Journal of Cyber Security Technology, 2018, Volume 2, Issue 3-4, pp. 201-237
DOI:10.1080/23742917.2018.1554986

A Framework for Operational Security Metrics Development for Industrial Control Environment.

Uchenna P Daniel Ani[1], Hongmei (Mary) He[2] and Ashutosh Tiwari[3]

[1,2]Manufacturing Informatics Centre, School of Aerospace, Transport, and Manufacturing, Cranfield University, Bedford, United Kingdom.

[3]Airbus / RAEng Research Chair in Digitisation for Manufacturing, Department of Automatic Control and Systems Engineering Amy Johnson Building, The University of Sheffield.

u.p.ani@cranfield.ac.uk[1] , h.he@cranfield.ac.uk[2] , a.tiwari@sheffield.ac.uk[3]

Abstract

Security metrics are very crucial towards providing insights when measuring security states and susceptibilities in industrial operational environments. Obtaining practical security metrics depend on effective security metrics development approaches. To be effective, a security metrics development framework should be scopedefinitive, objective-oriented, reliable, simple, adaptable, and repeatable (SORSAR). A framework for Operational Security Metrics Development (OSMD) for industry control environments is presented, which combines concepts and characteristics from existing approaches. It also adds the new characteristic of adaptability. The OSMD framework is broken down into three phases of: target definition, objective definition, and metrics synthesis. A case study scenario is used to demonstrate an instance of how to implement and apply the proposed framework to demonstrate its usability and workability. Expert elicitation has also be used to consolidate the validity of the proposed framework. Both validation approaches have helped to show that the proposed framework can help create effective and efficient ICS-centric security metrics taxonomy that can be used to evaluate capabilities or vulnerabilities. The understanding from this can help enhance security assurance within industrial operational environments.

Keyword:

OSMD Framework, Security Metrics, Operational Security Metrics, Industry Control Environments, Security Measurement

1. INTRODUCTION

The increasing occurrence of targeted cyber-attacks and successful incidences on Industrial Control Systems (ICSs) have stirred industrial control system engineers and owners to make effort on securing their critical industrial infrastructure platforms and setups. Deploying security solutions alone does not guarantee utter security and safety from malicious intruders, it has become very crucial to understand the degree of contextual security inherent in a system, and to grasp the state and capability enabled within the ICS domain. Security objectives in an industry control environment can be prominently achieved through Regularly checking the performance of systems and the environment, guided by security metrics derived from the security objectives. Quantitative security metrics are always preferred by system developers and owners, as quantitative metrics could provide a good way to compare the levels of security assurance, hence easily aid the resolution of trade-offs in security solutions [1].

Increasing complexities are introduced as a result of the convergence of divergent initially separated technologies and protocols into modern ICS, and the pressure from security and privacy legislations are swelling the need for sufficient validations of security features and solutions [2]. Evidence to support such security validations (assurances) could easily be obtained through the application of systematic approaches for measuring security. There are few ICS-specific security metrics development approaches that are holistic enough to meet the multifaceted nature of security in the Industrial environment. There is the absence of clarity in the outline of quantitative, effective security metrics in relations to current security standards and guidelines. There is also the lack of suitable and all-encompassing methods to guide ICS organisations to clearly outline security objectives, metrics, and measurements for mitigating current cyber malicious actions [3], [4].

It is difficult to setup apt and effective security metrics, as attackers' efforts are non-linear, even where enterprises and organisations are required to put in exponential efforts on security [5]. Also, security metrics developers should think themselves as pioneers, and be prepared to fine-tune their approaches as circumstances and experiences dictate [6]. Another notable issue is the lack of domain-specific methods for security metrics generation to guide the organisation in line with acceptable security frameworks requirements, like NIST SP 800-82 [6], NIST Framework for Improving Critical Infrastructure Cybersecurity [7], and Security of Industrial Control System Good Practice Guide [8]. Most current work focuses on Information Technology security metrics developments as in ISO/IEC 27001 guidelines [3], [4], [9], [10]. Although useful, the ISO guide does not specifically address the peculiar nature and characteristics of security in ICS domains. It is hypothesized that practical and relevant security metric quantities can be better achieved from holistic security metric development approaches that are contextual in scope and security objectives, reliable, adaptable, repeatable, and adaptive to dynamic changes in the security landscape. The methodology used in this

research is analytical, especially in the framework development phase and the resulting metric quantities. A real environment use case scenario is used for the practical validation of the proposed framework and example metrics, and further supported by expert opinion evaluations. The novelty and contributions made by this study include:

i. The study puts forwards and elaborates some essential characteristics of a good metrics development framework, which include being: scope-definitive, objective-oriented, reliable, simple, adaptable, and repeatable (SORSAR). These characteristics as expressed and prescribed in this work do not appear in their entirety in any any prior metrics development framework. Thus, these characteristics provide new and valuable insights into the significant and comparative attributes of ICS security metric development frameworks, existing deficiencies of existing frameworks, and requirements that should be considered in the development or adoption of any security metrics frameworks for metrics generations. The study also offers route guides for future metric development advances.
ii. The study also presents a new ICS-centric framework of Operational Security Metrics Development (OSMD) instance that typifies the good development framework characteristics prescribed in contribution (i). The framework incorporates several essential framework components and features such as security environment dimensions, security objectives, and control capability variations, which collectively offer a holistic guidance to the development of security metrics for the industrial control system environment

The rest of this paper is organised into the following sections. Section 2 reviews related work. Section 3 describes the OSMD framework. Section 4 provides the validation of the proposed OSMD framework, and section 5 gives conclusions and future work.

2. RELATED WORKS

Security metrics are designed to arrive at measure that facilitate decision-making, and improve performance and accountability through evaluations (collection, analysis, and reporting) of relevant system status [11]. They are also supportive for predicting system security states [12], [13]. Security metrics represent measurable properties of a system that quantify the degree to which system security objectives or goals are achieved [14]. It is a popular thought that except a thing can be measured, the knowledge of it remains essentially insufficient. Security metrics is useful in the management of cyber risks and the evaluation of security states or susceptibilities in an enterprise, in respects of processes, people, and technologies. Security metrics are crucial for performing security test of systems, determining security assurance levels of system constituents, and undertaking adaptive security monitoring and management [13], [15]. From an economic perspective, security metrics can be used to illustrate the business impacts of security, thus enabling the integration of security functions into the overall business process [16].

However, the development of an effective security metrics need to be guided by an effective, carefully planned and designed effective approach, which should be feasible, flexible, and adaptive to a wide range of ICS audience, including technical and non-technical audience. An effective security metrics should not only be SMART (i.e. *specific, measurable, attainable, repeatable*, and *time-specific*) [16], [17], but also be *actionable* [18], *cost-efficient* [3], [19], *objective* [20], *operational* [21], *relevant, reproducible*, and provide *a basis for comparison and claim* [22]. Moreover, the effectiveness of a security metric lies in its ability to specify the degree to which security objectives are being met, and to drive actions towards improving the security state of an organisation or system. This work emphasises the need for the clear articulation of the characteristics of a metric development approach. Characteristics that could guide the development of metrics formulation approaches, give basis, relevance, and acceptability to designed approaches, and their usefulness towards enhancing security assurance.

Generally, security metrics could be developed through adoption and adherence to customised, pre(existing) organisational/operational frameworks, or through the adoption of compliance-based approaches hinged on standards and best practices. In either case, directional process-adoption methods like *top-down* or *bottom-up* are considered when determining desirable assessment metrics [23]. The *top-down* approach starts with the goals and questions of the operators as a focus for outlining the metrics. Thus, the security objectives are first articulated, processes worked down to identify specific security metric quantities that meet the objectives, and the measurements needed to generate the security metrics. For instance, the Balanced Scorecard (BSC), is a top-down approach that has gained wide support and acceptability for measuring and reporting details on enterprise Information [24]–[26]. The Goal-Question-Metric (GQM) is yet another widely advocated method for prioritizing metrics, though from a software engineering perspective. It has got the potentials to be extended over a broader spectrum to cover organizational viewpoint [27]. This method has further seen improvements into what is called the GQM+ Strategies [28] addressing the limitations of the initial GQM in relations to higher-level objectives metric connections, and applicability to generic organizational structures. The bottom-up approach adopts a reverse process, categorising existing, easy-to-obtain data as a starting point for outlining the metric quantities, and working up to the security objectives of a target system accordingly [23], [29]. An example of this is the security posture evaluation approach in [23] where measurements that could be collected are first derived, followed by the determination of metrics that could be generated from the measurements, and finally determine the association between the derived metrics and established overall security objectives.

The I3P security metrics development report [24] [25] discusses seven broad stages for metrics development, which include: (i) identification of target audience, (ii) identification of metrics objectives for each target audience, (iii) measuring attribute components, (iv) comparing with benchmarks, (v) visualising results, (vi) interpreting security

result levels, and (vii) making decision. Although a useful guide, the outlined stages of this step-wise approach more practically describe a metric-based security analysis process rather than a metrics development process. Thus, the development perspective of the approach seems superficial yet compelling; such that adopting the process coerces one into engaging into security analysis, even if it is not intended in the development objective. It forcefully binds security analysis with metrics development, when these are ideally distinct processes with distinct objectives. It is important to distinguish security metrics development approach from metrics-driven security analysis/evaluation approach. The I3P security is devoid of clarity in clearly specifying the points in the process where security metrics are generated, and decision strategy for generating security metrics. Such phenomenon introduces subjectivity as weaknesses in the development process.

The work by [23] tried to resolve some of the gaps in [24] by putting forward a seven-step usable guide to the process of establishing a security metric program. These include; (i) Defining security metrics program goals and objectives, (ii) Deciding which security metrics to be generated, (iii) Developing strategies for generating the security metrics, (iv) Establishing security metrics benchmarks and targets, (v) Determining how the security metrics will be reported, (vi) creating an action plan and acting on it, (vii) Establishing a formal program review/refinement cycle [23]. It improves upon previous method by clarifying the point where metrics are generated (i.e., step 4). It also includes the part for formulating and implementing action plans, and the establishment of a refinement programme that takes cognisance of recurrent changes and updates. Although seemingly an improvement, the model does not capture some relevant security requirement trends such as the enumeration or primary, secondary security objectives. It rather proffers steps that cover high-level system specification. Also, left out is the feature for enumerating target system scope in the event that an ICS to be assessed could be a subsystem (sub-network) being part or connected to a larger enterprise system (network) to reduce complexity. It would be better to have a model that enables target system scoping, and the potentials for predictive capabilities.

In [15] the enhanced version of an earlier security metrics development approach [26] was presented. This revised model provides an iterative process for metric generation aimed at achieving balanced and comprehensive security metrics taxonomy for any given system. The model consists of seven (7) steps: (i) threat and vulnerability analysis (optional), (ii) application of suitable metrics taxonomies and/or ontologies, (iii) definition and prioritisation of security requirements attack modelling, (iv) decomposition, modelling, and integration, (v) definition of measurement architecture, (vi) integration of security metrics and selected Basic Measurable Components (BMC), and (vii) the balanced and detailed collection of security metrics. Although the steps are structured into an iterative form, introduced feasibility analysis as a separate stage linking to measurement architectures, individual metrics, and metrics taxonomy. It used a distributed message system GENOM for a case study, and demonstrated the smooth integration of a risk-based assessment of BMCs, a security-based trust model, and a trust-based security model into a single framework for evaluating the trustworthiness of the development of measurable security metrics.

In [28], a security metrics development framework based on operational system attributes is presented, and it is applicable to the ICS environment. The model combines the concepts of security and dependability, studying operational system's interaction with its environment via the system boundaries concepts [27]. The model regroups conventional security and dependability attributes into 3 attributes: *protective, behavioural,* and *correctness*. The relevant processes in the respective attributes are engaged, the outputs of one attribute process becoming the inputs of the next attribute process. The object system and possible environmental influences like threats, vulnerabilities, attacks, and/or system failures, are defined. The processes are used to achieve the enumerated attributes. The model provides capabilities for generating at least two possible types of security metrics: *protective*, which relates to the system input, and *behavioural*, which relates to the system output. The authors have not presented any opinion or approach through which correctness could be qualified, or presented any related metrics. However, they have explained *correctness* to mean a possible template state considered desirable of the system, and against which measures of actual deviation can be deduced. This template state can be viewed as an ideal state suggested in [20], and describing the state of metric quantities that is representative of the best and desirable security state of the system or entity being evaluated. This ideal-driven concept essentially blocks the gaps of the operational system model as described in [28].

