RESEARCH SPOTLIGHT

IIoT: INDUSTRIALS GETTING RESULTS

Companies Reducing Risk & Improving Productivity in Operations

Introduction

Manufacturers are increasingly deploying Industrial Internet of Things (IIoT) technologies to enable smart, connected operations. This digitalization trend has major implications for risk management in industrial operations and the impact it has on safety, security, and productivity.

Over the past decade, industrial organizations have used operational risk management (ORM) to manage safety and environmental hazards in production operations, with the goal of safeguarding people, assets, and the environment. Effective ORM processes have proven useful in preventing adverse events and the negative impact they have on operational and financial performance.

Safety systems are an essential element of effective ORM, to protect employee and process safety during operations and maintenance. With the trend towards Digital Transformation in manufacturing, concerns over cyber security, IIoT-enabled integrated safety controllers, and industrial networks with IIoT gateways have given industrial companies a whole new set of risk factors to consider.

Traditionally the safety systems debate has centered on balancing the trade-offs of creating a single point of failure versus reduced complexity and improved performance. Now, in an IIoT world, new approaches to safety and risk management are available. A significant development in this regard is the concept of offering a single integrated safety and process control solution using common controllers, input/output (I/O), and networks.

This research investigates how IIoT technologies are transforming manufacturing operations, and how this impacts productivity and safety on the plant floor and enterprise-wide. We'll present frameworks for using ORM to balance the decisions for incorporating IIoT technology and safety functionality into the process control system, while still maintaining the risk levels mandated by good design practice.

INDUSTRIAL INTERNET OF THINGS PLATFORM

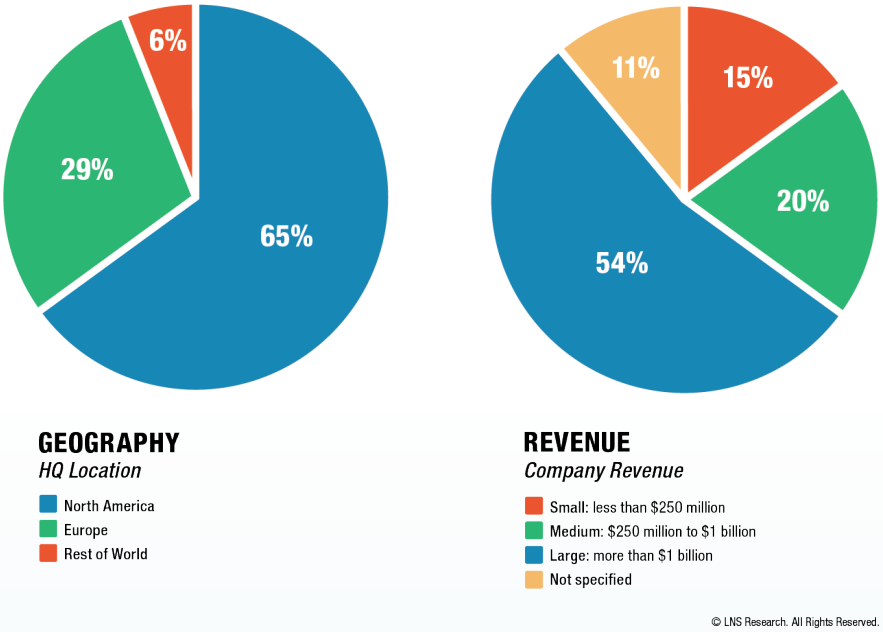
by LNS Research describes the connectivity, network styles, and applications framework to support smart connected operations and smart connected assets; within and across a plant, facility or production network in a manufacturing or other industrial operations setting.

Click to learn more about the **Industrial Internet of Things Platform**

Research Demographics

Most of the data and insights presented in this report are drawn from primary research conducted by LNS Research on the topic of safety and risk management best practices and their relationship to enterprise business performance. We gathered data via an online survey in quarter three of 2017, from 300 respondents across a variety of geographic regions and company sizes. Respondents reflected in the data presented are mainly operations, environment, health and safety (EHS), and engineering managers and professionals in industrial manufacturing organizations. The industry segmentation is diversified across discrete, process, and hybrid manufacturing, including the food and beverage, mining, and metals sectors.

