Deep Science Publishing
https://doi.org/10.70593/978-93-7185-253-1_3

# Chapter 3: Designing risk-aware industrial infrastructure aligned with legal and operational requirements

## 3.1. Introduction

Human beings have always faced risks, which have continually evolved in response to changes in technology and socio-economic demands. Generally speaking, risk management can be regarded as an attempt to reduce negative consequences associated with these risks. Appropriate design of risk-aware infrastructure can reduce the likelihood of realizing certain types of risks or mitigate their effects. The latter can be achieved through the incorporation of established safety and risk-mitigation measures, technologies and practices during the design phase. However, despite the long-standing existence of specific regulatory requirements to develop such safety-enabling elements, they are typically never capable of completely erasing the chances of their associated risks from happening. Therefore, once unsafe situations have occurred, risk management begins by means of securing their impact by applying risk-mitigation measures or emergency response and recovery strategies (Can & Latiff, 2024; Das & Mukherjee, 2024; Almashhour et al., 2025).

In today's highly interconnected world, different categories of risks that can impinge on physical infrastructure have gained particular significance. For example, natural hazards, man-made hazards, technological hazards as well as hazardous and extreme contingencies are posing increasing challenges to infrastructure operators and owners. In tandem with these evolving hazardous events, the relationships and interactions among infrastructure segments and systems regardless of their origin should also be recognized as drivers of systemic risk enlargement through interdependencies. These interdependencies reveal weak linkages allowing for the propagation of disruptions of critical infrastructure sectors discovered by other actors (Floros et al., 2025; Tallam, 2025).

### 3.1.1. Background and Significance

Our globally interconnected society relies on a vast collective infrastructure backbone, including food and agricultural systems, energy production and distribution networks, communication technologies, supply chain logistics, healthcare delivery, and financial markets. Due to actions taken by malicious actors, along with restrictive cybersecurity policies of third-party software and hardware vendors, cybersecurity has become a critical operational and risk management function of industrial organizations.

Threat actors appear to threaten loss of revenue or decrease in company profits using cyber-attacks. Cybercriminals threaten organizations with loss of financial data or patient records by disrupting centralized storage facilities or ransom functions of such databases. Fraudsters surreptitiously infiltrate automated control systems used to streamline factory assembly lines to bankrupt companies. State actors undermine supply chain companies responsible for the logistics of manufacturing products to impede national military build-up for war. With such prominent attacks on the foundations of our economy, the necessity to design risk-aware cyber-secure control systems for safety-critical industrial automation becomes a national priority. Industrial controllers used to control input and output commands within automated system protocols require deterministic response times to ensure the production of safe and operating products. Restricted deterministic response time for such systems becomes impossible due to delays introduced by firewall proxies defending the cyber border of the system.

State accreditation of organizations identifies third-party vendors providing design, evaluation, and cyber-physical assessments of automated control systems that secure and protect infrastructure industrial organizations. Successful accreditation allows for trusted interactions between vendors and the government. Penetration tests at infrastructure company sites confirm the ability of vendors to secure processes, workplaces, and proprietary data if they are found responsible. Cybersecurity contractors provide high-level risk and compliance management services with mitigation of risk as necessary. Risk-aware policies and procedures dictate trust and behavior as necessary for all contractors working on the site. Risk management strategies outline avoidance or reduction of risk caused by negligent acts at the site deliberate internal person sabotage or social and engineering acts. Cybersecurity readiness includes strategy, planning, physical and environmental security, incident management, business continuity, and disaster recovery.

## 3.2. Understanding Risk in Industrial Infrastructure

Industrial infrastructure are facilities wherein it hosts processes to transform materials into desired outputs. Potential risks for the operations of industrial infrastructures may

hinder the involved processes, lead to the blockage of product supply or energy/resource conversion, and increase maintenance and repair efforts. Moreover, risks can trigger emergencies and create public safety, security, economic, and environmental problems. These dangers affect the whole lifecycle of industrial infrastructures from their design and construction, through their packaging, use, and upkeep, to their demolition, letting their operation likely affect the civil and public security, and the life of an entire society. This should make governments and the related authorities considering the assignment of certified licenses for the design and management of such infrastructures only to companies and practitioners able to show an expertise in the risk assessment of the considered facility.