An Adversary View Security Evaluation (*ADVISE*) model-based security metrics approach is presented in [1]. The approach tried to create an executable model that combines system information, adversary information, and desired security metrics to produce quantitative metrics data. *ADVISE* captures a certain adversary's attack preferences, attack goals, and attack skills, and uses them in conjunction with a sequence of attack steps (from an attack execution graph) to mimic the likely attack behaviour of the adversary. The model is able to stochastically determine the outcome of each attack step attempted, in terms of the cost of the attacks and the probabilities of detection. The resulting metrics generated by *ADVISE* indicate the measurements recorded from discrete-event simulation, and are used to assess the probability of compromise within a specific time period. The metrics also give insight to the speed of compromise, and possible attack steps. A state look-ahead tree (SLAT) is used to recursively compute how future attack decisions could influence the attractiveness values of the current attack step options. The feasibility of *ADVISE* has been demonstrated with a case study on a SCADA system. ADVISE provides an approach to compare security strength or capability of system architecture variants, and analyse disparate adversarial threats.

A technical-centric security metrics development model for SCADA (TSMM SCADA) systems is presented in [30], guiding the generation of metrics used to measure the effectiveness of network security management controls and services such as firewalls, and Intrusion detection prevention systems (IDPS) in the protection of SCADA systems. The model adopts a four-step process of: *Plan, Do, Check*, and *Act* (PDCA), and the resultant metrics are basically targeted at meeting compliance requirements of ISO/IEC 27001 Information security management system (ISMA) standards. In the *Plan* phase, controls are selected, and both functional and non-functional constructs of the system are defined. The *Do* phase involves the analysis of risk-based threats, vulnerabilities and controls, and the resolution of priorities based on the most critical controls with high impacts. In the *Check* phase, ethnographic research methods are employed to measure expert perceptions of the security state in compliance with prescribed standard. The *Act* phase involves the evaluation of developed technical security measures and metrics in compliance with the prescribed standard.

Another metrics development approach in [25] proffers a framework that explores data mining techniques for creating predictive model encompassing historical data and security metrics. This is broken down into process stages as follows: filtering of historical data, future event predictions, security assessments, identification of system security state, and reporting/triggering of alarm to management. A key aspect of modern adaptive security concept, '*prediction'* is involved automatically. However, the step-wise procedures from one stage to another is unclear due to process automation. Hence, the difficulty in clearly establishing the security objectives targeted, and the system scope.

A resilience-centric approach to security metrics development for cyber infrastructure was presented in [31]. A matrix framework [32] was used to develop and organise effective resilience metrics for improving cyber security in cyber systems. The metrics formulation approach is such that policy goals are linked to certain system measures, translating resource allocation decisions into actionable interventions and investments. The developed matrix of resilience metrics combines the four stages of system event management cycle for resilience by the National Academy of Science (NAS) (*Plan/Prepare, Absorb, Recover, Adapt*), and the Network-Centric Warfare doctrine's situational awareness and decentralised decision-making domains (*Physical, Information, Cognitive, and Social*) [32]. In the system event management cycle, '*Plan/Prepare*' sets the base for keeping services available and assets functioning during any disruptive event that emerges from attacks or malfunctions; '*Absorb*' involves sustaining critical services and assets functioning while isolating or repelling disruptions; '*Recover*' emphasises the ability to restore all service and asset functionalities to their prior disruptive event status, and '*Adapt*' emphasises the application of event knowledge, system configuration, personnel training, etc., to achieve better resilience. These strategies collectively integrate actual data, technical judgement, literature-based measures to access system resilience across physical, information, cognitive, and social domains of a cyber system [31]. This approach enables actions in specific areas or domains to enhance the system's capacity to plan/prepare, absorb and recover from incidents, as well as adapt to various attacks. The merit of this approach lies in its applicability. It provides a multi-criteria decision-making aid and a scorecard for qualitative resilience information capture, and hence helps identify security gaps in systems [21].

An ASPIRE (*Aim, Select, Prepare, Introduce, Report, Establish*) metric development approach was presented in [16]. Although IT-centric, the addressed metrics are slightly related to the industrial environment. The model includes the following steps: define the aim and objectives of a metric program, select the metrics to be generated in line with business goals, prepare strategies for generating the metrics, introduce measurable performance targets, report the plan for metrics, establish the implementation plan, review and refine the plan as necessary. These steps provide organisations a *defense-in-depth* approach to managing and mitigating operational risks through the deployment of business information security program. A key advantage of ASPIRE is that it can be utilised in security programme formulation yet without upsetting existing system setups or processes.

The review of existing metrics development approaches/programs reveal some benefits and gaps as outlined in Table 1. It also unveils the need for an improved method that would be clear; proffering an inclusive, concise step-wise methods for developing cyber security metrics that would be aligned to prevailing trends and features. An improved model could be achieved through the aggregation of strengths in existing development models, and building upon existing vulnerabilities accordingly. Reviewed metrics development models are not robust enough to meet or adapt to the dynamic nature of security in the ICS domain. The best approach towards achieving or obtaining effective security metrics starts with getting the development approach right. The quality of being right would be determined by the ability to not leave out or leave ambiguous necessary features that would lead to the continual relevance of an adopted approach. A methodology that allows for the clear definition and scoping of the target system and objectives, allow for measurements and comparisons, refinements and predictions to guard against potential future harms, such a methodology would need to be adaptive, flexible, and holistic.

Table 1: Summarised benefits and gaps in security metrics development approaches

No/Label	Methodology	Strength	Gap
MT1	I3P security metrics development [24] [25]	i.) Combines security analysis with security metrics development.	i.) Lack of clarity in clearly specifying the points in the process where security metrics are generated, and decision strategy for generating security metrics.

No/Label	Methodology	Strength	Gap
MT2	Guide to establishing a security metric program [23]	i.) Improvement in MT1 : by clarifying the point where metrics are generated (i.e., step 4). ii.) Includes a section for formulating and implementing action plans. iii.) Also includes establishment of refinement programmes accounting for recurrent changes and updates.	i.) Lacks inclusion of some relevant security requirement trends like enumeration of secondary objectives in line with adaptive security paradigms, and target system scoping.
MT3	Enhanced security metrics development using threat and vulnerability analysis approach [26]	i.) Requirement-Centric Approach	i.) Non-generic application potential
MT4	In [28], a security metrics development framework based on operational system attributes	i.) Multi-dimensional attribute approach for security metrication	i.) Lack practical approach for the evaluation of correctness (ideal state) or any related metrics
MT5	Adversary View Security Evaluation (*ADVISE*) model-based security metrics approach [1]	i.) Uses the aggregation of multiple data sources to stochastically determine the outcome of an attempted attack step. ii.) Outcomes evaluated in terms of attack costs and probabilities of detection	i.) Uses Attack/Adversarial analysis approach, and ignores defensive analysis.
MT6	Metrics development framework via data mining technique [25]	i.) Speedy application due to Automated Approach	i.) Unclear step-wise transition from one stage to another. ii.) Indistinct establishment of security objectives.
MT7	A technical-centric security metrics development model for SCADA (TSMM SCADA) systems is presented in [30]	i.) Driven by security standards and requirements (ISO/IEC 27001 and 27002)	i.) Control requirement driven, No explicit security requirement definitions. ii.) Scoped to technical security controls alone, does not account for process and people control measures.
MT8	Resilience-centric approach to security metrics development for cyber infrastructure [31]	i.) Enables multi-criteria decision-making aid and a scorecard for qualitative resilience information capture, and security gaps analysis in systems ii.) Combines risk and resilience management processes iii.) Enables transparent connectivity of domains across an event management cycle. iv.) metrics developed are generalizable across many systems and can be used for comparative evaluation of system resilience	i.) Resulting metrics from the resilience matrix ii.) Framework cannot be measured directly, but via system-by-system specification basis.
MT9	ASPIRE metric development approach[16].	i.) A *defense-in-depth* approach to managing and mitigating operational risks ii.) Applicable in security programme formulation yet without upsetting existing system setups or processes.	i.) Lacks key metrics development aspect of scope definition with respect to security dimensions, segments, and constituents.

3. The Proposed OSMD Framework

A framework for Operational Security Metrics Development (OSMD) is presented with focus on the industrial environment (Figure 1). This OSMD framework tends to unify existing security metrics development approaches and methodologies with the improvement of adaptability. To eliminate the gaps in existing models, the OSMD framework combines the features of existing security metrics development frameworks, and best practice standards and guidelines, such as NIST SP 800-53 [33], NIST SP 800-82 [6], ISO/IEC 27001 [9], and NIST Framework for Improving Critical Infrastructure Cybersecurity v.1.0. [7]. It adopts the advantages from: top-down and bottom-up concepts in [23], [29], ideal-driven model [20], adaptive capability concept [25], [31], [34], hierarchical interdependency model [35], review and refinement concept [23], control and compliance-driven models in TSMM [30], and defense-in-depth strategy [16]. The OSMD framework aims to overcome the weakness of a lack of clarity and methodical guidance for producing security metrics in response to clearly defined security objectives by organisations.

A security metric development approach should be clearly contextual, easily adoptable, iterative, and adaptive, in response to the dynamic nature of ICS environment in terms of security targets and objectives. The process of security metrics development includes three phases: *(i) Target definition, (ii) Objective definition, and (iii) Metrics Synthesis* (See Figure 1). These offer a holistic and integrated approach for the development of security metrics for varied scopes, dimensions, and attributes. Typically, it is believed that good security metrics are products of a good development approach, and in the dynamic field of ICS security, a good metrics development approach should have some essential characteristics such as: scope-definitive, objective-oriented, reliable, simple, adaptable, and repeatable (SORSAR). *Scope-definitive* property of a security metrics development framework should make for the specification of scopes and constraints in relation to the dimension of security (offensive or defensive) for which metrics are required, target network segment (enterprise or industrial control), and the precise system constituents (people, processes, technologies) to be measured. *Objective-oriented* characteristic provisions for the precise articulation of security objectives targeted by the metrics. These could include both the primary (safety, availability, integrity, confidentiality, and accountability) and secondary (decomposed) security objectives, and the articulation of the violation principles being considered. *Reliable* outlines the requirement of a development framework to yield desired and consistent metrics in line with consistent objectives and scope. *Simple* emphasises the characteristic of framework to be easy to understand and straightforward to employ or use. *Adaptable* defines the requirement of a development framework to be easily bent or tractable. A good framework should be adaptable to different security scenarios, objectives, and tweaked to suite varied and dynamic dimensional changes. *Repeatable* emphasises the need for a development framework to provision for the repetitions of process and procedures where necessary; in response to the need for modifications and improvements in metric quantities of the outcomes of measurements. The concept of iterations is a necessary to meet the dynamisms that might emerge. While developing a security metrics frameworks, it is pertinent for experts and developers to consider these properties, as they contribute to achieving a holistic and robust framework structure that can meet the ever-dynamic changes in the current security landscape. A metrics development framework with the SORSAR properties is more likely to avoid weak metrics that slack in meeting objective capabilities drawn by system owners. The uniqueness and strength of the OSMD framework is that it assembles all the SORSAR framework characteristics into its structure by logically harnessing varied strengths of existing approaches, and producing an improved approach for security metrics development with relativity to the ICS environment.

3.1 Target Definition

This involves delineating the attributes that give clearer information about the target system or environment for which security metrics are being generated. It includes defining the measurement scope, the target segment and the specific constituent(s) from which metrics will be derived.

