YOKOGAWA

Digital Risk Management and Process Safety

White paper - May 11, 2020

Table of Contents

KEY TAKEAWAYS

- ✓ Most organizations recognize IEC 61511 and ISA84 as the global best practices for functional safety management.
- ✓ Digital Risk Management deploys a digital twin to vastly improve decision-making related to the process safety lifecycle.
- ✓ The Layer of Protection Analysis (LOPA) is the foundation for Digital Risk Management.
- ✓ Digital Risk Management closes the gap that typically exists between safety and operations.
- ✓ A simplified process exposes previously invisible risks and empowers end users to take action.
- ✓ The Digital Risk Management solution is vendor-agnostic.

Part 1 Introduction

> *The Digital Risk Management value proposition provides a justifiable payback that allows it to compete with other proposed projects.*

Most organizations operating under process safety management (PSM) programs recognize IEC 61511 and ISA84 as the global best practices for functional safety management. The challenge is in finding how to best comply with these standards over the operation and maintenance phases, which comprise 99% of an asset's lifecycle. Traditionally, the front-end engineering work from risk assessment to safety instrumented system (SIS) design has used hardcopy and disparate applications, which make it nearly impossible to leverage while the plant is running. Is there a way to close the gap between process safety and operations?

The objective of this whitepaper is to explain the many benefits of Digital Risk Management. Digital Risk Management is a result of Yokogawa leveraging its Co-innovating Tomorrow core business philosophy to engage in the co-creation of value through the development of solutions during long-term partnerships with clients. By embracing process safety technology as a digital twin, Digital Risk Management allows organizations to make their facilities safer on a daily basis, cost effectively sustain their Safety Instrumented Systems, and make better informed business decisions to optimize safely.

In today's business environment, capital expenditures (CAPEX) and operations expenditures (OPEX) are increasingly difficult to justify. Optimization projects with clear profit and return on investment (ROI) potential will always take priority over those whose goals are intangible. Often, data transformation and safety projects fall into the latter category. However, the Digital Risk Management value proposition provides a justifiable payback that allows it to compete with other proposed projects.

Part 2 What is a Digital Twin?

> *...a digital twin is a decision support tool that enables improved safety, reliability, and profitability in design and in operations.*

While companies today are running leaner, data is becoming more plentiful, sometimes to an overwhelming degree. To account for the flood of data and the need to harness its value, digital twin technology has emerged as one of the most powerful disruptive technologies in the process industries.

Yokogawa's definition of a digital twin is a virtual, digital copy of a device, system, human or process…

… that accurately mimics actual performance

… in real-time

… that is executable and can be manipulated

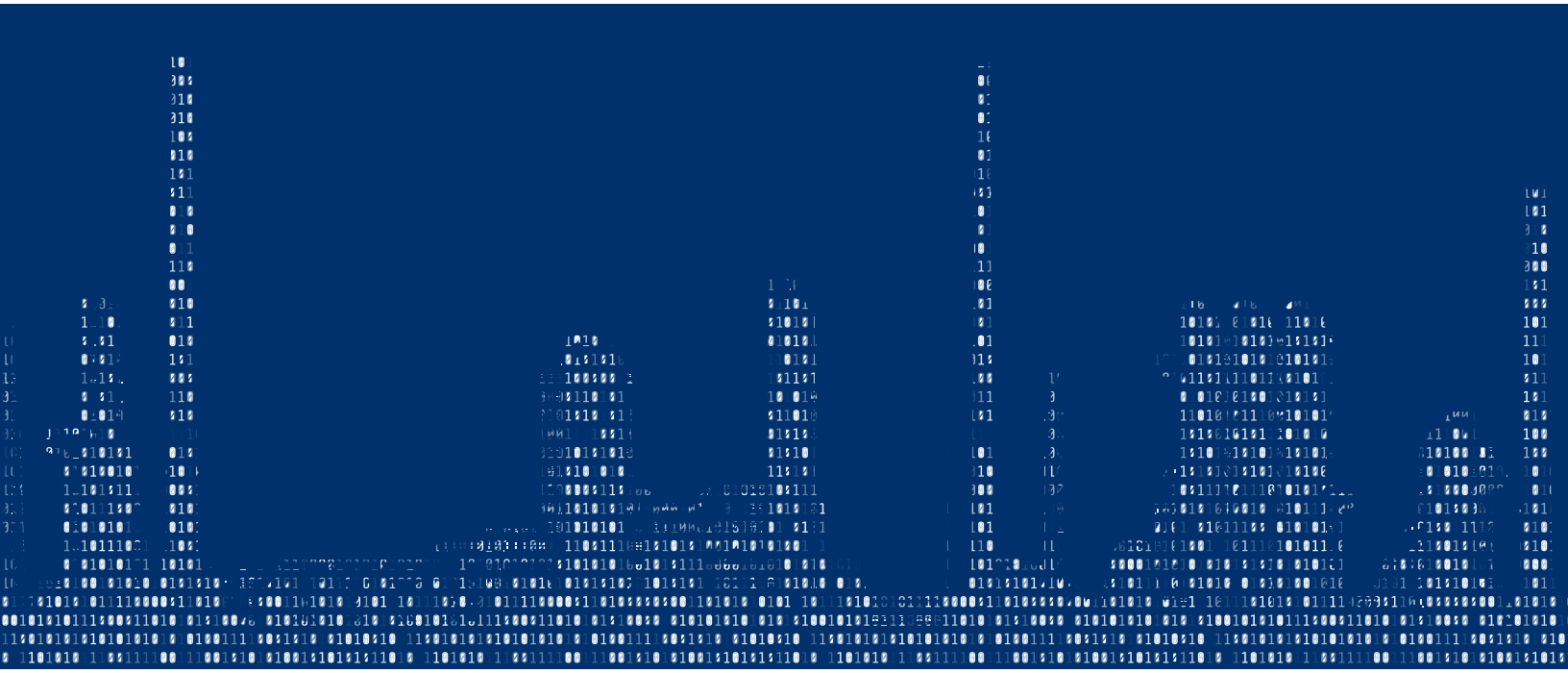
... allowing a better future to be developed.