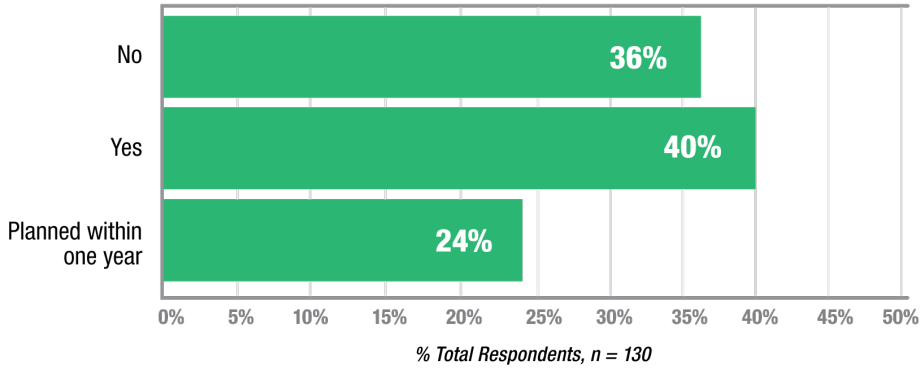
We selectively supplemented the data from this survey with data from the ongoing LNS Research IIoT survey, which has a similar industrial demographic profile.



The IIoT Enables Smart Connected Operations

The Digital Transformation trend sweeping across global industry goes by many names: Smart Manufacturing, Industry 4.0, and the Fourth Industrial Revolution, among others. Regardless of what it's called, Digital Transformation is here to stay, and it's disrupting industries, enabling new business models, and creating competitive advantage for organizations that embrace it.

Has your company started an IIoT initiative (i.e. smart manufacturing, Industry 4.0, etc.)?



% Total Respondents, n = 130

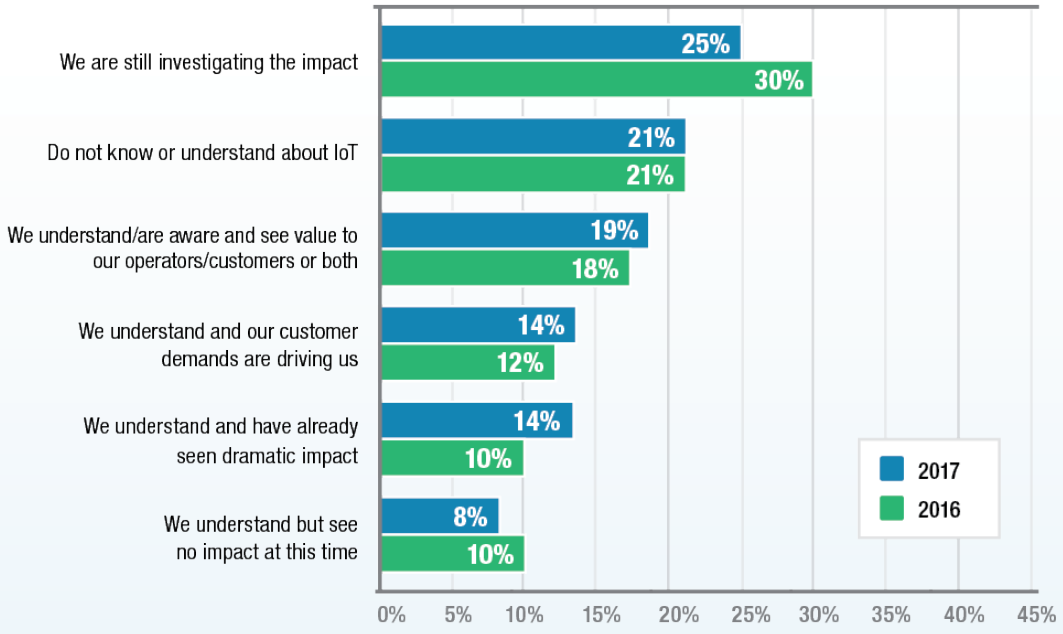
The essential enabler of this phenomenon is the IIoT — the use of cyber-physical systems to connect people, machines, and data in new ways. Several critical technology innovations underpin the IIoT, including sensor-equipped smart devices, Cloud computing, mobile apps, and Big Data analytics.

Smart connected operations leverage the IIoT to capture and gather large volumes of diverse data types on a breadth and scale not previously possible. The application of advanced analytics to this data provides new actionable insights and increased predictive/autonomous control of operations to optimize performance.

60% of companies have yet to leverage IIoT technologies.

