Life Is On | Schneider Electric

Five Steps for Enhancing Industrial Process Safety through IIoT and Digitization

by Steve J. Elliott
Schneider Electric Senior Director - Marketing

Executive summary

Industrial Internet of Things (IIoT) technologies and concepts can transform and enhance process safety practices if appropriately applied. In the past, the success or failure of industrial safety efforts have been reliant on trending models based on historical data. IIoT opens the door to forward-looking perspectives on safety that accurately predict when safety risk factors will exceed accepted thresholds. This paper provides guidance for leveraging IIoT tools and techniques to deliver industrial safety in a profitable manner.

Introduction

New marketplace demands, and especially short production cycles are stimulating the proliferation of Industrial Internet of Things (IIoT)-related technologies across industries. This technology influx has changed industrial work execution processes which, in turn, may require modifications to the way safety is managed, especially in high hazard industries. In such fast-moving environments, a high degree of discipline and a mix of proper technology are required to maintain high safety standards.

IIoT technologies enable data to be quickly gathered and analyzed, thereby driving rapid, highly accurate decisions. Such capabilities are a great fit for enhancing process safety across industries. When product is kept "in the pipe" instead of on the floor or in the air, risk management is succeeding. IIoT complements risk minimization by improving process safety performance through the avoidance of near misses and unexpected outages.

IIoT-driven algorithms and predictive analytics can be configured to identify looming threats to equipment safety. The process of deploying predictive analytics includes the gathering of equipment asset historical data, and the building of mathematical models that reflect different operational modes of that equipment. This is then combined with sensors that gather live data to form a profile on a given piece of equipment.

Once the profile or signature of that equipment is established, guidelines for how that particular piece of equipment is supposed to perform can be determined. That information is placed online and a data repository is built-up that compares actual performance to expected performance. If there is a larger-than-expected deviation between expected and actual performance, then alerts can be sent out to safety and maintenance teams who can then pay attention to emerging risks.

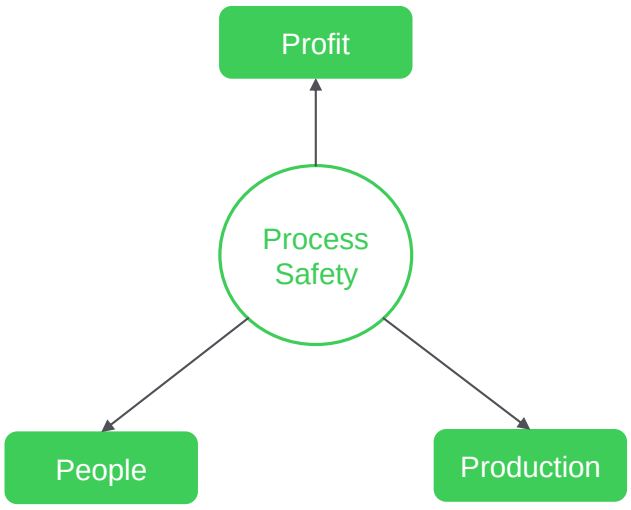

Figure 1

Improving process safety requires a delicate balance between profit, production and the minimization of human error

The alerts instruct the teams that an issue is likely to surface in the near future and that actions should be planned to avert future unanticipated downtime and potential safety issues. Consider a holding tank whose internal pressure control is beginning to show signs of failure and the risk of an explosion is increasing. By determining early enough in the failure sequence that a potential problem exists, a piece of equipment can be taken offline in a less costly, non-emergency situation and the fix can be applied before the asset experiences catastrophic failure.

Like purchasing insurance, safety costs money (as a result of the multiple investments required to assure a high level of safety), but safety also boosts corporate profitability (by maximizing process uptime) and lowers potential risk (by reducing the prospect of safety failure-related legal and corporate public image costs). This paper describes five steps for integrating new IIoT technologies to better manage risk and hazards and to avoid costly unscheduled asset downtime.

IIoT background and context

The amount of "things" or smart devices that are now being connected to the Internet is forecast to grow to almost 31 billion worldwide by 2020 (see **Figure 2**).[1] Since the cost of IP enablement is now so low, all sorts of devices are free to participate in the more open IP-style network. The shift in human behavior (i.e., the widespread use of mobile devices/smartphones) and the changing workforce (from retiring baby boomers to more social media savvy and "connected" millennials) is also driving the adoption of more IIoT technologies. The desire to measure and compare the effectiveness of objects that humans interact with is leading to a rapid acceleration in data creation, and more visibility to that data. For instance, a plant manager today has access to 10 times more data about his plant than he did 20 years ago.