A) Security Dimension (L1 Scoping)

This outlines the possible viewpoints through which security can be rationalised. Traditionally, security can be construed in two lookouts: *Capability* and *Vulnerability*. The security state of a system can be measure based on how strong or weak the system can be circumvented. It is, therefore, important to articulate the dimension of security especially at the beginning of every metrics development process. This concept presents a high-level (L1) scope definition that marks the beginning of carving out a clear direction for the security metrics development process.

i. Capability

Security capability characterises the might to uphold a protected state, and is measured by how difficult it is (or will be) to circumvent inherent protected capacities [36]. Metrics for evaluating security capability or strength try to measure the time, effort, and other resources necessary to breach a system's protections, and can be observed when taking the perspective of an attacker or adversary. For instance, the use of attack graphs and trees, and other security analysis paradigms [37]–[40] to arrive at metric attributes for evaluating system protective states. Attack graphs and tress typically characterise probable attacker actions in the light of a system scope or configuration. Understanding a system's security capability can support the decision to improve processes to make systems even stronger, and help the differentiation of more secure systems from the less secure ones [36].

ii. Vulnerability

This is the flip side of security capability, and emphasises the inability to achieve or sustain a certain protected state. Technically, it is referred to as '*vulnerability*', and it outlines the ease of rupturing a system's security state observed from a defensive point of view. For instance, defense trees [41], [42], the CVSS paradigm [43]–[45], the change-point detection evaluation approach [46], etc., have been used to derive metric values used to represent system susceptibilities to potential threats and attacks. Similarly, the knowledge of these vulnerabilities can help the easy identification and appropriation of security controls and efforts.

B) Network Segmentation (L2 Scoping)

This involves defining the section of an overall sy stem architecture for which security perspectives are desired, and metrics required. Typically, modern ICS architectures encompass a wide area network (WAN) integrating industrial operational technology (OT) networks with enterprise information technology (IT) networks [6]. The two networks are different in technologies and control protocols, and most times require different approaches,

metric quantities, and policy priorities for evaluating security features and states. These variations often account for application incompatibilities, hence the need to clearly specify the ICS network segment of focus for metrics development. Other segment delineation approaches could be based on asset/system functionality, configurations, or security requirement [47]. This is considered a mid-level (L2) scope definition that informs of the specific section of a larger ICS network to which security evaluation is focused.

C) System Constituent (L3 Scoping)

With an understanding of the target segment of a metrics development process, it is also necessary to identify the constituent of the segment being focused upon. Because a network segment would basically be made up of several constituents or entities. Both enterprise and industrial segments of an ICS are essentially information operations and management systems (IOMS), and are made up three inter-operating value provisioning structural constituents: *people, process, and technology* [48]–[50]. Every emergent metric quantity would measure characteristics of one or more of these three constituents, and express corresponding capabilities. Since security objectives may vary at different times for different system or organisations, it becomes necessary at every metric development stage to delimit the constituent focus of interest. This will help simplify the task of generating and analysing metric quantities, and generally speedup the development process. With this, it becomes possible to isolate the security states of one constituent from another for decision-making. This is quite helpful in situations where measures and insights into security status of specific/singular constituents are needed rather than the combined states of the three. This is considered a low-level (L3) definition of scope.

3.2 Objective Definition

Metric quantities should typically provide information that guides towards the attainment of pre-defined or pre-conceived security goal and objectives. Such goal-oriented security metrics requires defining security objectives first.

A) Primary and Secondary Objectives

In the ICS domain, *safety* is as important as *security* and should be considered a necessary critical objective, since it seeks to preserve from death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment [6]. On the other hand, security emphasises the protection of technologies, processes, and data from malicious compromise in the contexts of availability, integrity, and confidentiality [51], [52], which in this study are considered as *primary objectives*. The scope of this work does not extend in-depth to the concept of *safety*, but focuses on *security*.

For clarity in development process and outputs, where possible, it is also necessary to decompose the primary security objectives into corresponding *secondary objectives* in line with business/operational objectives, and the envisaged security violations that potentially threaten the actualisation of the desired business/operational objectives. These *secondary objectives* specify deeper actionable security principles targeted in the metrics development process. For instance, availability objectives could be decomposed into *timeliness, recoverability, redundancy*, etc. Integrity objective could be decomposed into *accountability, authentication, non-repudiation* [53], *dependability, veracity*, etc., while confidentiality objective could be decomposed to *authorisation, access control*, etc. [6], [10], [15], [33].

B) Contextual Description

The objective definition phase is concluded with a contextual description of the final state of the security objective to be achieved by resultant metrics, and the analysis of violation concepts. It is a good concept to have a single objective statement that plainly states the end towards which all measurement and metrics gathering efforts should be directed [23] in line with pre-defined primary and secondary security objectives. For instance, a contextual security objective description could read '*to provide security metrics that plainly and easily communicate the degree to which system technologies can effectively control security threats, vulnerabilities, and attacks, to guard against operational disruptions'*. Here, a primary objective could be *'availability' and 'integrity'*, and a secondary objective could be *'redundancy, reliability, and access control'*. It is required that contextual security objective descriptions be clear enough to enable the derivation of prospective action plans for the attainment of prescribed security objectives. Contextual description could be guided by relevant security standards like NIST SP 800-53 [33], NIST SP 800-82 [6], ISO/IEC 27001 [9], and NIST Framework for Improving Critical Infrastructure Cybersecurity v.1.0. [7], etc.

3.3 Metrics Synthesis

This phase describes the process of articulating dimensions to security metrics, and by dimension imply the focus for security control.

A) Control Capabilities

Existing security control efforts and implementations basically take on one of two broad control capabilities: proactivity and reactivity [53], [54]. Security metrics should thus mirror the same dimensions. Metrics could adopt proactive capability, where measures are derived to give perspectives about future security or vulnerability states [45], [55], [56], or would help guard against potential future security threats and risks. Proactive control capability attributes include: *prediction, detection*, and *prevention*. Security control efforts could also assume reactive

dispositions, in which case metric derivations are obtained to give outlooks to current states [57], what is required to control or counteract the effects and impacts of security compromises that already occurred. Control capabilities in this regards include *detection, prevention, response*, and *recovery*. Furthermore, security metrics could combine both capabilities into what is termed a '*hybrid*' capability that yields measures and metrics that capture the perspectives of both proactivity and reactivity. The occurrence of detections and preventions in both dimensions indicates their importance and relevance in any security metrics development process. Any security metric taxonomy should capture among others, quantities that articulate capacities for both detection and prevention. In a broader scale, a security objective could target both proactive and reactive dimensions, in which case all five (5) control attributes are considered in the development strategy.

B) Metric Quantities

With a clear definition of desired metrics control dimensions, it becomes easier to generate specific metric quantities and specify quantity constituent attributes. Metric quantities could be derived *computationally* applying mathematical concepts, or via *measurements* using scales and instruments. The outcomes can be as single measurable attribute that is representative of the state of a system or security phenomenon. For instance the *security evaluation deficiency count, known vulnerability days, and password crack time metrics* in [58]. However, metrics could also be derived from the combination of two or more disparate attributes, from which a single quantity emerges and is representative of the security perspective desired. This is referred herein as 'composite metrics' [59]. Metric quantities can be further defined based on the unit/base for measurement, and accordingly can be count/number-based, time-based [20], [55], probability-based [44], [60], proportion-based [61], or cost-based [62], [63]. It is appropriate to openly clarify these units in relation to each metric quantity in the taxonomy to be generated, and to understand the interpretation of each metric in relation to pre-defined security objectives of the system.

C) Metric Specification.

A metric specification profile is required for every metric quantity generated during the development process. A metric specification is described as a function of its current state/value (quantitative or qualitative), an ideal state specification, and an evaluation technique for obtaining the metric measures. These are relevant in describing a metric since consistency; expressed by the gain of repeatable results in measurement technique is considered of higher priority than the decision of measurement subjectivity or objectivity [64] and a characteristic of good metrics [16]. Since the goal of any measurement is to determine if a system constituent meets its security objective as defined in the metrics profile description, such descriptions help proffer quicker and clearer understanding and interpretation of each metric, and the corresponding implications in relations to targeted objectives.

3.4 Structural Flow and Review

The proposed model supports the top-bottom approach of metrics development. Nonetheless, it could still be adapted to a bottom-up approach as well, hence the reason for indicating two directional arrows (one directing up and the other directing down) surrounding the framework structures. The choice of direction should be entirely dependent on organisational convenience, expertise, and the perception of a most suiting approach towards achieving targeted goals. However, for easy, better structured, and most appropriate synthesis of security metrics, the top-down approach is recommended. It might be better that the security metrics development should follow the system development life cycle, where, the system in a broad concept can refer to security metrics of industry control environment. Effectiveness of development can be achieve with a good understanding of requirements, expectations, and outcomes of successive phases of the development lifecycle.

It is also pertinent to engage formal reviews and reassessments of metrics taxonomy periodically, to check the relevance and appropriateness of current metrics taxonomy in relations to evolving security trends and the operational dynamics of the industrial environment. The two directional arrows at the top and bottom of the framework structure are used to capture review and reassessment requirements accordingly. It is crucial to resolve questions about continual relevance, accuracy and reliability of metrics, and their usefulness in determining new courses of actions for the overall attainment of pre-defined security objectives [23]. The review will also assess the worth of efforts and techniques for generating metrics, and the reassessment of emergent external security metrics, standards, and best practices for improving existing internal metrics taxonomy. This study lends voice to the works in [6], emphasising that as trends continue to emerge and evolve in security threats, vulnerabilities, breach patterns and techniques, and impacts, it is important for metrics and their development approaches to take-on adaptive natures, adjusting to strategies as circumstances change.

3.5 Symbolic Representation

Symbolic representations offer an easy way to capture and make visible concepts, ideas, and attributes by showing the various attributes that encompass those concepts and their relationship structure. Hence, for easier understanding, the OSMD framework can be represented symbolically as a septenary set comprising seven state vectors, namely $\{D, S, d, PO, SO, CC, M\}$ based on the relationship among the three (3) development phases and their corresponding sub-phases as shown in Figure 1, and described in details as follows:

D : $\{Cap, Vul\}$ is a set of all security dimension for metrics development, where Cap and Vul represent capabilities and vulnerabilities respectively.

S : $\{Entr, Indr\}$ is a set of all target network segments within the ICS network for which security metrics are required. $Entr$ and $Indr$ represent Enterprise and Industrial Network segments respectively.

d : $\{d = 1, 2, 3, \ldots, n\}$ is a set of all system constituents or devices for a target network segment.

PO : $\{A, I, C\}$ is a set of all primary security objectives targeted by the metrics development approach, where A, I, and C represent availability, integrity, and confidentiality respectively.

SO : $\{so_i \mid i=1\ldots n, so_i \rightarrow A \cup I \cup C\}$ a set of all secondary security objectives related to a targeted primary objective.

CC : $\{Prd, Det, Prv, Rsp, Rcv\}$ is a set of all control capabilities, where Prd, Det, Prv, Rsp, and Rcv represent Prediction, Detection, Prevention, Response, and Recovery respectively.

M_d : $\{m_j \mid j = 1, 2, \ldots, n\}$ is a set of all metric quantities deducible from constituent d.

With this, a metric specification (subsection 3.3c) for a resulting metric quantity can also be represented using a quinary set comprising of five state vectors, namely $\{M_d, d, I, C, E\}$, such that:

$$(M_d) = f\,(I_d, C_d, E_d)$$

where:

I_d : $\{s_1, s_2, s_3, \ldots, s_n\}$ is the set of all respective ideal state values for the metric quantities M_d. The value of I is defined based on acceptable security states of M_d from prescribed security requirements.

C_d : $\{c_1, c_2, c_3, \ldots, c_n\}$ is the set of all respective current state values for the metric quantities M_d. The value of C is derived via measurements or computationally.

E_d : $\{e_1, e_2, e_3, \ldots, e_n\}$ is the set of all respective evaluation techniques (approaches) for the metric quantities M_d.

