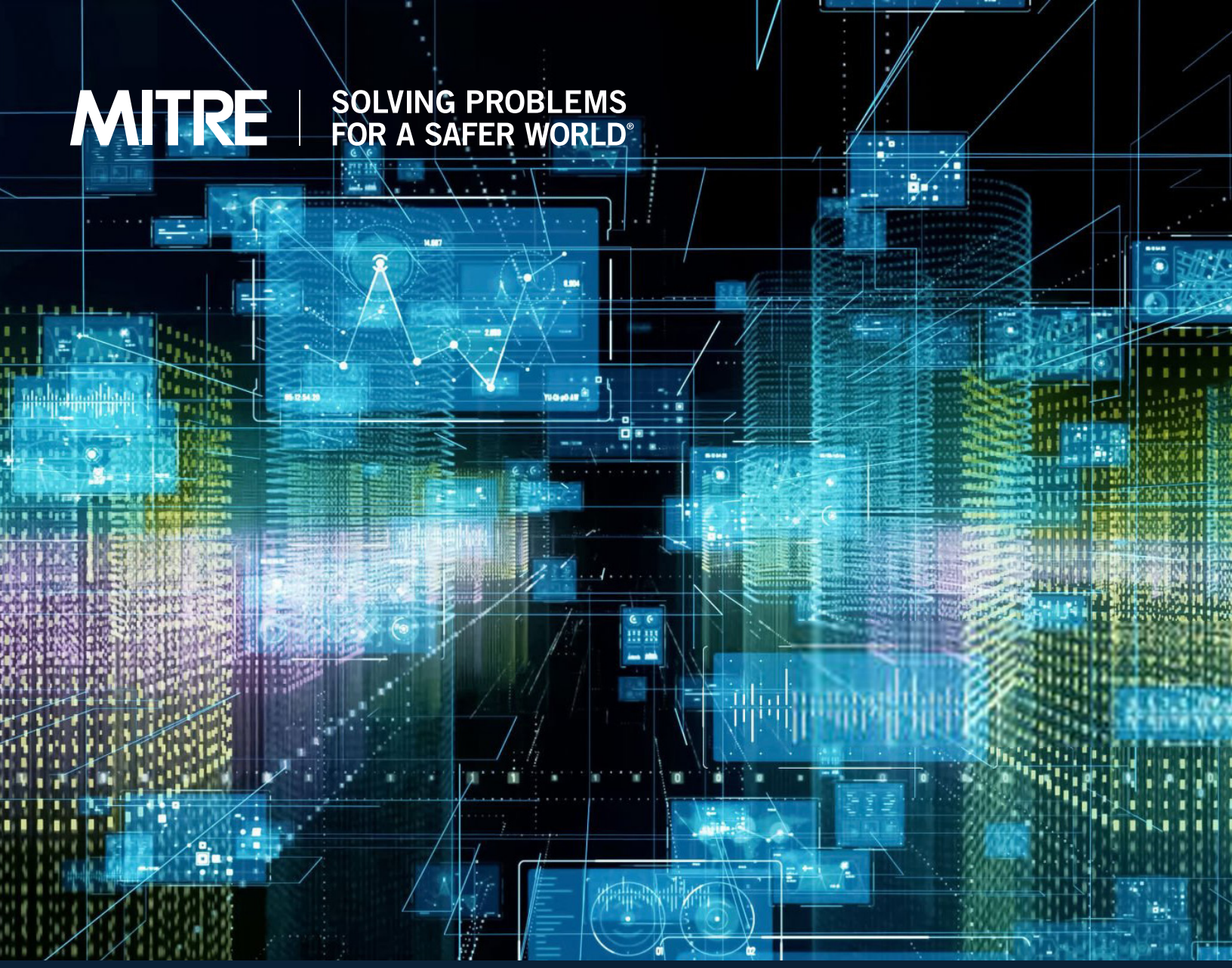

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®

THE NEXT LEVEL OF SAFETY: EVOLVING SAFETY IN THE DIGITAL AGE

The MITRE Corporation

May 2022

We are in the midst of a digital transformation of business and society that is fundamentally altering our lives. Entire industries, from healthcare to finance to transportation, are being re-imagined, driven by a radical rethinking of technologies, talent, and processes to improve operations. This digital transformation will impact the safety of these operations as well. How can we take full advantage of this information revolution to improve safety? How can we go beyond traditional retrospective approaches that will not scale, such as finding and correcting issues through compliance checking, to create resilient systems that naturally recover to a safe state?