For industrial safety stakeholders who hope to reap the benefits of the opportunities that this new flood of data represents, success will depend on their ability to integrate the proper software tools that drive the benefits of big data.

Advanced process safety means applying big data from manufacturing floor assets, from maintenance teams that are deploying digitization to enhance predictive maintenance techniques, and from analytics teams that are utilizing more detailed process information to optimize and speed up decisions.

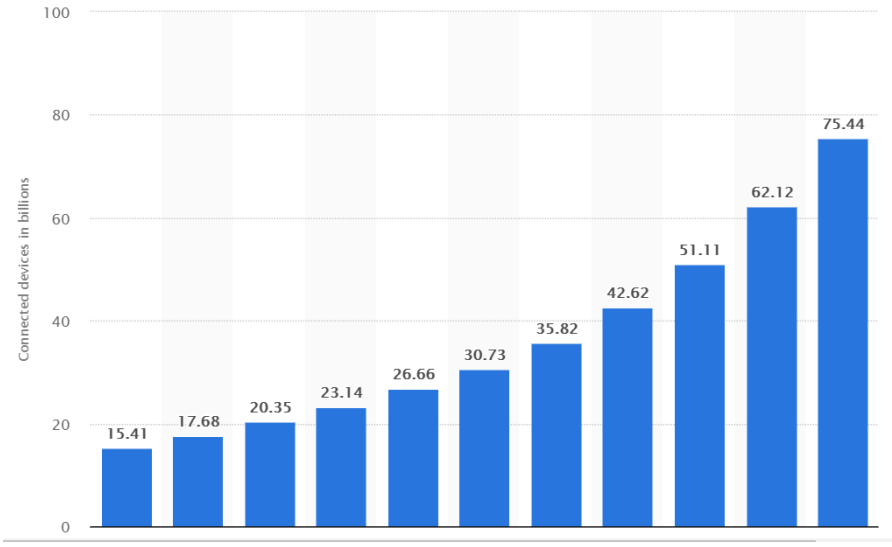

Figure 2

Projected growth of Internet of Things (IoT) devices in billions (courtesy of Statista)

In fact, from the safety engineer's perspective, digitization-driven process reliability improvements should help to improve safety as fewer assets fail. This means less human involvement and a diminished risk of human error. Since operators can potentially be given access to real-time operational data along with process control and real-time reliability risk data, their decisions can now directly foster both safety

[1] Statista, "Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions)", 2017

and profitability. Operators will be able to adjust set points and witness the impact their adjustments are having on process safety, profitability and reliability of the assets.

Most industrial safety incidents are rarely caused by a single event. More often it's the sum of seemingly small, disconnected events that, when combined, result in an incident. New analytics tools will now allow for much more precise identification of behavioral trends of assets. In this new world of advanced digitization, the safety engineer will need such analytics tools to understand the relationships and interdependencies between the data points. Patterns in the asset performance data can begin to emerge much earlier than what was previously possible. In this way operators and safety experts can pick up preliminary signals of impending danger before situations are allowed to spiral out of control.

Understanding IT / OT differences

The IIoT trend has emerged in part due to the convergence of Information Technology (IT) and Operation Technology (OT) teams. These two "worlds" are quite different in application, architecture and governance. Data experts versed in IT are rarely experts in OT-related process safety and vice versa.

IT and OT have evolved in different directions, timescales, and often use different data types and information structures and architectures. They are sufficiently different in purpose and nature to pose formidable barriers to making them compatible, let alone combining, synchronizing and exchanging data between them.

