IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier

Extended Dependency Modelling Technique for Cyber Risk Identification in ICS

AYODEJI O. ROTIBI[1], NEETESH SAXENA[1], PETE BURNAP[1] and ALEX TARTER[2]
[1]School of Computer Science, Cardiff University, Cardiff, UK
[2]Thales Ltd., UK

Corresponding author: Neetesh Saxena (e-mail: saxenan4@cardiff.ac.uk).

This research was conducted with the support of EU, KESS2, and Thales, UK

ABSTRACT Complex systems such as Industrial Control Systems (ICS) are designed as a collection of functionally dependent and highly connected units with multiple stakeholders. Identifying the risk of such complex systems requires an overall view of the entire system. Dependency modelling (DM) is a highly participative methodology that identifies the goals and objectives of a system and the required dependants to satisfy these goals. Researchers have proved DM to be suitable for identifying and quantifying impact and uncertainty in complex environments. However, there exist limitations in the current expressions of DM that hinder its complete adaptation for risk identification in a complex environment such as ICS. This research investigates how the capability of DM could be extended to address the identified limitations and proposes additional variables to address phenomena that are unique to ICS environments. The proposed extension is built into a system-driven ICS dependency modeller, and we present an illustrative example using a scenario of a generic ICS environment. We reflect that the proposed technique supports an improvement in the initial user data input in the identification of areas of risk at the enterprise, business process, and technology levels.

INDEX TERMS Dependency Modelling, Industrial Control System, Risk, Risk Identification Methodologies

I. INTRODUCTION

BUSINESSES no longer operate in isolation, and new business processes and operational models of complex systems are continuously expanding. Recent events such as the Colonial pipeline attack have proved that the data exchange and dependencies of the higher-level components within the enterprise systems mean that a successful attack on the enterprise system could impact the operability and function of the entire enterprise [1]. This has necessitated the desire to explore other techniques to identify risk in complex systems.

Cyber risk identification in ICS is non-trivial due to the multifaceted and ever-changing requirements and dependencies within the domain. Secondly, the security model of confidentiality, integrity, and availability (CIA triad) approach in ICS is significantly limited in identifying risks due to the characteristics of the ICS environment, such as the ability to control and observe the state of the environment, safety control measures, and reliability of the system. These characteristics are represented as the Safety, Reliability and Productivity (SRP) and Controllability, Observation and Operability (COO) triad, without which a comprehensive identification of risks is challenging [2]. In addition, recent literature on the analysis of cyber incidents trends involving ICS indicates that the adversary's TTP is increasingly expanding the attack surface beyond the traditional ICS technical processes, necessitating a clamour for a new approach to risk identification in the domain [3]–[5]. Other challenges are enumerated as follows:

- An attack in one business vertical can now propagate across interconnected supply chain. The recent attack on a third-party service provider in the ICS domain indicates that the previous assumption that malware can only enter the ICS via internet-facing devices has been debunked [6].
- As businesses continue to undergo digital transformation, cyber risk has become an essential component of the enterprise risk [7]. While enterprise risk is the overarching risk that defines what service is to

be protected, cyber risk examines all the associated factors that may prevent service delivery, such as threats, equipment vulnerabilities, and other external factors. Current practices however suggest that most cyber risk assessments are system component-based [8].

To identify the risks and vulnerabilities of the ICS (including safety and reliability) requires a thorough understanding of the system under consideration (SuC), including topology, components, behaviour, and operational objectives, and researchers have long used modelling methods and languages to understand the system. One such modelling methods is dependency modelling (DM) - a top-down success-focus (positivist) approach to expressing goals and objectives, and the preconditions to satisfy these goals.

In this paper, we summarise our contributions as follows.

- We proposed a novel technique that improves DM's capability to systematically treat the initial data input and unsure a pragmatic outcome. We examined DM as a viable modelling tool for risk identification in ICS and proposed a probability input that is based on prior knowledge and the likelihood of evidence.
- We have shown that the proposed technique can be applied in typical real ICS scenario to reflect its practical impact. We introduced Security Posture as a list of cybersecurity-related statements to enable us to extract prior knowledge and likelihood from the asset and process owners. This was another gap in prior techniques. We compared the results of our technique to the classical DM and highlight the differences.
- To the best of our knowledge, this is the first attempt at applying the Bayes Posterior computational technique to address the issue of the empirical input data to DM.

II. RELATED WORK

Based on the perception of risk, various authors and institutions have developed frameworks and techniques for risk identification and analysis in the enterprise. Over the years, stakeholders have used various methods such as Fault-Tree Analysis (FTA), Attack-Defence Tree (ADT), Dependency Modelling (DM), and Stochastic Modelling to address risk identification [9], [10].

The work by the Open Group [11] and Cherdantseva et al. [12], [13] are complimentary. While [12] demonstrated how dependency modelling could be utilised for risk assessment, [11] and [13] provided a dependency modelling technique standard for building and decomposing a system's abstract model. Cherdantseva et al. [12] also presented a comprehensive dependency template for a SCADA system and the application of the model to the SCADA system, highlighting the various features and validation of the model. These two works of literature provide the basis for our work as we examine the model's capabilities to address some of the issues raised earlier.

In our previous work, Burnap et al. [14] proposed an extension to dependency modelling to determine and share risk data in distributed systems. The authors postulated a zooming process where inter-dependent entities can link to a repository of external dependency data (risk model) to build a realistic "living" risk model. While this work focuses on realistic risk modelling, our work focuses on identifying such risk phenomena not currently addressed by dependency modelling. It is hoped that our work may in future incorporate the postulations as contained in [14].

Alpcan and Bambos [15] developed a framework for modelling and exploring how risk cascades between business units, security vulnerabilities and people within an enterprise. The authors used a risk-rank algorithm to systematically prioritise risks based on the propensity to transfer and cascade risk among the defined security risk factors (business units, threats and vulnerabilities, and people). Although this work presents a system-driven approach dependency model based on the assumption that all risks come through inter-dependencies, its aim and methodology are distinctly different from conventional dependency modelling. The entirety of the work is a variant of dependency modelling methodology as described by [11] and [12]. While their framework used bipartite graph to identify failures, our proposal uses directed acyclic graphs (DAG) to identify success factors (causal effects) to achieve the enterprise goal.

Ani et al. [16] and Akbarzadeh & Katsikas [17] introduced the concept of functional dependency modelling analysis that evaluates the cascading effect of physical connections of ICS components within a three-level architecture and analyses the security features in each level. Based on the identified assets, the authors used the Attack tree method to define cyber events (what would happen to the system), considering known threats and vulnerabilities within the level. They also evaluated the probability of each event and estimated the consequences and the cascading impact (cascading impact value metric). However, as opposed to our research, the work by Ani et al. [16] and Akbarzadeh & Katsikas [17] are component-driven, focusing on risk concerning data exchange within components while excluding information flow from the enterprise.

While focusing on constructing a dependency path, Watters et al. [18] used a matrix table to analyse the relative importance of mission/business objectives. With this approach, user provides a numerical factor to represent the dependency of one objective (or sub-objectives) over the other objectives within the business. The analysis results in a RiskMap model representing the business's dependency and priority (weight) information.

Although the goal might be similar, the approach and measure of dependency in [18] are significantly different from the traditional DM and our work.

Innerhofer–Oberperfler and Breu [19] used enterprise architecture to define dependencies between relevant business and technical objects. In proposing their method, the authors sought to resolve dependency complexity between the various business supporting information processes and the responsibilities of the various stakeholders. There are similarities in our approaches to defining the dependencies, but the methodology for risk identification is significantly different.

The Crown Jewel Analysis tool by MITRE [20] provided a failure-oriented attack modelling for identifying assets that are critical to a mission (mission-based risk identification). Unlike our approach, this model examines dependencies for criticality candidacy and predicts failure impact for individual assets without considering a combination of failures. Attack tree and fault tree analysis modelling adopt the failure-oriented approach to address the need for a comprehensive analysis, using directed acyclic graphs whose leaves represent component failures and whose gates represent failure propagation [21], [22]. Although these methods provide for analysis of local dependencies, a fundamental limitation is its inability to account for risk countermeasure. In addition, it does not show impact across the broader system, particularly where the nodes do not share a common dependency path. Similar limitations were observed in the work of Abdo et al. [23] even though the attack tree technique was extended using the bowtie technique.

III. CYBER RISK IDENTIFICATION MODELLING IN ICS

ICS describes a highly sophisticated hierarchically-structured and complex system where control actions flow from the higher level (Controller) to the lower level (Controlled Process), and feedback flow from the lower level to the higher level. In such architectures, the functionally dependent and highly connected processes, services, components, and networks within the environment mean that the state of one component or function can unilaterally or in combination with other components influence the state of other components within the system. However, this functional dependency is not transparent or obvious, resulting in the exposure of the ICS to a myriad of non-linear and sometimes intractable risks [2].