The Next Level of Safety is an approach that combines the ubiquitous data produced by the information revolution with advanced analytics to generate timely safety intelligence and accelerate safety improvements. It is characterized by a system-of-systems perspective, proactive monitoring and analysis leveraging the phenomenal increase in information connectivity, and performance-based standards and regulations.

THE NEXT LEVEL OF SAFETY IS AN APPROACH THAT COMBINES THE UBIQUITOUS DATA PRODUCED BY THE INFORMATION REVOLUTION WITH ADVANCED ANALYTICS TO GENERATE TIMELY SAFETY INTELLIGENCE AND ACCELERATE SAFETY IMPROVEMENTS.

In this paper we describe both the challenges and opportunities the information revolution presents for improving safety. We define four principles that distinguish the Next Level of Safety and propose potential next steps for accelerating its adoption.

Leveraging the Information Revolution to Improve Safety

The Next Level of Safety leverages the changes introduced by the information revolution, often referred to as the Fourth Industrial Revolution[1]. Building from the Third Industrial Revolution, where electronics and automation caused a digital transformation, the Fourth Industrial Revolution is a fusion of the physical, digital, and biological worlds[2]. This latest industrial revolution is based on a fundamental change in the way data are created, collected, processed, and analyzed. Billions of devices are generating unprecedented volumes of data on a continuous basis around the globe. Examples span healthcare (electronic medical records), transportation (highly automated vehicles), and critical infrastructure (industrial control systems). The vast potential of the Fourth Industrial Revolution lies in combining this ubiquitous data with advanced technologies to drive innovation. Examples of innovative new technologies that are already leveraging this data include artificial intelligence/machine learning (AI/ML), cloud computing, robotics, autonomous operations, 3D printing, the Internet of Things, and advanced wireless technologies.

The information revolution is accelerating dramatic shifts in scope, scale, speed, and complexity across many industries, from healthcare to transportation. Traditional safety approaches may be difficult to utilize in an interconnected world with so many dynamic variables. However, the information revolution also offers organizations and their leaders the chance to address safety in new and innovative ways. The safety challenges and opportunities related to these changes are further described in the following sections.

Scope

The breadth of the relevant operating environment is greatly expanded in today's connected world. Information can be exchanged throughout the entire design, production, management, and operational chain on a global scale. From an operational perspective, rather than functioning independently in a "stove-piped" manner, devices are increasingly part of a collaborative ecosystem, exchanging data in real time with each other and the broader environment and then making operational changes autonomously. This changing operational environment includes advances in human-machine teams, where the view is shifting from machines as tools to machines as teammates. For example, as technology advances, autonomous and highly automated vehicles will share speed and intent information with other vehicles and smart road infrastructure and adjust their speed accordingly.

THE INFORMATION REVOLUTION OFFERS ORGANIZATIONS AND THEIR LEADERS THE CHANCE TO ADDRESS SAFETY IN NEW AND INNOVATIVE WAYS.

[1] The First Industrial Revolution occurred in the 19th century and is characterized by the use of steam power to drive mechanization. The Second Industrial Revolution occurred at the turn of the 20th century, when electricity ushered in mass production. The Third Industrial Revolution started in the late 20th century, when electronics and computers accelerated the use of automation.

[2] "The Fourth Industrial Revolution: What it means, How to respond," Klaus Schwab, https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/

From a safety perspective, traditional functional analysis tools such as root-cause analysis are increasingly difficult to utilize in an interconnected world with so many dynamic variables. In contrast, the Next Level of Safety leverages the data-rich environment to empower a system-of-systems perspective and provide a more holistic view of potential safety issues, including new insights into the role of human-machine teams.

Scale

In the current industrial environment, the relative market size of many new products and services is increasing rapidly when compared to historical trends. For example, commercial aircraft production remained relatively stable at about 1,500 aircraft per year between 2014 and 2019, with the world's four largest manufacturers accounting for 98 percent of total global production[3]. In contrast, the uncrewed aerial vehicle (UAV) commercial market is forecast to grow 67 percent in 2023, with an estimated total production of 2.4 million vehicles[4]. IIn another example of rapidly increasing scale, the volume of data generated by aerospace vehicles is also increasing dramatically; new commercial aircraft such as Airbus A350 are generating almost a terabyte of data per flight—twice as much data per flight as their predecessors[5]. Moreover, as the number of connected devices grows, the number of potential interactions grows exponentially.