Risks can be divided into two main categories: operation risks and accidental hazards. Operation risks assess those conditions that reduce the operational income of the involved companies. Their causes can be linked to several factors, including the quality of the facility output, the cost amortization of the facility, the uncertainty of the market, and the production maintenance. Accidental hazards analyze the possibility of accidents with effects such as loss of human lives, diseases, or injuries; damage to machinery, resources, buildings, and other structures; and loss of economic assets and pollution of the surrounding environment. These effects can be triggered due to dangerous events involving natural threats, such as earthquakes or storms, and/or man-made threats originating from mistakes, terrorism, and other reasons.

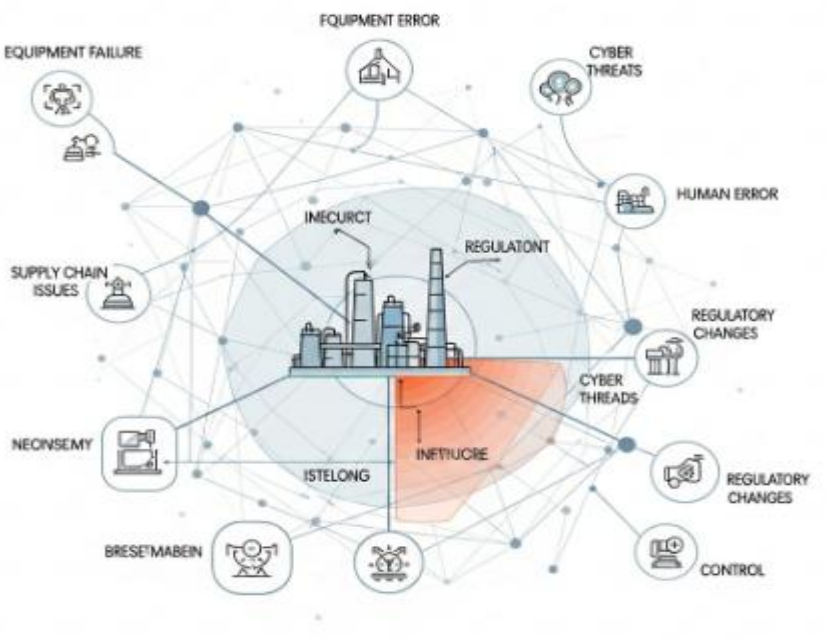


**Fig 3.1 :** Risk in Industrial Infrastructure.

### 3.2.1. Types of Risks

Types of Risks Different methods allocate risk into various categories. Distinctions are made between bureaucratic risks, financial risks, technical risks, and project management risks. Accident and emergency response risks may be classified as a category of their own but are often included in other classifications. Accident risks may be included in technical risks, response capabilities in project management, and the safety of the organization in bureaucratic risks. The categories of accident risks and inadequacy of response capabilities are however discussed at length in many other risk classifications.

The risk of a hazardous process may be considered a technical risk. The public concern about the risks of a project may become a barrier to obtaining approvals to start or change any project. This barrier is an aspect of the bureaucratic risk category. The likelihood of excessive costs, schedule delays, and unsatisfactory performance may be categorized as financial, project management, or technical risks. Risk transfer contracts such as insurance policies and indemnity clauses are commonly used for financial and project management risks.

A risk transfer contract does not always imply the risk has been reduced. Financial or project management risks are effectively transferred to the project insurer or indemnity writer who may charge a premium for assuming the risk which may be higher than the financial, project management, or technical risks of the design authority, contractor, or operator. Irrespective of how risk is classified, to avoid misunderstanding, it is prudent to qualify which types of risk are being described and elaborated.

### 3.2.2. Risk Assessment Methodologies

Risk assessment is the fundamental pillar of risk management, helping the manager decide whether there is a need for any intervention. Effective risk assessment has been distilled down to several systematic options that differ in detail but follow the same basic principles. All fundamentals of risk assessment are typically compiled into broad guidance. Zeroing in on IR risk, more specialized directives or guidance documents can be referenced, focusing on risk assessment of industrial control systems. A local version has been released by a national cyber security centre, and additional sources have been proposed by numerous other countries.