—PETER BUSSEY
Research Analyst

Please indicate how the IoT is impacting your business today



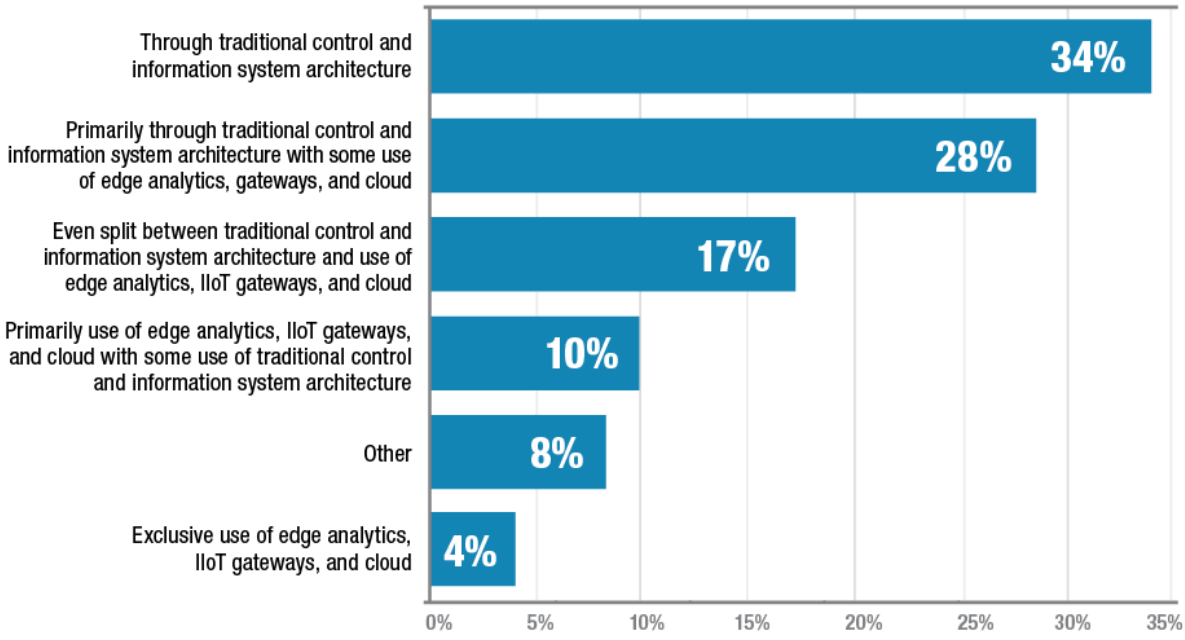
Does Digital Transformation and IIoT have a real impact on industrial organizations? Although many businesses are at an early stage in the adoption of IIoT technologies, that's changing rapidly. Our survey data show a consistent trend of companies moving from investigating the impact of IIoT to a clear recognition of potential business value, and acting to realize that value.

The Double-Edge Sword of IIoT: Opportunity and Risk

Industrial companies are picking up the pace of IIoT technology adoption to take advantage of the opportunity to optimize operations and boost financial performance. The first wave of investment has been aimed at improving vital areas such as asset reliability, operational efficiency, product quality, and safety and environmental performance.

The IIoT is enabling new information and data architectures. Two-thirds of manufacturers already deploying IIoT technology are using it to break down the traditional hierarchical approach to manufacturing systems. Technologies such as IIoT gateways, Edge analytics, and Cloud computing are increasingly enhancing and displacing traditional systems.

Today, how are you architecting the flow of IIoT data?
(N=167, companies with IIoT initiatives)