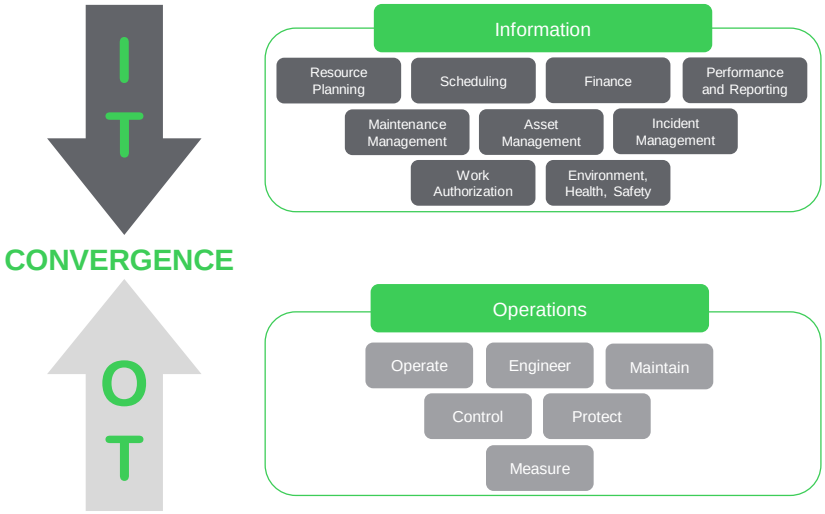

Figure 3

Converging worlds: Advanced connectivity is merging IT with plant physical infrastructure assets

IT has evolved from the top down, focusing primarily on the business needs (i.e., corporate operations and systems that were required to manage the business primarily from a financial perspective). IT also assumes a more substantial "consumer" connotation, as IT systems are resident on millions of personal home and business computers. IT systems are based on well-established standards that can accommodate the integration and management of large volumes of information across entire organizations.

OT systems, on the other hand, have grown from the bottom up, with many different and often proprietary systems, designed by different manufacturers to control specific processes and equipment in real-time environments. OT technology is often deployed in harsh environments and typically has a low tolerance for failure and significant requirements for recovery and redundancy. OT environments are characterized by focused governance models and highly insulated/localized processes. Companies like Schneider Electric have

developed expertise in both of these domains and are well positioned to help industries in their implementation of IIoT technologies. This includes support in improving process safety productivity, process safety performance, and ultimately deriving additional profitability from IIoT-driven safety measures.

Step 1: Digitize and connect

One high-level goal of harnessing IIoT and the associated digitization benefits is to drive cost-effective industrial safety. A first step in the process is to capture the data flowing from the various safety related tools such as Safety Instrumented Systems (SIS), Safety Instrumented Functions (SIF), Layer of Protection Analysis systems (LOPA), Process Hazards Analysis tools (PHA), and Hazard and Operability tools (HazOp). This data should be centralized into a digital database that will help to make safety critical design information consistent, quick to access and easy to use.

These traditional safety tools are designed to meet specific safety parameters. However, how they perform once deployed may be different from the original design intent. Therefore, the "as designed" data (e.g., demand rates, test intervals, time in bypass) should be digitally connected to the "as operating" data so that the potential safety risks presented by systems degradation can be assessed in real-time (for example, identifying potential gaps in Instrument Protection Layers and seeing what the real-world impact is on operational safety integrity). By digitally connecting to existing systems and data sources, the need for manual data collection and data handling is minimized and the new real-time information can then complement the safety information gleaned from existing reports. This digitization provides a more meaningful context than the traditional historical analysis of safety KPIs, enabling personnel to see what's coming, rather than analyzing incidents after the fact.

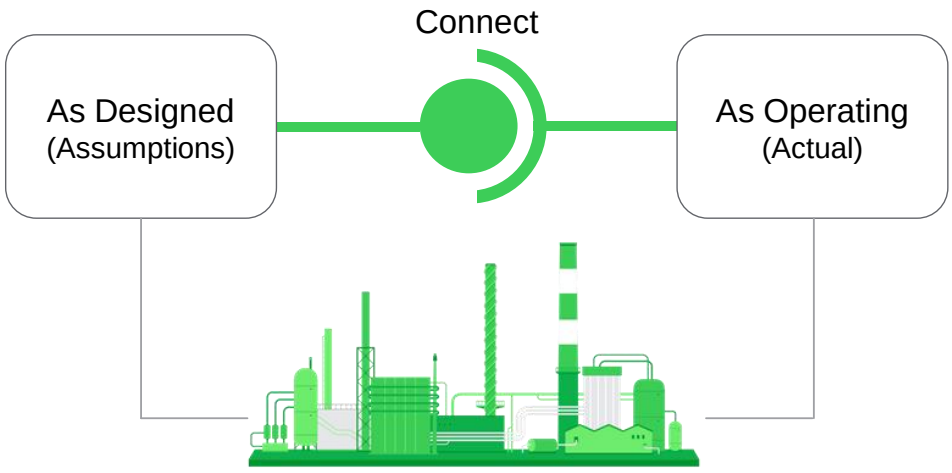

Figure 4

Digitization enables identification of safety gaps as independent protection layers transition from design to operation

Step 2: Adopt analytics to identify trends

Once the safety data is gathered and centralized, a second important pillar for leveraging the benefits of IIoT is to utilize analytics to obtain meaningful and actionable insight from the disparate data and systems. Before any analytics tools are deployed; however, the types of analytics required should be determined.