In other words, a digital twin is a decision support tool that enables improved safety, reliability, and profitability in design and in operations.

Digital twins allow for advanced data analytics and operational insight, which can be used to guide day-to-day decisions and drive improvements. A digital representation's ability to process enormous amounts of data and turn it into understandable formats enables better decision-making about manufacturing processes, predictive maintenance, and end-of-life cycles while ensuring that performance of a process meets the expectations placed on it.

Digital twins also allow data consumers the freedom to experiment with future scenarios. Pushing equipment to physical failure is a costly and potentially dangerous task; a digital twin offers insight into equipment limitations without the risk of real-world damage.

Part 3 Process Safety as a Digital Twin



The traditional process safety compliance approach is complicated and resource intensive. Ultimately, that translates to a significant, recurring investment.

The process safety lifecycle per IEC 61511 and ISA84 requires subject matter experts (SME), typically both internal and external to the company, to conduct a Process Hazard Analysis (PHA), which identifies potential scenarios that could lead to loss of containment events.

Upon completion of the PHA, a Layer of Protection Analysis (LOPA) quantifies the risk and ensures adequate protection is included in the SIS design. Using the LOPA report, a second group of SMEs executes a SIS design with reliability calculations and non-SIS layers of protection that are also necessary to maintain tolerable risk levels. An engineering team transforms the design into an operational SIS through configuration and programming then performs rigorous testing and commissioning prior to start-up.

The complicated and costly process does not stop at that point. It is inevitable that changes will be required and the entire process will repeat itself. In addition, operators must monitor "actual" performance and compare it with "expected" behavior to auto-correct when deviations occur. This is a new requirement in IEC 61511 Edition 2, Clause 16.2.9, which states, "Discrepancies between expected behavior and actual behavior of the SIS shall be analyzed and, where necessary, modifications made such that the required safety is maintained."

Since the majority of readers are likely to admit that their operations do not comply with this requirement, Yokogawa has found that a digital twin best addresses both the complexity of the front-end engineering design (FEED) and the challenge of monitoring performance in the live system.

> *"Yokogawa has found that a digital twin best addresses both the complexity of the front-end engineering design (FEED) and the challenge of monitoring performance in the live system.*

This Digital Risk Management approach begins with the foundation for all functional safety management programs, the LOPA, which specifies the "expected" behavior. The LOPA report identifies the SIS and non-SIS requirements that the safety SME team must incorporate into the design to achieve tolerable risk. The LOPA also sets targets for each layer of protection.

With the LOPA as the focal point, a Digital Risk Management solution still needs a way to close the gap between process safety and operations. That requires a translation of the LOPA report into information that operations and maintenance personnel could use on a daily basis.

