


## REVIEW

# Winning the battle with cyber risk identification tools in industrial control systems: A review

Ayo Rotibi | Neetesh Saxena  | Pete Burnap

School of Computer Science, Cardiff University,  
Cardiff, UK

## Correspondence

Neetesh Saxena.  
Email: [SaxenaN4@cardiff.ac.uk](mailto:SaxenaN4@cardiff.ac.uk)

## Funding information

The Welsh Government and Thales UK; The British Council, Grant/Award Number: IND/CONT/G/23-24/07; UKIERI, Grant/Award Number: IND/CONT/G/23-24/67; UKRI, Grant/Award Number: EP/Y026233/1; RITICS Fellowship

## Abstract

The modern Industrial Control System (ICS) environment now combines information technology (IT), operational technology, and physical processes. This digital transformation enhances operational efficiency, service quality, and physical system capabilities enabling systems to measure and control the physical world. However, it also exposes ICS to new and evolving cybersecurity threats that were once confined to the IT domain. As a result, identifying cyber risks in ICS has become more critical, leading to the development of new methods and tools to tackle these emerging threats. This study reviews some of the latest tools for cyber-risk identification in ICS. It empirically analyses each tool based on specific attributes: focus, application domain, core risk management concepts, and how they address current cybersecurity concerns in ICS.

## KEYWORDS

industrial control system, risk identification methods, risk identification tools

## 1 | INTRODUCTION

Cyber risk refers to operational disruptions or damage caused by digital technologies affecting an ecosystem's information and operational functions. This disruption includes unauthorised access, use, disclosure, modification, or destruction of systems. Risk identification is the first step in risk management involving the discovery, recognition, and description of events or conditions that may prevent an organisation from meeting its objectives [1]. The main goal is to detect potential negative events early to improve the security of the system or environment by identifying and protecting important assets and processes.

In the complex industrial control system (ICS) environment, different stakeholders such as ICS owners, automation engineers, safety engineers, information technology (IT) administrators, and cybersecurity analysts may have varying interpretations of risk [2]. To effectively identify risks, it is essential to understand the enterprise's goals and objectives, promoting a shared understanding among all stakeholders [3].

Modern ICS environments are no longer isolated. They use off-the-shelf hardware and software, connected through

standardised but mostly unsecured protocols such as Modbus remote terminal unit, Process Field Bus (PROFIBUS), distributed network protocol 3, International Electrotechnical Commission (IEC)-60870-5-101/104, IEC-61850, and Conitel. Many of these protocols have been adapted to work over Internet Protocol (IP) and ethernet networks. For instance, PROFIBUS has been replaced by Process Field Network, which runs on ethernet and IP, and Modbus transmission control protocol/IP (TCP/IP) has replaced Modbus [4]. These extensions have widened the attack surface, making ICS environments vulnerable to IT-related threats [5].

There has been a significant increase in cyberattacks between 2010 and 2023 [6]. Table 1, shows a notable rise in both the frequency and impact of attacks since 2010 especially compared to the previous decade. This demonstrates how ICS environments have increasingly come under cyberattack in recent years [7–9].

Modern tactics and attack methods, like ransomware and supply chain cyberattacks, have challenged traditional risk identification methods in ICS environments. In response, researchers, stakeholders, and asset owners have developed tools such as fault trees, attack trees, and attack–defence trees

This is an open access article under the terms of the [Creative Commons Attribution](https://creativecommons.org/licenses/by/4.0/) License, which permits use, distribution and reproduction in any medium, provided the original work is properly cited.

© 2024 The Author(s). *IET Cyber-Physical Systems: Theory & Applications* published by John Wiley & Sons Ltd on behalf of The Institution of Engineering and Technology.

**TABLE 1** Notable ICS cyberattacks—2000–2023 [6].

Year	Target	Method
2000	Australian sewage plant	Insider [10]
2010	Iranian uranium enrichment	Stuxnet [11]
2013	ICS supply chain attack	Havex [12]
2014	German still mill	Stuxnet [13]
2015	Ukraine power grid	BlackEnergy [14]
2016	Ukraine substation	CrashOverride [15]
2017	Global shipping company	NotPetya [16]
2017	Healthcare, automotive, others	WannaCry [17]
2017	Saudi Arabia petrochemical	TRITON [9]
2019	Norwegian aluminium company	LockerGaga [18]
2020	Colonial pipeline	Ransomware [19]
2021	JBS food	Ransomware [20]
2023	Johnson controls international (JCI)	Ransomware [21]
2023	Dole food	Ransomware [22]

Abbreviation: ICS, industrial control system.

(ADT). These tools help identify risks as part of a broader risk assessment programme [23, 24].

## 1.1 | Distinction from other research surveys

Although a comparative study of risk assessment tools for ICS exists, such as the work by [25, 26], there is none that has focused exclusively on risk identification. To fill this gap, our study presents a comparative analysis of some cyber risk identification tools, using standard attributes and features to determine their capabilities to address the current cyber risk attack vectors. We aim to find answers to the following questions.

- To what extent are existing risk identification tools able to offer support and address the current cyber risks landscape?
- How does each tool differ from the other tools in terms of scope and depth of risk identification?
- How do the results of risk identification using these new tools compare against each other?

Our work explored the current risk identification tools and identified any potential gaps in their capabilities to address the questions raised. We reviewed each tool based on a set of criteria including focus, categorisation, coverage, framework/standard alignment, applicability, strength/capabilities, and limitations. This enabled us to gain an understanding of how the tools can help detect cyber risks in the ICS environment. We have also compiled a list of commercial, research, and open-source tools which are featured in the survey. Finally, we proposed a tool that attempts to address some of the identified challenges in risk identification. We hope this study will

provide readers with an up-to-date overview of available tools and their capability to identify risks and vulnerabilities in ICS environments accurately. It may also help initiate discussion on how risk identification methods align with the changing ICS risk landscape.

## 1.2 | Challenges

Cyber risk identification in ICS is complex due to the sector's evolving requirements and dependencies. Risk identification involves identifying potential risks that could hinder an enterprise from achieving its objectives [27]. It is a crucial first step in the overall risk assessment process, as illustrated in Figure 1. Risk management encompasses risk assessment which begins with risk identification. However, distinguishing risk identification as a separate component within the broader context of risk assessment poses challenges. This difficulty is compounded by the fact that risk identification is often not clearly differentiated from risk assessment, and representations of risk assessment vary among practitioners.

Other challenges include the following:

- The traditional approach to risk identification focuses primarily on analysing IT protocols and network configurations, leading to a strong bias towards information security concerns [28]. ICS cyber-related attacks have typically targeted the technical components and devices situated in the lower layers of the ICS architecture. However, due to the fragility of common off-the-shelf industrial components, active network scanning is discouraged. This limitation hinders the ability to obtain an accurate asset inventory [29].
- Risk and security practitioners often have differing interpretations of key concepts such as risk versus fragility, fault tolerance versus resiliency, and security versus robustness. These conflicting views lead to varying priorities and goals, which impact how risk is interpreted. Information technology administrators typically model security according to the CIA triad—confidentiality, integrity, and availability. In contrast, control engineers emphasise the COO triad—control, observation, and reliable operation. Additionally, due to its operational characteristics, safety considerations are a major risk factor in the ICS environment where safety, reliability, and productivity shape the definition of risk [30].
- Within the ICS domain, there are two distinct sets of priorities, goals, concepts, and vocabularies: safety and security. This duality leads to different interpretations of risk. Security focuses on protecting corporate information from intentional threats, while safety aims to protect lives and system performance from unintentional events [25]. These contrasting yet complementary goals influence how risk is perceived, addressed, and identified. For instance, an emergency safety procedure that lacks access control might be considered a security risk, and conversely, stringent access control measures could impede safety protocols in an emergency.

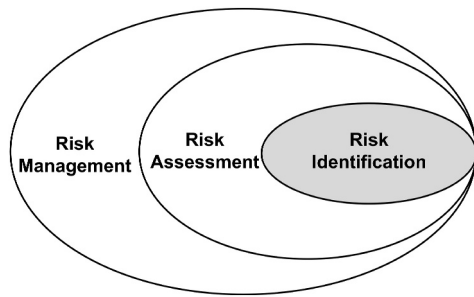


FIGURE 1 Risk identification.

- Recent events have demonstrated that the data exchange and dependencies between higher-level components and enterprise systems create a vulnerability wherein a successful attack on the enterprise system can significantly impact the operability and functionality of the ICS environment [7].

### 1.3 | The ICS architecture attributes

ICS represent a convergence of IT and operational technology (OT) devices with physical processes [31]. According to the Purdue reference model, the ICS architecture can be conceptualised as a layered integration of various interdependent and interoperable devices [29]. While this model is predominantly applied within manufacturing settings, it illustrates a hierarchical topology that distinctly separates the IT (corporate) zone from the OT (operations) zone, as depicted in Figure 2.