While more general assessment approaches, such as quantitative risk assessment or factor-based models, are available, their focus tends to be further removed from the wanted outcome than the more tailored cybersecurity risk assessment solutions. Cybersecurity solution tailoring can use the different abstraction levels on which it is considered; hence, the further feedback into asset, vulnerability, threat modeling, and

impact digitization, the more customized the modeling. Several specialized processes have been proposed, including but not limited to various methodologies. Typically, dimensioning of impacts and probabilities is based on expert interviews and on estimates from past events.

Due to the low probability of IR events, the assessments of the damage costs, plus the consequent downscaling based on the probability, tend to be uncertain, which is where the factor-based approaches can more easily cope due to their character of transversal estimates. Otherwise, gathering more accurate information will always be a process of revisiting the character of the organizations, in all cybersecurity assessments and recommended practices eventually mentioned.

## 3.3. Legal Framework for Industrial Infrastructure

Industrial infrastructure comprises public- and private-owned elements that facilitate and enable the production of products and services in an economy. This includes industrial products, such as smart factories, but also services that help create industrial products and services. Industrial infrastructure also includes the economy itself with the interaction of various industries, the national and international trade infrastructures, as well as the exchange with social infrastructures, and regular life. It comprises a national and global structure that enables industrial production, connecting manufacturers to suppliers and customers. The industrial infrastructure considered in this chapter is the part owned and operated by private actors, usually companies.

The design of industrial infrastructure is usually not regulated in detail. Open questions are, to some extent, the responsibility of the economy's internal quality assurance via companies' internal processes and the formalized industry standards that are agreed upon by stakeholders with relevant experience to define what is "good enough". Depending on the industry, design choices must also pass evaluation against a range of legal standards set by governments related to content protection, liability aspects, data privacy, and also data security. Analytical standards are often not explicitly listed, but have grown over time and are part of the "industrial singularity", i.e., the combination of normative and practical factors that drive an economy's industrial development into one particular direction that is generally accepted as "good and desirable".

### 3.3.1. Regulatory Compliance

In addition, related operations should be formally defined in contracts or program requirements. Since the legal exposure of participating companies will depend on how well companies performing the actual work manage foreseeable risk aspects, it becomes

important to capture these detail-oriented considerations in the appropriate level of regulatory compliance both for the sake of potentially significantly impacting public sector project budgets in various ways and for ensuring that assembly work and resulting infrastructure are of safe and suitable quality levels. Similarly, any related regulatory boards should have consideration and coordination among them related to different infrastructure tasks which need to be synchronized. Overall, infrastructure associated requirements additionally provide a guiding compliance framework. Companies engaged in construction, maintenance or longevity-related activities especially for federally funded transportation projects should ideally not only be aware of existing statutes but more importantly proactively take responsibility for continually keeping themselves informed about pertinent existing and upcoming laws. A background in principles and quality processes should facilitate this. In addition to governing bodies, state, local, and Tribal agencies issue construction-related permits as well as develop criteria and technical standards that apply to select projects, and impose requirements on contractors and subcontractors. State-funded projects are subject to federal funding agency guidelines regarding certain aspects, but have more flexible property acquisition plans. However, federal grant guidance notwithstanding, by avoiding conflicts of interest and ensuring fair competition, federal, state local boards can more generally award any size project contract to the lowest responsible bidder with the skills and resources necessary even as many agencies are formulating aspects of an overall continuity of operations plan. However, existing socioeconomic regulations prioritize certain groups for contracting opportunities when price and other factors are considered equal among competitors. Agencies can also enter into non-competitive contracts under limited special conditions.

### 3.3.2. Liability Considerations

To comply with the law, a designer must identify and ensure that all relevant and applicable obligations are satisfied to avoid liability or other adverse consequences, including civil or criminal enforcement actions and civil lawsuits. In particular, designers need to analyze whether the design may affect any employment or insurance-related rights of employees, whether it exposes affected individuals to an increased risk of criminal prosecution or punishment, and what impact their patent infringements may have on the intellectual property rights of third parties. Failure to adhere to design-related obligations may expose corporations to governmental enforcement actions and significant civil and criminal penalties, in addition to the potential for tort lawsuits, such as negligence or wrongful death, under specialized liability and tort regimes.