This increase in scale will challenge many traditional safety practices that focus on sequential, discrete, labor-intensive processes, such as product certification and post-event safety analysis.

However, these increases in data sources and volume, combined with rapid improvements in advanced analytics (such as AI/ML), provide a

unique opportunity to gain new insights by taking a different perspective on safety analysis. By focusing on trends, outliers, and what has gone right across the entire operation, safety leaders can leverage the increase in scale to their advantage.

Speed

The rate of change is accelerating due to the information revolution. In a traditional manufacturing environment, the functional operations of an item such as a refrigerator or television changed very little, if at all, once the manufacturing process was completed. Even those with digital components often could not be updated.

In today's digital environment, software is replacing traditional physical interactions in markets from finance to retail and is being updated on a continuous basis. For example, historically the operation of medical devices, such as insulin pumps, did not change once the devices were deployed to patients. However, with the digitization of these devices, the software is updated and new functionality delivered on a routine basis. In the transportation domain, continuous changes to aircraft flight deck and automobile automation are increasing human reliance on automation.

[3] https://www.statista.com/statistics/622779/number-of-jets-delivered-global-aircraft-fleet-by-manufacturer/

[4] https://www.businessinsider.com/drone-industry-analysis-market-trends-growth-forecasts

[5] https://www.nytimes.com/2021/04/20/business/airplanes-technology-data.html

From a safety perspective, conducting a safety analysis at a single point in time is less and less relevant. And asking industry to slow down to conform to this traditional approach will stifle innovation. Under the Next Level of Safety, stakeholders shift to a system of continuous, proactive monitoring and analysis.

Complexity

The dramatic shifts in scope, scale, and speed result in increasing systems complexity, characterized by nonlinearity, randomness, and collective dynamics.

Traditional safety models, built on a series of assumptions that no longer hold true in many cases[6],are increasingly insufficient. For example, the Reason, or Swiss Cheese, model[7] is a chain-of-events model that assumes each failure event is independent. Such models do not adequately reflect the complex socio-technical systems we face today, where failures often have common influences. In addition, these models do not address a host of other relevant issues, such as the role of management decision making, competing objectives (i.e., safety versus efficiency), and safety culture.

WITH OUR WORLD BECOMING MORE COMPLEX AND DYNAMIC, SAFETY NEEDS TO EVOLVE TO PROACTIVELY IDENTIFY HAZARDS BEFORE THEY MANIFEST INTO ACCIDENTS.

The Next Level of Safety incorporates a new approach to modeling complexity by leveraging the changes in the operating environment. By acknowledging the complexity, adopting a system perspective, and taking full advantage of the digital ecosystem and related changes in people, process, and technologies, we can improve safety by better understanding these multifaceted interactions. This includes the evolving interactions needed for effective collaboration between humans and machines.

The Next Level of Safety: Evolving Safety in the Digital Age

With our world becoming more complex and dynamic, safety needs to evolve to proactively identify hazards before they manifest into accidents. Traditional safety practices, such as spot checking and ad-hoc coordination, must be augmented by new approaches to ensure public safety in this rapidly changing environment. The Next Level of Safety combines ubiquitous digital data with advanced analytics and continuous learning from stakeholder experiences to accelerate safety advancements. Stakeholders comprise the entire safety community and include developers, manufacturers, regulators, operators, users, and the public.

[6] For example, the current approach assumes each element is random, independent, and time sequenced. The model decomposes each element of a system but doesn't address the emergent properties resulting from combining the parts in a system. The hazards often exist at the interfaces and are easily missed when decomposing a system. A chain of events can describe a specific accident, but it limits truly improving safety (emergent property) because the whole of the system is not considered.