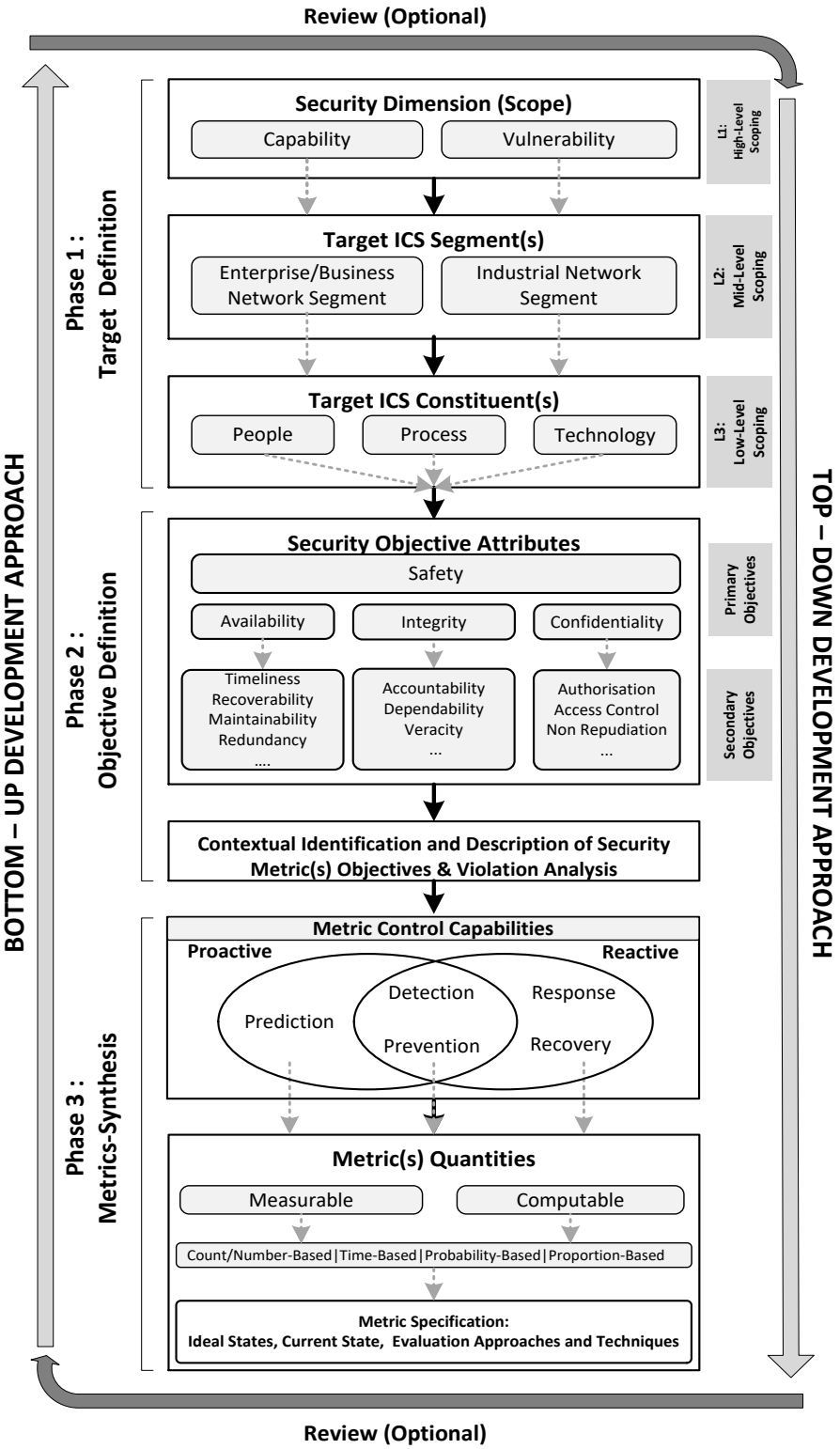

Figure 1: Operational Security Metrics Development (OSMD) Framework

3.6 Implementation and Application Concept

The OSMD framework can be implemented in various instances. The black-shaded phase and sub-phase transition arrows indicate mandatory implementation flow transitions, while the grey-shaded sub-phase transition arrows indicate optional/selective transition inclusions. By these, it means that it is not in all cases that that all phase and transion features will be reflected in a metrics generation process. Rather, the application environment's target security objective(s), choiced/desired security dimension, and control capabilities of interest, would determined the phase and sub-phase transition to be followed, and subsequently, also determine the varied security metric quantities that can emerge. For example, for an environment whose security improvement focus is fronm the people (human) perspectives, the security metric quantities that would be derived using the approach would clearly differ from the environment with

focus on technology security postures. Similarly, an organisation that desires to evaluate security capability of its system via a combined technology and process perspective, would most often use different security metric measures from the organisation that desires to learn organisational security vulnerability of technology, process, and people dimensions.

Typically, variations in the security objectives of organisations would also yield variations in corresponding and relevant security metric quantities. Hence, why it is not considered binding for all dimensions to be reflected in a metric generation process. The proposed framework presents an open approach to the enumeration of key dimensions, objectives, and control capabilities that can be considered in a security metrics development process. Security Capabaility and Vulnerability both represent different viewpoints through which security evaluations can be engaged. Such evaluations can focus on either the business network or the industrial operations network, or both. Similarly, people, process, and technologies, all represent distinct constituents where security evaluations can be focused. In some cases, security evaluations can includes any combination of the three. Regardless of the dimensions and control capabilities, the proposed framework emphasises adherence to a structured analysis process that allows for considering all possible security dimesnsions, objectives, an control capabilities to influence the correct identification and appropriate generation of security metric quantities that suit specific environments and situations. The key end goal is to ensure that suitable security metric quantities that suite every case scenario and(or) objectives be achieved using the prescribed framework in its totality or in parts, thus portraying the flexibility and adapatability property earlier emphasised.

4. VALIDATION

The proposed framework offers an easy way to generate cyber security metrics; the articulation of objectives for a narrowed target system scope, and precisely defining system attributes and constructs necessary for considerations prior and during the security metrics development process. However, it is necessary to justify the usefulness and relevance of the proposed framework via validation means. Validation describes the process of assuring that a model, framework, or structure is sufficiently or reasonably accurate to suit the purpose at hand [65]. In other words, a procedure for ensuring that the right model or framework is being built [66].

A two-level validation approach was adopted for the evaluation of the framework. The first level validation involved the adoption of a use case scenario that demonstrated the practical application of the proposed framework for security metrics development. The aim of the case study is to demonstrate the use of the framework, and assess the effectiveness of the framework for guiding cyber security metrics development process, yielding metric quantities, definitive attributes and measures that can be used to evaluate security capabilities, and providing information that can help improve security assurance based on pre-defined security objectives. The second level validation involved the use of expert intuitions/opinions undertaken using an online questionnaire validation tool which was targeted at expert personnel with understanding and (or) experience in security metrics generation, evaluations, and applications in relations to industrial cyber/information/network security metrics. This approach is generally supported and used in computer science for validating models and frameworks from previous research [67], [68], and especially as related to experts characterised in small samples [68], [69]. The significance of expert knowledge and disposition is also acknowledged in [70]. The reliability of this approach is also demonstrated in [71] and [72] with outcomes that showed that human-centred evaluation processes integrating expert opinions can significantly outdo simple function point models. Thus, this validation aimed at eliciting the views of experts other than the authors of this work on the validity of the proposed framework in the contexts described after careful examination. These views are also aimed at corroborating or contradicting the outcomes of level 1 validation outcomes.

4.1 Verification with a Case Study

This validation level involves the case study scenario on human capability evaluation for cyber security in critical industrial infrastructure [50].This scenanrio assumes the existence of adequate technology and process capability valuations within the case study manufacturing ICS environment. It also assumes the desire to learn of the security capacities of the case study environment people (workforce), and further characterise the security capability attributes of each workforce individual, and use same to influence security improvement decisions. In prior work, metric quantities were developed as part of a modelled approach for evaluating the cyber security capability of the human (people) constituents of an industrial working environment. There is an rapid rise in cyber-attacks on industrial networks and platforms, and particularly targeting the users (human constituents) of the system [50], [73], [74]. The employees within industrial environments are viewed to be weakest links in both the operations and supply chain [75], and they are the most vulnerable vectors of industry cyber cyber-attacks. The motivation for developing cyber security metrics in relation to the evaluation of human security capabilities is to show the security levels of human weak-links by determining their security capacities and vulnerabilities, and hence put necessary guided control efforts on security, thus to enhance security assurance of enterprises. It is essentially a formative decomposition validation technique for the proposed framework.The subsections below will demonstrate the process of generating the cyber security metrics in relations people (human) workforce security capacity following the structured flow of the proposed framework.

A) Phase 1: Target Definition

In line with phase 1 of the proposed framework, the following descriptions represent the outcomes of the scenario described above:

i. *Security Dimension (L1 Scoping):* Security metrics intended to capture both ***capability*** and ***vulnerability*** security dimension of the workforce (users). From the work in [50], determining workforce knowledge and skills emphasises capabilities in the people entities, while the weakest link objective describes a weakness status.

ii. *Target ICS Segment:* This focuses on the ***Industrial Network Segment***, which defines the working domain of all the workforce members in the scenario.

iii. *Target ICS Constituent:* this identifies the precise entities upon which measurements and evaluations are will be carried out. In this case, the focus is on the ***people (Human Users)*** in the industrial network segment.

B) Phase 2: Objective Definition

Based on the outlined objectives, safety though relevant is considered a silent requirement in this context since it is not the focus of this study. In terms of *security*, knowledge capability seeks to determine individual workforce acquaintance to the requirements of *availability, integrity,* and *confidentiality* within the system, and skills capability measure the level of practical capability to enforce the primary objectives as understood. In terms of *availability*, knowledge capability seeks to ensure that workforce members are aware and understand the relevant policies and trends that relate to *timeliness, maintainability*, and *recoverability* of their operating infrastructure in the face of a cyber-attack. *Integrity* ensure workforce members' awareness of relevant integrity policies and trends in relations to *accountability, dependability*, and *veracity*, etc, while *confidentiality* strives the same feet for *authorisation, access control*, and *non-repudiation*. The skills capability requirement seeks to determine the workforce practical aptitude to implement or enforce essential security policies in line with both primary and secondary objectives. Accordingly, a relationship can be identified between the security metrics development objectives (primary and secondary) and the contextualised evaluation points. This is represented in Figure 2, while Table 2 expands on the metrication contexts accordingly.

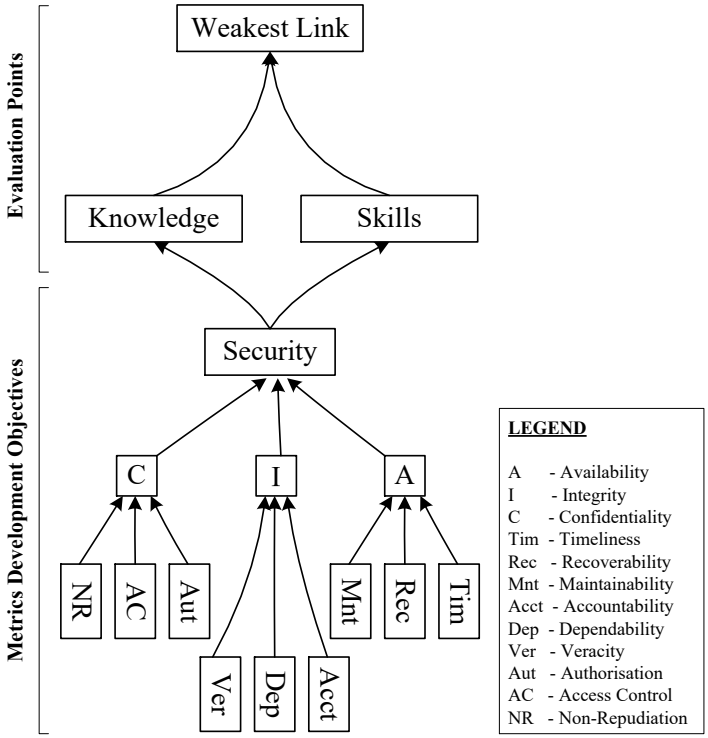

Figure 2: Mapping Relationship between Development and Metrication Objectives

Table 2: Metrics Development Objective Definition for Workforce Capability Evaluation

Contextual Definition	
Metrication Aim	**Evaluation Points**

Evaluate organisational cyber security posture through Workforce Capability assessment of knowledge of both primary and secondary system security objectives, the diagnostic skills in enforcing the objectives, and to determine the weakest-link capability for necessary Cyber security improvement	(i) Evaluate relative workforce cyber security ***knowledge*** in line with dynamic trends and requirements for both primary and secondary objectives. (ii) Evaluate relative workforce cyber security practical ***skills*** to enforce both primary and secondary system security objectives in line with dynamic security attack trends. (iii) Determine the potential ***weakest link*** security capability amongst the workforce, representing a potential security posture indicator of the system under evaluation.