Cyber risk is an operational disruption or damage introduced by digital technologies to an ecosystem's informational and operational functions. The consequences of disruption in the ICS environment could be severe and catastrophic, leading to damage to the environment, endangerment of life, heavy financial losses, and damage to equipment [24].

Understanding the cyber risk to the ICS environment is key to identifying risk and vulnerability in the environment. Traditional risk analysis of the ICS environment is based on the likelihood that a threat would exploit a vulnerability, and impact analysis results from the inability to achieve the desired outcome. It is a process of seeking answers to the three basic questions of (a) "what could fail in the system operation?", (b) "how likely is it to fail?", and (c) "what are the consequences of failure?" [25]. The first question seeks to define a failure scenario (S_i), the second question explores the probability of the failed scenario (P_i), and the third question dwells on the likely outcome described by the scenario (Y_i).

$$R_i = (S_i, P_i, Y_i)$$

These hypothetical questions define the traditional approach to risk management, and they are still relevant. However, Hubbard and Seiersen [26] described (Cyber) risk as a state of uncertainty, where uncertainty is the existence of more than one possibility out of many unknown outcomes. Here, risk is measured as a set of uncertainties (possibilities), each with quantified probabilities, providing a perfect alignment to DM.

The criticality of cybersecurity in ICS requires that risk measurement be empirical and acceptable. DM has provided a means to decompose a system into what we want to observe and analyse, but the result of its application to risk identification must be trusted. In view of the limited availability of data regarding some critical uncertainties in risk identification, this paper focused on the DM's capabilities to represent uncertainties in terms of probability distributions in probabilistic risk analysis (PRA). This allowed us to consider users' input information in terms of probability distributions.

A considerable amount of individual intuition is involved in risk management, resulting in various methods to score and scale a widely endorsed risk matrix for aggregated risks based on a subjective scale of "likelihood" and "impact". Colour-coded in green and red (and a shade of yellow), this qualitative method provides less intuitive information about how a certain event impacts a system, and to what degree. Cox [27] and Hubbard [26] argued that these methods only add noise to the risk assessment process, but do not improve it. On the contrary, DM enables us to ask factual questions such as "what is within the system that makes it functional?" and "what could have greater influence within the system?" Christopher [28] suggested that cyber risk management in ICS requires multiple stakeholders' contributions to aggregate the various views across verticals. This means new approaches to provide greater visibility to the ICS environment are required to capture some foundational assumptions, such as resiliency, reliability, and interdependencies among processes, and address the unique characteristics and complexity of the whole ICS environment [29].

This new approach requires viewing the ecosystem of the ICS domain (such as the people, technology, process

and supply chain) as a collection of functional parts, where the whole is greater than the sum of its parts and the overarching system's goal overrides the operational objective of the individual functions that make up the system. Here, the focus of cyber risk is no longer about the technology alone but about how the enterprise function. It is about understanding the behaviour, interactions, dependencies, and associated vulnerabilities inherent in the system, including seemingly-non-critical cyber components that are capable to bypass security controls and other defences [5], [30].

Recent rise in cyberattacks on ICS are evidenced in the various academic research publications [1], [30]–[34]. In particular, the rise in ransomware attacks and recent concerns about supply-chain attack vectors have proved that external events outside of the ICS environment could impact the ICS environment, if there is a functional dependency on the external factor [1]. To address this new approach, the UK's National Cyber Security Centre (NCSC) provided a guideline for cyber risk management that covers a variety of approaches, particularly from a business point of view [8].

The guideline provided the core concepts behind the different risk analysis approaches and viewed risk analysis from two broad concepts: (i) component-driven and (ii) system-driven. The component-driven concept (bottom-up) is a tactical, threat-based approach that focuses on a specific risk to a technical component, while the system-driven concept (top-down) analyses a system as a whole. The comparative benefits of the system-driven framework have inspired various models and techniques to perform cyber risk identification and analysis. Some of the existing adaptations of the system-driven framework are as shown in Table 1.

IV. DEPENDENCY MODELLING

DM belongs to the family of Probabilistic Risk Assessment (PRA) methods and focuses on the capability of the System under Consideration (SuC) to identify their controllable and uncontrollable phenomenon and provides a platform for multi-stakeholder participation and holistic analysis of a complex system. Advocates of its application argue that it enables a comprehensive identification of dependencies and improves understanding among stakeholders by revealing other intrinsic values that other techniques may otherwise miss [11], [12], [14].

DM views risk as the degree of uncertainty - uncertainty that a system will be at a required (desired) state. This is expressed as the probability of achieving the desired state of a goal and how it is impacted by things beyond the control, predictability or understanding of the system/process owner [11]. This probability is a measure of being in a state and not the severity of impact. It is typically a quantitative measure that presents a graphical description of a complex network of systems, using statistical inferences to compute the likelihood of the "state" (not the likelihood of an "event") of each node (sub-system goal) in the graph. The graph reflects the impact of dependencies as it computes the back-up propagation of the changes in the state of a lower node (sub-system goal) on the upper nodes that depend on it, up to the root node (system goal).

While other techniques and methods such as Consequence-driven Cyber-informed Engineering [29], Attack Tree modelling [45], and Bow-Tie modelling [46], [47] uses a consequence-focused methodology to identify the most critical processes or functions that must not fail, or finding what factors could lead to failure (threats) [29], DM focuses on the interactions and behaviours within the system and the required dependencies for desired outcomes. Similarly, while other methodologies focus on the capability of the adversaries and how to defend against their threats, DM reflects on what the impact of a manifested threat might look like. Rather than finding how the system could be compromised, DM is about what a successful attack on the system could mean. This is a paradigm shift in the risk identification model, to which Young and Porada [48] subscribed as a viable alternative to understanding vulnerabilities in the system. Furthermore, the three-point Sensitivity (3PS) plot included in DM analyses the root node's exposure (sensitivity) of the root node to each of the leaf nodes (the uncontrollable dependencies) in the dependency tree. The 3PS report helps the business owner determine where to effectively focus resources to mitigate the threats.

The goal-oriented approach of DM makes the technique well suited for identifying risks associated with process interaction flows such as in ICS, allowing for multiple optimisation and "what-if" analysis that aid in the prioritisation of responses [49]. The technique is widely accepted and has been adopted by the Open Group as a standard tool (O-DM) to highlight areas of highest risk sensitivity in a complex system [36].

A. RISK IN THE CONTEXT OF DEPENDENCY MODELLING

From ICS risk identification perspective, DM provides an excellent way of describing the interaction and exploring the relationship between procedures, processes, technology, and communication within and about the ICS environment. Cherdantseva et al. [12] classified DM as a probabilistic risk assessment (PRA) method where DM views a system as a combination of processes working together. Here, each process ("clients") depends either structurally or semantically on other processes or entities ("suppliers"), and the degree of dependency ("coupling") is a function of how much a change in the "supplier" impacts the "client". That is, based on the evidence available to the asset owner or the relevant subject matter experts (SME), the user provides a scoring (based on the scale of either 0-10 or 0-100) of how close to the "desired state" the leaf nodes are. The

TABLE 1. Existing Adaptations of the System-driven Framework

Organisation	Tool	Techniques	Features
MIT [35]	STPA-Sec.	Systems-Theoretic Accident Model and Processes (STAMP).	Focus is on causal loss scenarios, based on unacceptable control action
The Open Group [36]	Open Dependency Modelling (O-DM).	Dependency Modelling.	Focuses on required factors to achieve an objective (a goal).
Idaho National Laboratory [29]	Consequence-driven Cyber-informed Engineering (CCE).	Consequence-driven Cyber-informed Engineering (CCE).	Focus is how to quantify impact of attack.
DRAGOS [28]	Dragos BowTie model for ICS.	Bow-Tie.	Focus is on threat scenarios and consequences (specific events)
McQueen et al. [37]		Qualitative measurement Directed/Compromise graph	To calculate risk-reduction estimates for a specific ICS system
SABSA Institute [38]	SABSA Matrix.	Enterprise Architecture Standard.	Focuses on the duality of operational risk (opportunity and threat).
MITRE [20]	Crown Jewels Analysis (CJA).	Failure Mode and Effect Analysis (FMEA) and Fault Tree Analysis	Focus is on attack scenarios and attacker's capabilities
Brændeland et al. [40]	Risk graphs.	Using the CORAS threat modelling language to structure series of scenarios and events leading up to one or more incidents.	Focus is on modelling and analysis of risk scenarios with mutual dependencies
Hogganvik and Stølen [41]	CORAS	Based on CORAS threat modelling language and UML, the research proposed a formal semantic to capture how vulnerabilities enable security threats to harm the assets.	Provide a graphical approach for a common representation of the risk within a system
Guan et al. [42]	Digraph	Digraph	Proposed a digraph model for SCADA systems to identify areas of system vulnerability for SCADA systems.
Baiardi et al. [43]		Hypergraph	Proposed a formal risk management strategy based on security-related attributes of component attributes and dependency.
Chittester and Haimes [44]	Hierarchical holographic modelling (HHM)	Hierarchical holographic modelling (HHM)	Proposed a quantification of the probability of an attack to identify sources of risk to SCADA.

leaf nodes are the last (terminal) nodes towards the right of the graph.

