicators to the process, and therefore the most effective in providing early warning of incidents with catastrophic potential.

Closing the loop on real world safety lifecycle data

When companies adopt the IEC 61511 (S84) Safety Lifecycle even for just compliance purposes, we may not easily see how some very valuable PSPI metrics will be naturally created during the risk analysis and protection layer design phase (see Figure 1), as well as in the ongoing maintenance of Control and Safety Instrumented Systems (SIS).

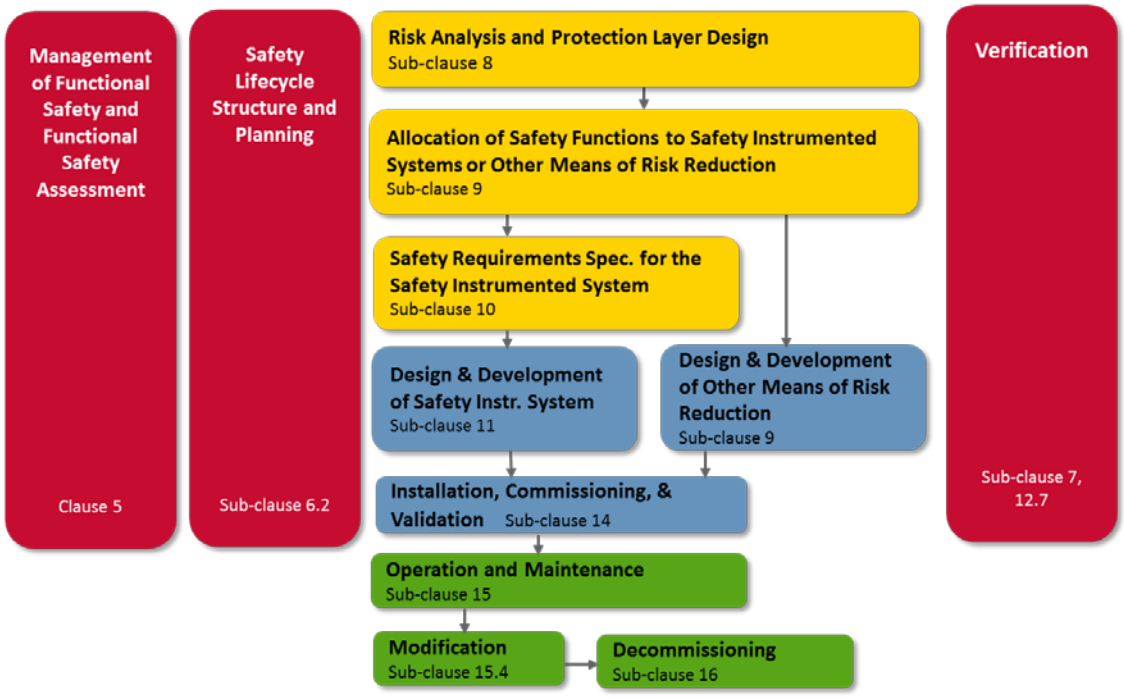


Figure 1: IEC 61511 Safety Lifecycle

Although the analysis of risk is clearly first conducted when plant and control systems are installed, risk analysis is very clearly an ongoing process that requires constant and consistent revalidation at

regular intervals. When these revalidation exercises occur, the Process Hazards risk register is revisited (often by re-conducting HAZOP or revalidating an existing hazard analysis of whatever form) and there is often re-consideration of protection layers and their efficacy.

With over ten years of seeing different end user implementations of the safety lifecycle since its inception in 2003, one issue that clearly remains is the lack of any linkage between the "real world" of operations and the ongoing risk analyses occurring over the plant lifetime. The standards clearly had a closing of the loop in mind when they were written (see Figure 2) , but in practice most companies carrying out HAZOP and subsequent Layer of Protection Analysis (LOPA) continue to use generic data, rule of thumb estimates and very little real-world input.