C) Phase 3: Metrics Synthesis

Based on the contextual description contained in the aim and objectives in table 1, the metric control capabilities of need include; ***detection, prevention***, ***response***, and ***recovery***. The control capabilities depict the organisation's desire to knowledge and skill measure to evaluate both individual and organisation to detect, respond, prevent, and recover from potential attacks when they occur. Accordingly, two essential sole metric quantities are deduced via a computation means from the target and objective definitions of ***Knowledge Capability (K_c)*** and ***Skills Capability (S_c)*** [50]. Knowledge capability is defined as the measure awareness and theoretical understanding about recurrent cyber threats, vulnerabilities, attack patterns and impacts to the target system that a user, employee or operator is working with, while skills capability outlines the measure of ability to use accrued knowledge either from experience or training to spot cyber-attack attempts, patterns and techniques, and the degree to which the user can respond, prevent or recover timely with appropriate countermeasures [50].

These two metrics are computable as ***number-based*** quantities that are dependent on the specific evaluation techniques, i.e., there measure are discrete values derived based on the nature and type od evaluation (questionnaire, survey, gamification, etc) approach adopted. Their respective maximum values represent their ideal states. Another metric referred to as ***Organisational Capability Rating for one person (CR_p)*** is used to represent the assumed organisational workforce capability potential, obtained from the harmonisation of K_c and S_c metrics for all workforce members into a set A = {$CR_1, \ldots, CR_n$}, and the identification of the least value in A, which is the *weakest-link* CR_p. Therefore, CR_p = min (A) = min ($CR_1, \ldots, CR_n$), $CR_p \in A$, n = number of workforce members under evaluation. CRp is thus a ***composite metric*** since it requires the combination of two metric quantities. The profile description of the three-metrics taxonomy for workforce cyber security capability evaluation are presented in Table 3. The ideal situation is the desirable state of every workforce member, while the current state would indicate the actual state of each workforce member after the questionnaire, statistical analysis, and weakest-link analysis evaluation approaches have been employed. These invariably aid the accomplishment of the initial security objectives, and toward towards attaining the pre-defined security aim of developing the metrics.

Table 3: Metrics Profile Description for Human Capability Evaluation

Metric No.	**Name**	**Symbol**	**Metric Specification** $f(I_d, C_d, E_d)$
M1	Knowledge Capability	*(Kc)*	$SP(K_c) = f(Kc_{max}, Kc_p, QA)$
M2	Skill Capability	*(Sc)*	$SP(S_c) = f(Sc_{max}, Sc_p, QA)$
M3	Organisational Capability Rating	*(CR_p)*	$SP(CR) = f(CR_{max}, \min(A), WLA)$
I = Ideal State, C = Current State, E = Evaluation Approach, *QA =Questionnaire Analysis, WLA=Weakest Link Analysis*			

D) Application and Analysis

The generated people-centred metrics outlined in table 3 were further evaluated using a real scenario involving a six-member team of postgraduate students undertaking a research project for the development of physical demonstrator of cyber security in manufacturing. The team's objective was to develop and keep operational a physical prototype manufacturing SCADA infrastructure, and explore the potentials for executing cyber-attacks on the prototyped systems with impact observations and recommendations for enhancing cyber security.

In this scenario, the goal of *'keeping operational'*, *'executing cyber-attack'*, and making *'impact observations and recommendations'* all depend on the security knowledge and skills capabilities of the team members, which in turn describe the team members' knowledge and skills in actualising the primary and secondary security objectives. Hence,

prior to the team's evaluation, the following assumptions were made; (i) the team represents a small-scale industrial (manufacturing) workforce, (ii) all the members of the team had equal capabilities in security knowledge and skills to achieve the prescribed objectives of the project. For this metrication scenario, all the objective attributes outlined in Table 1 were adopted, and an evaluation tool (questionnaire) was developed using the UK's *'10 steps to cyber security'* guidelines [76]. The questionnaire comprised of 40 security capability test questions (20 for knowledge, and 20 for skills). The evaluation tool was administered to each team member and responses analysed using the workforce capability evaluation approach, and corresponding knowledge and skills capability ratings derived using the appropriate evaluation functions [50]. Accordingly, the capability priority rankings included: $20.00 \leq h \leq 33.33$ for *high,* $33.33 < m \leq 66.67$ for *moderate, and* $66.67 < l \leq 100.00$ for *low.* The *low* priority range of scores represented the *'Ideal state'* of the metric quantities. The result of the evaluation of capabilities is presented in table 4.

Table 4: Capability Evaluation Results

Member ID	***Kc***	***Sc***	***CR***	***Priority***
WF01	42	39	40.47	*Moderate*
WF02	38	32	34.87	*Moderate*
WF03	23	48	**33.23**	***Moderate***
WF04	70	72	70.99	*Low*
WF05	53	73	62.20	*Low*
WF06	56	49	52.38	*Low*

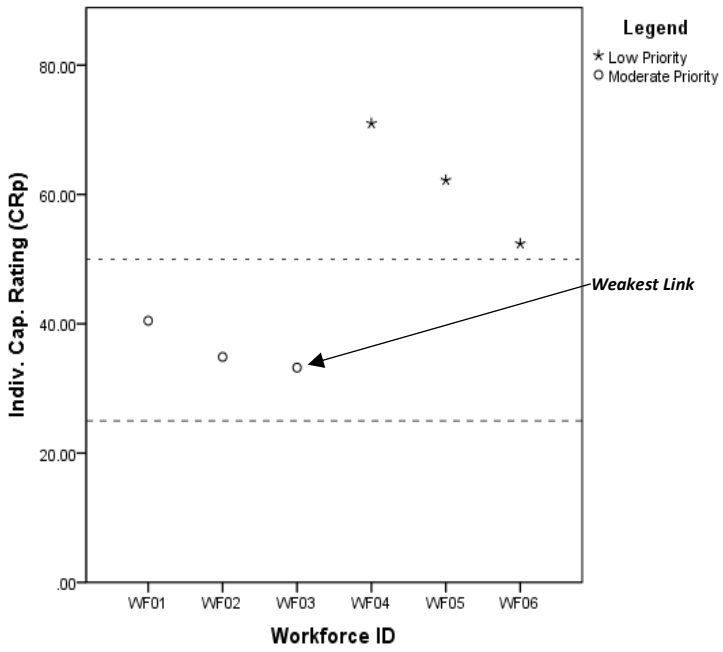

Figure 3: Workforce Capability Visualisation Chart

The evaluation yielded different levels of capabilities in knowledge, skills, and normalised capabilities for the team members and easily showed the team members' weak levels in cyber security (table 3 and figure 3). If an organisation is potentially as weak as its weakest link, then the resulting weakest link value herein represents the security capability of the small-scale industrial organisation or enterprise. Identifying such weak links reveals to organisations their easier compromise vector of successful attacks, since attacks typically target the most vulnerable points of an organisation or enterprise. Hence, organisation should improve the security assurance from this point. It can be assumed that the security capability of the weakest link potentially represents the security capability of the organisation. If such weakest link is identified, then it potentially provides the easiest means for compromising the organisation. In this scenario, the weakest link capability is attributed to the team member ID *WF03 (Kc = 23, and Sc = 48)* with a normalised capability rating *CR* = 33.23. Therefore, organisations or enterprises need to ensure that the weakest link will be as strong as possible against cyber-attacks or crimes

4.2 Validation by Experts

The second level validation adopted an approach for validating improvement structures, frameworks, and measurement mechanisms by eliciting a group of experts to complete a detailed questionnaire, or respond to oral structured interviews. The online questionnaire approach offers ample time and opportunity for completion to the experts, while

allowing for flexibility of preferred times and places. Experts could also pause and return to the questionnaire at their convenience. This method enables experts to view the model framework, and consider the validity of its output based on practical implementations in their localised environment or theoretic analysis of feasible outputs based on inherent experiences in security metrication. Therefore, a survey questionnaire approach was used in this research.

A) Validation Questionnaire Design

The questionnaire tool was designed with the evaluating charactristics in mind. Evaluations were undertaken to determine the relevance of the suggested good metrics framework characteristics (i.e., scope-definitive, objective-definitive, reliable, simple, adaptable, and repeatable - SORSAR), and against six other recommended framework validation criteria which include: scope-delineation, consistency, understandability, ease of use, tailorability, and verifiability [77]. Scope-delineation advocates the importance to know the scope of the framework, i.e. both exclusion and inclusion of the framework. Consistency emphasised the need for a common language, and the description of processes at similar granular levels at each stage of the framework. Understandability emphasised the importance to ensure clear definitions that allow all users of the framework to have a shared understanding of the process, especially when needing improvements. Ease of Use property advocates that frameworks and models should be decomposed to a level that is simple to grasp and follow. Tailorability advocates that a framework should be responsive to the need for changes, it should be structured such that can be extended and tailored to specific development environments. Verifiability emphasises the need for a framework to provide for test and measurement on how well the framework satisfies its objectives, and what quality magnitudes are achieved. This is to help affirm confidence and usefulness in the design and(or) implementation structure of the model [78]. Other characteristics evaluated included: industrial and academic usefulness, and applicability of the framework for yielding desirable security metrics relative to industrial operations scenarios. The layout and sequence of the questions was suc that a first array of questions linked a one-to-one relationship with the charactereistics, and then a similar approach was used to present the second round of questions. This was to ensure that no characteristic had two relative questions in succession to control the potentials for cheap response consistencies due to question proximities. To properly achieve the validations aim, closed-ended questions were used. The questionnaire was contextually structured in three sections to capture all aspects of this work as presented in Appendix A.

Section A (consisting of 3 questions) is to capture the demographic work details about the experts who join the survey. This was aimed at determining how long and level of experience in cyber security capabilities of the experts, and their scope. This information is necessary to support and justify eventual views asserted by each expert, and also to lend credence to the validation process and result.

Section B (consisting of 1 question with 6 attribute queries) is to gain expert views concerning the proposed characteristics of good metrics development framework. This was aimed at gauging professional views about the relevance or unrelated the prescribed good metric framework characteristics are to contemporary security metrics development. By this, any characteristic widely viewed to be irrelevant or redundant in the group could be eliminated, while emphasizing the foundational requirements for developing and(or) adopting effective security metrics development frameworks and models.

Section C (consisting of 14 questions) is to obtain expert views of how and if proposed framework satisfies the initial criteria for its development in relations to the needs of different users and environments. The framework is thus validated in this context to demonstrate that its constituents and attributes possess an acceptable range of correctness consistent with the proposed application of the framework [79]. The overall purpose was to investigate whether the essentially generic framework meets the initial criteria for its development in the first place,with reasonable emphasis on satisfying the need of individual users.

B) Response and Feedback Mapping

Eleven (11) cyber security experts from both industry and academic environment took part in the survey. The evaluation produced notable findings following the aggregation, grouping and mapping of expert responses to corresponding evaluation criteria. For the characteristics of good metrics framework, each attempted mapping to a criteria was characterised as either a ‘Strong Relevance’, ‘Average Relevance’, or ‘Weak Relevance’. A ‘Strong Relevance’ included the combination of clearly affirmative responses (high and very high), and indicated that such attribute characteristic should be considered as reasonably required, be an incorporated feature in any ICS security metrics framework. An ‘Average Relevance’ encompassed only the ‘moderate’ responses which indicated a fair significance for a characteristic as requirement feature in ICS security metrics frameworks. Hence, could be considered. A ‘Weak Relevance’ included the cumulative of less affirmative expert responses (low and very low), indicative of the attribute characteristic being hardly important for consideration and representation in a security metrics framework, thus should be negligible. The mappings are clearly outlined in table 5.

Similarly, a second mapping of expert responses was done for the validity of the framework against earlier outlined criteria. Each attempted mapping was characterised as ‘Strongly Represented’, ‘Weakly Represented’ or ‘Not Represented’. A ‘Strongly Represented’ map encompassed the cumulative of the two most affirmative expert responses, and indicated a higher representation or expression of the criteria in the proposed framework (see table 5). A ‘Weakly Represented’ map encompassed the cumulative of the two least affirmative expert responses, and indicated a feeble and

faint representation or expression of the criteriain the proposed framework. Possible sets of cumulative responses and their context groupings are shown in table 5.