Part 4 Completing the Solution

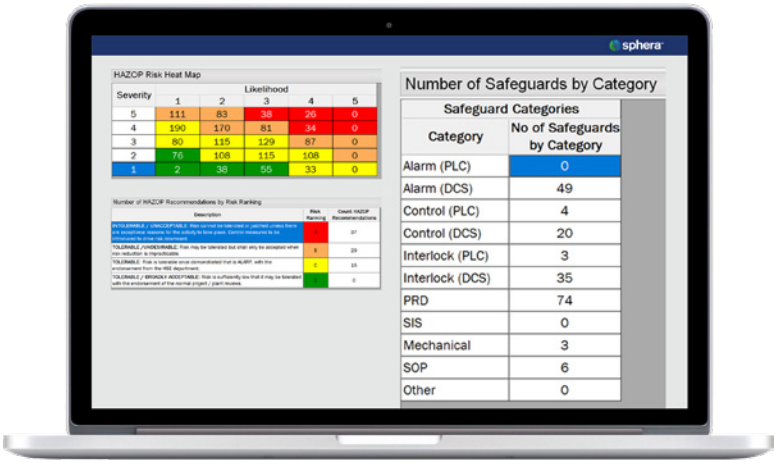


Figure 1 – The PHA Pro multi-function summary display provides safety system metrics and status at a glance.

By co-innovating with a software supplier for configuration of PHA and LOPA reports, Yokogawa has been able to complete the risk management portfolio in a manner that addresses the entire plant lifecycle. This enables Yokogawa's customers in improving the quality of their risk assessment activities and allows them to leverage the results to develop more accurate, efficient, and productive safety management systems.

Co-innovation partner, Sphera, offers PHA Pro, an industry leading software environment for configuration of PHA and LOPA reports. The Yokogawa Digital Risk Management solution uses PHA Pro as the configuration source for performance monitoring using real-time operating data. The combination makes front-end engineering and performance monitoring more cost-effective.

As changes occur, the engineering team can simply upload the new data in PHA Pro to update the interface with real-time instrument data and maintenance activities.

The Digital Risk Management solution provides a configurable interface for alarm rationalization, functional safety assessments, safety requirements specifications, SIL calculations and many additional functions. In daily operations, the configuration environment is the single source of truth for the key assumptions regarding the asset lifecycle. It readily supports functional safety audits and MoC events that impact process safety. It also provides a context for real-time event data and enables operators to quickly identify risks associated with overriding a safety critical device. It further enables understanding and synchronizing testing intervals with integrity level targets.

Benefits of Yokogawa Digital Risk Management and PHA Pro

- No training requirements for new tools or systems
- No laborious data migration, configuration from legacy reports, or custom guidelines
- No need to reinvent content management and management of change (MoC)

Part 5 Four Steps to Digital Risk Management

> *By flagging discrepancies, companies are now empowered to take action to minimize previously invisible risk.*

Having established the LOPA as the foundation of a successful functional safety management program, the next step is to import the "actual" system behavior for comparison with the "expected" behavior in the LOPA report.

The real-time data that is necessary falls into two categories: instrument data and maintenance activities. The Digital Risk Management solution retrieves event data directly from the DCS, SIS, or the plant historian. It also retrieves maintenance activity information from the computerized maintenance management system (CMMS).

By flagging discrepancies, companies are now empowered to take action to minimize previously invisible risk. The following chart shows the simplified workflow to manage information in a sustainable manner.