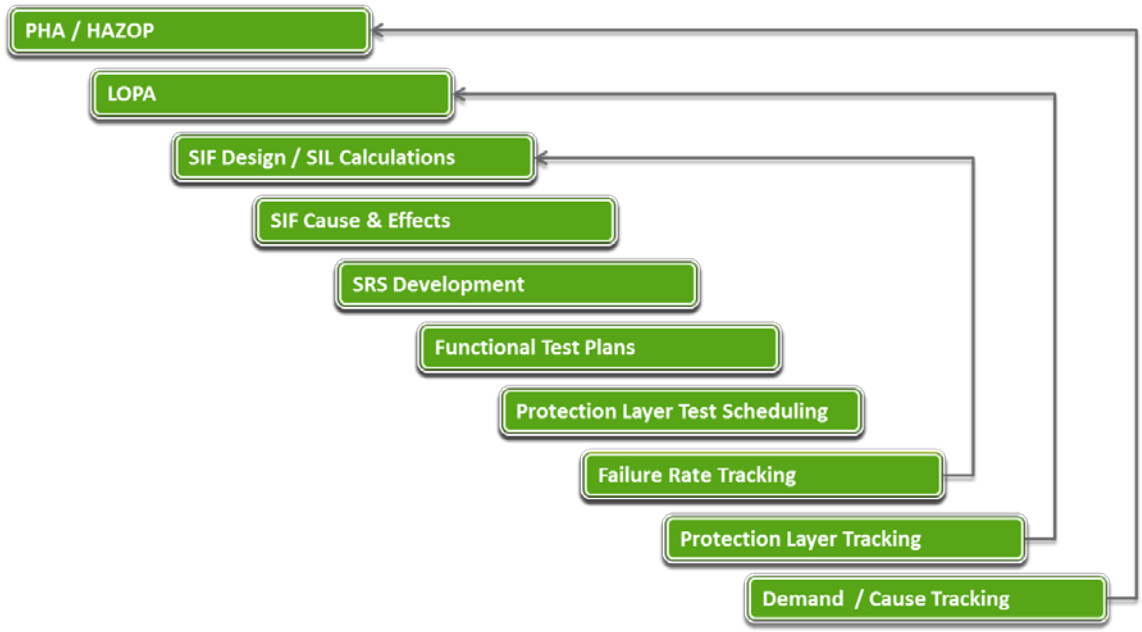


Figure 2: Closing the loop on process safety parameters – feedback from operations to risk analyses and SIF Design

The following elements should be linked in order to close the loop from operations back to risk assessment and SIF Design phases:

1. Safety system equipment failures should be recorded and linked back to theoretical SIF reliability calculations in order to drive modifications where performance of the SIF is not meeting the required risk reduction.[vii]
2. Independent Protection Layers (IPL) should be monitored to ensure they are still effective over the plant lifetime. The LOPA should be constantly updated and reflect "actual" rather than "desired" status.
3. Demands on the SIS and cause of trips should be logged and fed back into the assumptions made during the PHA/HAZOP phase. False assumptions should be replaced with real-world data and this should drive modifications where necessary.

Without these loop-backs, ongoing process hazard and risk analysis is at best using assumptions, and more worryingly sometimes assumptions which are not provably conservative.

So where is the critical PSPI data?

What is less clear is how good data relating to critical parameters can be generated, stored and monitored to create effective PSPI's that show up-to-date status of the safety lifecycle being in a healthy condition. Part of this challenge lies in the disparate types of flat file generated in the hazard and risk assessment process, and the later phases of design and implementation (see Figure 3).

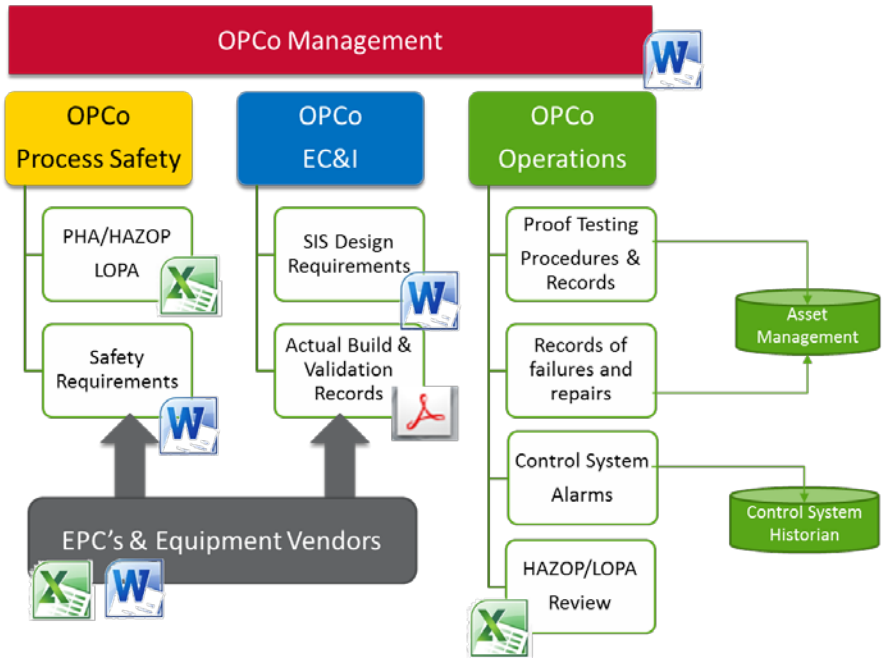


Figure 3: Flat files have embedded PSPI data that is difficult to get to and often out of date

Very typically, end users will employ outside facilitators, consultants and contractors in larger projects due to the drain on their own resources that is typical of study methods like HAZOP. This in itself is not a bad thing, but the deliverables are very typically spreadsheets or reports that have very little basis for being data-mined for later phases. Often the term "instrument tag" is not even on the radar in a HAZOP. Subsequently, on reaching operations, a HAZOP and/or LOPA record may not even be very clear with respect to the equipment that ended up being "as-built" and handed over to operations. This can of course be improved over time when baselining exercises occur, but this is typically some years later when the plant has been operating for some time.