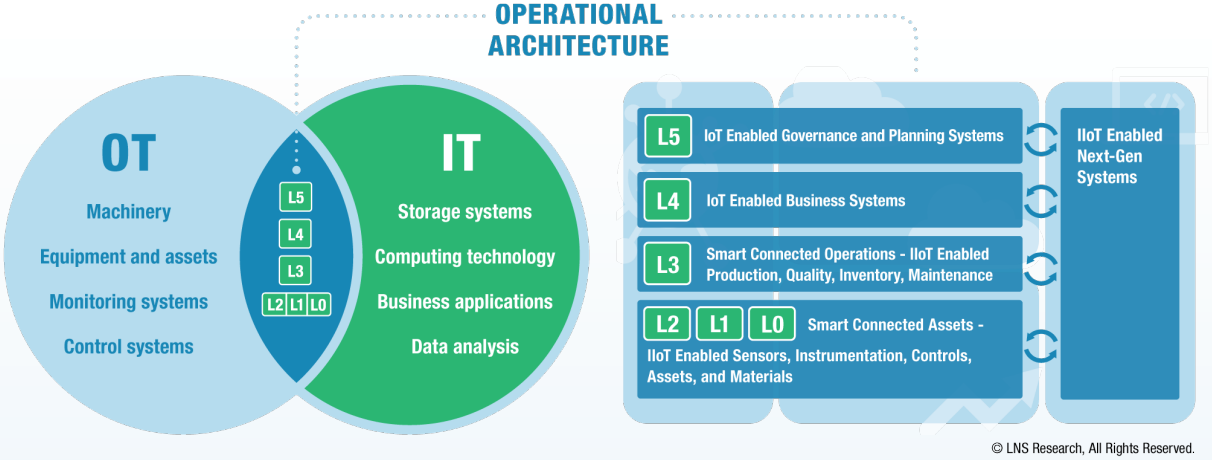


The proliferation of IIoT-enabled devices and networks of connected assets represents downside risk as well as upside potential. As is often the case, the introduction of technology innovations creates new risks. Fundamental changes in business models (e.g., service provider versus manufacturer) and work processes (e.g., autonomous production) can quickly change the portfolio of operational risks an organization has traditionally managed — namely safety, health and environmental risks that can harm people, assets, and the environment.

IIoT also exposes companies to new-to-the-world risks which are less understood and more difficult to manage using traditional ORM processes. Many of these novel risks are driven by the IT/operational technology (IT/OT) convergence trend; two formerly independent domains of information technology and operational technology are coming closer together.

IT/OT convergence creates the need for — and enables — a more integrated approach to safety and risk management, especially to manage new types of risk such as industrial cyber security. This approach should certainly consider direct cyber-attacks via internet-connected devices, and vectors such as removable media devices and email spear phishing. Cyber attackers commonly use these to deliver malware and they potentially threaten industrial systems. In this dynamic environment, a strategic approach to operational architecture that incorporates IT and OT becomes more critical to provide a framework of process, data, application technology standards.

> Only **28%** of industrial organizations use a lifecycle approach to risk management.
>
> **—PETER BUSSEY**
> *Research Analyst*

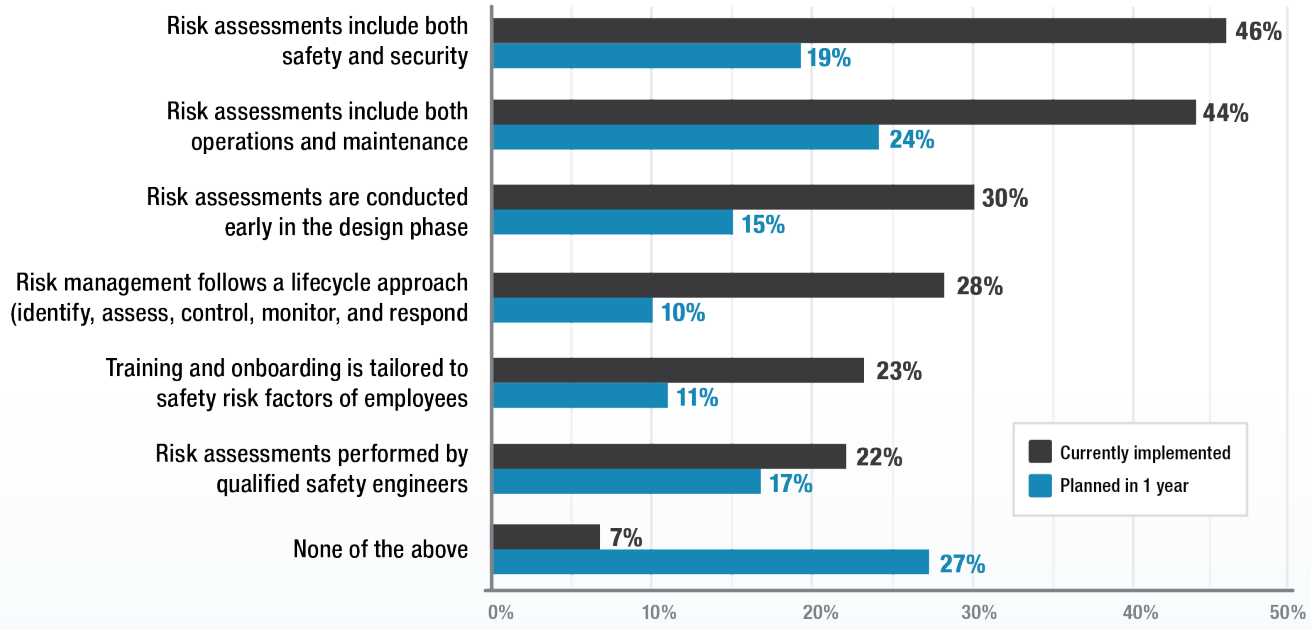


Disconnected ORM Processes Prevalent

Many widely-adopted industry standards call for a systematic risk management process in industrial operations. Examples include IEC 61508 (functional safety), IEC 61511 (safety instrumented systems), ISO 27005 (information security risk management), OHSAS 18001 (occupational health and safety) and ISO 31000 (risk management). These standards reflect best practices at various levels of operational architecture ranging in granularity from process control systems to equipment and assets, to business systems, to enterprise governance and planning systems.