[7] Reason, James (1990). "The Contribution of Latent Human Failures to the Breakdown of Complex Systems." Philosophical Transactions of the Royal Society of London. Series B, Biological Sciences. 327 (1241): 475–484

SYSTEMS LEVEL APPROACH

"Holistic 360-degree view"

PROACTIVE MONITORING AND ANALYSIS

"Right data at the right time"

DATA DEMOCRATIZATION

"Expand sources and perspectives"

SMART POLICY

"Focus on safety outcomes"

The Next Level of Safety is distinguished by four principles:

1. **Systems Level Approach:** A system-of-systems safety management perspective delivers a holistic 360-degree view that spans people, process, and technology, expanding information sources and perspectives.
2. **Proactive Monitoring and Analysis:** A data-driven, risk-based approach continuously monitors the system, proactively identifies risk, and delivers in-time mitigations.
3. **Data Democratization:** Access to safety data and information is maximized by incentivizing stakeholders to share.
4. **Smart Policy:** Performance-based, data-driven standards and regulations focus on safety outcomes over compliance and promote self-discovery, disclosure, and correction.

Systems Level Approach

The complexity of the information revolution environment requires adopting a systems level approach, where all aspects of the system (people, process, and technology) are accounted for when considering safety, including the increasing role of human-machine teams. A system-of-systems perspective also facilitates a shared, comprehensive understanding of the trade-offs between competing system objectives, such as safety, efficiency, and cost.

To achieve this common understanding, stakeholders can use safety management system principles to engage in proactive risk management, sharing risk discoveries and mitigation strategies across the community. Under the Next Level of Safety, the focus of safety management systems (SMS) greatly expands from the traditional single-organization focus to a holistic 360-degree review of safety that incorporates all stakeholders. For example, in commercial aircraft manufacturing, a systems level perspective would include other airframe manufacturers (e.g., peer organizations), sub-system contractors (e.g., landing gear manufacturers), operators (e.g., airlines), maintenance (e.g., aircraft maintenance repair and overhaul organizations), regulators (e.g., certification authorities), and end users (e.g., passengers).

This expansion of observation points is referred to in the nuclear safety community as "observability-in-depth" and is seen as an essential principle to complement "defense-in-depth" for more complex systems of systems[8]. The growth in shared operational data and information enables stakeholders to conduct proactive monitoring, produce more robust predictive analyses and safety intelligence insights, coordinate their mitigations, and understand how to recover from unforeseen hazards.

The systems level approach moves beyond operational data sharing to include insights from safety risk management and safety assurance findings. The move to cross-organizational SMS allows multiple organizations to analyze and manage their common risks and also understand which mitigations are ineffective. The customer-supplier and peer-to-peer relationships among these organizations create opportunities to share discoveries before accidents or incidents occur. Systems level safety management enables the community to discover better solutions and offer faster feedback than any one organization operating independently.

Proactive Monitoring and Analysis

Today's increasingly data-rich environment is enabling the shift from a retrospective to a predictive safety mindset. Proactive monitoring and analysis leverages a sophisticated network of fused operational, systems, and environmental data with AI/ML-based technologies to generate timely safety intelligence in both strategic and tactical timeframes. This information is delivered at the appropriate time (in-time) to the appropriate people (decision makers) in an appropriate manner, for both tactical and strategic decision making.

Under the Next Level of Safety, human decision makers and autonomous systems work together as a team of peers, using connected data and information to automatically monitor system performance; identify unanticipated system interactions, anomalous events, and emerging hazard trends; and understand operational impacts. Near-term forecasts provide tactical support to operational actions, while long-range forecasts of accident risk inform strategic safety investment priorities.

Cross organizational sharing will move beyond raw data to include findings generated automatically by AI/ML systems. These findings will focus on "what to look for"—in essence the patterns for leading indicators are identified by the AI/ML system. The organizations can then work together to improve the depth of the analysis with insights from all the organizations involved to determine the best solution.

Data Democratization

Open access to the large volumes of data generated by the information revolution is a key element to successfully implementing both the Systems Level Approach (e.g., expansion of observation points) and Proactive Monitoring and Analysis (e.g., utilizing AI/ML technologies) principles. Data democratization is the process of ensuring that data and information are accessible to as many stakeholders as possible, from a system-of-systems perspective.

To maximize the availability of data, members of the community must be incentivized to share safety data and information, from local to global levels. As a foundational step, issues related to data security, governance, trust, and standards need to be addressed. For example, a set of shared, common frameworks and data standards facilitates the broad adoption of interoperable solutions and accelerates the impact of data sharing.