Table 5: Context - Response Mapping Groups

Contexts	Response Map	Cumulative Mapping Group Selections
Characteristics Relevance	Strong Relevance	*High + Very High*
	Average Relevance	*Moderate*
	Weak Relevance	*Low + Very Low*
Framework Validity	Strongly Represented	*Consistent + Strongly Consistent*
		Little + Very Little
		Appropriate + Strongly Appropriate
		Agree + Strongly Agree
		Realistic + Strongly Reaslistic
		Easy + Strongly Easy
		Useful + Strongly Useful
		Applicable + Strongly Applicable
	Weakly Represented	*Inconsistent + Strongly Inconsistent*
		Much + Very Much
		Inappropriate + Strongly Inappropriate
		Disagree + Strongly Disagree
		Unrealistic + Strongly Unreaslistic
		Uneasy + Strongly Uneasy
		Not Useful + Strongly Not Useful
		Not Applicable + Strongly Not Applicable
	Not Represented	*No Opinion/Don't Know*

C) Analysis of Response Mappings

Prior to the analysis of the contexts and response mappings as enumerated in table 5, the work and capability demographics of the 11 experts used for this evaluation indicates a 4 years mean working experience in operational security aspect of the industry for the 9 experts that responded to the question. 2 experts did not indicate their years of work experience, however, they both rated themselves *'very high'* in knowledge, skill, experience, and expertise in cyber/information security, metrics development and assessment. More than half (54.54%) of the experts indicated to have worked for at least 2 years in the industrial/operational security. It is notable 90.91% (10) of the experts accented to *'both security knowledge and skill capability'* classification, which suggests that most of the experts were reasonably equipped with adequate information and technical know-how in ICS cyber security enough to enable them lend judgements as professionals in the validation process. This is supported further by the security capability rating mean value of 3.36, with 81.81% (9) of the sample indicating at least *'moderate'* security capability. Most of the experts admit to having a relatively good knowledge, skills, experience, and(or) expertise in industrial cyber security and metrication.

i. Analysis Good Security Metrics Framework Characteristics

After mapping expert responses to corresponding cumulative mapping groups to evaluate the views on the degree of relevance of each of the good security metric framework characteristics proposed, analysis showed that for all of the characteristics, considerably large fractions of the relevance attribute mapped to *'Strong Relevance'* (70%). It is particularly noteworthy that there was a general unanimity amongst all the experts with 100% *'Strong Relevance'* of the *'scope-definitive'* characteristic. This was followed by a 90.9% *'Strong Relevance'* on the *'Reliable'* characteristic. *'Simple'* and *'Repeatable'* characteristics had the least valuations, although both reflected a *'Strong Relevance'* mapping as well. The responses of experts did not indicate any *'Weak Relevance'* fractional map on any of the characteristics, but had minimal fraction values on *'Average Relevance'* as shown in table 6. The Chart representation of the three classes of 'relevance' maps is presented in figure 4.

Table 6:Good metrics Characteristics Evaluation Results

Characteristics	Strong Relevance	Average Relevance	Weak Relevance	Total
Scope-definitive	100%	0.0%	0.0%	100%
Reliable	90.9%	9.1%	0.0%	100%
Objective-definitive	81.8%	18.2%	0.0%	100%
Adaptable	81.8%	18.2%	0.0%	100%
Simple	72.7%	27.3%	0.0%	100%
Repeatable	72.7%	27.3%	0.0%	100%

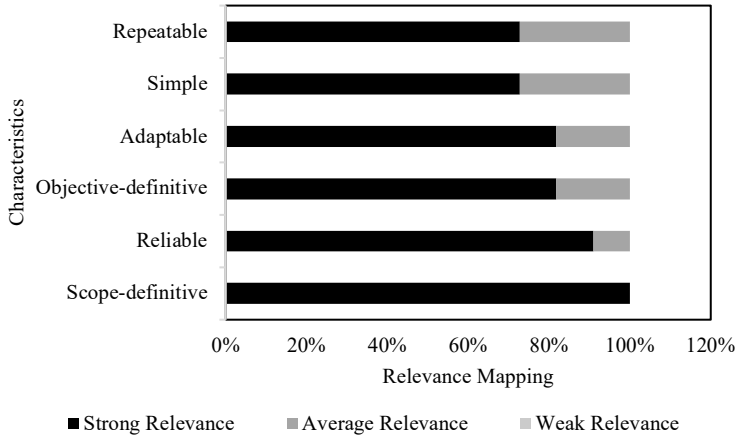

Figure 4: Relevance Mappings

ii. Analysis of Framework Validity Characteristic Mappings

To assess the validity of the proposed security metrics development framework, the questionas covering this context were further mapped to corresponding validation criteria, which had been earlier mapped to grouped/cumulative response selections as represented in table 7. This was done to relate expert responses to attribute evaluation criteria, and to help simplify the process of evaluation through taking the mean (average) of multiple mapping results that are related or attributed to a single criteria. In this section, somew of the questions were unanswered by some experts in the group, which resulted that some questions had a total count response record of 11, while some had lower total count of 9. These were aptly considered in the analysis of overall mapping reults for each critera, and used to evaluate the cumulative records.

The results of individual questions and related average mapping values for multiple questions were used to assess the degree of representation or expression of the corresponding criteria in the proposed security metrics development framework. This helped to determine whether the criteria outlined were reasonably captured or satisfied in the proposed framework, and to what opinionated extent. For example, two questions (C.Q1 and C.Q7) mapped to *'scope-delineation'*, and while C.Q1 had a total count of 11, C.Q7 had a total count of 9. It implied that two experts did not respond to C.Q7. As shown in table 7, all the other criteria followed a similar pattern in outcomes for number of questions mapping, and the total count values. However, only one question mapped to *'verifiability'* property of the validation criteria, and had a total count of 11. Each of the total counts was aggregated to a 100%. Results also show that 90.9% (10) for C.Q1 and 100% (9) for C.Q7 all mapped to *'scope-delineation'* were in the *'Strongly Represented'* map, and had a mean percent count of 95.45%. A result in like manner was replicated in the *'understandability'* criteria as presented in table 7. In a similar but slightly diminished pattern, the *'tailorability'* property had an 18.18% (2) *'Weakly Represented'* fractional response for one of its questions (C.Q5), but had an overall mean of 90.91%. The *'verifiability'* property had a single question mapped to it with 90.9% *'Strongly Represented'* and 9.1% *'Weakly Represented'* response maps. The questions C.Q2 and C.Q8 that mapped to *'consistency'* criteria each yielded a 100% map in *'Strongly Represented'* mapping response. However,a slight variation from others is observed with the *'ease of use'* validation criteria. The question (C.Q4) that had a total response count of 11 showed a 45.45% (5) *'Strongly Represented'* fractional map response, and a 54.54 (6) *'Weakly Represented'* fractional map response. The second question (C.Q10) that mapped to *'ease of use'* yielded a 100% *'Strongly Represented'* map, which introduced some inconsistency in the behaviours results, and required further analysis towards uncovering possible influences to the variations observed. The supplementary validation criteria : *usefulness to industry, usefulness to academic R&D*, and *applicability* evaluated, each yielded a 100% *'Strongly Represented'* mapping as shown in table 7. Figre 5 shows the 'average representation' values accordingly.

Table 7: Framework Validation Mapping Results

Questions Nos	Criteria Mapping	Evaluations Recorded		Weakly Represented Map		Strongly Represented Map		Average
		Total Count	Percent	Total Count	Percent	Total Count	Percent	Percent
C.Q1	Scope-Delineation	11	100%	1	9.1%	10	90.9%	95.45%
C.Q7		9	100%	-	-	9	100%	
C.Q2	Consistency	11	100%	-	-	11	100%	100%
C.Q8		9	100%	-	-	9	100%	

C.Q3	*Understandability*	11	100%	1	9.1%	10	90.9%	95.45%
C.Q9		9	100%	-	-	9	100%	
C.Q4	*Ease of Use*	11	100%	6	54.54%	5	45.45	72.73%
C.Q10		9	100%	-	-	9	100%	
C.Q5	*Tailorability*	11	100%	2	18.18%	9	81.82%	90.91%
C.Q11		9	100%	-	-	9	100%	
C.Q6	*Verifiability*	11	100%	1	9.1%	10	90.9%	90.90%

Questions Nos	**Criteria Mapping**	**Evaluations Recorded**		**Weakly Represented Map**		**Strongly Represented Map**		**Average**
		Total Count	**Percent**	**Total Count**	**Percent**	**Total Count**	**Percent**	**Percent**
C.Q12	*Usefulness to Industry*	9	100%	-	-	9	100%	100%
C.Q13	*Usefulness to Academy*	9	100%	-	-	9	100%	100%
C.Q14	*Applicability*	9	100%	-	-	9	100%	100%

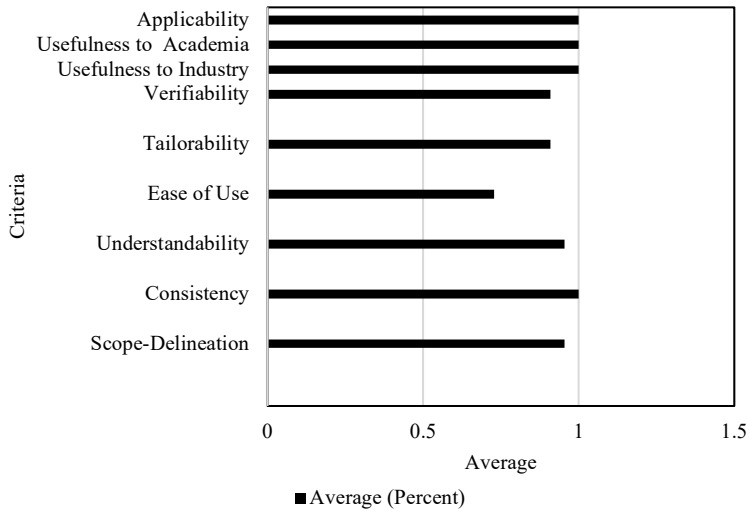

Figure 5: Criteria Representation Maps

4.3 Discussion

From the case study verification (level 1), it is observed that the outcome of a security metric development will be dependent on the clear and concise articulation of system scope, and target security objectives. Primary security attributes (e.g. availability) might vary in meaning, and supplementary secondary objectives will depend on the constituent of the target systems and environments, and the context of security definition. Adopting the OSMD developed security metrics together with the evaluation model to the test scenario helped the identification and understanding of the capability of each workforce member with respect to cyber security knowledge and skills. It also aided the identification of the weakest-link amongst the workforce. A more detailed application of these metrics for workforce capability evaluation is demonstrated in a prior work [50]. Metric quantities could also be reviewed as deemed necessary, especially when in response to changes, which weaken or nullify the reliability of the outcomes expected. The nature of the development model also allows for the development of security metrics that focus on other ICSs, segments, and constituents of control processes, which are expected to yield varied lists of metrics quantities depending on security objectives.

From the expert validation (level 2), results from the framework characteristics evaluation suggest a wide affirmation and acknowledgement of relevance for the prescribed characteristics of good security metrics framework. Based on the *'Strong Relevance'* mapping cumulative values obtained, *'scope-definitive'* criteria topped the list of affirmations by the experts. This was followed by the *'reliable'*, *'objective-definitive'*, and *'adaptable'* criteria. The last two in the order included; *'simple'* and *'repeatable'*. Accordingly, this suggests that for an effective security metrics development framework, being *definitive in scope, objectives, reliable, and adaptable*, were viewed as considerably more prioritised characteristics than being *simple* and *repeatable* in situations where preferences became necessary during design and developments. The framework validation result also shows that five of the framework validation criteria (*scope-delineation, consistency, understandability, tailorability and verifiability*) showed a consistently *'Strong*

Representation' in the proposed security metrics development framework. It implied that that these criteria were considerably characterised and expressable in the proposed framework. However, for the criteria (*ease of use*) that showed a slight variance with others, C.Q4 sought expert feedbacks on the perceived scale of previous knowledge of security metrication required to interpret the proposed framework. A further decomposition of the results revealed that 3 out of the 6 experts whose responsed resulted to the *'Weakly Represented'* (Much + Very Much) response had at least four years work experience in industrial/operational security; with good security knowledge and skills. Their probable elongated and diverse experience might justify a probable deeper insight they have about the *'ease of use'* shortcomings that might have been noticed by the less experienced experts. 2 of the other experts did not indicate their number of years of experience in the field. However, the nearly half (45.45%) *'Strongly Represented'* responses suggests that the framework had some measure of *'ease of use'*, although might not have been as clear as expected, and dependent on the volume and diversity of experience and knowledge at the disposal of a user or developer. Nonetheless, the 100% count for *'Strongly Represented'* map of the counterpart question (C.Q10) does suggest that inspite of the possible imprecision of the *'ease of use'* criteria in the proposed framework, the framework is yet considerably reaslistic for industrial orgabisations to use.