Liability may flow not just from the design of the facility but also from the design of tools, processes, software, and other aspects of production. Implementers conducting

operations that deviate from the design or that attempt to leverage productivity-enhancing AI assistants for tasks not covered by the design might be sued for damages, but the plaintiff likely would have to bear the burden of liability insurance to pursue the designer. Importantly, both adverse tort liability and beneficial tort immunity are likely to depend on the precise structuring of the designer-implementer relationship, rooted in both the particulars of state law and the contract associated with the design. Such matters generally lie beyond the purview of licensing discussions and are issues of common interest to affected stakeholders.

### 3.4. Operational Requirements in Industrial Settings

Assuring human-safety and efficiency during operation of machinery are essential elements in the Industrial internet of Things. The European Directive laying down machinery establishments essential health and safety requirements emphasizes safeguarding persons and environment against possible accidents caused by machinery. It contains a list of risks concerned and their possible avoidance, such as mechanical risks, such as failure of pressure equipment, radiation risks, such as laser emission, electromagnetic fields, and noise risk, and ergonomics and operational risks. Furthermore, tools and robots coming into contact with humans are classified into four categories, explained in the list below.

- Category I: Tools or robots separated from the worker.

- Category II: Tools or robots only used with limited interactions, such as collaborative robots.

- Category III: Tools or robots support the work of humans without being programmed.

- Category IV: Tools or robots fully operate without human interactions.

Categories II, III, and IV require risk assessment and risk reduction, and involve operational efficiency. Hence, in the context of the current paper, the collaborative nature of Category II and III challenge evaluation of operational safety and related metrics.

Optimized safety and efficiency are known issues of human-centered automation. However, today's industrial environment is challenged by increasing customized production, volatile demands, and lifetime entrepreneurship. This demands a MORE AND NEW: More diversity, more flexibility, more sustainability, more quality in scope, costs, and time; guaranteed lifetime quality. Considering such, tight customer-specific time budgets force also reduction of process time of operations involving humans.

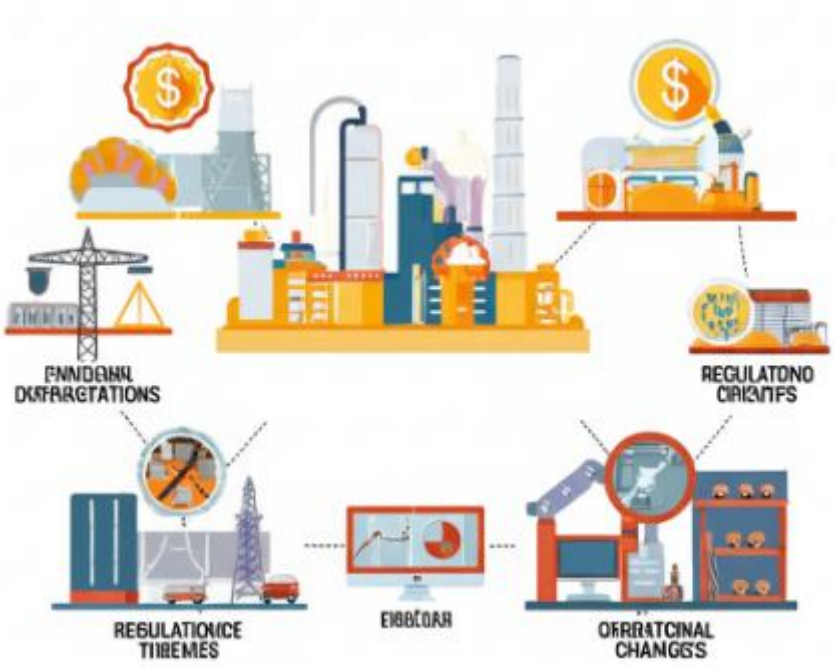

**Fig 3.2:** Operational Requirements in Industrial Settings.

### 3.4.1. Safety Standards

In a study of six factories with levels of industrial process automation ranging from 0% to 99%, it was found that, when considering people's basic survival, safety is the major precondition for the establishment of higher automation levels. Safety is a vital and vitally regulated requirement for many of the industries that are the subject of industrial process automation. The need for efficient solutions and a fast market entry reduced the consideration of safety aspects during the design process. Therefore, developers must strictly follow the regulations by testing prototypes and new solutions. However, the ability to implement safety solutions in a design phase is limited. Moreover, the increasing complexity of multi-manufacturer production systems that involve collaboration between humans and robots, as well as among industrial machines, has led to a growing tendency to implement the so-called out-of-the-box walk-away designs.