Below is a list of relevant types of safety analytics that should be considered:

- **Descriptive analytics** – These analytics illustrate what happened surrounding specific safety incidents and answer the question of which pieces of equipment are failing and over how much time.

- **Diagnostic analytics** – These data points will explain the reason why the safety incident occurred and will identify the primary causes of failure to determine whether any correlation exists between unique failure incidences.

- **Predictive analytics** – This type of information will forecast what kind of safety incident are likely to happen in the near and (somewhat) distant future. The predictions made are tied to business decisions (like when to perform maintenance). The analytics engine uses rules either based on actual conditions or behavior patterns and leading indicators to determine which parts or equipment are likely to fail.

- **Prescriptive analytics** – These analytics serve to prompt safety personnel on what actions to take. These tools incorporate external data sources such as personnel tracking and environmental conditions to create prescriptive capabilities.

Together, this analytical data crunching can help plant personnel determine the optimal production and maintenance activities across multiple assets to reduce cumulative risk and to minimize downtime.

From a safety perspective the data gathered can also be useful for companies working with industry regulators to help certify the safety levels of their plants.

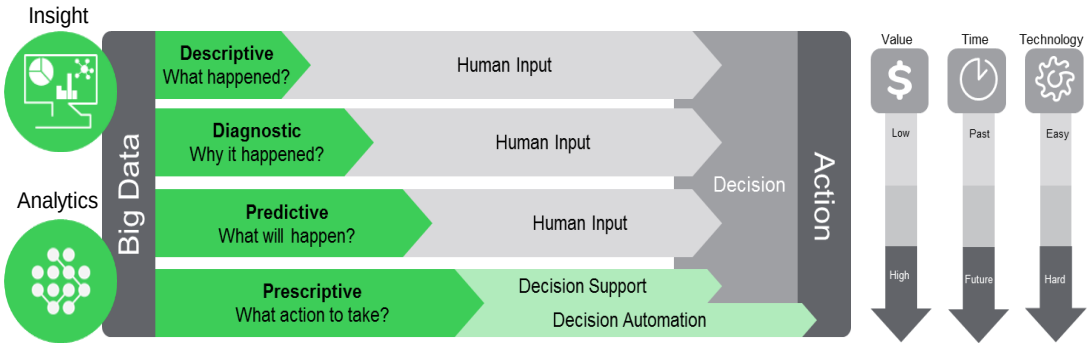

Figure 5

Use analysis tools and techniques to create meaningful and actionable insight

The implementation of an analytics solution can reveal the interdependencies between different systems, highlight safety critical elements, and calculate the cumulative effect of multiple deviations or degraded conditions. In addition, by also factoring-in and comparing historical conditions and performance patterns, trends for unconsidered scenarios can emerge. Conditions that could escalate to an unsafe state if not properly managed are also identified.

The human interface to the analytics engine can provide contextual visual clues that make it quick and simple for operators to understand the current situation and identify potential issues before they arise. The information can also be accessed and shared remotely so that safety administrations don't have to be tied down to a particular control room, office or specific geographical region.

The information provides key stakeholders—such as operations, maintenance, engineering, reliability and safety personnel—with an understanding of operating risk levels (i.e. are you operating under a state of higher risk than intended) and warns administrators of potential deviating conditions. Through this digitization-driven collaborative sharing of information, potential consequences, elevated risk levels,

and cumulative risk are recognized *before* a change is made or a restriction is placed on an Instrument Protection Layer (IPL). As a result, administration of safety best practices is less costly and more efficient.

Step 3: Deploy cloud solutions to control costs

Cloud computing and/or Software as a Service (SaaS), are driving changes across the process industry. In the past, a plant manager might have only a few options for bolstering safety systems. The solution was to buy software and hardware, hire the IT professionals to manage the infrastructure, and hope it all worked. This was very costly, especially in low-margin industries. But cloud computing is now offering affordable options. Now, third-party providers can offer solutions through a monthly subscription fee, with no upfront fees for hardware and software.