The IT zone constitutes the traditional enterprise resource planning environment, encompassing the enterprise network (Level 5) and site business and logistics (Level 4). This zone is responsible for tracking business resources, such as raw materials and production capacity as well as the status of business flows, including orders and billing, and managing the overall IT environment. The OT zone comprises the lower levels: Level 3 (Operational Demilitarised Zone, or Demilitarized Zone) acts as a security buffer, providing segregation (air gap) between OT and IT systems. This level implements a defence-in-depth strategy to mitigate cyberattack progression. Level 2 translates IT zone requirements into operational directives using engineering workstations and human-machine interface devices to configure programmable logic controllers and monitor operations. Control servers and data historians located at Level 2 are integrated with the IT zone. Programmable logic controllers and remote terminal units at Level 1 control the field network and physical processes, interpreting input from sensors and sending output via actuators. The lowest layer, Level 0, comprises field instruments such as sensors, actuators, and physical processes which are managed and controlled from Levels 1 and 2.

Real-time strategic business information flows from the IT zone to the OT zone while real-time operational information (corporate decisions) flows in the opposite direction. Additionally, a bidirectional information flow exists within the OT

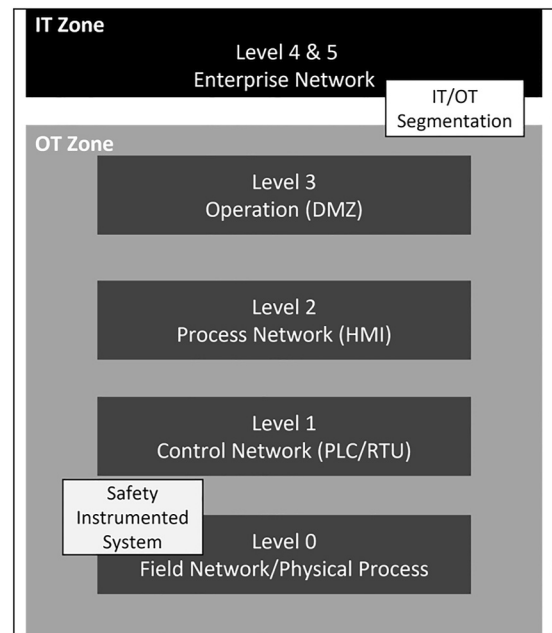


FIGURE 2 ICS architecture. ICS, industrial control system.

zone, between Level 2 and Level 0. Real-time event decision inputs travel from Level 2 to Level 0 and real-time feedback from physical devices flows back to Levels 1 and 2.

The two domains—IT and OT—have distinct security requirements and specifications. Information technology risk management adheres to information security standards such as the National Institute of Standards and Technology (NIST) SP-800-39 [32] and International Organization for Standardization (ISO)/IEC 27005:2022 [33] designed to assist organisations of various types, sizes, and industry sectors in conducting information security risk assessments and implementing risk treatment processes. Conversely, ICS security is guided by standards such as IEC-62443 [34] and SP-800-82-Rev-3 [35]. IEC-31010:2019 also provides guidance on the application of risk techniques [36]. Some ICS operators have encountered operational challenges, such as screen locking (posing safety risks) when leveraging IT/OT standard commonalities. To address these issues, the International Society of Automation (ISA)/IEC 62443 series offers a platform enabling ICS environments to conform to complementary IT standards.

Traditional risk assessment activities typically follow three sequential steps [37].

- **Asset Identification and System Characterisation:** This step involves identifying and assessing the criticality of all assets within the system.
- **Vulnerability Identification and Threat Modelling:** This phase entails discovering potential vulnerabilities, evaluating their severity, and assessing the likelihood and consequences of a compromise.
- **Risk Calculation and Mitigation:** In this final step, the overall impact of each identified vulnerability is assessed, and appropriate mitigation measures are determined.

These three steps are fundamental to the risk identification process, forming the cornerstone of any organisation's security programme. Our study has considered these steps, the specific attributes of ICS environments, and emerging challenges within the domain.

The remainder of this paper is organised as follows: Section 2 reviews related work. Section 3 provides an extensive discussion of risk management and the elements of the risk identification process. Section 4 offers a detailed analysis of each tool, evaluating standard attributes and features to highlight their strengths and limitations. Section 5 presents a comparative analysis of all the tools. Finally, Section 6 addresses open issues and limitations, proposes potential solutions and concludes the paper.

## 2 | RELATED WORK

Although ISO3100 [38] makes a clear distinction between risk identification and risk assessment, some authors equate risk assessment to mean vulnerability or threat assessment [23]. In contrast, others did not clearly distinguish between risk identification and risk assessment [25, 26, 39].

In addition to the ISO3100 are two standards worth mentioning: the NIST Special Publication 800-82 Revision 3 (NIST 800-82r3) and NIST Special Publication 800-37 (NIST 800-37).

NIST 800-82r3 [40] focuses mainly on ICS. It provides a detailed framework with a holistic approach to security, covering various aspects from risk management to incident response. NIST 800-82r3 offers a mix of best practices, strategies, and methodologies specifically designed for identifying and assessing risks in ICS environments. Key activities include asset cataloguing, threat and vulnerability assessment, impact analysis, and risk assessment.

For the United States federal information systems, NIST 800-37 [41] outlines a six-step, risk-based framework to help organisations manage information system security. This framework includes the following key activities: system categorisation, threat and vulnerability assessment, risk analysis, control selection and implementation, and continuous monitoring and review.

Using NIST 800-37 and NIST 800-82r3 for risk identification means integrating their guidelines into the organisation's overall risk management strategy. This involves systematically following the framework steps to identify, assess, and address risks associated with information systems and using both automated tools and manual processes to identify and assess risks.

In regards to this topic, scholars form two streams of the related work that are relevant to this paper: (i) studies on the application of risk identification methodology on ICS and (ii) studies on security risk assessment methods for ICS. For inclusion, we selected those publications that either integrate risk identification approaches into risk assessment or that address risk identification tools as a stand-alone or as part of the risk management concept.

Sheehan et al. [42] introduced a comprehensive framework for cyber risk classification and assessment aimed at

underscoring the importance of both proactive and reactive barriers in mitigating organisational vulnerabilities to cyber risks. This framework highlights the critical role of these strategies in addressing cyber threats and provides a means for quantifying such risks. The publication emphasises the need for a structured approach to cyber risk management, offering organisations a valuable tool to enhance their protective and response capabilities.

Motivated by the critical role of the industrial Internet of Things (IIoT) in enhancing manufacturing processes through connectivity, automation, and intelligence, Dhirani et al. [31] evaluated the IIoT landscape, associated cyber threats, and prevailing standards. The authors explore the challenges imposed by cyber threats within the IIoT context and stress the importance of standards for addressing interoperability, cybersecurity, and artificial intelligence in IIoT systems. Dhirani et al. [31] proposed a roadmap for developing and implementing standards to mitigate cyber threats and improve IIoT system performance. The study concludes by emphasising the urgent need for robust cybersecurity measures and standardised protocols to ensure secure and efficient IIoT operations in industrial settings.

Cherdantseva et al. [25] reviewed risk assessment methods in Supervisory Control and Data Acquisition (SCADA) and analysed these methods in terms of the application domain, the stages of risk management addressed, key risk management concepts covered, impact measurement, sources of probabilistic data, evaluation, and tool support. While some of the methods calculate risk scoring, others provide steps and processes for the assessment. Risk reduction, attack countermeasures, and cyberterrorism framework were included in the review. The authors proposed an intuitive scheme for categorising cybersecurity risk assessment methods, distinguishing them as guidelines versus activity-specific, model-based versus formula-based, qualitative versus quantitative, and probabilistic versus non-probabilistic. Building upon this work, our research focuses on risk identification within the ICS domain rather than risk assessment. We elaborate on the capability and suitability of each analysed method and associated tools for addressing emerging risks in ICS environments. Furthermore, we expanded the method categorisation to reflect the two broad risk assessment approaches proposed by the National Cyber Security Centre (NCSC) [43], irrespective of the primary focus of the method or tool.

Elhady et al. [26] conducted a thorough investigation of scientific articles, guidelines, and databases related to SCADA risk identification parameters, providing a comparative analysis among them. Their study proposed a comprehensive risk identification model for SCADA systems based on ISO 31,000 risk management principles and guidelines [38]. This model detailed risk identification parameters, identified relationships between those parameters, and utilised a hierarchical approach to developing complete risk scenarios. Additionally, the model defined an inter-dependency risk map among all stated risks.

While Elhady et al.'s work focused on a single framework, our research explores multiple frameworks including IEC-62,443, ISO-27,001 and ISO-31,000 to broaden the criteria for method capability. Furthermore, we extend the scope



beyond risk identification methods to include an analysis of risk identification tools.

Peng et al. [44] conceptualised cyber–physical systems as a three-level architecture and analysed the security features at each level. They utilised the attack tree method to outline potential cyber events, taking into account known threats and vulnerabilities at each level while evaluating the probability and estimating the consequences of these events. However, their research primarily focused on risks related to data exchange within system components and did not address information flow from the enterprise level.

In a separate study, Khodabakhsh et al. [39] employed a three-step cyber-risk identification methodology to assess risks in a digital substation (DS). They identified cyberattack vectors targeting DS, mapped these vectors to MITRE ATT&CK metrics and the CIA triad, and developed mitigation plans. By basing their methodology on a playbook of attackers' tools, tactics, and procedures, they estimated the impacts on the system according to the attackers' capabilities. Nevertheless, their research did not cover other attack vectors outside the OT domain such as supply chain threats, safety concerns, and ransomware.