These standards share a common requirement for closed-loop risk management across the lifecycle of the relevant scope of risk, whether it be safety systems, process safety, worker health and safety, cyber security, operational continuity, and so forth. However, only 28% of industrial organizations use a lifecycle risk management approach.

Risk Management Process Capabilities

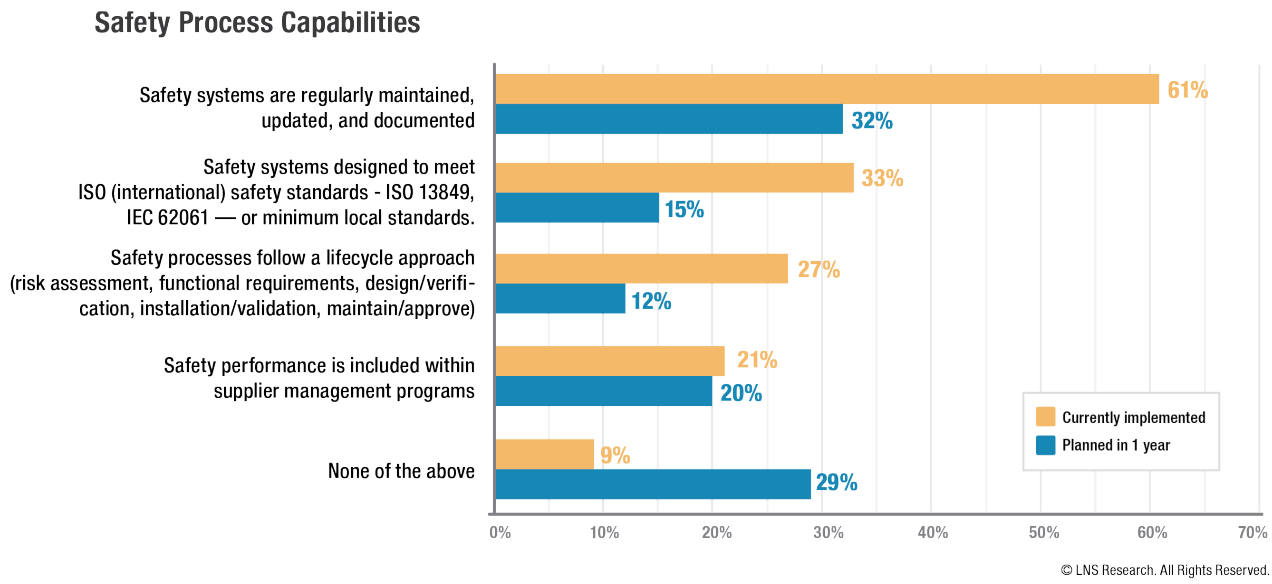


This lack of adoption means that fragmented approaches to risk management are common, contributing to unnecessary exposure. When companies do conduct risk assessments, it often involves cross-functional collaboration between domains such as safety and security, and operations and maintenance. So, there is a good basis for a more unified approach that addresses both traditional operational risks as well as new threats such as industrial cyber security. In context, IIoT technologies

are both part of the problem by creating new risks, as well as part of the solution by enabling better lifecycle risk management processes.

Room for Improvement in Safety Process Capabilities

System safety is essential to effective ORM, especially in asset-intensive and high-risk industries such chemicals, oil and gas, mining, mill products, and many others. These types of industry sectors rely heavily on operational technology including process control and safety systems to ensure safe, smooth-running operations.



The survey data show that adoption of safety system process best practices is similar to overall risk management. Industrial organizations generally do a good job on the fundamentals of managing safety systems, with a majority regularly maintaining, updating and documenting safety systems. A significant percentage (33%) design safety systems to standards.