Contextually, the use case results demonstrates that the proposed framework is usable and workable. The results of use case scenario people-oriented metric generations demonstrates that the framework can be effective in guiding cyber security metrics development processes, yielding relevant security metric quantities, definitive attributes and measures that can be used to evaluate security capabilities, effective incidence response, and providing information that can help to improve cyber security assurance based on pre-defined operational security objectives. Expert intuition supports this further with characterised outcomes that suggests that non of the the outlined characteristics of good security metric framework is entirely irrelevant. The results also do not indicate any form of redundancy in the characteristic outline. This view is also replicated in the framework validation criteria. Expert views suggests that the proposed framework does reasonably satisfy (at varied levels) the initial criteria for its development, and with considerable flexibility to individual user needs and environments. Thus, in the study context, the framework demonstrates that its constituents and attributes possesses a reasonably acceptable range of correctness consistent with the proposed application.

5. CONCLUSION AND FUTURE WORK

Operational Cyber Security metrics are very crucial tools for specifying the measurement of security states and susceptibilities in the industrial environments, thus to improve security assurance. However, good security metrics are essentially products of good development approaches. Existing security metrics development frameworks are not robust enough to handle the current dynamic nature of cyber security stakes in the industrial (ICS) operational environment. To achieve a framework that meets this need, an improved unified framework for security metrics is developed and validated. This framework leverages on the outcome of the analysis and integration of capabilities of existing approaches, to proffer the good characteristics of being scope-definitive, objective-definitive, reliable, simple, adaptable, and repeatable, while aligning with existing global security standards and best practices.

By formatively decomposing the requirements of the case study scenario that involved determining the security capability from a people (human) workforce perspective demonstrated in 4.1A, the outline of example security objectives in 4.1B, and indication of metric synthesis of attributes in 4.1C; all yielding knowledge, skill, and organisational capability rating metric quantities, this work demonstrates that the proposed OSMD framework can be reasonably used to arrive at security metric quantities that can suit certain security scenarios and objectves. Thus, it supports the contextual and adaptive articulation of security metric scopes and other evaluation attributes. Also, by further applying the resultant people-oriented (human-factored) security capability metric quantities in a sample evaluation, the actualisation of potential knowledge, skills, and organisational capabilities, this work demonstrates relevance, reliability, and practicality of the proposed gramework to support the generation of ICS security metrics. These justifications are further consolidated by the outcome of the expert opinions that showed that the usability and workability to support the process of generating ICS security metrics of different security dimensions, scopes, objectives, and (or) control capacities.

In general, it can be concluded that practical and relevant security metric quantities can be better achieved through holistic security metric development approaches that are clear on scope-delineations, easily usable, consistent in process applications, and can be verified and tailored to suite various environmental security objectives and changes. A security metrics development approach essentially evaluates capabilities of at least one of the three operational system constituents: people, process or technology. It also prescribes a security capability or vulnerability perspective with the target of engaging either a proactive or reactive control capabilities, or the combination of both into a hybrid control capability. The choice of either a top-bottom or bottom-up approach is based on the convenience of system owners. Two metrics development phases, definition of the target system, and definition of target security objectives, should never be ignored in an overall security metrics development process. These two phases when contextually articulated, make it easy to generate relevant security metrics. Future endeavours in this regard include the application of the metrics development approach towards the development of a security metrics taxonomy focusing on the process and technology constituents of an ICS platform, and the development of a metrics-driven critical control point risk assessment methodology for industrial cyber security assurance, which will be greatly supported by the symbolic representation of the framework.

Reference

[1] E. LeMay, M. D. Ford, K. Keefe, W. H. Sanders, and C. Muehrcke, "Model-based security metrics using ADversary VIew Security Evaluation (ADVISE)," in *8th International Conference on Quantitative Evaluation of Systems, QEST 2011*, 2011, pp. 191–200.

[2] R. M. Savola, "A security metrics development method for software intensive systems," *Commun. Comput. Inf. Sci.*, vol. 36, pp. 11–16, 2009.

[3] R. Barabanov, S. Kowalski, and L. Yngstrom, "Information security metrics: Research directions," 2011.

[4] C. Fruehwirth, S. Biffl, M. Tabatabai, and E. Weippl, "Addressing misalignment between information security metrics and business-driven security objectives," in *6th International Workshop on Security Measurements and Metrics*, 2010, p. 7.

[5] S. M. Bellovin, "On the brittleness of software and the infeasibility of security metrics," *IEEE Secur. Priv.*, vol. 4, no. 4, p. 96, 2006.

[6] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, and A. Hahn, "Guide to Industrial Control Systems (ICS) Security - NIST.SP.800-82r2," 2015.

[7] N. I. of S. and T. NIST, "Framework for Improving Critical Infrastructure Cybersecurity," 2014.

[8] CPNI, "RESILIENCE IN CONVERGED NETWORKS Resilience in Converged Networks :," London, 2009.

[9] I. O. for S. E. C. ISO/IEC, "ISO/IEC 27001: 2013," *Information Technology Standard*, 2013. [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en. [Accessed: 02-Mar-2015].

[10] M. . Azuwa, R. Ahmad, S. Sahib, and S. Shamsuddin, "Technical Security Metrics Model in Compliance with ISO/IEC 27001 Standard," *Int. J. Cyber-Security Digit. Forensics*, vol. 1, no. 4, pp. 280–288, 2012.

[11] J. Chaula, L. Yngström, and S. Kowalski, "Security metrics and evaluation of information systems security," in *Conference on Information Security for South Africa*, 2004, pp. 1–12.

[12] Y. Beres, M. C. Mont, J. Griffin, and S. Shiu, "Using Security Metrics Coupled with Predictive Modeling and Simulation to Assess Security Processes," in *Third International Symposium on Empirical Software Engineering and Measurement*, 2009, pp. 564–573.

[13] R. M. Savola, "Towards a Security Metrics Taxonomy for the Information and Communication Technology Industry," in *International Conference on Software Engineering Advances (ICSEA 2007)*, 2007, no. Icsea, pp. 60–60.

[14] P. Reichert, M. Borsuk, M. Hostmann, S. Schweizer, C. Sp??rri, K. Tockner, and B. Truffer, "Concepts of Decision Support for River Rehabilitation," *Environ. Model. Softw.*, vol. 22, no. 2, pp. 188–201, 2007.

[15] R. Savola and H. Abie, "Development of Measurable Security for a Distributed Messaging System," *Int. J. Adv. Secur.*, vol. 2, no. 4, pp. 358–380, 2009.

[16] T. Chandrakumar, S. Parthasarathy, R. Maragathameena, and S. A. R. Pandian, "Security Metrics for a Business Information System," *Int. J. Comput. Appl.*, pp. 33–38, 2013.

[17] D. Juneja, K. Arora, and S. Duggal, "Developing Security Metrics for Information Security Measurement System," *Int. J. Enterp. Comput. Bus. Syst.*, vol. 1, no. 2, pp. 1–10, 2011.

[18] B. Marr, "How to Design Key Performance Indicators," Milton Keynes, 2010.

[19] M. Mateski, C. M. Trevino, C. K. Veitch, J. Michalski, J. M. Harris, S. Maruoka, and J. Frye, "Cyber Threat Metrics," Albuquerque, New Mexico, 2012.

[20] M. McQueen, W. Boyer, S. McBride, M. Farrar, and Z. Tudor, "Measurable Control System Security Through Ideal Driven Technical Metrics SCADA Security Scientific Symposium," INL/CON-07-13581, 2008.

[21] Z. A. Collier, M. Panwar, A. A. Ganin, A. Kott, and I. Linkov, "Security Metrics in Industrial Control Systems," in *Cyber-security of SCADA and Other Industrial Control Systems, Advances in Information Security*, vol. 66, E. J. M. Colbert and A. Kott, Eds. Switzerland: Springer International Publishing, 2016, pp. 167–185.

[22] G. Cybenko and G. Cybenko, "TIM Lecture Series Cybersecurity Metrics and Simulation," Talent First Network, 2014.

[23] S. C. Payne, "A Guide to Security Metrics," SANS Institute, 2006.

[24] C. Glantz, M. Stoddard, A. Mcintyre, J. Santos, D. Bodeu, L. O'neil, and B. Gennert, "The Development of Security Metrics for Process Control System," I3P, 2003.

[25] D. N. Nguyen, "Security Metrics in SCADA System," University of South Australia School, 2012.

[26] R. M. Savola and H. Abie, "Development of security metrics for a distributed messaging system," in *2009 International Conference on Application of Information and Communication Technologies, AICT 2009*, 2009, pp. 1–6.

[27] E. Jonsson, "Towards an integrated conceptual model of security and dependability," in *First International Conference on Availability, Reliability and Security, ARES 2006*, 2006, vol. 2006, pp. 646–653.

[28] E. Jonsson and L. Pirzadeh, "A framework for security metrics based on operational system attributes," in *3rd International Workshop on Security Measurements and Metrics, Metrisec 2011*, 2011, pp. 58–65.

[29] M. Stoddard, R. Carlson, Y. Haimes, D. Bodeau, C. Lian, J. Santos, C. Glantz, and J. Shaw, "Process Control System Security Metrics – State of Practice," Institute for Information Infrastructure Protection (I3P), 2005.

[30] M. P. Azuwa, R. Ahmad, S. Sahib, and S. Shamsuddin, "A propose technical security metrics model for SCADA systems," *Int. Conf. Cyber Secur. Cyber Warf. Digit. Forensic, CyberSec 2012*, pp. 70–75, 2012.

[31] I. Linkov, D. A. Eisenberg, K. Plourde, T. P. Seager, J. Allen, and A. Kott, "Resilience metrics for cyber systems," *Environ. Syst. Decis.*, vol. 33, no. 4, pp. 471–476, 2013.