The biggest challenge with flat files is that they simply do not remain fresh or evergreen. The embedded data becomes stale or simply never updated over time as modifications occur. Some organizations may attempt to control this by sound document control, review and authorization, but the fact is that it becomes very cumbersome when practically any fundamental change to plant or protection layer will affect every other phase of the lifecycle. This ripple-through effect is very difficult to manage even with good document control systems in place.

A possible solution: Tag-centric Enterprise Safety Lifecycle Management

One possible solution to the challenge of monitoring critical operational PSPI metrics is the adoption of a new business and enterprise-level database which is tag-centric. What this means in practice is adopting a new approach to the safety lifecycle, including the key phases of hazard and risk analysis right through to operations. It does not change the type of work or study conducted, but it does require a change in philosophy for the recording of Process Hazard Analyses, LOPA, Independent Protection Layers (IPL's), Safety Requirements Specifications (SRS), SIS Design Calculations and Proof Test Procedures. Each of these must be recorded and updated via the enterprise safety lifecycle management database for the power of this solution to be realized.

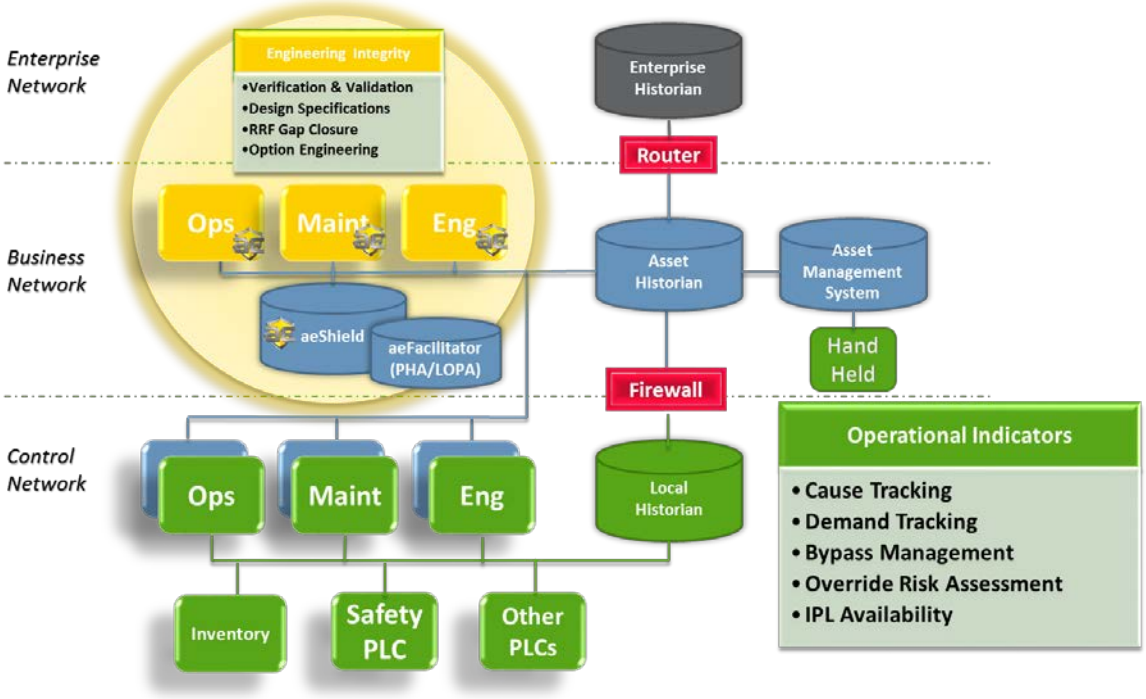


Figure 4: Where Enterprise Safety Lifecycle Management fits with other systems

Instead of recording data generated during the lifecycle in disparate flat files and paper based documents which become stale with time, users gain access to tool that inter-relates all hazards, IPL's, safety requirements, SIS equipment and Proof Test Procedures with unique identifiers in a relational database that sits on the business network alongside existing asset management systems and historians. The database becomes part of everyday operations and is accessed via a web-based interface that is unique to every user's role in the organization. For instance, those who are responsible for conducting PHA (HAZOP) or LOPA need only have access to that part of the tool. However, in the background, the data they generate during the study gets carried forward into the safety requirements in a relational database. Linking these steps together in a relational database ensures that no single part of the safety lifecycle will become an island of data which is out of date or inaccurate.