The cloud can be considered a central rallying point and a means for reducing the infrastructure and deployment cost of safety tools, applications and data (but only where and when it makes sense). The cloud computing/SaaS model makes possible the option of bringing safety data and its context to experts anywhere in the world so that discrete IPLs can be analyzed for safety decisions to be more consistent.

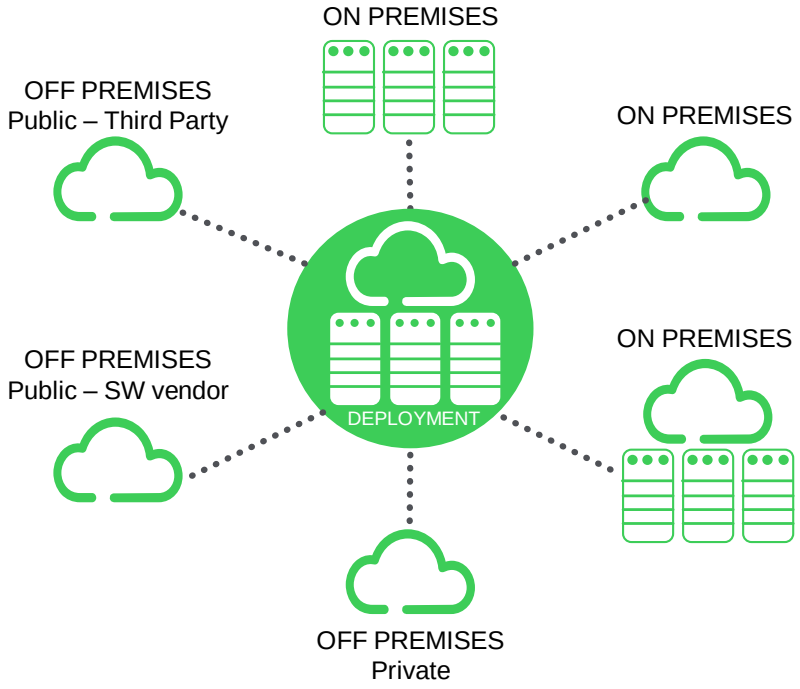

Figure 6

Consider the cloud as a central rallying point

Such a solution also drives transparency throughout the organization and removes the traditional barriers and silos within departments, management structures, assets and/or fleets of assets. Using the cloud as the single “source of the truth” for digital safety design, analysis and validation makes it easily accessible to everyone, anywhere and at any time.

Step 4: Introduce simulation to bolster safety

New generation Operator Training Systems (OTS) use dynamic simulation technology to produce a high definition representation of industrial processing systems including the process equipment, controls, and automated procedures. Modern instrumentation collects data on tens of thousands of variables. All of that data is accessible in order for simulation process models to be optimized as they are tied into the plant control system. Therefore, when simulation-driven changes are

applied to live production systems, they are the best changes for the plant from a safety, efficiency and productivity perspective.

Virtual models referred to as “digital twins” analyze the gathered data and then use it to run simulations and to benchmark performance, allowing plant operators to pinpoint where efficiency gains can be made. By pairing both virtual and physical worlds (the twins), problems can be actively averted before they occur, preventing potentially threatening safety situations.

The digital twin can be utilized, for example, to validate the safety system design *before* the system is physically manufactured. It can be used in an ‘offline’ mode to run “what if” scenarios, determining potential elevated risk levels. Used in ‘online’ mode, the digital twin can provide a dynamic model of the operating asset to head-off problems before they occur or to identify the root cause of an issue.