As shown in Figure 1, the concept of dependency conditional probability is represented in a probabilistic graphical model (PGM), where the nodes in the graph represent goals (and sub-goals) and the edges (acyclic) that connect the nodes represent the probabilistic dependency relationship. The conditional probability of a successful parent node is derived based on the success probabilities of child nodes. The leaf nodes are the "uncontrollable" – nodes that cannot be controlled. The colour coding indicates that the red segment is the probability that the required state will not be attained, and the green segment indicates the probability that the desired state will be attained.

In effect, the quantitative probability estimates of the leaf nodes (referred to as uncontrollable) produce quantitative estimates of the states of all the parent nodes that are dependent on a collection of child nodes. That is; if the parent node is represented as A, and child nodes are represented as B, then the probability estimate that parent A will be in the required state is:

$$\mathrm{P(A)} = \prod_{\mathrm{i=1}}^{\mathrm{N}} \mathrm{P(B_i)} \tag{1}$$

The above is true where the relationship between the

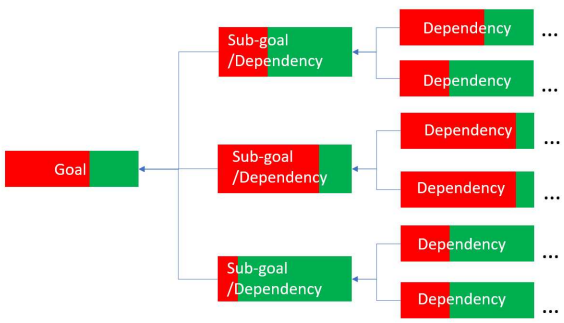


FIGURE 1. Dependency Modelling Graph

child nodes of one parent is an "and" relationship. Where the relationship is an "or" relationship (which means that one node is a countermeasure), then the probability estimate of the parent node is:

$$\mathrm{P(A)} = \prod_{\mathrm{i=1}}^{\mathrm{N}} \mathrm{P(1 - B_i)} \tag{2}$$

B. LIMITATIONS OF DEPENDENCY MODELLING

The accuracy of the risk identification using DM depends on the quality of the input data because DM is subject to a domino effect of wrong probability assump-

tions if the input is inaccurate. Cherdantseva et al. [50] stated this as a major obstacle for probabilistic Risk assessment methods. The authors could not find any indication of where probabilistic data came from, even after they had examined the work of other authors. In a further work, Cherdantseva et al. [12] suggested that the input data be objective and pragmatic. Where there is historical data to support its assertion, the input data will produce accurate results. However, in its current state, there is no known or standardised form to subject the input data to any acceptable objectivity and practicability. As briefly mentioned earlier, DM technique is limited in its primary function to calculate the impact of the failure of subsystems and components function. While it can show impact to a smaller degree on the local process (leaf of a dependency tree back up to its root), it cannot show impact across the broader system and across other branches of the tree. This limits the ability to understand and accurately access any direct or indirect impact of a change of state on other parts of the tree. Thirdly, from the perspective of the ICS, the binary probability equations 1 and 2 formalise the likelihood of each node at the exclusion of other factors, pieces of evidence (prior knowledge) and characteristics of the system (such as the level of coupling, resiliency and control measures) that may influence the outcome. The consequence of this limitation is that the probability values could be subjective without empirical evidence [51], [52].

In addition, the typical composition of the ICS environment meant that multiple independent failures could occur simultaneously or sequentially within the system. Here, the nature of dependencies and coupling within the ICS (interaction failures), where the combination of seemingly low-level impact could result in a higher impact. Presently, DM is not able to analyse this phenomenon. Lastly, DM requires all "what-if" analysis to start from the leaf node. This practice limits the stochastic scenarios that could be created.

V. PROPOSED TECHNIQUE

Complex systems such as ICS are known to have emergent properties and can fail due to a combination of unrelated stochastic events and phenomena. This makes risk identification non-trivial. A business-oriented approach to security analysis of enterprise information systems requires recognising and understanding the dependencies and interrelationships of the business supporting information process and providing sufficient and relevant security requirement information at the right level of abstraction. As a result of the enumerated limitations in Section I, we propose an extension to the capabilities of DM to address one of the limitations in the context of the unique ICS characteristics and phenomenon and answer the question raised.

A. METHOD

Since DM is underpinned by probability theory, we introduced posterior probability as a means to derive empirical user's input data from the initial subjective data. We compared results from using the two input and observed the differences in outcome. Leveraging DM's Directed Acyclic Graph (DAG) structure and the independence properties of probability graphical model (PGM), we proposed a capability extension that uses Bayes' Posterior probability [52] to draw inferences, given the evidence. This is achieved by defining security requirements (SR) for the enterprise and each business objective, and we expand the determinant factors for the state of each node to include other security-related coefficients such as existing security controls and resiliency factor, all within a time-frame.

B. POSTERIOR PROBABILITY (A POSTERIORI)

A Posteriori relates to information (data) that was derived by reasoning from observed facts. Bayes' rule is a rigorous method for interpreting evidence in the context of knowledge or previous experience. Posterior probability or "weighted likelihood" is the conditional probability of a given event. It is computed based on observing the known conditional and unconditional probabilities of a prior event [52]. This is the probability of effects, based on causes where, causes are the things we know about the node (sub-goal) based on observation, history, records or data, and effects are the things we do not know. The posterior distribution is interpreted as a summary of information from two sources: information we know about the system and the information we observed or recorded about the system. This is expressed as follows:

$$\text{Posterior} = \frac{\text{Likelihood} \times \text{Prior}}{\text{Evidence}}$$

$$\text{P(A|B)} = \text{P(A)} \times \frac{\text{P(B|A)}}{\text{P(B)}} \tag{3}$$

Where:

- P(A|B) is the posterior probability - updated probability after the evidence is considered
- P(A) is the prior probability - the probability based on prior knowledge
- P(B|A) is the likelihood of evidence, given the belief is true
- P(B) is the marginal probability of the evidence

We chose Posterior probability because it enables us to consider available knowledge of the system, such as its level of dependency, functional success rate (over a time period), and compliance with some SR as stipulated in ISA/IEC 62443 [24]. For convenient sake, we represent all these as "Security Posture" (SP). The result will produce the probability of desired state of each node.

The probability $P(S_n|SP)$ can be read as: "what is the probability that node S_n will be in the desired state, given that SP is true." The computation is derived as shown in the example of "Technology OK" in Figure 2 below:

Here, the user's input was 0.60 which represents the prior probability. The posterior probability is derived as 0.28 from the computation of both the conditional probability and marginal probability.

C. SECURITY POSTURE (SP)

Hansson and Aven [53] used a model that incorporates domain experts and decision makers in risk analysis. Leveraging on some of the elements of the model namely: evidence, knowledge base, and managerial review and judgement, we proposed SP as a set of security enterprise-specific statements that require responses from domain experts and decision makers. It is assumed that the response is based on evidence and knowledge, offering different perspective on the cyber risk posture of the enterprise that enables us to establish a baseline of security posture for the ICS environment and provides a formality by which we could use some of the responses as empirical evidence to improve the initial data input. To do this, we present a set of security-related and cyber resilience statements to the asset owners using the following sources as a guide: (1) IEC-62443 [24] - a suite of standards that relates to clearly defined obligations and responsibilities for maintaining resilient cyber security programs in industrial and automation control systems (IACS), (2) Dragos Annual Industrial Cybersecurity "Year in Review" Reports [54], (3) MITRE cyber resilience engineering framework (CERF) [55], and (4) SANS Annual OT/ICS Cybersecurity Survey [56]. In particular, we adopted some of the standardised cyber resiliency objectives. Each statement measure confidence and coverage of response. For example, where a user is asked to respond to a statement such as "There are security controls within the system,", there may be effective controls, but they do not apply to all parts of the system. In this case, the user will scale the confidence higher than the coverage. User's response is a scale of weighted scale of "Strongly agree", "Agree", "Neutral", "Disagree" and "Strongly disagree", where 5 means "Strongly agree" and 1 means "Strongly disagree" as shown in the application snapshot in Figure 3. A full list of all the statements is shown in Table 2.