The safety standards are prepared by various international organizations with involved countries from around the world. There are basically three levels of safety standards concerning applied technologies: (1) safety guidelines for general implementers of systems, (2) safety standards for manufacturers providing components with safety certificates, and (3) safety standards for machines or installations. Each of these documents specifies a few topics that are divided into requirements, risks, and obligatory

tests that are closely related in the area of reporting. Such a hierarchical classification of topics should be respected in the design and research so that finally proposed implementations will be adopted.

### 3.4.2. Efficiency Metrics

For the design and construction of buildings, bridges, and highways, and the production of goods by experts, a model exists. It is a working model that is based primarily on the economic benefit of delivering a product to the market correctly and in an acceptable time. This concept of an efficient system is so strong that a cluster of highways, interconnected offices, factories, customer-support centers, and so on are all designed, built, and operated according to the practice of the efficiency model. Such a model has been the starting point in developing many efficiency metrics, which can be categorized into:

- Flow: The average number of delivering goods, usually to customers, of the flow of the system.

- Flow time: The time required for flow at each stage of preparation, transit, wait and servicing.

- Capacity: The limitations to flow and flow time. Limited capacity creates much of the variance in the system.

- Utilization: The fraction of time that the subsystem is actually servicing.

- Size of the system: The length, area, and volume of storage spaces, the number of servicing stations, the number of vehicles in transit, and the typical load of a vehicle.

- Inventory: The average stock in storage, waiting for servicing in service.

- Cost: The investment cost of the physical system and operating costs that depend on flow time and service demand. Operating costs usually include interest, labor, storage, maintenance, and transportation.

- Variance: The variance in flow time, capacity, and service demand. Variance produces queues and, if large enough, idle time and excess inventory.

## 3.5. Integrating Risk Management into Design

A critical aspect of risk management is evaluating risks early enough so that the design can be modified to ensure that such risks are driven to the lowest acceptable levels possible. Unfortunately, the majority of risks are identified long after the design is frozen

and cannot be practically addressed without costly retrofitting. Design teams that employ risk management practices understand the importance of strategically evaluating the impacts of design in the conceptual phase of development. With the help of engineers and risk managers, the overall cost and consequences of negative risk events can be much lower earlier in the design stage than later in the development cycle or in operations. While certain risks are difficult or impractical to eliminate, there may be strategies available to mitigate them, both to reduce the probability of the event occurring and to reduce the severity of the consequences. The two key principles behind risk mitigation are to eliminate the event or its effects through avoidance, or to build resilience against the event through acceptance, limitation, or transfer.

The concept of risk reduction has important implications for design. For safety and liability purposes, the costs associated with risk mitigation strategies should be balanced against the costs associated with the consequences or severity of the event addressed by the risk mitigation strategy. Design systems may have the greatest influence on aspects of operations for which most risk cost factors are incurred. Therefore, intelligent prioritization of risk factors can have a profound impact on successful event avoidance and reduction. While it may not be viable to avoid every event with risk costs associated with operational risk factors, the desire to minimize action costs associated with risk factors across the event spectrum can and must inform and direct the design conversation throughout the design process.

### 3.5.1. Risk Mitigation Strategies

A key benefit of the Risk Assessment Phase is its integration of security knowledge and risk management into the design and evaluation activities. Risk Assessment and Design work together iteratively to create an intention-aware design to improve security. Risk mitigation strategies can be generalized into four categories: obligation (also referred to as deterrence): maintaining security policy compliance through appropriate control and penalties for deviations; minimization: reducing the chances of attacks; detection and response: decreasing risk impact by early detection of security violations and performing responses to them; and acceptance: leaving some level of insecurity unattended.