Hurd and McCarty [29] conducted a survey of tools used to investigate, detect, mitigate, and prevent cyberattacks in an ICS environment. Their report compiled a list of relevant tools and examined their coverage within ICS architecture. Each tool's purpose was analysed from a cybersecurity perspective and categorised accordingly. While Hurd and McCarty [29] provided detailed insight into individual components and technical solutions, our work takes a more holistic view of the ICS environment.

Giannopoulos et al. [45] reviewed risk assessment methodologies for the protection of critical infrastructures in Europe. Their findings classified these methodologies into three main approaches: application of risk assessment methodologies to infrastructure, structural analysis, and behavioural analysis. However, each tool and methodology was evaluated independently, lacking comparative analysis. Additionally, the study did not make a clear distinction between risk identification and risk assessment, nor did it address the advanced challenges previously mentioned.

As summarised in Table 2, the primary distinction between our work and the studies reviewed in this section lies in our focus on risk identification tools as opposed to risk assessment methods. Additionally, we utilised the methods and categorisations proposed by the NCSC [43] to accurately position each tool within the ICS architecture and the Purdue reference model.

### 3 | RISK AND ELEMENTS OF RISK

According to the risk analysis and management for critical asset protection (RAMCAPTM) framework [48], cyber risk constitutes a critical component of enterprise risk, making risk assessment an integral part of risk management [49]. Using the quantification formula for calculating risk as proposed by the

Department of Homeland Security, [50, 51] estimated risk using the following formula:

$$Risk = Threat \times Vulnerability \times Consequence \quad (1)$$

where

- *threat* is internal or external agents intended to disrupt or cause harm to the organisation.
- *vulnerability* is a weakness in the (ICS) system that can be exploited, and
- *consequence* is the result on the system if the threat has successfully exploited vulnerability.

Finally, risk is the impact on the organisation. Usually expressed in terms of sources, potential events, consequences, and likelihood risk is the effect of uncertainty on objectives. Equation (1), however represents risk as a multiplication of attributes rather than a function of the probability of the threat and consequences, where practitioners seek to provide answers to the three basic questions [52].

- *What can go wrong?* This question aims to identify and define the potential failure scenarios ( $S_i$ ) that could occur within the system, process, or activity under analysis. It comprehensively identifies risks or adverse events that may lead to undesirable outcomes.
- *How likely is it to go wrong?* This question determines the probability ( $P_i$ ) or likelihood of the identified failure scenarios occurring. It involves assessing the factors or conditions contributing to the failure scenario's realisation. The goal is to quantify the likelihood of the failure scenario occurring.
- *What are the consequences?* This question evaluates the potential consequences ( $Y_i$ ) or impacts associated with the identified failure scenarios. It involves assessing the severity of the outcome.

Based on the above risk questions, the following risk equation can be derived:

$$R_i = \{S_i, P_i, Y_i\} \quad i = 1, 2, \dots, n \quad (2)$$

where

- $R_i$  represents the risk associated with the  $i$ th failure scenario or risk event.
- $S_i$  represents the failure scenario or adverse event itself for the  $i$ th risk.
- $P_i$  represents the probability or likelihood of the  $i$ th failure scenario occurring.
- $Y_i$  represents the consequences or impacts associated with the occurrence of the  $i$ th failure scenario.
- $i = 1, 2, \dots, n$  indicates that the equation accounts for multiple risks, where  $n$  is the total number of identified failure scenarios or risk events.

TABLE 2 Related work.

Study	Summary	Risk focus
Peng et al. [44]	Peng et al. Proposed a risk assessment framework that includes risk identification. Peng et al. Distinguished between traditional (IT) assessment methods and adopted the attack tree method. Risk identification is not clearly distinguished from risk assessment. No justification was provided for the choice of method used. Other methods were not considered.	Risk assessment
Hurd and McCarty [29]	Hurd and McCarty provided categorised tools according to the following: Indicator of compromise (IOC) detection; network traffic anomaly detection; outlier analysis; log review; system artefacts review; reverse engineering (RE) analysis. They provided an availability gap analysis showing the lack of tools for certain functions.	None
Khodabakhsh et al. [39]	Khodabakhsh et al. Distinguished between risk identification and risk assessment and adopted the attack's impact on assets and the CIA triad as a methodology to identify risks in a digital substation (DS). They followed a three-step approach of discovering attack vectors, evaluating impact using MITRE metrics and defining mitigation plans. The methodology is focused on the MITRE metric only. Risk identification is limited to components	Risk assessment
Cherdantseva et al. [25]	The authors presented a structured overview of cyber security risk assessment methods in a SCADA environment. Provided a comprehensive and detailed overview of methods under review. Methods are categorised into model-based and formula-based. Analysis and evaluation are based on criteria. Risk identification is not clearly distinguished from risk assessment.	Risk assessment
Giannopoulos et al. [45]	Cherdantseva et al. Focused on the state of the art of risk assessment methodologies for critical infrastructures. They provided criteria for evaluation and analysed each methodology and tool, highlighting their strengths and capabilities. Although they provided a gap analysis, they did not compare the methodologies. In addition, they did not give a clear distinction between a methodology and a tool.	Risk assessment
Elhady et al. [26]	This study introduced a new methodology (model) for risk identification and mapped risks, vulnerabilities, and system components. It presented risk identification parameters and a comprehensive risk identification model for SCADA systems. The risk identification parameters were based on publicly-available vulnerability resource databases such as NDV, CVE, MITRE, and ICS-CERT.	Risk identification
Eggers and le Blanc [46]	Focussing on the nuclear industry, eggers and le Blanc surveyed and rated cyber risk analysis techniques based on three criteria of scope, adoptability, and repeatability to better understand cyber risk analysis techniques for use in nuclear power plants. Each technique is evaluated based on whether its capability aligns with the security requirements at a nuclear power plant. They highlighted gaps in current techniques in relation to the nuclear industry.	Risk assessment
Qassim et al. [47]	Focussing on power networks, the authors provided a comparative analysis of methodologies, based on assessment focus: Vulnerability, patch management, and risk. They reviewed and compared SCADA security assessment methodologies and examined their strengths against assessment requirements for the electrical power networks. Risk identification is not clearly distinguished from risk assessment.	Risk assessment

Abbreviations: CIA, confidentiality, integrity, and availability; ICS-CERT, Industrial Control Systems Cyber Emergency Response Team; SCADA, Supervisory Control and Data Acquisition.

Conversely, NIST [53] defines risk as a measure of the extent to which a potential circumstance or event threatens an entity. Risk is typically a function of (i) the adverse impacts that would arise if the circumstance or event occurs and (ii) the likelihood of occurrence. Similarly, Stouffer et al. [54] characterise risk as the consequence of the likelihood of a vulnerability being exploited by a given threat. In the context of ICS, risk is defined as *a function of the likelihood of a given threat source exploiting a potential vulnerability and the resulting impact of such exploitation* [54]. However, Burnap [55] suggests that risk should be described rather than universally defined, as a single definition may exclude certain viewpoints and perspectives. Burnap concurs with the National Cyber Security Centre's (NCSC) [43] description of risk as the likelihood of an undesirable event occurring and the net negative impact resulting from the exploitation of a

vulnerability, considering both the probability and the impact of occurrence.

Following the above, Burnap [55] suggested the adoption of a common language as a baseline terminology for risk management, and defined risk assessment as a composition of four concepts as follows.

- *Vulnerability* is a weakness in a socio-technical object or process that is open to an attack or exploitation by a threat. In the IT domain, security professionals focus their resources on finding weaknesses in a system to mitigate them. On the other hand, attackers aim to exploit only one weakness.
- *Threat* is a socio-technical element (person, event, and action) with the capability to exploit a vulnerability and give rise to risk. Threats have the potential to disrupt or harm a

system. Threat sources are the intent or methods of an exploit and they include adversarial, accidental, structural, and environmental.

- **Likelihood** is the degree of possibility that a threat will exploit a vulnerability, measured in frequency, probability, or probability of frequency.
- **Impact** is a negative effect or consequence of the successful exploitation of a vulnerability.

Regardless of the specific definition, risk can be understood as a tri-sector function encompassing threat, vulnerability, and consequences. As illustrated in Figure 3, the risk is the intersection of three key elements: threat, vulnerability, and impact.

Threat analysis involves identifying threats to a goal, system, or process. The overlap between threat and consequence (Region A) reveals the intent of the adversary. Conversely, focussing on identifying system weaknesses constitutes a vulnerability analysis, where the intersection of threat and vulnerability (Region B) indicates the likelihood of the adversary's capability to exploit those weaknesses. Additionally, the intersection of vulnerability and consequence (Region C) determines the likelihood of an impact. An impact analysis assesses the consequences arising from the inability to achieve a mission.