Responses obtained are classed as "Evidence". This is applied to the user's probability input for leaf nodes to compute the posterior probability for each leaf node. We restrict our focus to the role and responsibilities of asset owners – the end users of the ICS devices. The ISA/IEC 62443-2 standard provides guidance to asset owners on how to create and maintain a secure system, define their system-level requirements, and how to measure these requirements. We assume two scenarios for our SP; (a) that the asset owner has some level of security program in their system, and (b) that the asset owner rely on services provided by third-parties suppliers such as system integrator. In this case, they will be keen to ensure that those suppliers meet their security requirements.

However, the sum of the scale values obtained from the table is not a probability distribution, we, therefore, applied normalisation to get a probability distribution such that the total sum will always be less than or equal to 1. This becomes the security posture coefficient for the category and it is applied to the user input for each leaf node. Initial probability value to each of the 73 leaf nodes is received and the dependency coefficient for the 34 dependants (nodes) are computed. A high-level algorithm for the application is shown below.

Algorithm 1 Security Posture

```
for statements = 1, 2, ... do
    Accept user's response
    Compute mean of each response
    Apply normalisation to responses by category
end for
Normalise responses by category
Compute security coefficient by category
for node = 1, 2, ... do
    Accept user input values
    Compute posterior probability
end for
Compute dependency without SP
Compute extended dependency with SP
```

D. DESCRIPTION OF ICS SCENARIO

The description of a typical ICS scenario is non-trivial given that the enterprise management requirement verticals are not distinctly differentiated between an ICS environment and a larger ICT environment, for example, a large retail shop. The top-Level entities of a SCADA System by Cherdantseva et al. [12] could otherwise apply to a non—SCADA environment as well as to a SCADA environment. To address this, we build an abstract model of a typical ICS enterprise by simplifying the top six key areas of a SCADA system [12] to three broad areas of abstraction, namely People, Process and Technology, and associated predetermined sub-goals based on the IEC 62443 requirements for ICS asset owners. Figure 4 provides a high-level description of a generic ICS environment and Figure 5 enumerates the security requirements of such environment.

Here, the enterprise model is adapted to represent the three broad areas of abstraction, namely People, Process and Technology, and associated predetermined sub-goals based on the IEC 62443 [24] and SABSA Institute [38] security enterprise architecture requirements for ICS asset owners. The dependency relationships among the various nodes (or paragons) are decomposed to the fourth level as a minimum requirement as shown in Figure 6 below. The user could provide further levels of abstraction if so desired. In this paper therefore, we

Event & P[x]	Prior (given)	P[x]	CP (from SP)	P[x]	JP	P[x]	PP
People = OK (Specialist Training OK)	0.96	P[System=OK | People=OK] (0.424 * 0.566)	0.239984	P[People=OK & System=OK] (0.96 * 0.239)	0.230	P[People=OK | System=OK] (0.230/0.238)	0.97
People ≠OK (Specialist Training not OK)	0.04	P[System=OK | People≠OK] (0.424 * 0.433)	0.184016	P[People=OK & System≠OK] (0.04 * 0.184)	0.007	P[People=OK | System≠OK] (0.007 * 0.238)	0.03
				P[System = OK]	0.238		

FIGURE 2. Example of Bayes Computation Table

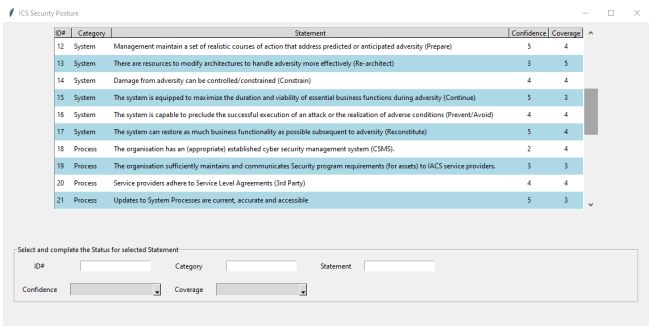


FIGURE 3. ICS Security Posture

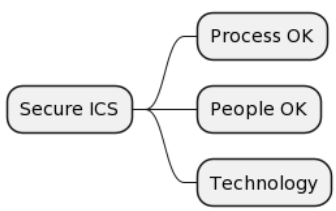
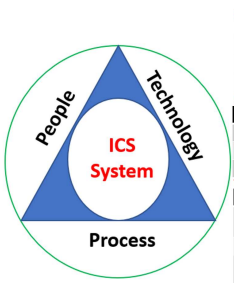


FIGURE 4. ICS Top-level Dependency



PEOPLE

Sub-Goals	Dependencies
Training	Needs, Awareness, Specialist, Policy, Compliance
Recruitment	Qualification, Background Check, Policy, Compliance
HR Policy	Policy, Compliance

PROCESS

Sub-Goals	Dependencies
Governance	Security Policy, Operational Procedures Guidelines
Compliance	Government & International, Standards
Performance	Measurement metrics, Monitoring

TECHNOLOGY

Sub-Goals	Dependencies
Reliability	System Maintenance, Patching, Monitoring, Change Control
Resiliency	Redundancy Policy, Business Continuity, System Backup
Productivity	Bespoke Application, Third Party Application, System Vendor, Supply chain
Security	Security Controls, Defined Security Requirements, System Segmentation, Network Architecture, Perimeter Defense

FIGURE 5. ICS Dependency Goals

have expanded to the fifth level to provide some ICS-specific requirements, as shown in Figure 7. We postulate that beyond this level of granularity, the modelling may become component- driven.

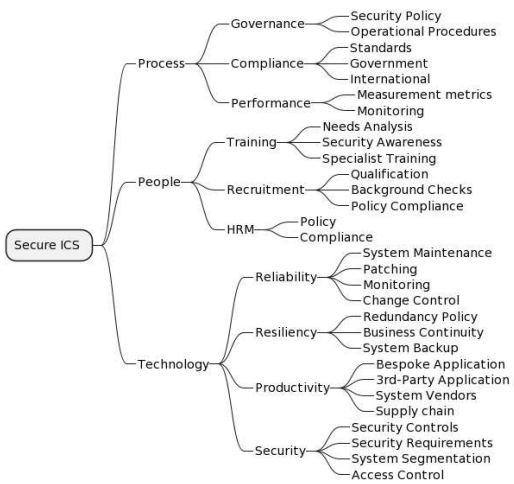


FIGURE 6. Minimum levels of model abstraction

E. USER DATA INPUT

Based on the ICS scenario, we designed a user input interface that accepts information from the users to build the ICS model for the user. The interface includes pre-populated information about the model to align with the dependency model in Figure 6. Users provide information for each node. If the value for dependants is zero, it is a leaf node and a second screen comes up to accept the probability value for the node as shown in Figure 8. If, however, the value for dependants is greater than zero, the node is not a leaf node and the probability screen will not be displayed.

VI. RESULT ANALYSIS AND DISCUSSION

In this analysis, we explain the derivation of the posterior values from users' initial input to the leaf nodes

TABLE 2. ICS Security Statements For Risk Identification

System	
1	The system has been in the desired state for a sufficient number of days within the last 90 days.
2	The current state of the system is the desirable state.
3	The organisation meets ICS regulatory compliance.
4	The organisation maintains budget allocation for ICS cybersecurity efforts.
5	There are security controls within the system.
6	The organisation subscribes to relevant ICS Cyber security risk management standards.
7	The organisation is prepared to forestall compromises of business function from potential adverse conditions.
8	The business is capable of providing essential business functions despite adverse conditions (withstand).
9	The business is capable of restoring essential business functions after adverse conditions (recover).
10	The business is capable of change business functions and/or supporting capabilities to minimise adverse impacts from actual or predicted adverse conditions.
11	Management maintain useful representations of mission dependencies and the status of resources with respect to possible adversity (Understand)
12	Management maintain a set of realistic courses of action that address predicted or anticipated adversity (Prepare)
13	There are resources to modify architectures to handle adversity more effectively (Re-architect)
14	Damage from adversity can be controlled/constrained (Constrain)
15	The system is equipped to maximise the duration and viability of essential business functions during adversity (Continue)
16	The system is capable to preclude the successful execution of an attack or the realisation of adverse conditions (Prevent/Avoid)
17	The system can restore as much business functionality as possible subsequent to adversity (Reconstitute)
Process	
18	The organisation has an (appropriate) established cyber security management system (CSMS).
19	The organisation sufficiently maintains and communicates Security program requirements (for assets) to IACS service providers.
20	Service providers adhere to Service Level Agreements (3rd Party).
21	Updates to System Processes are current, accurate and accessible.
22	There is a named custodian for the Enterprise Control System Integration documentation.
23	The organisation maintains a formal process of Asset inventories.
Technology	
24	The organisation has well-defined security requirements for system components.
25	There are controls to ensure reliability and availability of control systems.
26	There are external connections to the Industrial Control System (ICS).
27	The Enterprise Network is segmented from ICS Network.
28	User privileges are well assigned and enforced.
29	The organisation maintains a Patch management program for all required technology.
People	
30	The organisation provides suitable Security Awareness Training for all personnel.
31	The organisation provides suitable Specialist (Operational) Training for all personnel.
32	IT staff understand ICS operational requirements.
33	Management maintains capabilities to identify, measure and analyse human-initiated behaviours that introduce risk to the organisation.
34	Background checks for appropriate personnel are performed.
35	Personnel understand their roles and responsibilities.
	NOTE: User's response to each statement scaled: Strongly agree | Agree | Neutral | Disagree | Strongly disagree