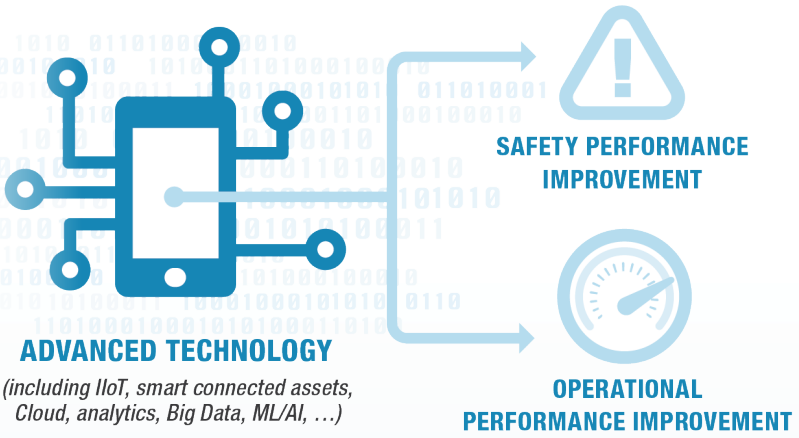
However, only 27% use a lifecycle approach to safety system management that includes risk assessment. Safety system management processes often exist in silos. Companies can benefit by moving towards a lifecycle approach that incorporates risk assessment as part of a holistic ORM process.

Untapped Potential of IIoT Technology to Mitigate Risk and Improve Performance

Two-thirds of respondents report that their safety systems are designed to mitigate risk and improve performance, or that they have plans to do so soon, and nearly half say this capability is already in place today. These numbers indicate that companies clearly recognize that safety and productivity are not mutually exclusive, and have the potential to synergistically improve operational performance.

A relatively low portion of respondents (11%) indicate their organization is using IIoT technologies to holistically manage operations and safety performance, including engineering and maintenance. Considering that doing so is an ambitious undertaking, this strikes us a positive indication of an aspirational posture.

Notably, 20% of companies say they will start using IIoT this way in the next 12 months; this is a relatively high figure compared to the current adoption rate. Evidently, companies recognize the potential of advanced technology to simultaneously improve safety and productivity, and are embracing IIoT technology to get there faster.



20% companies plan to adopt IIoT technology in next 12 months to improve safety and operational performance.

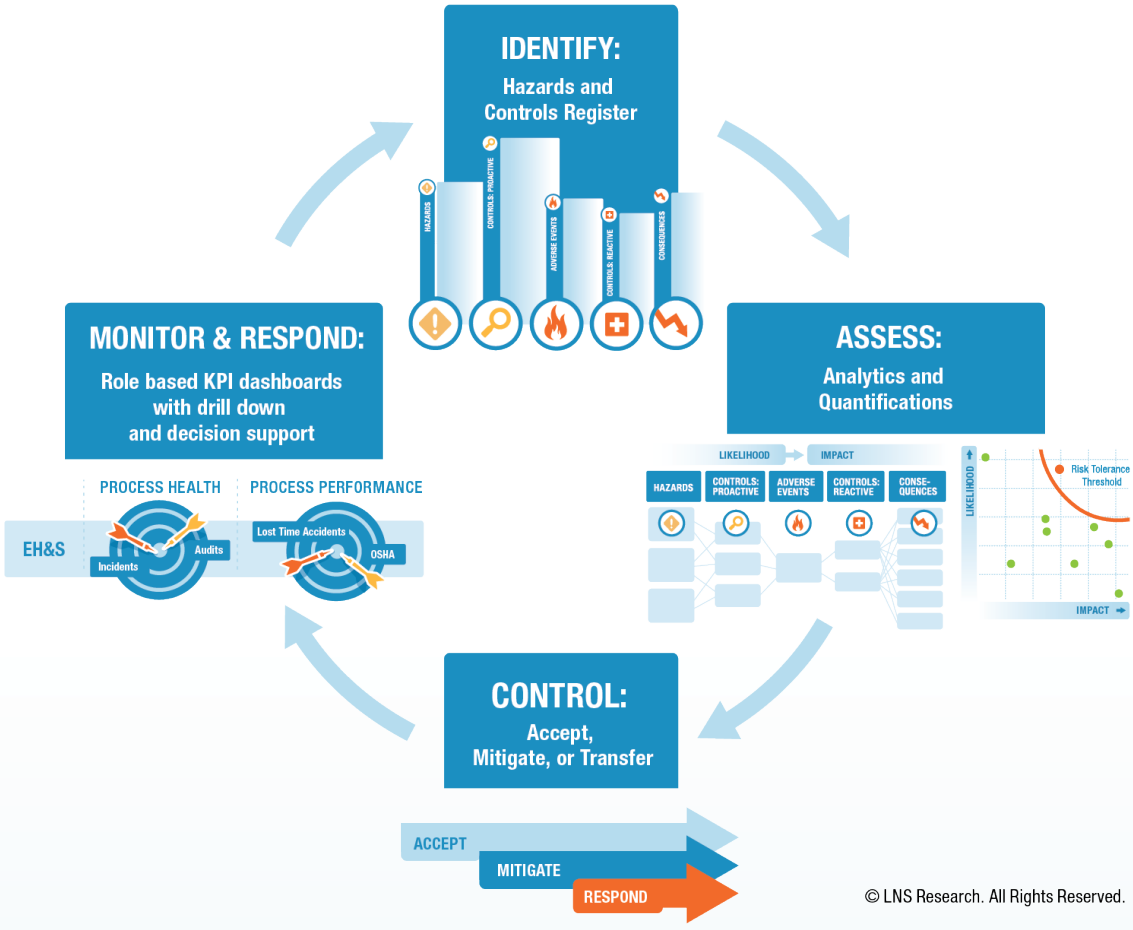
plan to adopt IIoT technology in next 12 months to improve safety and operational performance.