Conclusion

The proposed solution might sound too good to be true, but there are already commercially available Tag-Centric Enterprise Safety Lifecycle Management tools. It is possible to start the journey to realizing the goal of closing the process safety loop and providing evergreen and effective operational PSPI's. It will of course still take time and effort, but the potential gains are more than just assurance of safety layer effectiveness. The gain will be to deliver risk reduction more efficiently to where it is needed most, which in turn will save money on risk reduction efforts that have little associated gain.

REFERENCES:

[i] "So how do you manage major hazards if you don't have effective Key Performance Indicators" – Presentation to EPCS/CEFIC International Conference on Process Safety Performance Indicators, 31 Jan – 1 February 2012, Brussels – Ian Travers, Head of Chemical Industries Strategy Unit, HSE, UK.

[ii] Developing Process Safety Indicators, A step-by-step guide for chemical and major hazard industries, HSG254 - Health & Safety Executive – 2006. ISBN 978 0 7176 6180 0.

[iii] API RP 754, Process Safety Performance Indicators or the Refining and Petrochemical Industries, (First Edition, April 2010).

[iv] Process Safety – Recommended Practice on Key Performance Indicators, Report No. 456, November 2011, International Association of Oil and Gas Producers (OGP).

[v] Is cost effective compliance with the IEC61511 Safety Lifecycle sustainable? Paper presented at Texas A&M University Instrumentation and Automation Symposium for the Process Industries. Michael Scott and Carolyn Presgraves.

[vi] Developing KPIs that drive process safety improvement. Megan Brown, Lloyds Register EMEA, Aberdeen, UK. Hazards XXI symposium series No.155.

[vii] IEC 61511 (Ed.1) clause 16.2.6 – "discrepancies between expected behaviour and actual behaviour of the SIS shall be analysed…"

Managing critical operational Process Safety Performance Indicators (PSPI)

10 th European Congress of Chemical Engineering

aesolns.com

Visit us at www.aeshield.com
Email us at info@aeshield.com

Process Safety Performance Indicators

What to monitor?