An intention-aware design to improve security should begin with developing an integrated strategy across all four risk management principles - failing to implement an integrated strategy may result in a design that is lacking in some areas or that contradicts the objectives of others. To illustrate this, compliance controls may be ignored by the users if they are not appropriate for the context, the minimum risk level is greater than the cost of providing compliance controls, some risk-related contexts are harder to enforce than others, and short response times are required if detection controls are based on alarm generation as opposed to a proactive analysis of risk exposure.

Thus, if the activities that have been identified as vulnerable were to be of a high inherent risk in a specific context, it may be preferable to implement detection sensors and alerts combined with rapid response mechanisms. On the other hand, if these activities were of a low inherent risk in their corresponding context, compared to the cost of implementing deterrence obligations or reducing the chances of success, it may be preferable to do nothing.

### 3.5.2. Design for Safety and Compliance

Designing and building industrial infrastructures is resource-consuming and typically takes a long time. Therefore, both opportunistic and preemptive risk management options are favorable while designing and building infrastructure to balance cost and time advantages against risk, safety, and compliance. Design and engineering efforts that cannot prove their ability to manage safety and compliance specifications will typically lead to costly interventions and remediations, increasing lifecycle costs. In particular, well-structured and applied automation technology solutions will contribute to risk-aware infrastructure decisions from the earliest possible planning stage on, to assess and balance safety and compliance in the technical design and building tasks.

While such automation technology solutions already perform both assessment and calculation of the most cost-effective safety and compliance-forcing implementations, the assessment required to create trustworthy foundations is still done manually with generally much more risk of being wrong and having too large a negative impact on the overall costs of an industrial site both in the investment phase and in the operating phase. Mandated, calm periodic assessments on safety and compliance can support this technology management effort with a simple assessment of the latest engineering standards and regulations or laws in the different locations of the infrastructures.

## 3.6. Technological Innovations in Risk Management

Risk management is traditionally heavily reliant on expert knowledge, the application of heuristic methods, and limited objective quantitative analysis. These limitations are however being addressed through the increasing infusion of technological innovations into risk management. These innovations can allow quantitative risk assessments to be performed more accurately and faster than previously possible allowing risk assessments and analyses to be performed much more frequently in a much wider set of applications than has previously been the case. In these particular applications, the operational practices and decisions can become risk aware which allow the identification of many more mitigative opportunities. The two general classes of technological innovations which are being utilized are automation, monitoring and data analytics.