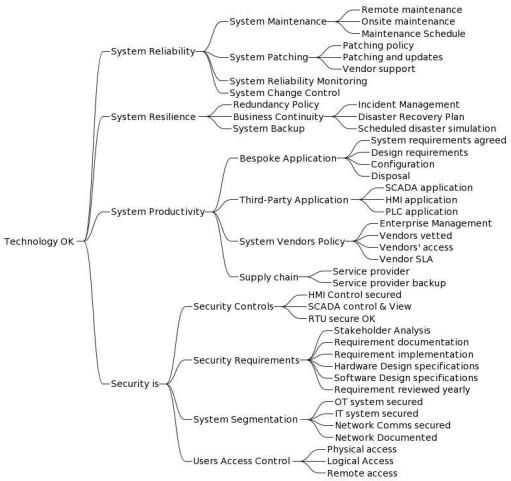


FIGURE 7. ICS Dependency Model: Technology

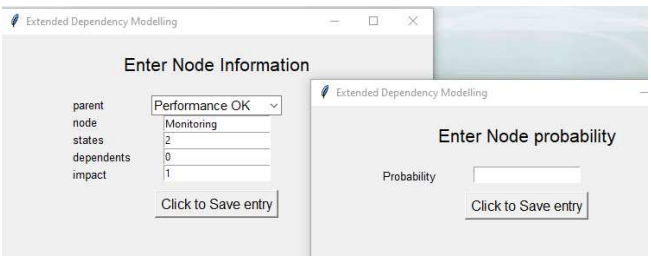


FIGURE 8. User Data Input Screen

(uncontrollable) and analyse the results. To derive the posterior probability from the users' data input, there are four steps as follows:

1) The user provides responses to a list of cybersecurity-related statements. These responses serve as a security indicator (we refer to it as the security posture of the enterprise) and are analysed to derive a security coefficient for each of the four categories: System, People, Technology, and Process. We compute the standard deviation of all the responses based on categories. We divided each response by five (the response scale is one to five [1-5]) to standardise them. We then summed by category for each of confidence and coverage. Sample Standard Deviation is then applied to the sums. An example of the computation for People and Process SP categories is shown in Figure 9. Here, the sum for confidence and coverage for People category are 4.2 and 5, respectively, and the standard deviation of the two values is 0.565. Standard deviation helps to determine how far apart the two responses of "confidence" and "coverage" are from each other. The farther apart, the higher the standard deviation value. If the standard deviation values are high, it indicates an inconsistency in the responses with a category. Table 3 is the result (SP

coefficient) of the responses by category.

2) The user is presented with a window (see Figure 8) to provide information to build the model and probability for the leaf node. This probability value is used as input to the Bayes computation.
3) The SP coefficient is applied to the leaf nodes (nodes without dependants) using the Bayes computation table [57] in Figure 2. In the Bayes table, the user's input is the prior probability, representing what the user already knows. The SP coefficient is the conditional probability, representing the evidence. From these two probabilities, we compute the joint probability and marginal probability and finally derive the posterior probability.
4) DM is applied to compute the results for all nodes across the tree and the root node as shown in Figure 10 and Figure 11.
A 3-point sensitivity for the model is computed for as shown in Figure 12 and Figure 13.

TABLE 3. Security Posture (SP) Coefficient

Category	Coefficient
People	0.566
Process	0.424
Technology	0.141
System	0.424

The result of our computation is shown in Table 4. The Probability User (third column in the table) showed the user's input, and the Probability Posterior (fourth column in the table) showed the computed values. Obtaining empirical data input is not necessarily a reduction in the value provided by the user, rather, it is a combination of factors, the chief of which is the SP responses. Specifically, in this table, the SP coefficient for the "People" category was 0.566 (the highest value among the categories). This value impacted the outcome of the posterior probability for all the nodes in the "People" category, i.e. The difference between the user input and the computed posterior is an increase. On the contrary, most of the posterior values in "Process" category are a decrease. As mentioned earlier, when the SP coefficient is high, it may be an indication that the responses are not consistent. This could be because Human Resources (HR) was not involved, or the risk analyst does not have enough knowledge to respond to the statements in this category accurately. For example, responses to a statement such as "Personnel understand their roles and responsibilities" can only be provided by the HR team based on the performance of individual personnel. On the other hand, the fact that the SP coefficient for the "People" category is the highest in this experiment may not necessarily indicate wrong responses as the difference to other SP coefficients is marginal (0.124), with the exception of the "Technology" category. This indicates consistency in the responses which may therefore represent the true security posture. This research work has avoided defining a "high" SP coefficient.

TABLE 4. Posterior Data Input Computation

Category	Node	Probability User	Probability Posterior
People	Alignment with business needs	0.990	0.992
People	Background Check Performed	0.990	0.992
People	Documented policy	0.990	0.992
People	Enforced Policy	0.990	0.992
People	Recruitment Policy Compliance	0.990	0.992
People	Regular audit	0.990	0.992
People	Regular update	0.990	0.992
People	Relevant to roles	0.990	0.992
People	Required capabilities	0.990	0.992
People	Requisite skills	0.990	0.992
People	Security Awareness Training OK	0.990	0.992
People	Specialist Training OK	0.990	0.992
People	Stakeholder analysis	0.990	0.992
People	Visible Policy	0.990	0.992
Process	3rd Party Security Guidelines	0.990	0.989
Process	Business obj is clear	0.990	0.989
Process	Business planning OK	0.990	0.989
Process	Compliance	0.990	0.989
Process	Customer request is analysed	0.990	0.989
Process	Documented compliance	0.990	0.989
Process	International Regulations Compliance	0.990	0.989
Process	Performance Measurement Metrics OK	0.990	0.989
Process	Performance Monitoring OK	0.990	0.989
Process	Physical Security Guidelines	0.990	0.989
Process	Political landscape OK	0.990	0.989
Process	Resource constraints noted	0.990	0.989
Process	Standards certification	0.990	0.989
Process	Standards compliance	0.990	0.989
Process	Standards documentation	0.990	0.989
Process	System Security Guidelines	0.990	0.989
Technology	Configuration OK	0.990	0.937
Technology	Design requirements OK	0.990	0.937
Technology	Disposal OK	0.990	0.937
Technology	Documented network OK	0.990	0.937
Technology	DR Plan OK	0.990	0.937
Technology	Enterprise mgt OK	0.990	0.937
Technology	Hardware Design spec OK	0.990	0.937
Technology	HMI App OK	0.990	0.937
Technology	HMI Control secured	0.990	0.937
Technology	Incident magt OK	0.990	0.937
Technology	IT system secured	0.990	0.937
Technology	Logical access to premises	0.990	0.937
Technology	Maintenance schedule	0.990	0.937
Technology	Network comms secured	0.990	0.937
Technology	Onsite maintenance access	0.990	0.937
Technology	OT system secured	0.990	0.937
Technology	Patching policy OK	0.990	0.937
Technology	Physical access to facilities	0.990	0.937
Technology	PLC App OK	0.990	0.937
Technology	Redundancy Policy OK	0.990	0.937
Technology	Remote access to systems	0.990	0.937
Technology	Remote maintenance access	0.990	0.937
Technology	Requirement documentation	0.990	0.937
Technology	Requirement implementation	0.990	0.937
Technology	RTU secure	0.990	0.937
Technology	SCADA App OK	0.990	0.937
Technology	SCADA control & View	0.990	0.937
Technology	Scheduled disaster simulation	0.990	0.937
Technology	Scheduled patching and update	0.990	0.937
Technology	Service provider backup	0.990	0.937
Technology	Service provider OK	0.990	0.937
Technology	Software Design spec OK	0.990	0.937
Technology	Stakeholder analysis	0.990	0.937
Technology	Sys Requirements agreed	0.990	0.937
Technology	System Backup OK	0.990	0.937
Technology	System Change Control Mgt OK	0.990	0.937
Technology	System Reliability Monitoring OK	0.990	0.937
Technology	Vendor Support OK	0.990	0.937
Technology	Vendors' access	0.990	0.937
Technology	Vendors SLA OK	0.990	0.937
Technology	Vendors vetted	0.990	0.937
Technology	Yearly Requirements review	0.990	0.937

	category	statements	confidence	coverage	std_conf	std_cove	sum_con	sum_cov	STD_DEV
34	People	Personnel understand their	4	4	0.8	0.8			
32	People	Management maintains ca	3	5	0.6	1			
31	People	IT staff understand OT ope	3	5	0.6	1			
30	People	The organisation provides :	4	4	0.8	0.8			
29	People	The organisation provides :	3	3	0.6	0.6			
33	People	Background checks for app	4	4	0.8	0.8	4.2	5	0.56569
22	Process	The organisation maintains	4	2	0.8	0.4			
21	Process	There is a named custodiar	3	2	0.6	0.4			
20	Process	Updates to System Process	5	3	1	0.6			
19	Process	Service providers adhere tc	4	4	0.8	0.8			
18	Process	The organisation sufficient	3	3	0.6	0.6			
17	Process	The organisation has an (ap	2	4	0.4	0.8	4.2	3.6	0.42426