Operational Indicators

Control system alarms

Safety system demands

Protection layer failures

General Indicators

Permit to work

Maintenance to schedule

Procedural Indicators

Audits to programme

Actions closed

MOST EFFECT

LEAST EFFECT

Visit us at www.aeshield.com
Email us at info@aeshield.com

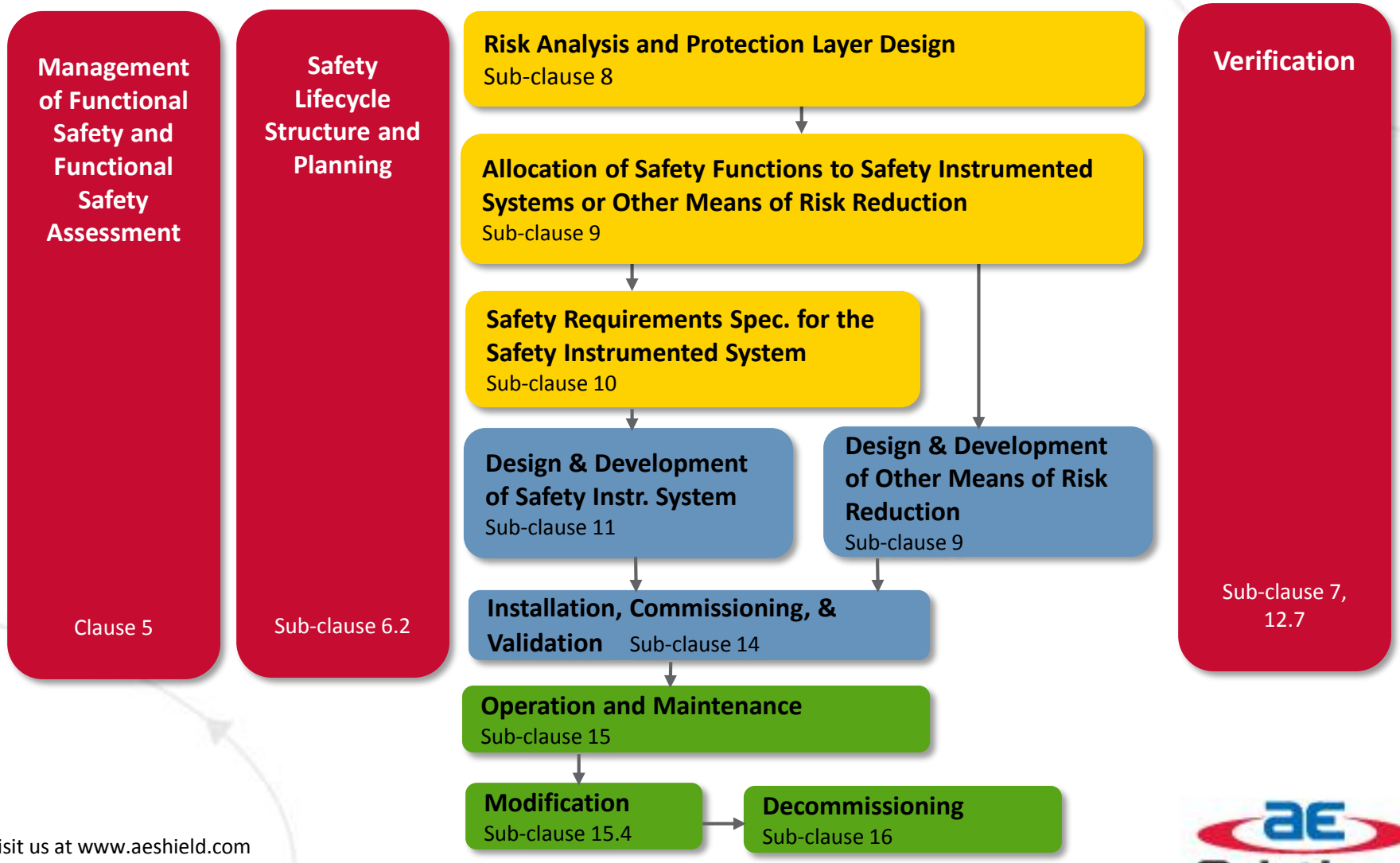
Focus on Operational Indicators

Leading and lagging examples

- Controlling risk is an ONGOING process of
  - **Active** Monitoring of leading indicators
    - e.g. percentage of Safety Instrumented Function (SIF) proof tests which occurred as planned without equipment failure
  - **Reactive** Monitoring of lagging indicators
    - e.g. number of demands on a specific Safety Instrumented Function (SIF)
- The challenge…
  - How do you collect good indicators of either type and keep the data fresh, or “evergreen”?