### 3.1 | Risk identification process

Risk identification is a critical component of the risk assessment processes outlined in both NIST SP 800-82 [35] and ISO 27005:2022 [33]. Burnap [55] has highlighted the similarities between these two processes, concluding that the activities involved are fundamentally comparable. The risk identification process can be decomposed into four stages as illustrated in Figure 4. The initial stage involves identifying the enterprise goals, which provide the scope for risk identification. This stage includes determining the processes to be considered in the risk assessment and establishing the level of impact that is acceptable to the business.

The risk identification process aligns with the guidance provided by NCSC, which categorises risk management into two broad approaches: (i) component-driven and (ii) system-

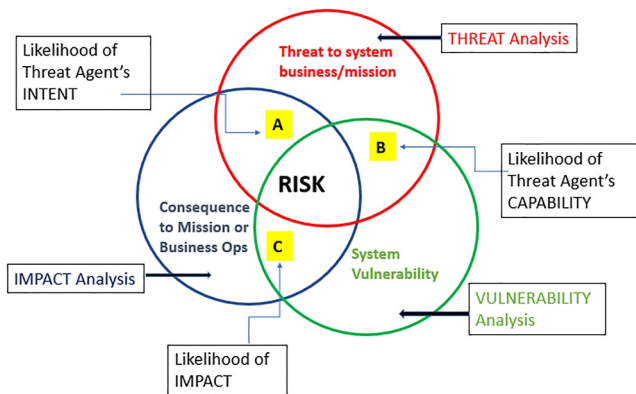


FIGURE 3 Core elements of risk.

driven [43]. The component-driven approach focuses on specific risks to individual technical components, whereas the system-driven approach analyses the system as a whole. Burnap [55] observed that although each approach has its distinct applicability, they are complementary. He concluded that the system-driven approach is more applicable at the enterprise level, while the component-driven approach is more suited for operational employees. A summary of the distinctions between these two approaches is provided in Table 3.

## 4 | DESCRIPTION OF RISK IDENTIFICATION TOOLS

Selecting risk identification tools is a complex task due to the frequent conflation of risk identification and risk assessment processes. However, guidance provided by Eggers and Le Blanc [46] and Cherdantseva et al. [25] aids in selecting appropriate tools for performing risk identification in an ICS environment.

While an extensive array of risk assessment tools and models exists, we present and analyse a selected subset. Each tool was evaluated and compared based on the following criteria: focus, method (according to NCSC's categorisation), coverage (based on the ICS Purdue model), standard/guidance alignment, applicability, strengths and capabilities, and limitations. A summary of each tool's description is provided in Table 4. Detailed analyses of each tool are as follows.

### 4.1 | Security posture analysis (SPA-by Clarity)

SPA [56] is an offline assessment tool that focuses on vulnerability assessment by providing visibility and insight into

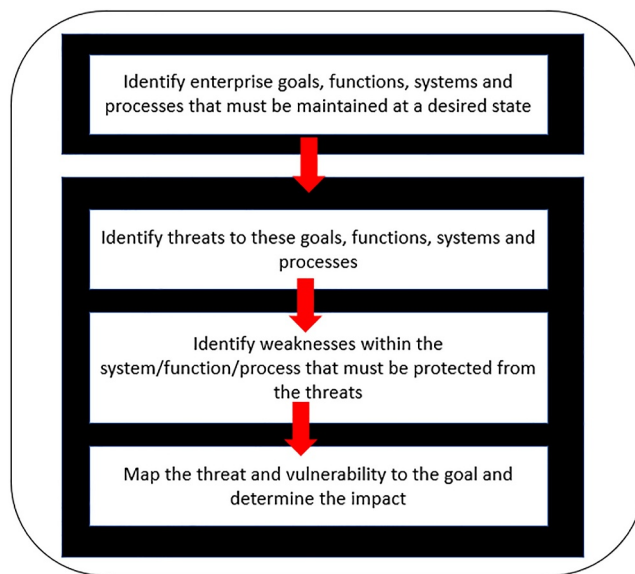


FIGURE 4 Risk identification process.

**TABLE 3** The distinction between system-driven and component-driven concepts of risk management [43].

System-driven	Component-driven
Top-down analysis.	Bottom-up analysis.
Exploring security breaches that emerge from complex interactions of many system parts.	Analysing the risks faced by individual (specific) technical components.
Establishing system security requirements before it is decided based on the system's exact physical design.	Working at levels of abstraction where stakeholders have already agreed upon a system's physical function.
Analysing security breaches that cannot be tracked back to a single point of failure.	Deconstructing less complex systems with well-understood connections between components.
Bringing together multiple stakeholders' views on what a system should and should not do (e.g. safety, security, legal views).	Requires only the system's input and the cyber analyst's input to determine what risk exists, based on component vulnerabilities.

**TABLE 4** Risk assessment tools and their methods.

Tool	Description
SPA [56]	The tool provides visibility and insight into the security risk posture of an OT network. It utilises packet capture (pcap) data files from the industrial control system (ICS) environment to discover assets and communication protocols present within the OT network.
CIARA [57]	The tool constructs a digital model of the ICS network environment using a pcap file and additional data sources. It leverages the MITRE ATT&CK repository to map threats to the network components and performs a gap analysis on the model.
ADT model [23]	The tool employs fuzzy theory and the attack-defence tree methodology to identify potential attack paths, suggest corresponding defence strategies, and evaluate various scenarios.
CRIM [26]	The tool utilises six risk identification parameters—what, who, why, how, where, and when—to construct an attack scenario matrix from a risk scenario database.
CyberPHA [58]	The tool identifies potential consequences and maps the possible threat scenarios (the kill chain) that could lead to these identified consequences.
STPA-Sec [59]	The tool employs a failure-focused methodology to define risks to a system, mapping the system's mission, purpose, and goals to cybersecurity considerations.
DM [61]	The tool employs a top-down, success-focused methodology to identify risks by articulating goals and the controllable and uncontrollable preconditions necessary to achieve these goals.
CCE [62]	The methodology identifies the most critical processes or functions—such as operational goals, critical functions, and critical services—that must not fail in an ICS environment.
Bow tie [63]	It identifies threat scenarios using the four components of event, hazard, threat, and consequence.
ATT&CK (ICS) [67]	The tool serves as a curated knowledge base for post-compromise analysis, detailing how an attacker compromises the system and their subsequent behaviour.
CIS-RAM [69]	The tool utilises a workbook to analyse risk, evaluating each control to determine how threats can be detected or prevented.
CyRA [71]	The tool focuses on threat modelling, vulnerability identification, and consequence analysis to deliver adequate and efficient authentication and authorisation for all registered components within the ICS.

Abbreviation: STPA, Systems Theoretic Process Analysis.

the security risk posture of an OT network. It utilises the component-driven approach to analyse and compute hygiene scores and common vulnerabilities and exposures (CVE) scores for each identified vulnerability. The tool applies primarily to the lower levels of the Purdue model, making it purely technical and lacking references to enterprise process objectives. Notably, the tool does not align with any ICS standard.

The SPA solution adheres to traditional risk identification methods. However, due to its limited scope and application

area, specifically its focus on vulnerability assessment, it does not significantly support addressing the current cyber risk landscape or emerging cyberattack trends.

## 4.2 | Cyber industrial automated risk analysis (CIARA—by Radiflow)

CIARA [57] focuses on threat and vulnerability assessment by employing a component-driven approach to construct a digital



model of the ICS network environment from pcap files and other data sources. The tool aligns with IEC 62443 standards and is applied primarily to the lower levels of the Purdue model, making it purely technical and devoid of references to enterprise process objectives.

Among its strengths and capabilities, CIARA operates offline without interfering with operational services and is sector- and geography-agnostic. Similar to SPA, CIARA adheres to traditional risk identification methods. However, due to its limited scope and application area, specifically its focus on threat and vulnerability assessment, it does not provide significant support for addressing the current cyber risk landscape or emerging cyberattack trends.

### 4.3 | Cybersecurity risk assessment method of ICS based on the attack–defence tree (ADT) model

The ADT Model tool proposed by Wang et al. [23] focuses on threat assessment through a component-driven approach, utilising fuzzy theory to address the probability questions within an ADT. While this tool does not align with any ICS standards it is applied to the lower levels (1–3) of the Purdue model, making it purely technical and not concerned with enterprise process objectives.

One of the tool's strengths is its ability to mitigate the impact of subjective factors on cybersecurity risk assessment computations. However, similar to SPA and CIARA, the ADT Model tool adheres to traditional risk identification methods. Due to its limited scope and application area, specifically its focus on threat and vulnerability assessment, it does not provide significant support for addressing current cyber risks or emerging cyberattack trends.

### 4.4 | Comprehensive risk identification model for SCADA systems (CRIM)

The comprehensive risk identification model for SCADA Systems (CRIM) employs a component-driven approach to focus on threats, vulnerabilities, and impacts for identifying risks within a SCADA system. It utilises vulnerability database sources such as CVE Industrial Control Systems Cyber Emergency Response Team, Mitre, and National Vulnerability Database to correlate the risk identification parameters from ISO 31000 to various risk scenarios. The tool aligns with ISO 31000 ICS standards and is applied to the lower levels (1–3) of the Purdue Model, making it purely technical and not concerned with enterprise process objectives.