FIGURE 9. **Example of Security Posture Coefficients**

Two dependency modelling outcomes are presented: (1) dependency analysis based on users' input data - Figure 10, and (2) dependency analysis based on posterior - Figure 11. The proportion of the two colours (red and green) is equivalent to a probability value. For example, the Secure ICS (goal/root node) in Figure 10 is 48.5% and the value for the equivalent node in Figure 11 is 4.9%. As previously discussed, the numbers are not the severity of impact but the degree of uncertainty that a system will be at a required (desired) state based on the input provided by the user. Both charts indicate that the success probability of the goal is low. Figure 11 shows a 4.9% probability that the system would be in a secured state based on the posterior data. This was because the factors/nodes (process, people, and technology) that directly support the goal (Secure ICS) are 83.8%, 89.4% and 6.5% respectively. Of particular concern to the risk analyst and the business owner would be the Technology OK node. This has raised a red flag that requires investigation. However, our analysis is focused on the comparison between the two outcomes. There is a significant difference in the probability of the root (goal) of the two results. The result of the modelling using nominal values (Figure 10(a)) indicates that the degree of certainty to achieve a desired "Secure ICS" is 48.5% when the DM is computed using the nominal data provided by the user. However, this degree falls to 4.9% when we apply posterior probability to the input data based on the user's response to the security statements. This is due in part to the impact of the responses and the depth of dependency level. Particularly, the difference in users' data input and derived posterior for the "Technology" category is significant (up to 8% reduction in some cases). Analysing the dependencies in Figure 10 and 11 reveal that the People node in 11 has a higher probability of success when compared to its equivalent in 10. However, the low probability of success on the Technology node reduced the overall probability due to the multiplication effect.

In addition to the above factors, the technology node showed the lowest degree of certainty (highest degree of uncertainty) among the child-nodes to the goal (root node). This is due to the number of dependants in the technology node. In Figure 10, the probability of the technology node (65%) means that the nominal probability (root node) is low due to the cascading nature of the model. Figure 7 provides a clue as to the low probability value; where the number of dependencies in a branch is many, the dependency value is low. Both charts indicate that the success probability of the goal is low.

Further analysis of the results is the impact of posterior probability on the input data. Here, we compare the sensitivity to uncontrollable (leaf nodes). The 3-point sensitivity graphs in Figures 12 and 13 represent the degree to which the chances of achieving goals are affected by the uncontrollable – where the bars indicate the degree of sensitivity of each leaf node to the goal. The red colour segment (to the left) indicates a decrease (how much worse) in success probability for the goal, while the green indicates an increase (how much better) in success probability could be as the probability of each node is increased. The intersection between the two colours represents the nominal success probability for the goal (i.e. Secure ICS). Using Figure 12 as an example, the nominal success probability for the goal is 48.5% (0.45), and the sensitivity of system reliability monitoring OK to the Secured ICS is 49% (0.49). The red colour segment shows the decrease in success probability for Secured ICS if system reliability monitoring OK fails (or has zero probability of success). The green colour segment shows the increase in success probability for Secured ICS if system reliability monitoring OK has 100% success probability.