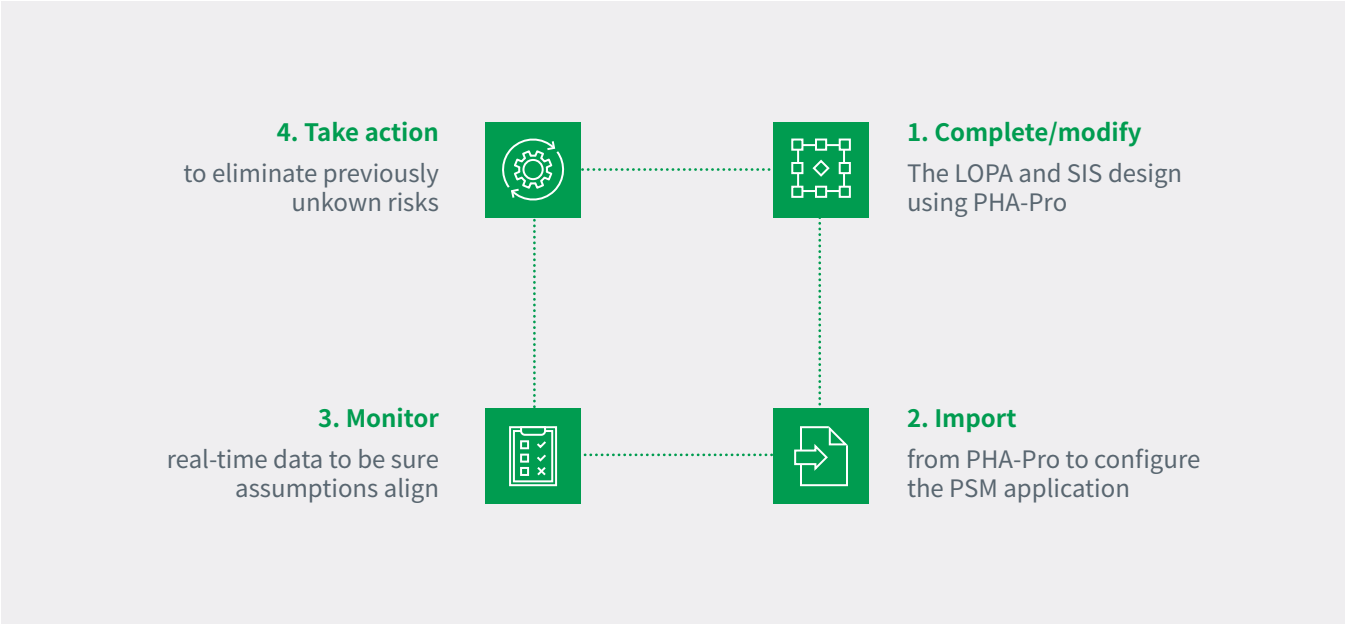
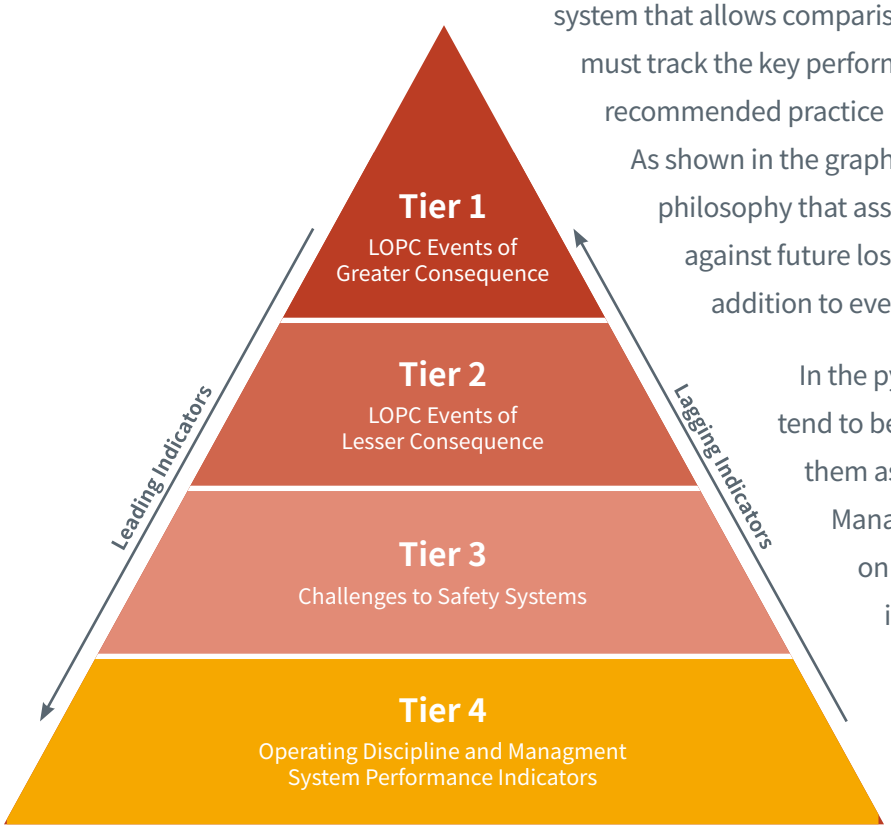


Figure 2 – The simplified Digital Risk Management process exposes risks and empowers end users to take action.

Part 6 Key Performance Indicators (KPI)

In daily operations, a sustainable Digital Risk Management system that allows comparisons of actual vs. expected behavior must track the key performance indicators with risk impacts. API recommended practice RP-754 provides very good guidance. As shown in the graphic, below, API RP-754 establishes a philosophy that assesses leading indicators to protect against future loss of primary containment events in addition to events that have already occurred.