One of the key strengths of CRIM is its scalability and the unlimited range of hypothetical scenarios it can generate. However, similar to SPA, CIARA, and the ADT model tool, CRIM adheres to traditional risk identification methods. Due to its limited scope and application area, specifically its focus on threat and vulnerability assessment, CRIM does not provide

significant support for addressing the current cyber risk landscape or emerging cyberattack trends.

### 4.5 | CyberPHA (by AESolutions/Deloitte)

CyberPHA employs a consequence-focused safety-oriented risk methodology to define cyber risk as a function of threats, vulnerabilities, and consequences [58]. It is based on the ISA/IEC 62443 standard [34] and can also be mapped to the NIST SP 800-82 framework. Utilising a component-driven approach, CyberPHA aims to understand how a cyber incident could occur by analysing the system's inventory, data flow, and architecture diagram information, ultimately delivering a risk-ranked mitigation plan.

Unlike other component-driven tools, CyberPHA incorporates a comprehensive multidisciplinary approach. It identifies potential consequences and maps possible threat scenarios (the kill chain) that could lead to these consequences. However, due to its limited visibility of the upper levels of the Purdue model, CyberPHA cannot effectively link to the IT domain where enterprise systems reside. Consequently, it falls short in sufficiently addressing the current cyber risk landscape and emerging cyberattack trends.

### 4.6 | Systems theoretic process analysis for security (STPA-Sec)

STPA-Sec addresses the three elements of risk: threat, vulnerability, and impact [59]. Unlike traditional risk methods, STPA-Sec employs a failure-focused methodology to define risks within a system, linking the system's mission, purpose, and goals to cybersecurity. It utilises a system-driven approach to identify design flaws, component interactions, and human factors that contribute to system failure. Based on the STAMP (Systems-Theoretic Accident Model and Process) collection of techniques [28], STPA-Sec aligns with the NIST SP 800-160 standard.

STPA-Sec's coverage spans all five levels of the Purdue model, addressing early engineering designs (cybersecurity by design) by using business and mission objectives to define problems and unacceptable losses. The tool relies on business owners to provide system objectives and describe system functions, enabling STPA-Sec to approach risk identification as a control problem. This methodology allows STPA-Sec to address emerging cyberattack trends, such as ransomware and supply chain attacks.

However, while STPA-Sec covers (cyber)security identification broadly, it does not specify cyber risk identification in detailed terms.

### 4.7 | Dependency modelling

Dependency modelling (DM) is a top–down risk quantification method used for identifying, analysing, and managing risk in

complex systems [60, 61]. Unlike other methodologies, DM does not rely on a thorough knowledge of potential threats but instead focuses on integrating all elements contributing to an organisation's desired outcomes. Unlike STPA-Sec, DM emphasises positive outcomes and their dependencies, enabling business and asset owners to understand the highest sensitivities to the risk of failure in achieving strategic goals.

Dependency modelling requires business owners to provide system objectives and describe the system functions necessary to analyse the impact of failing to achieve the desired goals. Dependency modelling serves as both a tool and a standard (O-DM), which has been adopted by the Open Group for risk management and is complementary to ISO/IEC 31000:2018. It aligns with ISO/IEC 27001:2022 and covers all five levels of the Purdue model.

Although DM is not specific to risk identification, its versatility makes it adaptable and capable of addressing emerging cyberattack trends such as ransomware and supply chain attacks.

#### 4.8 | Consequence-driven cyber-informed engineering (CCE—by Idaho National Laboratory)

The CCE methodology addresses threats, vulnerabilities, and impacts within complex ICS systems [62]. As a consequence-focused methodology, CCE aligns with ISO/IEC 27005 and NIST SP 800-82 standards to identify the most critical processes or functions—such as operational goals, critical operations, and critical services—that must not fail in an ICS environment. It utilises both system-driven and component-driven concepts to prioritise consequences using the high consequence event score and identifies the system-of-systems within the ecosystem that supports those critical processes or functions.

Similar to CyberPHA and STPA-Sec, CCE covers all five levels of the ICS Purdue model, from top management to the operator level. This comprehensive coverage ensures that IT domain threats are included in the cyber risk assessment and that emerging cyber threats are considered. Compared to traditional risk management methods, CCE provides a holistic platform that views the system as an integrated whole rather than as a collection of parts. However, it should be noted that risk identification is not clearly delineated within the CCE framework.

#### 4.9 | Bow tie modelling (by Dragos)

BowTie is a modelling methodology that addresses threats and impacts through both component-driven and system-driven concepts. It takes a threat-and-consequence approach, combining various risk analysis techniques such as fault tree analysis, event tree analysis, and causal factor charting to identify threat scenarios. The four components of

the BowTie method directly map onto existing ICS cybersecurity frameworks such as MITRE ATT&CK and are applicable across all levels of the Purdue Model. This methodology provides a visual linkage among events and predicts interrelated events, including those involving external service providers.

Although BowTie is not explicitly aligned with any standard, it has been adopted by organisations such as Dragos [63] and CGE [64] for ICS risk modelling and visualisation. Additionally, Abdo et al. [65] proposed its adaptation for ICS, and Hale [66] suggested integrating CyberPHA and BowTie methodologies. However, the model may become overly complex for management purposes due to the interrelations among events. Moreover, while BowTie addresses risk management, it does so without a clearly defined boundary for risk identification.

#### 4.10 | ATT&CK for ICS mitigation (by MITRE)

ATT&CK is a threat- and capability-focused tool that leverages a component-driven concept [67]. The framework is a versatile tool used for threat analysis and risk assessment within the cybersecurity domain. It is a curated knowledge base designed for post-compromise analysis, detailing how attackers compromise systems and their behaviours [68]. ATT&CK for ICS aligns with IEC 62443 and NIST SP 800-53 standards to develop specific threat intelligence models as part of a system's risk assessment programme.

Unlike other tools, when ATT&CK for ICS is combined with ATT&CK for enterprise, they provide full coverage of the Purdue model levels. However, ATT&CK for ICS is less effective in addressing emerging cyberattacks such as ransomware and supply chain attacks. Nonetheless, it serves as a valuable resource for other tools, such as CIARA and BowTie.

#### 4.11 | CIS-RAM for ICS

CIS-RAM [69] provides step-by-step instructions to evaluate whether a control is reasonable based on the threat and impact to objectives [70]. Utilising a system-driven approach, it employs a workbook to analyse the risk associated with each control, considering how threats may be detected or prevented. CIS-RAM aligns with existing risk standards such as NIST SP 800-30 and ISO/IEC 27005, accounting for the unique mission and business requirements specific to ICS environments and the unique risks that prioritise security requirements.

Similar to STPA-Sec, CyberPHA, and CCE, CIS-RAM covers all levels of the Purdue model, treating cyber risk holistically rather than as separate, compartmentalised components. Furthermore, this methodology addresses emerging cyberattack trends, such as ransomware and supply chain attacks. However, it should be noted that CIS-RAM is a manual text-based tool.

## 4.12 | CyRA: a real-time risk-based security assessment framework

CyRA is a real-time component-driven security assessment framework that concentrates on threat modelling, vulnerability identification, and consequence analysis. While the primary focus is on authentication and authorisation, CyRA aims to identify and mitigate unknown malware threats within system components [71]. Utilising zero-knowledge proof of knowledge, CyRA performs multi-factor authentication on every component that requests resource access.

CyRA does not align with any established ICS risk standards. Although it can identify unknown threats, its coverage is confined to the lower levels of the Purdue Model. Moreover, its functionality is limited to authentication and authorisation. While CyRA can address issues such as ransomware it does not comprehensively tackle emerging threats like supply chain attacks.

## 5 | COMPARATIVE ANALYSIS

Twelve tools were selected for analysis due to their inclusion (or implication) of various degrees of risk identification features within their risk assessment functionalities. Only four of these tools [59, 62, 63, 69] perform risk identification based on the established ICS risk elements of threat, vulnerability, and impact. The remaining eight tools focus on one or two of the core risk elements as illustrated in Figure 3. Three of the analysed tools [59, 61, 62] have the capacity to identify and map threats and vulnerabilities to enterprise goals, correlating with the risk identification process shown in Figure 4.

Although most of these concepts and tools are relatively new they are linked to existing, mostly established methods and technologies. For example, ATT&CK for ICS is derived from ATT&CK for enterprise, STPA-Sec is based on STPA, CIARA leverages the MITRE ATT&CK database, and CyberPHA adapts the safety-oriented methodology of process hazard analysis. Additionally, ATT&CK for ICS [67] and CIS-RAM [69] provide functional repository resources for other tools. This indicates the potential for integrating many component-driven tools to leverage functionalities available in other tools.

Recent cyber incidents have prompted a shift from fragmented and compartmentalised risk assessment methods to holistic frameworks that view risk as an integrated whole. Many system-driven tools offer comprehensive risk identification for the entire system, covering all levels. In contrast, component-driven tools typically adopt only a partial risk identification process. Consequently, only tools based on the system-driven concept are capable of adequately addressing current cyber-attack challenges such as ransomware and supply chain attacks.