—PETER BUSSEY
Research Analyst

An Integrated Approach to ORM for an IIoT World

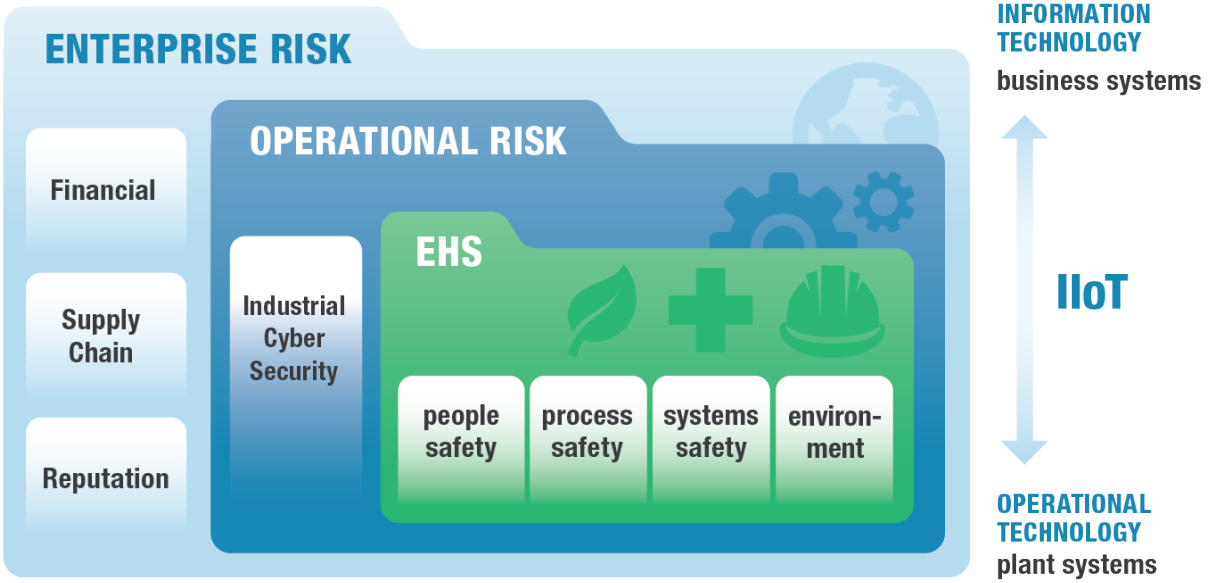
The LNS Research ORM model is a closed loop process for systematic risk management consistent with best practices in the ISO 31000 risk management standard. Many companies have implemented such a process (with varying degrees of success), usually to manage risks associated with basic safety and environmental hazards.

As mentioned previously, the IT/OT convergence trend enabled by IIoT technology is changing the historical relationship between enterprise business systems and plant/process control systems. On the one hand, the implementation of smart connected assets and operations has greatly expanded the scope of information security risks to be managed, mainly in the form of industrial cyber security threats. On the other hand, IIoT can provide vastly greater volumes and variety of data and advanced analytics capabilities to leverage for predictive risk management and autonomous operations.



Industrial organizations should consider adopting a more integrated framework for managing risk. At the high level, all risk categories including strategic enterprise risk, should be managed with a systematic risk management process a la ISO 31000. Within that framework are traditional operational risks related to people, process and system safety, and environmental management. Although these risk categories are

governed by different standards, and typically by different business domains, they share a common requirement for lifecycle risk management. Companies may find many commonalities in organization, process, and technology that they can leverage for a more unified, cost-effective approach.



For the same reason, it's advisable to consider including industrial cyber security risks within the scope of operational risk management processes. Doing so will also facilitate the innovative use of IIoT technology to improve safety and operational performance together with connected ORM. For example, best practices as dictated by industry design standards require that process control and safety functions remain independent to avoid failure of one to compromise the other.