Safety Lifecycle

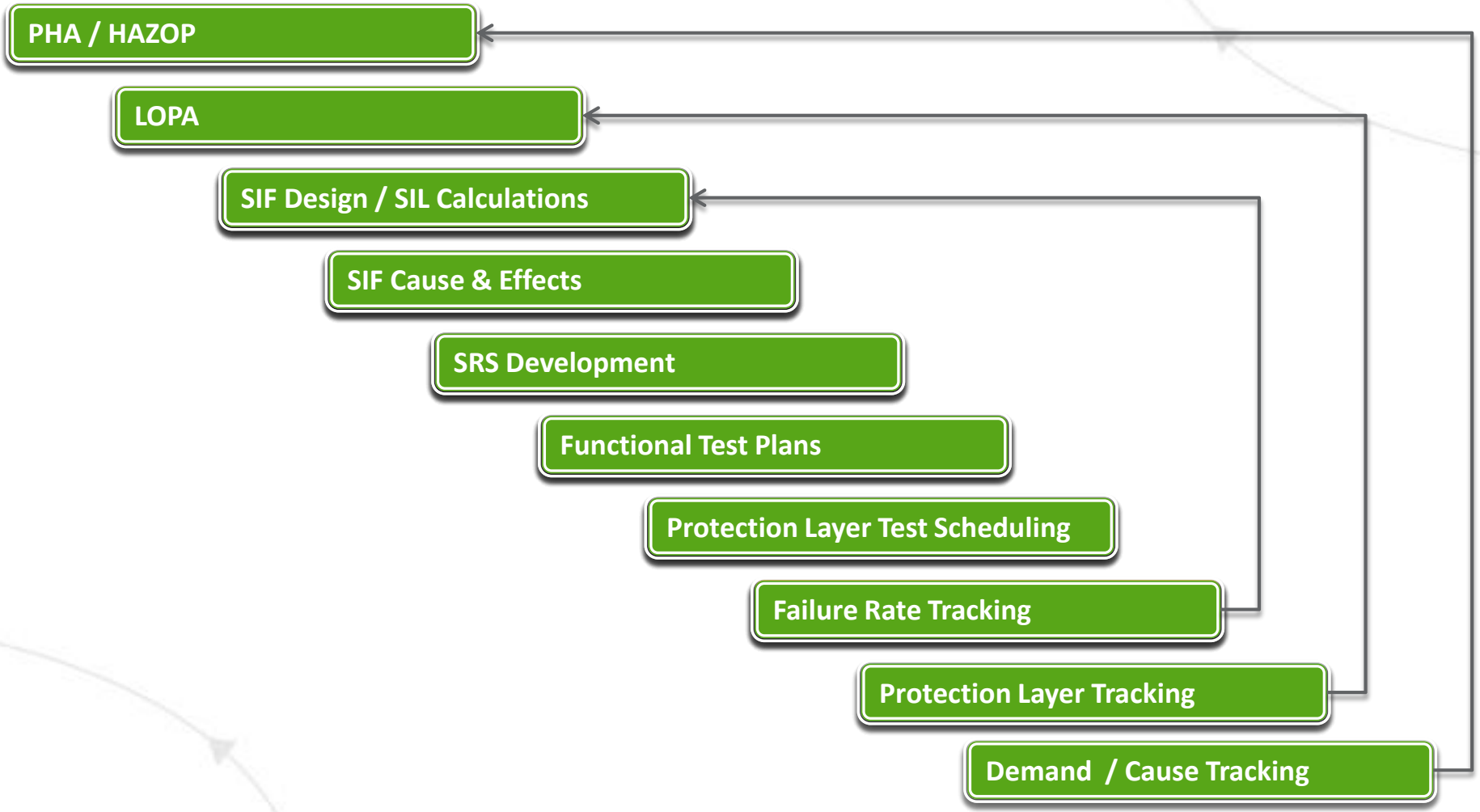
EN IEC 61511



Visit us at www.aeshield.com
Email us at info@aeshield.com

Closing the loop on Process Safety

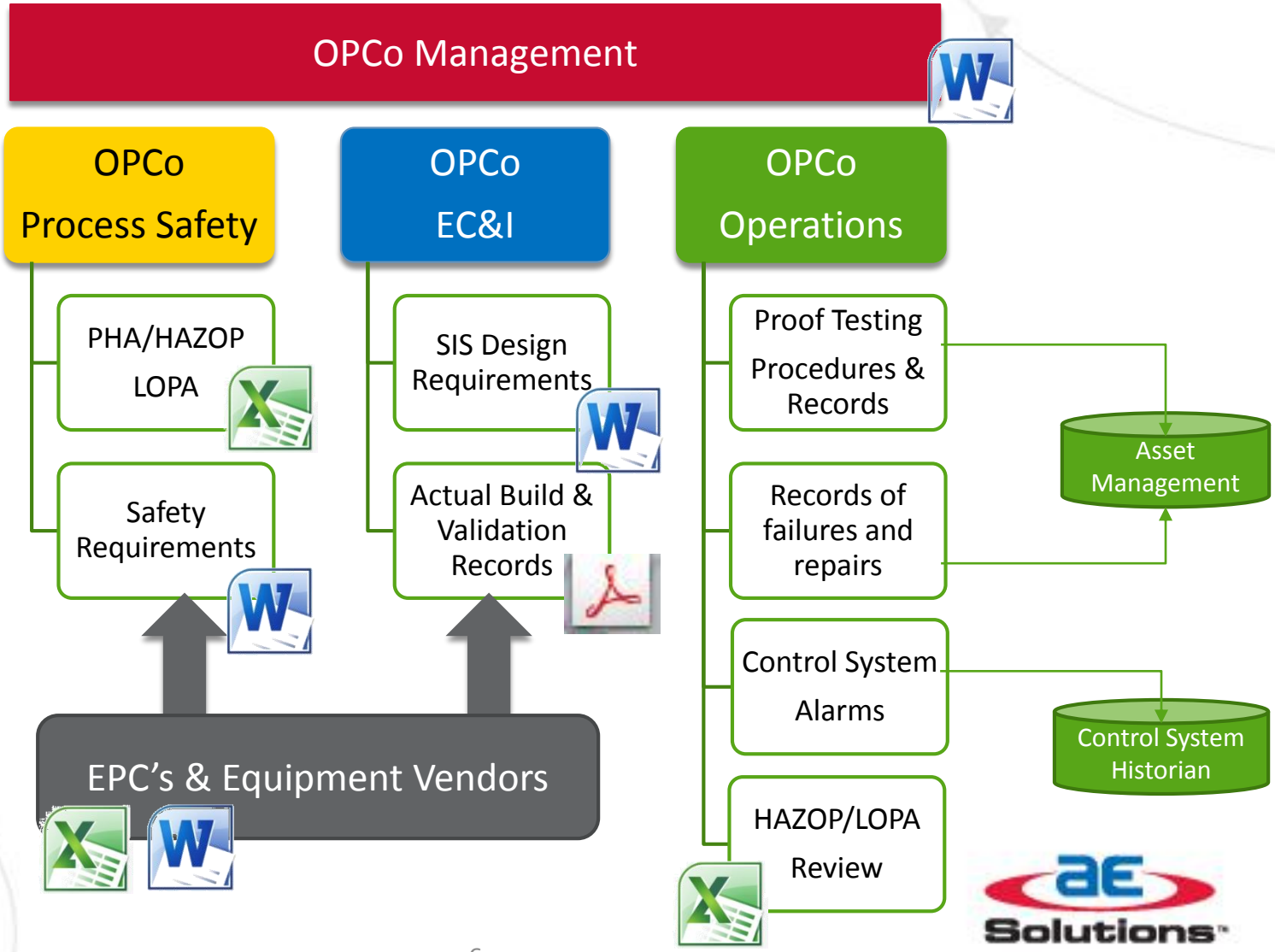
for Evergreen safety lifecycle management



Visit us at www.aeshield.com
Email us at info@aeshield.com

Where is the critical PSPI data?