### 5.1 | National Cyber Security Centre categorisation

Using the risk assessment concept classification proposed by NCSC [43], seven of the analysed tools are component-driven, as

observed in Table 5. This indicates a clear preference for focusing on hardware and communication protocol components rather than the whole system. Although complementary, it is argued that the system-driven approach allows for an iterative articulation of the system's goals and functions, facilitating a deeper understanding of the interactions among components and processes. According to the NCSC categorisation shown in Table 5, five tools are system-driven while the remaining tools are component-driven. Only system-driven tools can provide comprehensive enterprise coverage for risk identification.

### 5.2 | Tools' coverage and focus

Table 6 shows that seven tools are limited to identifying risks only at the lower levels of the Purdue model. Consequently, these tools are unable to address emerging security challenges. Risk comprises three elements: threat, vulnerability, and impact. As indicated in Table 7, only four tools encompass all these elements, qualifying as true risk identification tools, while the others are primarily focused on either vulnerability or threat identification. An exception is DM [61], which focuses solely on impact.

There is a clear correlation between the methods, risk identification processes, and the Purdue Model layer coverage. Cross-referencing Table 5 with Tables 6 and 7 reveals that component-driven tools adopt only a partial risk identification process and cover only the lower levels of the Purdue Model. These tools fail to provide visibility into the IT domain, resulting in an incomplete risk assessment that focuses solely on specific components. Only tools that cover all levels of the Purdue Model have the capability to address current cyber-attack challenges, such as ransomware, supply chain threats, and unknown risks.

The dichotomy within ICS, wherein IT domain security concerns often conflict with those of the OT domain, justifies distinguishing between the applicable security controls in these two domains. This is reflected in the tools developed for risk identification, where seven out of 12 examined tools lean towards a component-driven approach, thus primarily addressing OT risks. However, there is a potential danger of protecting the wrong assets, especially if the protection is not aligned with the enterprise's overall risk goals.

### 5.3 | Tool's capability

Following a similar pattern, as previously observed, the capacity of each tool to address emergent security concerns—such as business risk, ransomware, supply chain threats, and safety—relies on its focus and categorisation. As shown in Table 8, four of the selected tools are unable to address any of these security concerns, even when their risk identification focus includes comprehensive analyses of vulnerability, threat, and impact. Generally, tools restricted to the OT domain are inadequate for addressing emergent security concerns. However, an exception to this rule is the CyRA tool [71] which is capable of identifying unknown risks, such as ransomware, at the OT level.

**TABLE 5** Categorisation of the methods into the National Cyber Security Centre (NCSC) concept.

Category	Tool reference
System-driven	STPA-Sec [59], DM [61], CCE [62], bow tie [63], CIS-RAM [69]
Component-driven	SPA [56], CIARA [57], ADT model [23], CRIM [26], CyberPHA [58], ATT&CK (ICS) [67], CyRA [71]

Abbreviations: ICS, industrial control system; STPA, Systems Theoretic Process Analysis.

Tool	Process	Level 5	Level 4	Level 3	Level 2	Level 1
SPA [56]	Partial			+	+	+
CIARA [57]	Partial			+	+	+
ADT model [23]	Partial			+	+	+
CRIM [26]	Partial			+	+	+
CyberPHA [58]	Partial			+	+	+
STPA-Sec [59]	Full	+	+	+	+	+
DM [61]	Full	+	+	+	+	+
CCE [62]	Full	+	+	+	+	+
Bow tie [63]	Full	+	+	+	+	+
ATT&CK ICS [67]	Partial			+	+	+
CIS-RAM [69]	Full	+	+	+	+	+
CyRA [71]	Partial			+	+	+

Abbreviations: ICS, industrial control system; STPA, Systems Theoretic Process Analysis.

**TABLE 7** Risk identification: tool focus.

Tool	Applicability	I	V	T
SPA [56]	Any OT domain with PCAP logs		+	
CIARA [57]	Any OT domain with PCAP logs		+	+
ADT model [23]	ICS system components		+	+
CRIM [26]	ICS components	+	+	+
CyberPHA [58]	ICS components	+	+	+
STPA-Sec [59]	Whole system	+	+	+
DM [61]	Whole system	+		
CCE [62]	Whole system	+	+	+
Bow tie modelling [63]	Whole system and external factors	+		+
ATT&CK for ICS [67]	ICS components	+		+
CIS-RAM [69]	Whole system	+		+
CyRA [71]	OT components			

Note: I= Impact — V=Vulnerability — T = Threat.

Abbreviations: ICS, industrial control system; STPA, Systems Theoretic Process Analysis.

## 6 | OPEN ISSUES AND CONCLUSION

In this paper, we identified new and evolving risk identification tools developed in recent years. We examined each tool to assess its focus, scope, applicability, and capability to address current cybersecurity challenges in the ICS environment. Our study revealed that ICS cyber risk identification tools are

**TABLE 6** Risk identification: tool coverage.**TABLE 8** Risk identification: tool capabilities.

Tool	BR	R	SC	UR	S
SPA [56]					
CIARA [57]					
ADT model [23]					
CRIM [26]					
CyberPHA [58]		+			+
STPA-Sec [59]	+	+	+	+	+
DM [61]	+	+	+	+	
CCE [62]	+	+	+	+	
Bow tie [63]	+	+	+	+	
ATT&CK for ICS [67]		+	+		
CIS-RAM [69]	+	+	+		
CyRA [71]		+		+	

Note: BR= Business Risk — R=Ransomware — SC=Supply chain — UR=Unknown Risk — S=Safety.

Abbreviations: ICS, industrial control system; STPA, Systems Theoretic Process Analysis.

pivotal to effective risk management and that this ecosystem is vibrant and active, with contributions from academia, business, and government sectors. Among the 12 tools and concepts reviewed, there was nearly equal representation from both academia and business domains. However, our study also highlighted several open issues related to cyber risk and its identification.



## 6.1 | Open issues

In consideration of the comparative analysis, the research has revealed the following issues.

- Risk is an inherent part of everyday business operations, and effective risk management begins with accurate identification. However, proper risk identification must align with business goals, as identifying risks that are too broad, too narrow, or misaligned with the organisation's requirements can lead to ineffectiveness. In the ICS environment, understanding the risk to the enterprise is crucial for identifying and assessing cyber risks. Cyber risk constitutes a component of corporate risk, and risk assessments must support the overall objectives of the organisation.

For instance, a system shutdown due to the end of life of a system or component may not be categorised as a cyber-risk issue, but it represents a significant business risk, particularly if the system is critical to the organisation's objectives. Without identifying risks in relation to these overarching goals, a cyber-risk assessment of the system may not be accurate or comprehensive.

- Three traditional risk analysis methods and classifications are widely used: qualitative, quantitative, and semi-quantitative. Among these, the risk matrix is the most prominent method, capable of incorporating either qualitative or quantitative scoring, as illustrated in Figure 5. However, recent academic discourse has questioned the effectiveness of traditional risk matrix assessments in the context of cybersecurity. Scholars such as Cox [72] and Hubbard [73] have argued that the method is subjective and insufficient for effectively identifying, evaluating, and managing risk.
- Every factor that affects the degree of risk—including processes, systems, and components—contributes to determining the risk rating based on the likelihood of their manifestation. Business owners can estimate the impact of risks on the overarching goals or objectives of the business or asset by considering several factors such as survivability, economics, environment, safety, and quality of service. However, the current focus has primarily been on high-impact risks, with insufficient attention given to low-

impact risks. When synchronised or sequentially manifested, these low-impact risks could result in significant consequences.

The Stuxnet incident [13] exemplifies this scenario: the frequency of centrifuge replacement was not initially considered a high-impact risk, but its synchronised manifestation led to substantial consequences. To address this gap, risk identification tools should include features to systematically map process dependencies and interactions among low-impact risks. The results can then be compared to high-impact risks to identify necessary mitigation measures.

- Cyber resiliency in ICS remains an open issue that is gaining importance as a critical feature in engineering design. However, much of the published research on system resiliency primarily focuses on availability rather than the system's ability to complete its function with the desired (correct) output and align with the overall goals of the organisation or process [74]. Given its operational context, Bishop [75] proposed two key variables to measure resilience: (i) the time required for the system to return to its desired state after an attack and (ii) the maximum perturbation that will not prevent the system from returning to its desired state. These variables are functions of the system's operational goals which, in turn, determine the risk to the enterprise. Unfortunately, there is limited research incorporating these variables into risk identification and measurement.
- To comprehensively identify risks in a system, both safety and security must be included as a breach in one can compromise the functionality of the other. Efforts to synergise these elements are gaining traction within the research community. However, the challenge of balancing security requirements with the safe operation of the ICS environment remains a critical factor in the overall success of cybersecurity. Safety is a primary concern for any significant ICS system, and there cannot be a fail-secure system without a corresponding fail-safe system [76]. The underlying concepts of security and safety are inherently complementary. Tools must analyse the alignment of cyber risk goals with hazard risks to ensure that protection mechanisms are triggered in response to security-related risks. This alignment is essential to creating a cohesive strategy that integrates both safety and security considerations.
- Furthermore, Filkins et al. [77] emphasise that the misalignment of IT and OT security concerns poses a more significant threat than those associated with accidental insiders, supply chain issues, and malicious external actors. One approach to aligning goals and bridging this gap is to fully implement the risk identification process in every risk assessment exercise [78]. The discussion has now broadened to encompass consequence-based risk assessment, DM, and system-theoretic analysis approaches. These approaches analyse the goals and functions of the ICS system as well as the interactions between processes to identify associated risks.