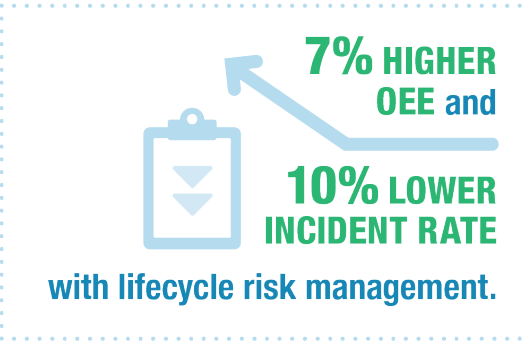
Historically, this has been accomplished by a programmable controller to control non-safety plant functions, and a separate system to control safety functions. Now, IIoT-enabled common safety controllers provide a single, integrated safety and process control solution while still maintaining the risk levels mandated by good design practice. Such systems are designed with industrial cyber security risk in mind and can reduce cost, risk and time to value.

Evidence of Value: Safety and Operational Performance

A long-held view in many industrial organizations is that safety comes at the expense of profitability. This perspective asserts that procedures and processes required for safety compliance reduce productivity and increase costs. Fortunately, as companies have evolved towards an Operational Excellence approach to continuous improvement, there has been a shift away from this trade-off mentality.

The survey data strongly support the notion that adoption of safety and risk management best practices lead to better operational performance across safety, reliability, and efficiency dimensions:

- 7% higher overall equipment effectiveness (OEE) with a lifecycle approach to risk management
- 50% lower incident rates when safety systems designed to both mitigate risk and improve performance
- 25% lower incident rates when IIoT technology used to holistically manage safety and operational performance



IMPACT OF PRACTICES ON INCIDENT RATE*

BEST PRACTICE	IMPLEMENTED	NOT IMPLEMENTED
Lifecycle approach to risk management	1.8	2.0
Safety systems designed to both mitigate risk and improve performance	1.5	3.0
IIoT technology to holistically visualize and analyze engineering, maintenance, operations and safety performance	1.5	2.0

*Total recordable incident rate per 100 employees per year

Recommendations

Industrial organizations are increasingly deploying Industrial Internet of Things (IIoT) technologies to enable smart, connected operations. This has major implications for managing operational risks related to safety, cyber security, and productivity in a digital world. Effective ORM processes have the potential to drive improvement in terms of safety performance and operational performance measures including quality, reliability, and efficiency. Operations, EHS, cyber security, IT and risk business leaders should develop a strategy to seize the performance opportunities while mitigating risk:

1. **RECONSIDER THE SCOPE OF OPERATIONAL RISK MANAGEMENT (ORM).** It may make sense to expand the categories of risk covered by ORM processes. Identify commonalities and potential synergies across people, process, and technology capabilities to drive more cost-effective risk management.
2. **ZERO IN ON INDUSTRIAL CYBER SECURITY RISK.** Adopting innovative digital technologies creates new risks to manage. Many organizations haven't adequately assessed the cyber security threats to take appropriate action. It's likely that current information security risk measures are inadequate to deal with the risks resulting from IIoT technologies. Given the potential impact of an industrial cyber security breach on safety and operational integrity, it could make sense to address this new breed of risk within your ORM framework.

3. **EMBRACE INNOVATIVE TECHNOLOGY TO REDUCE COMPLEXITY AND INCREASE EFFICIENCY**. While IIoT technologies tend to complicate the IT/OT landscape, they can also be used to simplify and optimize operational performance. IIoT-enabled devices have the potential to reduce cost, risk, and time to value.

4. **DON'T FORGET ABOUT PEOPLE**. Improving safety and operational performance is a team sport that requires cross-functional collaboration across multiple domains including operations, engineering, maintenance, EHS, and other disciplines. Viewing technology as a solution without adequate regard for stakeholder buy-in, process improvement, and a strong business case could derail a project before it evens gets started.

Presented by:

LNS research

ACRONYM QUICK REFERENCE
VIEW ON BLOG

Author:

Peter Bussey,
Research Analyst
peter.bussey@lns-global.com

License to distribute this research report has been granted to:

Schneider Electric
www.schneider-electric.com

LNS Research provides advisory and benchmarking services to help Line-of-Business and IT executives make critical decisions. Our research focuses on the Industrial Internet of Things (IIoT), Digital Transformation; and providing insights into the metrics, leadership, business processes, and technology capabilities needed for achieving Operational Excellence. Learn more at www.lnsresearch.com.