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2023.3263671

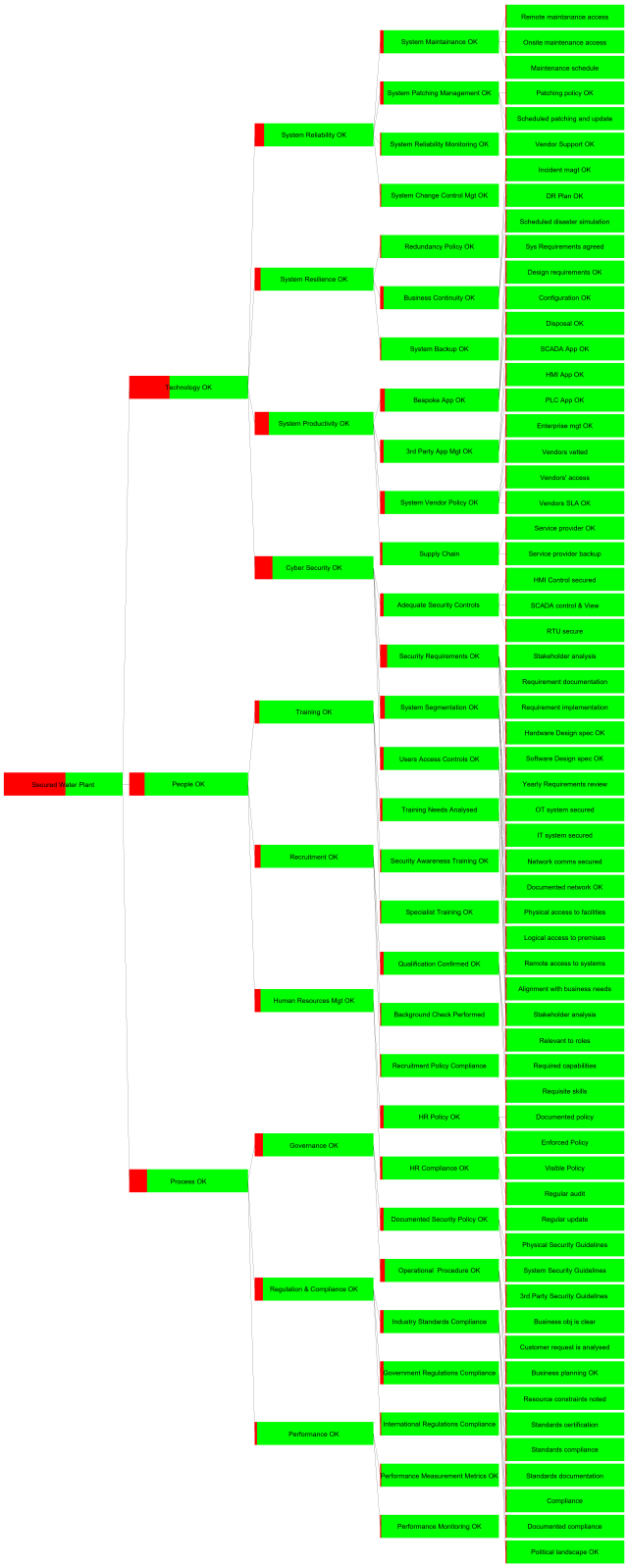


FIGURE 10. Dependency Model Graph - User Input

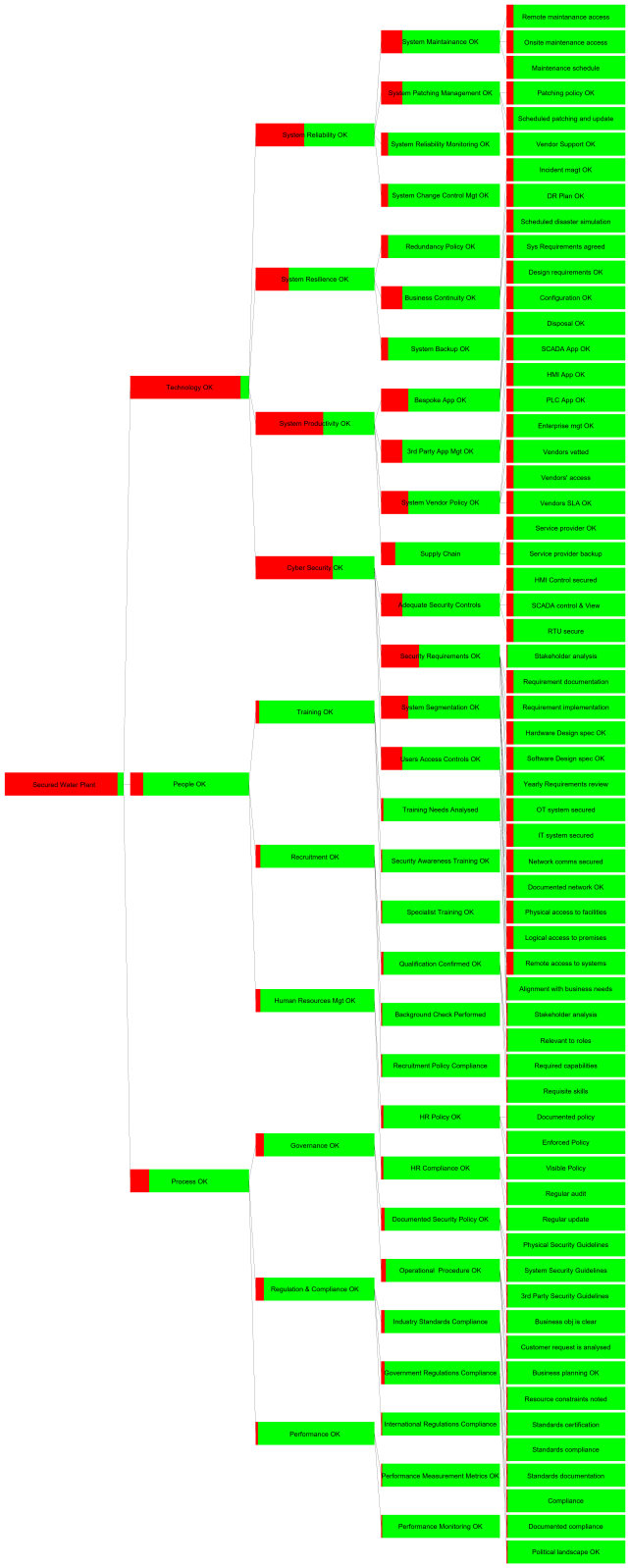


FIGURE 11. Dependency Model Graph - Adjusted

Comparing the outcomes from the two results revealed contrasting sensitivities of the uncontrollable. The nominal probability in Figure 12 is 48.5%, compared to 4.9% (0.049) in Figure 13. This means the probability of a successful Secured ICS is higher when we used the user data input than when we used derived (posterior) data input. Significantly different is the list of the top 10 nodes with the highest sensitivity values. The top-ten nodes list in both Figures (12 and 13) are different. The top-three on the list in Figure 12 are the bottom-three in 13. That is; the three most-sensitive nodes in Figure 12 are the three least-sensitive nodes in Figure 13 list in One node made the top 10 list of most sensitive nodes on both graphs. So, Redundancy policy OK appeared as the third most sensitive node in Figure 12 and the 10th most sensitive in Figure 13. It means the node (Redundancy policy OK) is more sensitive to success Secured ICS in Figure 12 than in Figure 13. That is, if its value of Redundancy policy OK changes negatively (tending to zero), it will have a greater impact on the success of (Secured ICS) in Figure 12 than in Figure 13. Conversely, if the value changes positively (tending towards one), the Redundancy policy OK in 13 has a higher sensitivity to the success of the goal. One other significant difference between the two graphs is the scale of measurement which makes the nodes in Figure 12 100% more sensitive to changes that those in Figure 13.

FIGURE 12. 3-point Sensitivity Analysis - User Input

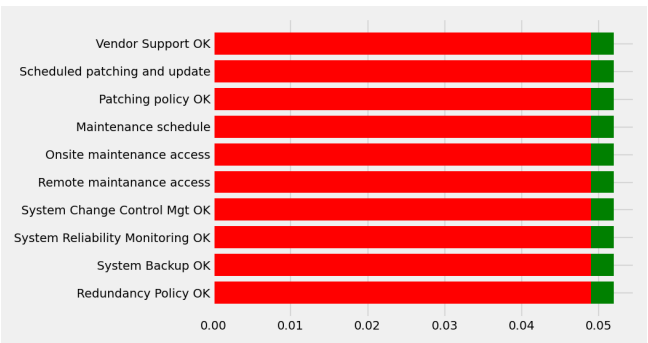


FIGURE 13. 3-point Sensitivity Analysis - Adjusted

It was also observed that the level of granularity (the depth) in DM impacts the nominal probability. Limiting the model to four levels resulted in a 0.75 and 0.32 nominal probability for DM and extended DM, respectively. This was a significant improvement on the five-level model analysed earlier.

VII. CONCLUSION

In this literature, we have explored the various capabilities of DM and proposed ways to extend these capabilities. In particular, we proposed a technique to support an improvement in the initial user data input. We developed an application that accepted user input and we analysed the results, comparing the existing DM offering to the proposed extension. The comparison showed that the proposed technique would improve the accuracy, confidence and reliability of the risk identification process using DM methodology.

DM offers a considerable advantage over other methods where the graph is capable to reveal areas of immediate intervention needs. As enumerated in Section IV-B, however, there are yet a few issues that require further work with the space. DM is incapable to provide an analysis of impact across the broader system and lacks formalism on how to measure the direct and indirect impact of a change of state on other parts of the tree. It also lacks the formalism to stochastically test the multiple and independent failures in a system – a common phenomenon in an ICS environment.

In the future, we seek to research exploring how to observe the stochastic values of one or more of the nodes using probabilistic reasoning principles and providing a significant extension to the power of the dynamic Bayesian network and graphical models and also to explore ways by which DM could be extended to analyse the combination of independent events within the dependency graph and the propagation impact across subsystem goals, as well as up to a root goal. We believe this would further increase the understanding of the behaviour, interactions, dependencies, and associated vulnerabilities inherent in the system.

ACKNOWLEDGEMENT

This work has been supported by the Knowledge Economy Skills Scholarships (KESS2) - a major pan-Wales operation supported by European Social Funds (ESF) through the Welsh Government, and Thales UK.

REFERENCES

[1] J. R. Reeder and C. T. Hall, 'Cybersecurity's Pearl Harbor Moment: Lessons Learned from the Colonial Pipeline Ransomware Attack', -, 2021.
[2] R. Mattioli and K. Moulinos, 'Analysis of ICS-SCADA cyber security maturity levels in critical sectors', European Union Agency for Network and Information Security (ENISA), 2015.
[3] A. Ginter, 'The Top 20 Cyberattacks on Industrial Control Systems. Waterfall Security Solutions'. 2017.

[4] U. J. Butt, M. Abbod, A. Lors, H. Jahankhani, A. Jamal, and A. Kumar, 'Ransomware Threat and its Impact on SCADA', in 2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3), 2019, pp. 205–212.

[5] T. Miller, A. Staves, S. Maesschalck, M. Sturdee, and B. Green, 'Looking back to look forward: Lessons learnt from cyber-attacks on Industrial Control Systems', International Journal of Critical Infrastructure Protection, vol. 35, p. 100464, 2021.

[6] L. Constantin, 'SolarWinds attack explained: And why it was so hard to detect', 2020. [Online]. Available: https://tinyurl.com/2yxpmmae.

[7] SecurityScorecard, 'The Role of Cybersecurity in Enterprise Risk Management (ERM)', 2021. [Online]. Available: https://tinyurl.com/54ettr6z.

[8] Ncsc, 'Risk Management Guidance', 2017. [Online]. Available: https://tinyurl.com/47mym4nz.

[9] J. Shen and D. Feng, 'Vulnerability analysis of CSP based on stochastic game theory', Journal of Control Science and Engineering, vol. 2016, 2016.

[10] S. Wang, L. Ding, H. Sui, and Z. Gu, 'Cybersecurity risk assessment method of ICS based on attack-defense tree model', Journal of Intelligent & Fuzzy Systems, pp. 1–14, 2021.

[11] D. Slater, 'Open group standard dependency modeling (O-DM)'. Nov-2016.

[12] Y. Cherdantseva, P. Burnap, S. Nadjm-Tehrani, and K. Jones, 'A configurable dependency model of a SCADA system for goal-oriented risk assessment', Applied Sciences, vol. 12, no. 10, p. 4880, 2022.

[13] Y. Cherdantseva, P. Burnap, S. Nadjm-Tehrani, and K. Jones, 'A configurable dependency model of a SCADA system for goal-oriented risk assessment', Appl. Sci. 2022, 12(10), 4880; https://doi.org/10.3390/app12104880.

[14] P. Burnap et al., 'Determining and sharing risk data in distributed interdependent systems', Computer, vol. 50, no. 4, pp. 72–79, 2017.

[15] T. Alpcan and N. Bambos, 'Modeling dependencies in security risk management', in 2009 Fourth International Conference on Risks and Security of Internet and Systems (CRiSIS 2009), 2009, pp. 113–116.

[16] U. D. Ani, N. C. Daniel, and S. E. Adewumi, 'Evaluating industrial control system (ICS) security vulnerability through functional dependency analysis', J Comp Sci Appl, vol. 25, no. 1, pp. 73–89, 2018.

[17] A. Akbarzadeh and S. K. Katsikas, 'Dependency-based security risk assessment for cyber-physical systems', Int. J. Inf. Secur. (2022). https://doi.org/10.1007/s10207-022-00608-4.

[18] J. Watters, S. Morrissey, D. Bodeau, and S. C. Powers, 'The risk-to-mission assessment process (RiskMAP): a sensitivity analysis and an extension to treat confidentiality issues', MITRE CORP MCLEAN VA, 2009.