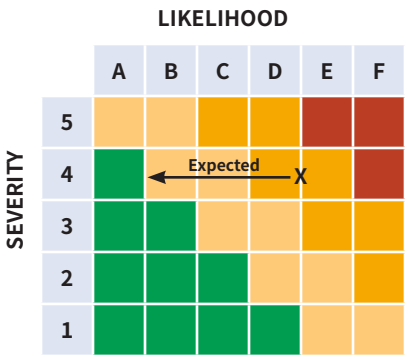


In the pyramid, Tier 1 and Tier 2 events tend to be reactive. API RP-754 refers to them as lagging indicators. The Digital Risk Management solution puts more emphasis on Tier 3 and Tier 4 events as leading indicators. While API RP-754 does not specify exactly which KPIs to track, Digital Risk Management focuses on the assumptions made in the LOPA or SIS design that could alter a risk profile.

Figure 3 – Four-tiered safety monitoring per API RP 754 with leading and lagging indicators

The Digital Risk Management solution tracks the following KPIs:

- Demand rate
- Initiating cause association
- Spurious trip rate
- On-time testing
- Process safety time
- Device failures
- Time in bypass
- Bypass counts



From the LOPA ("Expected")
Severity 4 - single fatality

- X - BPCS failure
- Occupancy rate is low (1 order of magnitude
- SIL 2 SIF

Figure 4 – Risk matrix for a BPCS failure

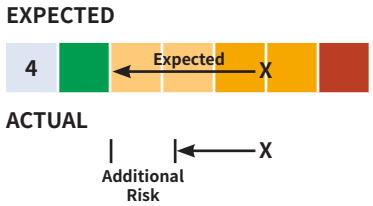


Figure 5 – Risk matrix for change to production turnaround

Since risk is a combination of the likelihood of occurrence of an event and its severity, a two-dimensional table, or risk matrix, is a useful assessment tool. If the value of any KPI listed above is below the assumed level, its location in the risk matrix is in a tolerable zone, or risk rank. For example, a SIL 2 safety instrumented function (SIF) activates upon a basic process control system (BPCS) failure with a single fatality at severity level 4.

In another example, plant management decides to take advantage of market conditions by increasing the turnaround interval. Although the profit margin justifies the decision, what is the safety impact?

The actual can no longer reach the tolerable area on the risk matrix because by extending the turnaround interval, the company is also increasing the test interval of the SIF. A longer test interval degrades the reliability of the SIL 2 SIF into a SIL 1 SIF.

With information for hundreds if not thousands of scenarios readily available, management can make much better business decisions. As an advanced decision support tool, the digital twin can rapidly process such scenarios and allows safety to be at the forefront of management decisions.

The digital twin applies across the entire enterprise. All the performance data can roll into a single metric that measures overall performance across all protection layers against assumptions made during initial design and maintained over the life of the facility. The fundamental concept behind the KPI is leveraging logic used in a LOPA study, where the team evaluates potential hazardous scenarios by establishing the severity of the event and the likelihood of the event occurring.

Part 7 Conclusion

> *...a Digital Risk Management solution can accelerate the process of increasing plant safety on a daily basis.*

The intention of this white paper is to help the reader assess where the company stands in its safety compliance journey and how a Digital Risk Management solution can accelerate the process of increasing plant safety on a daily basis. Key points and business benefits are summarized as follows:

- Yokogawa co-innovates with Sphera to utilize PHA Pro as the configuration engine in its Digital Risk Management solution.
- The LOPA represents the foundation for Sustainable SIS; with the Digital Risk Management configuration environment, no new training is required.
- Digital Risk Management requires little to no configuration and legacy data migration is not an issue.
- There is no need for new forms or management of change tools.
- It is easy to identify and quantify assumption differences between the LOPA and operating data.
- Operators can use real performance data during revalidations to minimize assumptions in the future.
- Operators can take action to eliminate intolerable risk or use extra precautions when further exposed.
- The Digital Risk Management solution is vendor agnostic.

Digital Risk Management also allows the process safety team to focus on risk reduction in terms of financial impacts and benefits to the business. Not only does this bring them into alignment with senior management, it allows them to justify investments in safety projects in a manner that is comparable to all other prospective capital projects. The safety lifecycle program thus transitions from purely a cost of doing business to an asset.

WP-S-20200511-01