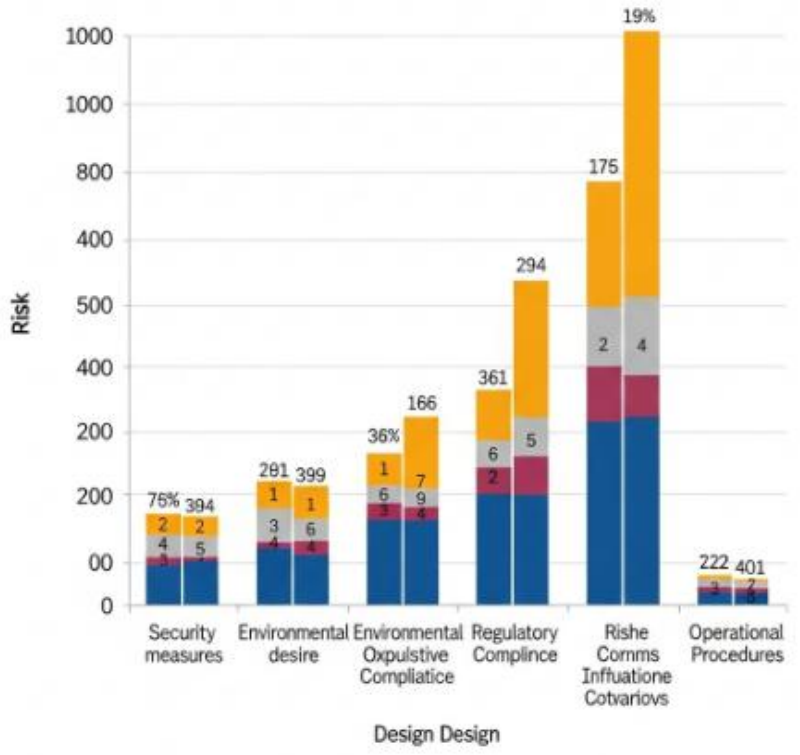


**Fig :** Designing Risk-Aware Industrial Infrastructure Aligned with Legal and Operational Requirements.

Automation of operational practices, monitoring of systems, and the tracking of physical asset characteristics over time is facilitated by the increasing sophistication and lowering cost of sensors and actuators together with the decreasing cost and increased capacity of data storage with additional evolution provided by the advent of the Internet of Things. Risks can thus be continually assessed, or observed through the identified strong correlations with monitored characteristics, and visible to operators and automation systems of more elements within their risk context. Data analytics is the second innovation area that is assisting with improved risk assessment and decision-making. The availability of vast historical or near-real-time data sets is allowing for innovative solutions using artificial intelligence, machine learning and deep learning to make data-driven predictions of risk assessment elements, identifying elements of risk exposure and consequence which may otherwise not have been recognized. These analytics improvements are normally best used in combination with existing expert structural reliability approaches which are continually being enhanced and integrated with the automated monitoring capabilities now being utilized.

### 3.6.1. Automation and Monitoring

Sensitive equipment, processes, and areas are under continuous monitoring, and any violations of rules and behavior are reported. Alarms can trigger an automatic response that minimizes the harm of the incident. Although this approach typically has a high upfront cost, it is compatible with existing regulations for monitoring sensitive physical infrastructures. The current software design allows for automation that covers more of the operational and legal requirements in scenario-based rules, accelerating the security posture improvement over a time frame acceptable by the investors for various hazards and hazard sources. Big Data automates the risk analysis process and helps detect changes in space and time, covering pre-and post-measurement steps. The spatial-temporal approach is becoming a common feature of generalized frameworks for technology design. Technology is becoming an integral part of risk management, from physical protection systems employing sensors, automatic responders, and chronic violators' address projects to automated, remote monitoring of conditions that help detecting, mitigating, and attributing the cause of environmental hazards. Cyber risk is also included, incorporating protection against unauthorized system access and data alteration, automation of detection of system anomalies and susceptibility to pre-explosion data modification, and remediation through disclosure and/or insurance agreements. Challenges of technology in terms of design, ethics, and practicality are understood, including: the high upfront implementation cost; the need for 24/7 manpower; the question of legal responsibility in case the automated intervention through smart fences and other automatic and semi-automatic devices does not wake up the on-duty personnel, the smart fence fails, or false alarm systems initiate violent reaction; potential use of drones and robots to cause deaths while bypassing pro-human regulations; ethical aspects of social monitoring, including on social media; and limitations in design of micro- and macro-scale transparent systems for on-demand auditing. Despite the ethical questions, legal requirements are emerging that allow the use of automation.

### 3.6.2. Data Analytics for Risk Assessment

Technological innovation is being integrated into organizations and shaping corporate risk management. More and more companies are starting to ask how they can leverage data available in digital systems to increase efficiency and improve outcomes of organizational activities. Increasing access to vast amounts of data and the adoption of innovative methods of data exploration and analysis offer a wealth of opportunities in risk assessment. The nature of modern risk management is changing from retrospective investigations based on the discovery of existing patterns in portfolio performance to forward-looking predictions of future losses.

Technological innovations in risk management increase efficiency and improve outcomes of organizational activities. Risk management is becoming less and less of a standalone corporate function – one that can be performed for a company by a handful of experts detached from business processes and decisions – and increasingly an integral part of business operations and decision-making. Legal and regulatory requirements are increasingly demanding that organizations implement risk awareness into business processes, whether directly, through controlled self-reporting or through the monitoring and assessment of incorporated algorithms. New approaches to risk management incorporate advanced risk assessment and predictive capabilities based on the use of contemporary data analytics techniques, including streams of structured and unstructured data created by company transactions and beyond. Analytics or prediction-driven risk management, or data-enabled risk management, has the potential to reshape the risk management landscape by creating new opportunities for operational improvements and enhanced risk mitigation for traditional risks like product safety and quality, information security, fraud, compliance, and project financing, for emerging risks like climate change, and even for chronic risks resulting from long-term trends like socio-political changes.