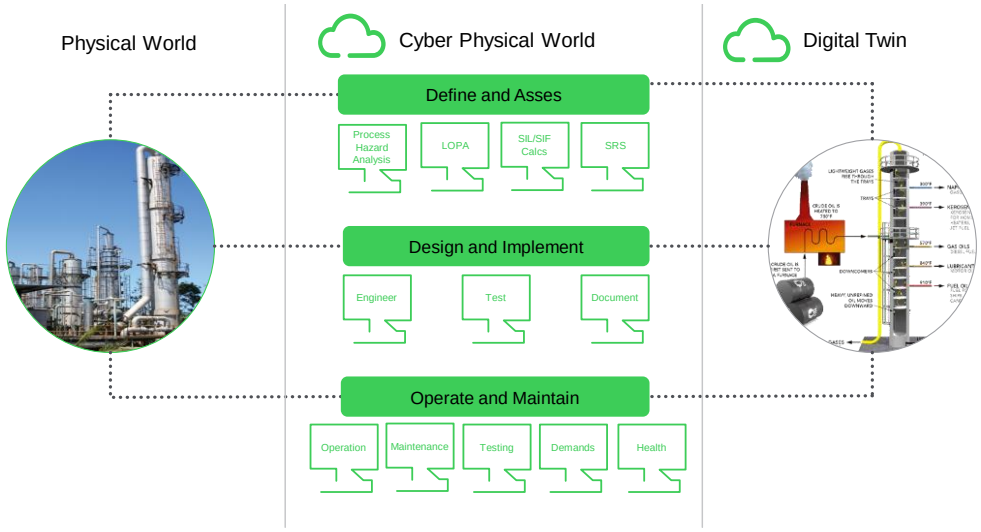

Figure 7

Virtual models such as digital twins greatly reduce plant equipment deployment safety risks

Step 5: Integrate a cybersecurity strategy

Although IIoT and the related digitization initiatives offer many opportunities for improving industrial safety, connection to the broader internet also introduces the new risk of subjecting safety systems to cyberattacks. To counter this threat, an ongoing cybersecurity strategy needs to be implemented that complements the safety strategy.

In all cases, local safety teams must examine whether it makes sense to enable safety systems internet connectivity at all and, if so, under what conditions. In some cases, a tool such as the plant historian might require access to safety-related data or information. Again, digital risks will need to be assessed on a case-by-case basis. Updated safety-related standards such as IEC61511 and IEC62443 can provide guidance on how to account for cybersecurity risks.

Affected stakeholders will need to merge their current practice of protecting “man from machine” (i.e., how a safety system protects workers from chemical and mechanical process risks) with a new practice that protects “machine from man” (i.e., how factory floor operational equipment is protected from outside cyberattack).

The sources of threats include not only invisible hackers that are patrolling the internet in search of soft targets, but also internal employees and outside suppliers that come into the industrial sites. The weakest links are the people who administer and use the systems. Their actions, either intentional or unintentional, can increase

the security risk to systems. As a result, cybersecurity training of employees and outside suppliers coming in is just as important as the implementation of cybersecurity software solutions.

Responsible control systems manufacturers are now designing cybersecurity into every module they build and deliver so that clients don't have to concern themselves with building in cybersecurity after they purchase a new product.

Manufacturers like Schneider Electric, for example, apply a Secure Development Life Cycle (SDL) approach to product development. Within the context of SDL, secure architecture reviews are performed, threat modeling of the conceptual security design takes place, secure coding rules are followed, specialized tools are utilized to analyze code, and security testing of the product is performed. These actions help to 'harden' products, making them more resilient against cyber-attacks, right out-of-the-box. In this way, as new products replace old, entire systems evolve to become more cyber secure. Examples of Schneider Electric safety-related products that have undergone such scrutiny and achieved Achilles Level 2 Certification include the Triconex range of logic solvers (Tricon, Trident, Tri-GP) and Modicon M580 control and safety ePACs.

Figure 8

Cybersecurity process is naturally aligned to industrial process safety

Conclusion

The world of process safety has for many years pursued a philosophy of managing safety systems as separate entities, independent, unconnected and certainly secluded from the internet as much as possible. This approach is now changing; the benefits of digitization and using safety-related data are outweighing the risks of a more open connectivity (provided that sound cybersecurity strategies are implemented). The advent of the Industrial Internet of Things and the related digitization technologies now enable industrial safety experts to analyze safety issues from past, present and future perspectives. This leads to safety-related simplification in two key areas – risk management and operations management – and helps with the everyday integration of the two.

The use of IIoT tools and techniques represents tremendous potential for smarter and faster execution of safety best practices. These tools can empower the industrial workforce to make more informed, better operating and business decisions, helping them drive a profitable, safe operation.

About the author

Steve Elliott is a Schneider Electric Senior Director of Process Automation Offer Marketing and is responsible for formulating future directions and go-to-market strategies. He is a TÜV certified functional safety engineer with more than 20 years of experience in the process control and automation industry. He has extensive experience designing safety systems and industrial safety lifecycles.