		Impact					
		Negligible	Minor	Moderate	Critical	Catastrophic	
		1	2	3	4	5	
Likelihood	Frequent	5	Medium	Medium	High	High	High
	Likely	4	Medium	Medium	Medium	High	High
	Occasional	3	Low	Medium	Medium	Medium	High
	Seldom	2	Low	Low	Medium	Medium	Medium
	Improbable	1	Low	Low	Low	Medium	Medium

FIGURE 5 Typical risk matrix.

- Our study focused on cyber risk identification. However, the results of this study necessitate an extension to encompass the broader domain of risk management to investigate the capabilities of other risk assessment tools. We intend to consider this extension in future studies. Additionally, the proposed tool's requirements do not include capabilities for real-time, dynamic-response risk identification; therefore, future research should address this requirement.

## 6.2 | Proposed solution

In light of the issues discussed above, we propose a consequence-driven tool that integrates both system-driven and component-driven approaches, employs system-theoretic principles, utilises quantitative probability techniques, and features graphical modelling and safety capabilities. Our proposal is based on the following assertions.

- Cherdantseva et al. [25] assert that probabilistic risk assessment methods are preferable over other quantitative, non-probabilistic, and qualitative methods due to their ease of comprehension for security decision-makers, particularly in terms of numeric risk estimation.
- Burnap [55] concludes that the top-down approach inherent in the system-driven concept makes it more suitable for enterprise-wide analysis.

This tool will be capable of addressing both current and future cyber risk concerns in the ICS domain. Although such a tool does not currently exist, a combination of STPA-Sec [59] and DM [61] would fit this framework. Our proposed solution is feasible, not as a real-time risk identification tool but as a component of a comprehensive risk management process analysis. Additionally, the proposed tool offers a graphical interface that provides a clear interpretation of the risk identification results, eliminating the need for a dedicated risk analyst. This feature enhances the tool's practicality and cost-effectiveness in the long run.

## 6.3 | Conclusion

We conducted a comprehensive review of cyber risk identification tools, evaluating their capacities and limitations in addressing the emergent cybersecurity challenges faced by the ICS environment. Recent events, such as the Colonial Pipeline ransomware attack [7] and the third-party attack on the largest train operating company in Denmark [79], underscore the critical importance of cyber risk identification across all facets of operations, including IT, OT, and external domains. To address some of the issues raised, we have proposed a new tool and aim to extend this research for further development.

We are currently exploring the use of DM as an option to enhance the proposed tool. We invite well-positioned

researchers and practitioners to extend the list of tools, propose new solutions, and continue the discussion on this vital topic.

## AUTHOR CONTRIBUTIONS

**Ayo Rotibi:** Conceptualisation; Methodology; Validation; Writing - original draft. **Neetesh Saxena:** Conceptualisation; Methodology; Supervision; Writing - review & editing. **Pete Burnap:** Writing - review & editing.

## ACKNOWLEDGEMENTS

This work was supported by the Knowledge Economy Skills Scholarship (KESS) through the Welsh Government and Thales UK. Also, the work was supported by the British Council (IND/CONT/G/23-24/07), UKIERI (IND/CONT/G/23-24/67), UKRI (EP/Y026233/1), and RITICS Fellowship.

## CONFLICT OF INTEREST STATEMENT

The authors declare no conflicts of interest.

## DATA AVAILABILITY STATEMENT

Data sharing not applicable to this article as no datasets were generated or analysed during the current study.

## ORCID

*Neetesh Saxena*  <https://orcid.org/0000-0002-6437-0807>

## REFERENCES

1. Möller, D.P.F.: NIST cybersecurity framework and MITRE cybersecurity criteria. In: Guide to Cybersecurity in Digital Transformation: Trends, Methods, Technologies, Applications and Best Practices, pp. 231–271. Springer (2023)
2. Buganová, K., Šimíčková, J., Brutovský, M.: Impact of global changes in the business environment in relation to risk management. SHS Web of Conferences 92, 03004 (2021). <https://doi.org/10.1051/shsconf/20219203004>
3. Brandt, E., Silva, M., Beck, F.: Influence of family culture on enterprise risk management in Brazilian companies. Revista De Administração Contemporânea 25(6) (2021). <https://doi.org/10.1590/1982-7849-rac2021190082.en>
4. Kayan, H., et al.: Cybersecurity of industrial cyber-physical systems: a review. ACM Comput. Surv. 54(11s), 1–35 (2022). <https://doi.org/10.1145/3510410>
5. Eric, D.K.: Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems. Elsevier (2024)
6. Rotibi, A.O., et al.: System-level operational cyber risks identification in industrial control systems. In: Cyber-Physical Systems, pp. 1–32 (2024)
7. Reeder, J.R., Tommy Hall, C.: Cybersecurity's Pearl Harbor Moment: Lessons Learned from the Colonial Pipeline Ransomware Attack (2021)
8. Javed Butt, U., et al.: Ransomware threat and its impact on SCADA. In: 2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3), pp. 205–212. IEEE (2019)
9. Giles, M.: Triton Is the Worlds Most Murderous Malware, and its Spreading (2019). <https://tinyurl.com/4xtsj7pj>. Accessed 11 Oct 2022
10. Slay, J., Miller, M.: Lessons learned from the Maroochy water breach. In: International Conference on Critical Infrastructure Protection, pp. 73–82. Springer (2007)
11. Albright, D., Brannan, P., Walrond, C.: Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Institute for Science and International Security (2010)