[19] F. Innerhofer-Oberperfler and R. Breu, 'Using an Enterprise Architecture for IT Risk Management', in ISSA, 2006, pp. 1–12.

[20] T. Mitre, 'Crown Jewels analysis', The MITRE Corporation. MITRE, Sep-2017.

[21] E. Ruijters and M. Stoelinga, 'Fault tree analysis: A survey of the state-of-the-art in modeling, analysis and tools', Computer science review, vol. 15, pp. 29–62, 2015.

[22] P. Kordy and P. Schweitzer, 'The ADTool Manual', University of Luxembourg, 2012.

[23] H. Abdo, M. Kaouk, J.-M. Flaus, and F. Masse, 'A safety/security risk analysis approach of Industrial Control Systems: A cyber bowtie–combining new version of attack tree with bowtie analysis', Computers & security, vol. 72, pp. 175–195, 2018.

[24] T. I. S. of Automation, 'Quick Start Guide: An Overview of ISA/IEC 62443 Standards', 2020. [Online]. Available: https://tinyurl.com/2rhyds29.

[25] S. Kaplan and B. J. Garrick, 'On the quantitative definition of risk', Risk analysis, vol. 1, no. 1, pp. 11–27, 1981.

[26] D. W. Hubbard and R. Seiersen, How to measure anything in cybersecurity risk. John Wiley & Sons, 2016.

[27] L. Anthony (Tony) Cox Jr, 'What's wrong with risk matrices?', Risk Analysis: An International Journal, vol. 28, no. 2, pp. 497–512, 2008.

[28] J. D. Christopher and Dragos, 'Industrial Cyber Risk Management', Dragos. Dragos, May-2021.

[29] A. A. Bochman and S. Freeman, Countering Cyber Sabotage: Introducing Consequence-driven, Cyber-informed Engineering (CCE). CRC Press, 2021.

[30] U. J. Butt, M. Abbod, A. Lors, H. Jahankhani, A. Jamal, and A. Kumar, 'Ransomware Threat and its Impact on SCADA', in 2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3), 2019, pp. 205–212

[31] A. Morse, 'Investigation: WannaCry cyber attack and the NHS', Report by the National Audit Office. Accessed, vol. 1, 2018.

[32] M. Giles, 'Triton is the worlds most murderous malware, and its spreading', 2019. [Online]. Available: https://tinyurl.com/4xtsj7pj.

[33] D. U. Case, 'Analysis of the cyber attack on the Ukrainian power grid', Electricity Information Sharing and Analysis Center (E-ISAC), 2016.

[34] T. H. Morris and W. Gao, 'Industrial control system cyber attacks', in Proceedings of the 1st International Symposium on ICS & SCADA Cyber Security Research, 2013, pp. 22–29.

[35] W. Young and N. G. Leveson, 'An integrated approach to safety and security based on systems theory', Communications of the ACM, vol. 57, no. 2, pp. 31–35, 2014.

[36] The Open Group, 'Data security', The Open Group Website. The Open Group, Sep-2020.

[37] M. A. McQueen, W. F. Boyer, M. A. Flynn, and G. A. Beitel, 'Quantitative cyber risk reduction estimation methodology for a small SCADA control system', in Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06), 2006, vol. 9, pp. 226–226.

[38] J. Sherwood, A. Clark, and D. Lynas, 'Enterprise security architecture', SABSA, White paper, vol. 2009, 1995.

[39] The Mitre, 'Crown Jewels analysis', The MITRE Corporation. MITRE, Sep-2017

[40] G. Brændeland, A. Refsdal, and K. Stølen, 'Modular analysis and modelling of risk scenarios with dependencies', Journal of Systems and Software, vol. 83, no. 10, pp. 1995–2013, 2010.

[41] I. Hogganvik and K. Stølen, 'A graphical approach to risk identification, motivated by empirical investigations', in International Conference on Model Driven Engineering Languages and Systems, 2006, pp. 574–588.

[42] J. Guan, J. H. Graham, and J. L. Hieb, 'A digraph model for risk identification and management in SCADA systems', in Proceedings of 2011 IEEE International Conference on Intelligence and Security Informatics, 2011, pp. 150–155.

[43] F. Baiardi, C. Telmon, and D. Sgandurra, 'Hierarchical, model-based risk management of critical infrastructures', Reliability Engineering & System Safety, vol. 94, no. 9, pp. 1403–1415, 2009.

[44] C. G. Chittester and Y. Y. Haimes, 'Risks of terrorism to information technology and to critical interdependent infrastructures', Journal of Homeland Security and Emergency Management, vol. 1, no. 4, 2004.

[45] T. R. Ingoldsby, 'Attack tree-based threat risk analysis', Amenaza Technologies Limited, pp. 3–9, 2010.

[46] J. Carlson and D. Michaud-Soucy, 'Using Bow Tie Risk Modelling for Industrial Cybersecurity', 2021. [Online]. Available: https://tinyurl.com/rb9jardz.

[47] CGE, 'How to be prepared for cyber attacks', 2020. [Online]. Available: https://tinyurl.com/4xek45uz.

[48] W. Young and R. Porada, 'System-theoretic process analysis for security (STPA-SEC): Cyber security and STPA', in 2017 STAMP Conference, 2017.

[49] D. Slater, 'A dependency modelling manual - Working Paper', A Dependency Modelling Manual - ResearchGate. Aug-2016.

[50] Y. Cherdantseva et al., 'A Review of Cyber Security Risk Assessment Methods for SCADA Systems', Computers & security, vol. 56, pp. 1–27, 2016.
[51] A. Ankan and A. Panda, Mastering probabilistic graphical models using python. Packt Publishing Ltd, 2015.
[52] J. V. Stone, Bayes' rule: a tutorial introduction to Bayesian analysis. Sebtel Press, 2013.
[53] S. O. Hansson and T. Aven, 'Is Risk Analysis Scientific?', Risk Analysis, vol. 34, no. 7, pp. 1173–1183, 2014.
[54] Dragos, '2020 ICS Cybersecurity Year in Review', 2021. [Online]. Available: https://tinyurl.com/3sawx893.
[55] D. Bodeau, R. Graubart, W. Heinbockel, and E. Laderman, 'Cyber resiliency engineering aid-the updated cyber resiliency engineering framework and guidance on applying cyber resiliency techniques', MITRE CORP BEDFORD MA BEDFORD United States, 2015.
[56] B. Filkins, D. Wylie, and A. J. Dely, 'SANS 2019 State of OT/ICS Cybersecurity Survey', SANS Technology Institute, 2019.
[57] Harper, 'Dr. Harper's Classroom: Statistical Bayesian Analysis With Excel', 2016. [Online]. Available: https://tinyurl.com/357jvyms.

AYODEJI O. ROTIBI received the B.SC. degree in computer science from University of Benin, Nigeria in 1990 and the M.Sc. degree in computer system security from University of Glamorgan, Pontypridd, United Kingdom in 2006. He also received the M.Sc. degree in information security and privacy from Cardiff University, Cardiff, United Kingdom in 2018. He is currently pursuing the Ph.D. degree in cyber security Cardiff University, Cardiff, UK.

His research interest includes cyber risk assessment and analysis in complex environments and the development of tools to simplify cyber risk identification.

NEETESH SAXENA is currently an Associate Professor in Cyber Security with the School of Computer Science and Informatics at Cardiff University, United Kingdom with 16+ years of teaching/research experience. Before joining Cardiff University, he was an Assistant Professor at Bournemouth University, United Kingdom. Prior to this, he was a Post-Doctoral Researcher in the School of Electrical and Computer Engineering at the Georgia Institute of Technology, USA, and with the Department of Computer Science, Stony Brook University, USA and SUNY Korea. He was a DAAD Scholar at Bonn-Aachen International Center for Information Technology (B-IT), Rheinische-Friedrich-Wilhelms Universität, Bonn, Germany and a TCS Research Scholar. His current research interests include cyber security and critical infrastructure security, including cyber-physical system security: smart grid, V2G and cellular communication networks

PETE BURNAP is a professor of data science and cybersecurity at Cardiff University, United Kingdom. He is director of Cardiff's NCSC/EPSRC Academic Centre of Excellence in Cyber Security Research. He also leads artificial intelligence for cybersecurity research at Airbus DTO. His research interests include socio-technical security and the understanding of risks to society from cyber-enabled systems.

ALEX TARTER has worked in the fields of defence and critical national infrastructure cyber security for over 15 years. He is currently Chief Cyber Consultant and CTO at Thales UK. He also supports NATO as a civil expert on cyber security for the Civil Emergency Planning Committee, and has contributed to the development of international cyber security standards. We caught up with him ahead of his appearance on an Alumni Insights panel event, to find out more about his work.