## 3.7. Conclusion

The challenge of ensuring the safety and security of industrial systems that their designers, owners and operators are facing is becoming ever-more complex. The systems are growing, the hazards they face are becoming more numerous, and the threats and vulnerabilities they endure are growing in number and complexity. Potential consequences, including loss of life and enormous financial costs, as well as ecologic impacts and irretrievable effects, can be catastrophic and should force the industry to reconsider how to conceive and design those systems. There are indications that at least in some systems, previous schemas that separated the consideration of life safety from industrial security and system operational safety are becoming inefficacious. This ineffectiveness can imply that many systems might be designed incoherently with legal and operational requirements and their risk-aware characteristics are headed to deteriorate – with the resulting potential fatal consequences for their designers, operators, and owner infrastructure organizations.

It is envisaged that in the not-too-distant future, the infrastructure is controlled, independently or jointly with human agents, by digital twins, ensured to perceive events and actions at a higher frequency and in more detail than human agents. Those enhance and extend fundamentally the human perception of the world, but there are no guarantees they are better. Further, those agents will represent real-world entities, decisions and actions and their trust, risk-aware characteristics and pattern of actions, the relative trust,

the reduction of trust in them, and the control over them by developers, owners, and operators, will need to be addressed and designed. Ensuring the agents are decision- and action-wise aligned with the legal and operational requirements that need to be logically linked and extensible in the digitally enhanced and extended dynamic world, will be paramount.

### 3.7.1. Future Trends

The future of risk-aware design requires advances across multiple levels. Research on tools and techniques for risk assessment is necessary to support decision-making. Tools are necessary that can help design companies understand and influence their risk profile. A clear research challenge is assisting design companies in dealing with and profiting from the high risk involved in their business. Research is needed that helps bridge the scientific and practical worlds of risk. It is dangerous to build models that dredge for too much generality and away from sound intuition. It is equally dangerous to dive into practical, specific modelling without connecting with a body of scientific principles. Ongoing interaction between the scientific models and the models of real design practice will yield tools, schemas, and techniques for risk-aware design.

Support for risk-aware design should not assume that companies always benefit from knowing what risks they are taking on. There may not be much profit for a company in elaborating and perfecting its risk profile if it is patently evident that it is more interesting to pick off the wild performers than it is to invest heavily at such a company. Distinguishing between companies embarking on risk-aware design and those merely embarked on avoiding risks is an essential element of support for risk-aware design. Also necessary are models of risk that hinge on a company's position in a market sector, rather than on economic characteristics internal to a company. There are several risk characteristics that usefully distinguish a design company's position in its market sector. Foremost among these is whether the market distinguishes between better designs and worse ones.

## References

Tallam, K. (2025). Engineering Risk-Aware, Security-by-Design Frameworks for Assurance of Large-Scale Autonomous AI Models. arXiv preprint arXiv:2505.06409.

Can, H., & Latiff, A. R. B. A. (2024). Strategic Alignment of Risk Management and Corporate Governance: Boosting Manufacturing Performance. Journal of Digitainability, Realism & Mastery (DREAM), 3(05), 109-127.

Floros, E., Stavrou, E., Smyrlis, M., Nikoloudakis, N., Potamos, G., Apostolidis, A., ... & Papadakis, S. E. (2025, April). Towards the Design of Cyber Range Training Programs for

Enhanced Preparedness: Investigating the Training Needs in Critical Infrastructures. In 2025 IEEE Global Engineering Education Conference (EDUCON) (pp. 1-10). IEEE.

Almashhour, R., Al-Mhdawi, M. K. S., Daghfous, A., Qazi, A., & Ojiako, U. (2025). Traditional to sustainable risk management in the construction industry: a systematic literature review. International Journal of Managing Projects in Business.

Das, S., & Mukherjee, S. (2024). Navigating cloud security risks, threats, and solutions for seamless business logistics. In Emerging technologies and security in cloud computing (pp. 252-275). IGI Global Scientific Publishing.