Flat files and some databases with embedded PSPI Information



Visit us at www.aeshield.com
Email us at info@aeshield.com

Enterprise Safety Lifecycle Management

Tag-centric database

one database

“tag-centric”

Process Hazards Analysis / HAZOP
(the risk register)

Safety Lifecycle Documentation
(Safety Requirements, SIF Design, SIL Calculations, Proof Test Procedures)

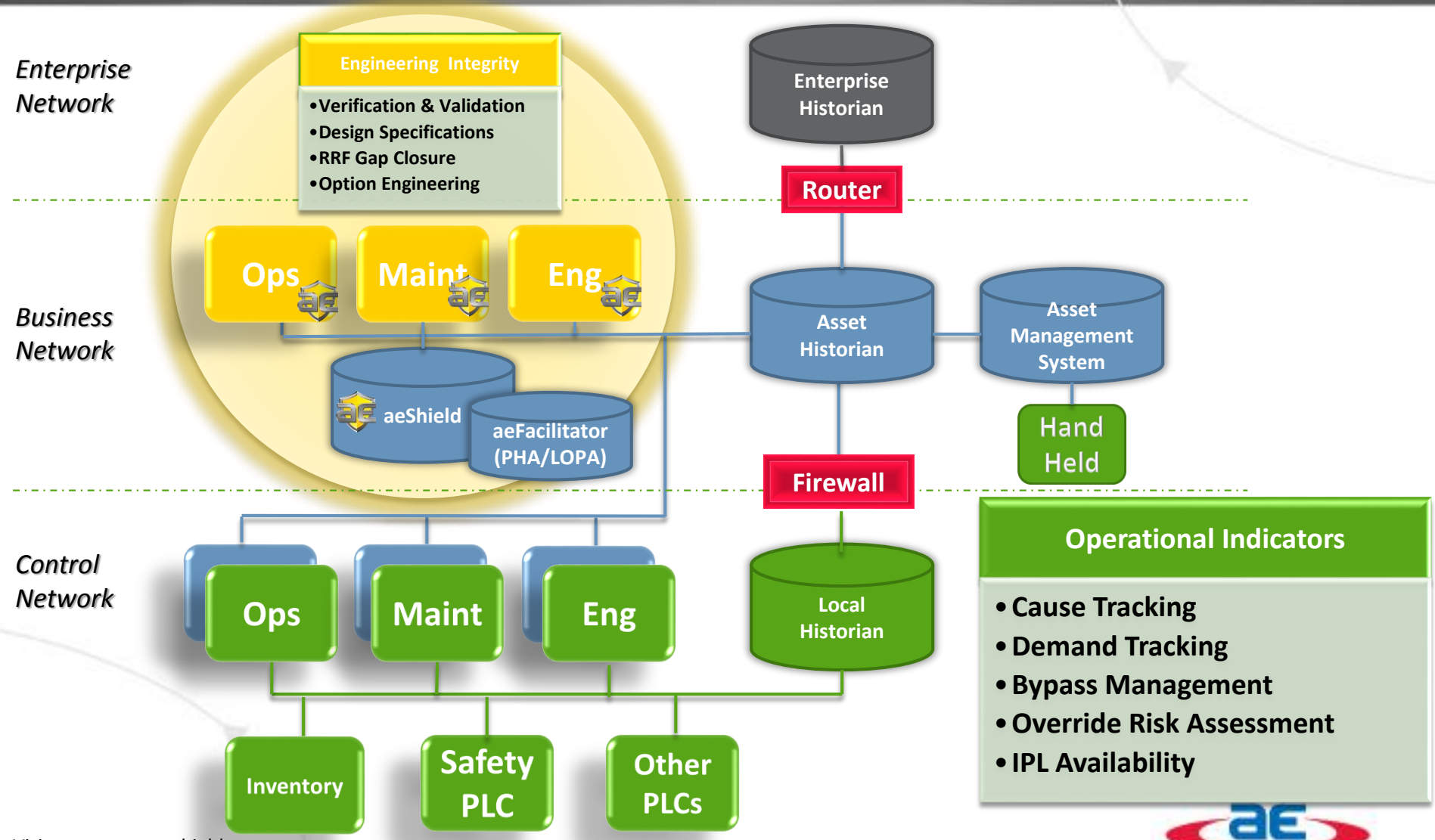
Critical success criteria

- Eliminate flat files
- Unlimited users – no specialist knowledge for data entry
- Centrally hosted
- Link to existing asset management systems