12. Assante, M.J., Lee, R.M.: The industrial control system cyber kill chain. SANS Institute InfoSec Reading Room 1(24) (2015)
13. Lee, R.M., Assante, M.J., Conway, T.: German steel mill cyber attack. *Industrial Control Systems* 30(62), 1–15 (2014)
14. Greenberg, A.: The Untold Story of Notpetya, the Most Devastating Cyberattack in History (2018). <https://tinyurl.com/4b522pcs>. Accessed 12 Oct 2022
15. Lee, R., Assante, M., Conway, T.: Analysis of the cyber attack on the Ukrainian power grid. *Electricity Information Sharing and Analysis Center (E-ISAC)* 388(1-29), 3 (2016)
16. Schouwenberg, R.: Notpetya Ushered in a New Era of Malware (2019). <https://tinyurl.com/5ewutxcu>. Accessed 12 Oct 2022
17. Morse, A.: Investigation: Wannacry Cyber Attack and the NHS, vol. 1. Report by the National Audit Office (2018)
18. Nargiza, A.: Ransomware: analysis of 2019 lockergoga cyber-attack to Norsk hydro multinational company and its countermeasures. *Eurasian Journal of Media and Communications* 9, 1–9 (2022)
19. Beerman, J., et al.: A review of colonial pipeline ransomware attack. In: 2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW), pp. 8–15. IEEE (2023)
20. Beulah Rani, I., et al.: Intrusion detection system for cyber attacks in food and beverage industry. In: 2022 International Conference on Automation, Computing and Renewable Systems (ICACRS), pp. 1287–1291 (2022)
21. Seals, T.: Johnson Controls Ransomware Cleanup Costs Top 27m and Counting (2024). <https://tinyurl.com/yc3wwedr>. Accessed 27 2 2024
22. Zurier, S.: Dole Now Says February Attack Spilled Employee Data (2023). <https://tinyurl.com/33swzwz6>. Accessed 17 2 2024
23. Wang, S., et al.: Cybersecurity risk assessment method of ICS based on attack-defense tree model. *J. Intell. Fuzzy Syst.* 40(6), 1–14 (2021). <https://doi.org/10.3233/jifs-201126>
24. Shen, J., Feng, D.: Vulnerability analysis of CSP based on stochastic game theory. *J. Control Sci. Eng.* 2016, 1–12 (2016). <https://doi.org/10.1155/2016/4147251>
25. Cherdantseva, Y., et al.: A review of cyber security risk assessment methods for SCADA systems. *Comput. Secur.* 56, 1–27 (2016). <https://doi.org/10.1016/j.cose.2015.09.009>
26. Elhady, A.M., El-bakry, H.M., Abou Elfetouh, A.: Comprehensive risk identification model for SCADA systems. *Secur. Commun. Network.* 2019, 2019–2024 (2019). <https://doi.org/10.1155/2019/3914283>
27. Metzger, L.S., et al.: Systems Engineering Guide: Collected Wisdom from Mitres Systems Engineering Experts. Technical report. MITRE CORP BEDFORD MA BEDFORD United States (2014)
28. Young, W., Leveson, N.G.: An integrated approach to safety and security based on systems theory. *Commun. ACM* 57(2), 31–35 (2014). <https://doi.org/10.1145/2556938>
29. Hurd, C.M., McCarty, M.V.: A survey of security tools for the industrial control system environment. *Carbohydr. Res.* 330(3), 431–435 (2017)
30. Mattioli, R., Moulinos, K.: Analysis of Ics-Scada Cyber Security Maturity Levels in Critical Sectors. European Union Agency for Network and Information Security (ENISA) (2015)
31. Luxmi Dhirani, L., Armstrong, E., Newe, T.: Industrial IOT, cyber threats, and standards landscape: evaluation and roadmap. *Sensors* 21(11), 3901 (2021). <https://doi.org/10.3390/s21113901>
32. Joint Task Force Transformation Initiative: SP 800-39. Managing Information Security Risk: Organization, Mission, and Information System View. National Institute of Standards & Technology (2011)
33. Hyseni, V., Kabashi, E.: ISO/IEC 27005:2022: Main Changes and Implications — pecb.Com. <https://pecb.com/article/isoiec-270052022-main-changes-and-implications> (2023). [Accessed 15-07-2024]
34. The International Society of Automation: Quick Start Guide: An Overview of ISA/IEC 62443 Standards (2020). <https://tinyurl.com/2rhys29>. Accessed: 11 Feb 2022
35. Ribeiro, A., et al.: Adapting NIST SP 800-82r3 to Tackle Complexity of Cyber Threats across OT Environments (2023). <https://shorturl.at/i7P4t>. Accessed 15 07 2024
36. British Standards Publications: S en iec 31010:2019 risk management. risk assessment techniques (2019). <https://tinyurl.com/y84jruf>. Accessed: 12 Dec 2022
37. Ackerman, P.: Industrial Cybersecurity: Efficiently Secure Critical Infrastructure Systems. Packt Publishing Ltd (2017)
38. BSI: Risk Management — Guidelines. British Standards Institution (BSI), London (2018). Standard
39. Khodabakhsh, A., et al.: Cyber-risk identification for a digital substation. In: Proceedings of the 15th International Conference on Availability, Reliability and Security, pp. 1–7 (2020)
40. Stouffer, K., et al.: Guide to Operational Technology (OT) Security. US Department of Commerce, National Institute of Standards and Technology (2023)
41. NIST: Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. SP 800-37 Rev. 1. National Institute of Standards & Technology (2010)
42. Sheehan, B., et al.: A quantitative bow-tie cyber risk classification and assessment framework. *J. Risk Res.* 24(12), 1619–1638 (2021). <https://doi.org/10.1080/13669877.2021.1900337>
43. NCSC: Risk Management Guidance (2017). <https://tinyurl.com/47mym4nz>. Accessed 30 May 2022
44. Peng, Y., et al.: Cyber-physical system risk assessment. In: 2013 Ninth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, pp. 442–447. IEEE (2013)
45. Giannopoulos, G., Filippini, R., Schimmer, M.: Risk Assessment Methodologies for Critical Infrastructure Protection. Part I: A State of the Art. *JRC Technical Notes* (2012)
46. Shannon, E., Blanc, K.Le: Survey of cyber risk analysis techniques for use in the nuclear industry. *Prog. Nucl. Energy* 140, 103908 (2021). <https://doi.org/10.1016/j.pnucene.2021.103908>
47. Saif Qassim, Q., et al.: A review of security assessment methodologies in industrial control systems. *Information & Computer Security* 27(1), 47–61 (2019). <https://doi.org/10.1108/ics-04-2018-0048>
48. Brashear, J.P., Jones, J.W.: Risk analysis and management for critical asset protection (RAMCAP Plus). In: *Wiley Handbook of Science and Technology for Homeland Security*, pp. 1–15 (2008)
49. SecurityScorecard: The Role of Cybersecurity in Enterprise Risk Management (ERM) (2021). <https://tinyurl.com/54ettr6z>. Accessed 15 Dec 2022
50. Morgan, H.: Cyber security risk management in the SCADA critical infrastructure environment. *Eng. Manag. J.* 25(2), 38–45 (2013). <https://doi.org/10.1080/10429247.2013.11431973>
51. Anthony Cox, L., Jr: Some limitations of “risk= threat×vulnerability×consequence” for risk analysis of terrorist attacks. *Risk Anal.: Int. J.* 28(6), 1749–1761 (2008). <https://doi.org/10.1111/j.1539-6924.2008.01142.x>
52. Kaplan, S., Garrick, B.J.: On the quantitative definition of risk. *Risk Anal.* 1(1), 11–27 (1981). <https://doi.org/10.1111/j.1539-6924.1981.tb01350.x>
53. Al Fikri, M., et al.: Risk assessment using NIST SP 800-30 revision 1 and ISO 27005 combination technique in profit-based organization: case study of ZZZ information system application in ABC agency. *Procedia Computer Science* 161, 1206–1215 (2019). <https://doi.org/10.1016/j.procs.2019.11.234>
54. Stouffer, K., et al.: Guide to Industrial Control Systems (ICS) Security—Nist Special Publication (SP) 800-82 Revision 2. NIST (2015). Tech. Rep
55. Burnap, P., et al.: The Cyber Security Body of Knowledge, vol. 12 (2020). KA. UK. 2019
56. Clarity: Clarity Security Posture Assessment (2018). <https://tinyurl.com/fudw4fjx>. Accessed 11 Sept 2022
57. Radiflow. Ciara: Cyber Industrial Automated Risk Analysis IEC-62443-Based Risk Assessment in ICS/SCADA Network (2020). <https://tinyurl.com/nn9xs9ts>. Accessed 30 Sept 2022
58. Jacob, M.: Cyberpha: A Proven Method to Assess Industrial Control System Cybersecurity Risk (2019). <https://tinyurl.com/cuj4thbw>. Accessed 15 Sept 2022
59. Young, W., Porada, R.: System-theoretic process analysis for security (STPA-SEC): cyber security and STPA. In: 2017 STAMP Conference (2017)
60. Slater, D.: A Dependency Modelling Manual - Working Paper (2016)
61. Slater, D.: Open Group Standard Dependency Modeling (O-DM) (2016)

62. Bochman, A.A., Freeman, S.: Countering Cyber Sabotage: Introducing Consequence-Driven, Cyber-Informed Engineering (CCE). CRC Press (2021)
63. Carlson, J., Michaud-Soucy, D.: Using Bow Tie Risk Modelling for Industrial Cybersecurity (2021). <https://tinyurl.com/rb9jardz>. Accessed 25 September 2022
64. CGE: How to Be Prepared for Cyber Attacks (2020). <https://tinyurl.com/4xek45uz>. Accessed 12 Sep 2022
65. Abdo, H., et al.: A safety/security risk analysis approach of industrial control systems: a cyber bowtie—combining new version of attack tree with bowtie analysis. *Comput. Secur.* 72, 175–195 (2018). <https://doi.org/10.1016/j.cose.2017.09.004>
66. Hale, G.: Visualizing Cyberpha via Bow Tie (2020). <https://tinyurl.com/6mzcke88>. Accessed 30 Oct 2022
67. Alexander, O., Belisle, M., Steele, J.: Mitre Att&ck® for Industrial Control Systems: Design and Philosophy (2020)
68. MITRE: Att&ck for Industrial Control Systems (2020). <https://tinyurl.com/ygkz46mn>. Accessed 16 June 2022
69. Centre for Internet Security: Cis Risk Assessment Method (RAM) Version 2.0 (2021). <https://tinyurl.com/fudw4fx>. Accessed 3 Oct 2022
70. Groš, S.: A critical view on cis controls. In: 2021 16th International Conference on Telecommunications (ConTEL), pp. 122–128. IEEE (2021)
71. Sadiq Sani, A., et al.: Cyra: a real-time risk-based security assessment framework for cyber attacks prevention in industrial control systems. In: 2019 IEEE Power & Energy Society General Meeting (PESGM), pp. 1–5. IEEE (2019)
72. Louis Anthony (Tony) Cox Jr: What's wrong with risk matrices? *Risk Analysis. Int. J.* 28(2), 497–512 (2008)
73. Douglas, W.H., Seiersen, R.: How to Measure Anything in Cybersecurity Risk. John Wiley & Sons (2016)
74. Bodeau, D.J., et al.: Cyber Resiliency Engineering Framework. Technical report. MITRE CORP BEDFORD MA (2011)
75. Bishop, M.: Resilience and Security (2017). <https://tinyurl.com/y6l8ot3d>. Accessed 30 June 2022
76. Knowles, W., et al.: A survey of cyber security management in industrial control systems. *Int. J. Crit. Infrastruc. Prot.* 9, 52–80 (2015). <https://doi.org/10.1016/j.ijcip.2015.02.002>
77. Filkins, B., Wylie, D., Dely, A.J.: Sans 2019 State of OT/ICS Cybersecurity Survey. SANS Technology Institute (2019)
78. Claroty: The Global State of Industrial Cybersecurity (2020). <https://tinyurl.com/y9ekkk7w>. Accessed 11 April 2022
79. Kovacs, E.: Cyberattack Causes Trains to Stop in Denmark (2022). <https://tinyurl.com/mu2y3rcx>. Accessed: 5 Nov 2022

**How to cite this article:** Rotibi, A., Saxena, N., Burnap, P.: Winning the battle with cyber risk identification tools in industrial control systems: a review. *IET Cyber-Phys. Syst., Theory Appl.* 1–16 (2024). <https://doi.org/10.1049/cps2.12105>