[8] J. H. Saleh, K. B. Marais, and F. M. Favaró, "System safety principles: A multidisciplinary engineering perspective," Journal of Loss Prevention in the Process Industries, vol. 29, pp. 283–294, May 2014, doi: 10.1016/j.jlp.2014.04.001

Government regulators can serve as a catalyst in fostering information sharing among industry stakeholders. This includes sharing insights from regulatory monitoring activities as feedback to assure the effectiveness of safety controls. Trusted third parties can assist in building trust between government and industry stakeholders.

Smart Policy

As described earlier, traditional safety regulatory approaches are often insufficient in today's increasingly dynamic, non-deterministic, and highly complex digital environment. As a result, government regulatory policy is shifting from prescriptive standards to be more performance-based, focusing on the safety goals, objectives, and outcomes to be achieved, and the methods that can be used to demonstrate meeting them. In addition, smart policy enables innovation by granting industry flexibility on how to achieve the desired safety outcomes, while promoting industry self-discovery, disclosure, and correction.

From a Next Level of Safety perspective, regulators take an integrated approach, supporting the oversight responsibilities of all organizations in a "shared mission" operational chain (i.e., manufacturers, maintenance organizations, operators, and regulators). Adoption of a safety continuum is an example of this approach. In the aviation domain, for example, not all aircraft need to be held to the same costly requirements in order to maintain consistent safety outcomes. Depending upon the aircraft's mission and operational needs, different safety requirement levels can be established. A safety continuum aligns the regulator's and industry's safety management goals with the public's safety level expectations, while also granting industry innovation flexibility.

On an operational level, with the smart policy approach, regulators use oversight to promote greater shared understanding of the system level operational environment, potential risks, and associated impacts among stakeholders, in addition to determining compliance to the regulations. Oversight attention is focused on the shared discovery of risks and better coordinating the layers of mitigation—or defense-in-depth—across stakeholder organizations. A smart policy regulatory environment enables fail-fast development, with limited operations staged through gates to contain risk during the discovery process. Privileges grow as risks are proven to be managed in an expanding operational environment.

> ALL MEMBERS OF THE SAFETY COMMUNITY MUST COME TOGETHER AND ACCELERATE IMPLEMENTATION OF THE FOUR NEXT LEVEL OF SAFETY PRINCIPLES.

Accelerating the Next Level of Safety

The information revolution is transforming the operating environment for both business and society by creating more connectedness than ever before between systems and human users. Understanding the safety implications of this greater connectivity requires broad community engagement, with a more diverse set of users, to generate new safety insights.

To achieve this vision, we believe all members of the safety community must come together and accelerate implementation of the four Next Level of Safety principles on a global scale. The following

are recommended next steps for moving adoption of these principles forward:

- To advance a systems level approach, stakeholders should fully adopt and implement SMS, and move toward system level SMS by sharing both safety data and findings with all stakeholders, including manufacturers in other domains, suppliers, regulators, and consumers.
- To advance proactive monitoring and analysis, MITRE will continue to connect key government and industry stakeholders, facilitate data sharing, and generate timely safety intelligence. We will leverage our whole-of-nation perspective across industries and domains to advance the science of AI/ML technologies in support of short- and long-term safety forecasting.
- To advance data democratization, MITRE will continue working with government and industry to develop and promote a set of common frameworks and data standards, while addressing data security and governance issues. By sharing data and insights from regulatory monitoring activities, governments can serve as a model.
- To advance smart policy, governments can continue to pursue a uniform safety continuum approach that aligns safety management goals with the public's safety level expectations.

The Next Level of Safety is an important element in building the safe, resilient systems of the future. By encouraging organizations to adopt and implement Next Level of Safety principles, we have the opportunity to accelerate safety improvements across the globe in multiple domains, from aerospace to healthcare. By taking a systems perspective, proactively monitoring and identifying risks, sharing data and information, and implementing smart policy, we can create a safer world.

About MITRE

MITRE's mission-driven teams are dedicated to solving problems for a safer world. Through our public-private partnerships and federally funded R&D centers, we work across government and in partnership with industry to tackle challenges to the safety, stability, and well-being of our nation.

The views, opinions, and/or findings contained herein are those of the author(s) and should not be construed as an official government position, policy, or decision unless designated by other documentation.

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®