Visit us at www.aeshield.com
Email us at info@aeshield.com

Enterprise Safety Lifecycle Management

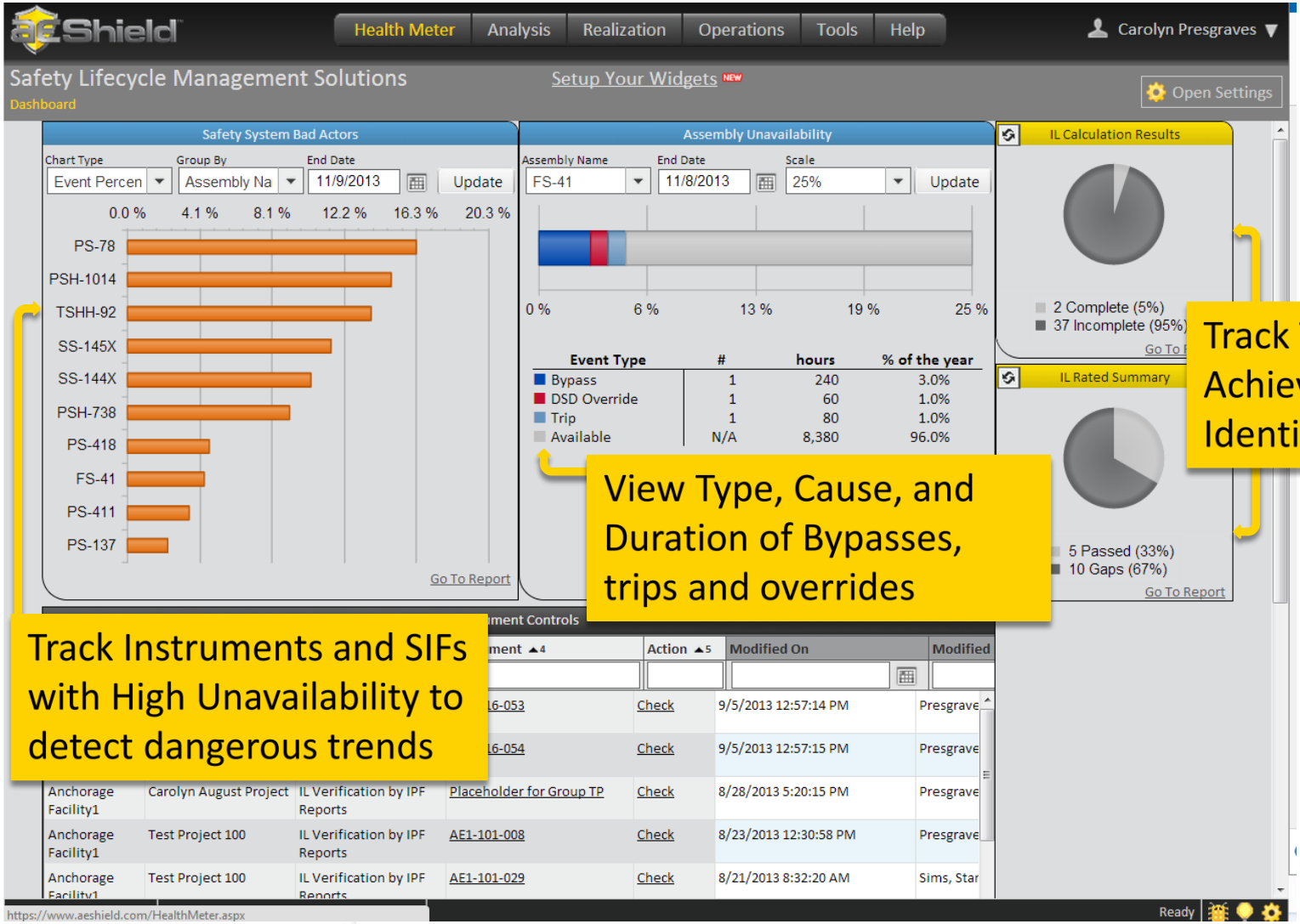
Where it fits



Visit us at www.aeshield.com
Email us at info@aeshield.com

Process Safety Performance Indicators

Validate Assumptions, Track Performance Against Design



Track Target vs. Achieved RRF to Identify Gaps

View Type, Cause, and Duration of Bypasses, trips and overrides

Track Instruments and SIFs with High Unavailability to detect dangerous trends

aeSolutions

Thank You!

Further information: www.aeshield.com

Taylor Schuler
Product Manager
Taylor.Schuler@aesolns.com
Office: +1 (864) 404-3052
Mobile: +1 (214) 597-8880

Jon Keswick
Global Process Safety Consultant
Jon.Keswick@aesolns.com
Mobile: +44 7813 676560