[32] I. Linkov, D. A. Eisenberg, M. E. Bates, D. Chang, M. Convertino, J. H. Allen, S. E. Flynn, and T. P. Seager, "Measurable Resilience for Actionable Policy," *Environ. Sci. Technol.*, no. ii, pp. 10108–10110, 2013.
[33] NIST, "Security and Privacy Controls for Federal Information Systems and Organizations," National Institute of Standards and Technology (NIST), 2013.
[34] R. M. Savola and H. Abie, "Metrics-Driven Security Objective Decomposition for an E- Health Application with Adaptive Security Management," in *International Workshop on Adaptive Security Article No. 6*, 2013, pp. 1–8.
[35] CIS, "The CIS Security Metrics v1.1.0," The Center for Internet Security, 2010.
[36] S. E. Schechter, "Computer Security : A Quantitative Approach," Harvard University, Cambridge, 2004.
[37] I. Kotenko and A. Chechulin, "A Cyber Attack Modeling and Impact Assessment Framework," in *5th International Conference on Cyber Conflict*, 2013, pp. 1–24.
[38] P. Wang and J. C. Liu, "Threat Analysis of Cyber Attacks with Attack Tree+," *J. Inf. Hiding Multimed. Signal Process.*, vol. 5, no. 4, pp. 778–788, 2014.
[39] S. Jajodia, S. Noel, and B. O'Berry, "Topological analysis of network attack vulnerability," in *Managing Cyber Threats*, Springer Publishers, 2005, pp. 247–266.
[40] M. Cremonini and P. Martini, "Evaluating Information Security Investments from Attackers Perspective: the Return-On-Attack (ROA)," in *4th Workshop on the Economics of Information Security*, 2005, p. 4.
[41] S. Bistarelli, F. Fioravanti, P. Peretti, and F. Santini, "Evaluation of complex security scenarios using defense trees and economic indexes," *J. Exp. Theor. Artif. Intell.*, vol. 24, no. 2, pp. 161–192, 2012.
[42] S. Bistarelli, F. Fioravanti, and P. Peretti, "Defense trees for economic evaluation of security investments," in *Proceedings - First International Conference on Availability, Reliability and Security, ARES 2006*, 2006, vol. 2006, pp. 416–423.
[43] FIRST, "Common Vulnerability Scoring System v3.0: Specification Document," *Forum Incid. Response Secur. Teams*, pp. 1–21, 2015.
[44] M. Keramati and M. Keramati, "Novel security metrics for ranking vulnerabilities in computer networks," in *7th International Symposium on Telecommunications, 2014 IST*, 2014, pp. 883–888.
[45] S. Abraham and S. Nair, "Cyber security analytics: A stochastic model for security quantification using absorbing markov chains," *J. Commun.*, vol. 9, no. 12, pp. 899–907, 2014.
[46] C. Lei, D. H. Ma, H. Q. Zhang, and L. M. Wang, "Moving target network defense effectiveness evaluation based on change-point detection," *Math. Probl. Eng.*, vol. 2016, pp. 1–11, 2016.
[47] Defence Signals Directorate, "Network segmentation and segregation," 2012.
[48] M. King-Turner, "Three Keys to IT System Success: People, Process, Technology (National B2B Centre)," *The National B2B Centre, UK.*, 2014. [Online]. Available: http://www.nb2bc.co.uk/managing_it_projects/articles/?id=181. [Accessed: 12-Aug-2015].
[49] S. Ramakrishnan and M. Testani, "People , Process , Technology - The Three Elements for a Successful Organizational Transformation," *IBM Path Forward to Business Transformation*. IBM Centre for Learning and Development, pp. 1–21, 2011.
[50] U. P. D. Ani, H. M. He, and A. Tiwari, "Human Capability Evaluation Approach for Cyber Security in Critical Industrial Infrastructure," in *Advances in Human Factors in Cyber Security: Proceedings of the AHFE 2016 International Conference on Human Factors in Cybersecurity, July 27-31, 2016, Walt Disney World®, Florida, USA*, vol. 501, D. Nicholson, Ed. Florida: Springer International Publishing, 2016, pp. 169–182.
[51] R. D. Larkin, J. Lopez Jr., J. W. Butts, and M. R. Grimaila, "Evaluation of Security Solutions in the SCADA Environment," *Data Base Adv. Inf. Syst.*, vol. 45, no. 1, pp. 38–53, 2014.
[52] R. K. Shyamasundar, "Security and Protection of SCADA : A Bigdata Algorithmic Approach," in *Proceedings of the 6th International Conference on Security of Information and Networks*, 2013, pp. 20–27.
[53] F. Y. S. Lin, Y. S. Wang, and M. Y. Huang, "Effective proactive and reactive defense strategies against malicious attacks in a virtualized honeynet," *J. Appl. Math.*, vol. 2013, pp. 1–11, 2013.
[54] J. Kwon and M. E. Johnson, "PROACTIVE VS. REACTIVE SECURITY INVESTMENTS IN THE HEALTHCARE SECTOR," 2015.
[55] S. Abraham and S. Nair, "Exploitability analysis using predictive cybersecurity framework," in *Proceedings - 2015 IEEE 2nd International Conference on Cybernetics, CYBCONF 2015*, 2015, pp. 317–323.
[56] V. Jaganathan, P. Cherurveettil, and P. M. Sivashanmugam, "Using a prediction model to manage cyber security threats," *Sci. World J.*, vol. 2015, pp. 1–5, 2015.
[57] D. J. Musliner, S. E. Friedman, T. Marble, J. M. Rye, M. W. Boldt, and M. Pelican, "Self-Adaptation metrics for active cybersecurity," in *Proceedings - IEEE 7th International Conference on Self-Adaptation and Self-Organizing Systems Workshops, SASOW 2013*, 2014, pp. 53–58.
[58] Homeland Security, "Primer Control Systems Cyber Security Framework and Technical Metrics," 2009.
[59] NSA, "A Framework for Assessing and Improving the Security Posture of Industrial Control Systems (ICS)," National Security Agency, U.S.A, 2010.
[60] P. O'Neill, "Protecting Critical Infrastructure by Identifying Pathways of Exposure to Risk," *Technol. Innov. Manag. Rev*, no. August, pp. 34–40, 2013.
[61] Z. Abbadi, "Security Metrics What Can We Measure ? What is a ' Metric ,'" *Presentation*, 2006. [Online]. Available: https://www.owasp.org/images/b/b2/Security_Metics-_What_can_we_measure-_Zed_Abbadi.pdf. [Accessed: 15-Sep-2016].
[62] A. Ben Aissa, L. B. A. Rabai, R. K. Abercrombie, A. Mili, and F. T. Sheldon, "Quantifying availability in

SCADA environments using the cyber security metric MFC," in *Proceedings of the 9th Annual Cyber and Information Security Research Conference on - CISR '14*, 2014, pp. 81–84.
[63] K. Peuhkurinen, "Plans for a Balanced Scorecard Approach to Information Security Metrics," in *Metricon 3.0.*, 2008.
[64] R. Henning, M. Abrams, J. Kahn, D. Peoples, R. Vaughn, J. Connolly, J. McHugh, and J. Tippett, "Information System Security Attribute Quantification or Ordering (Commonly but improperly known as ìSecurity Metricsî)," in *Workshop on Information Security System Scoring and Ranking*, 2002, pp. 1–70.
[65] J. S. Carson, "Convincing Users of Model's Validity is Challenging Aspect of Modeler's Job," *Ind. Eng.*, vol. 18, no. 6, pp. 74–85, 1986.
[66] S. Robinson, "Simulation model verification and validation: increasing the users' confidence," in *Proceedings of the 1997 Winter Simulation Conference*, 1997, pp. 53–59.
[67] K. El Emam and A. Birk, "Validating the ISO/IEC 15504 measure of software requirements analysis process capability," *IEEE Trans. Softw. Eng.*, vol. 26, no. 6, pp. 541–566, 2000.
[68] T. Dybå, "An Instrument for Measuring the Key Factors of Success in Software Process Improvement," *Empir. Softw. Eng.*, vol. 5, no. 4, pp. 357–390, 2001.
[69] K. El Emam and N. H. Madhavji, "An instrument for measuring the success of the requirements engineering process in information systems development," *Emperical Softw. Eng.*, vol. 1, no. 3, pp. 201–240, 1996.
[70] T. Rosqvist, M. Koskela, and H. Harju, "Software quality evaluation based on expert judgement," *Softw. Qual. J.*, vol. 11, no. 1, pp. 39–55, 2003.
[71] S. Lauesen and O. Vinter, "Preventing Requirement Defects: An Experiment in Process Improvement," *Requir. Eng.*, vol. 6, no. 1, pp. 37–50, 2001.
[72] B. Kitchenham, S. L. Pfleeger, B. McColl, and S. Eagan, "An empirical study of maintenance and development estimation accuracy," *J. Syst. Softw.*, vol. 64, no. 1, pp. 57–77, 2002.
[73] C. Debo, "Preventing Cyberattacks and Data Breaches via Employee Awareness Training and Phishing Simulations," *Website Article*, 2015. [Online]. Available: http://www.schneiderdowns.com/preventing-cyberattacks-data-breaches-employee-awareness-training-phishing-simulations. [Accessed: 14-Jul-2015].
[74] IRM, "Amateyrs attack technology. Professional hackers target people," *Website Article*, 2015. [Online]. Available: https://www.irmplc.com/issues/human-behaviour/. [Accessed: 15-Jun-2015].
[75] Kaspersky-Labs, "KASPERSKY LAB: EMPOWERING INDUSTRIAL CYBER SECURITY," 2015.
[76] UK-Cabinet-Office, "10 Steps to Cyber Security," *Cyber Security Strategy*, 2012. [Online]. Available: https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility/10-steps-summary. [Accessed: 26-Mar-2015].
[77] S. Beecham, T. Hall, C. Britton, M. Cottee, and A. Rainer, "Using an expert panel to validate a requirements process improvement model," *J. Syst. Softw.*, vol. 76, pp. 251–275, 2005.
[78] B. A. Kitchenham, L. Pickard, S. Linkman, and P. Jones, "A framework for evaluating a software bidding model," *Inf. Softw. Technol.*, vol. 47, no. 11, pp. 747–760, 2005.
[79] R. G. Sargent, "VERIFICATION AND VALIDATION OF SIMULATION MODELS," in *Proceedings of the 2010 Winter Simulation Conference*, 2010, no. 2001, pp. 166–183.

Appendix A: Survey Questionnaire Validation Tool

Section A : Demographics Details

A.Q1 How long (in years) have you worked in the operational security aspect of the industry?

❍ _____

Q2 Which of these security capability (knowledge and skill) classifications best describes you?

❍ Security Knowledge
❍ Security Skill
❍ Both Security Knowledge and Skill

Q3 Using a rating range of 1 – 5; 1 being least, and 5 being highest, how do you rate your knowledge, skills, experience, or expertise in security metrics development, security metrics-driven assessment, and general information/cyber-security?

❍ 1
❍ 2
❍ 3
❍ 4
❍ 5

Section B: Evaluation of Framework's Characteristics

A good security metrics development framework should possess/retain the following characteristics:

1. Scope-definitive: Guide the clear outline of targeted system scope.
2. Objective-definitive: Guide the clear delineation of targeted security objectives.
3. Simple: Easy and straightforward to employ or use.
4. Adaptive: Enable the adoption of reviews in response to dynamic changes in scope and objectives.
5. Iterative: Enable repetitions of processes or procedures where necessary.
6. Reliable: Trusted to yield a consistent desirable outcome (metrics)

Q1 To what degree do you consider the above-mentioned framework characteristics relevant and suitable in the contemporary cyber security situation?

	Very High	**High**	**Moderate**	**Low**	**Very Low**
Scope-definitive	❍	❍	❍	❍	❍
Objective-definitive	❍	❍	❍	❍	❍
Simple	❍	❍	❍	❍	❍
Adaptive	❍	❍	❍	❍	❍
Iterative	❍	❍	❍	❍	❍
Reliable	❍	❍	❍	❍	❍

Section C: Framework Feasibility Evaluation

Q1 The proposed OSMD framework for ICS Environment is considered complete in providing adequate means for process and objective scoping.

- ❍ Strongly Agree
- ❍ Agree
- ❍ Disagree
- ❍ Strongly Disagree
- ❍ No Opinion / Don't Know

Q2 How consistent is the level of details given in the proposed OSMD framework?

- ❍ Strongly Consistent
- ❍ Consistent
- ❍ Inconsistent
- ❍ Strongly Inconsistent
- ❍ No Opinion / Don't Know

Q3 How easy do you think it is to understand the path from initial 'security dimension' to final process of 'metrics specification' in the proposed OSMD framework?

- ❍ Strongly Easy
- ❍ Easy
- ❍ Uneasy
- ❍ Strongly Uneasy
- ❍ No Opinion / Don't Know

Q4 How much previous knowledge of security metrics development do you think you need to be able to interpret this framework?

- ❍ Very Much
- ❍ Much
- ❍ Little
- ❍ Very Little
- ❍ No Opinion / Don't Know

Q5 How easy would it be to adapt (add/remove/mend) security target(s), objective(s), and(or) metrics from the proposed OSMD framework?

- ❍ Strongly Easy
- ❍ Easy
- ❍ Uneasy
- ❍ Strongly Uneasy
- ❍ No Opinion / Don't Know

Q6 The level of detail provided by this OSMD Framework can yield metrics that will enable a fair assessment of the security strengths and weaknesses of an ICS domain

- ❍ Strongly Agree
- ❍ Agree
- ❍ Disagree
- ❍ Strongly Disagree
- ❍ No Opinion / Don't Know

Q7 How appropriate is it to include/consider people, process, and technology security attributes/dimensions to gain an overall, system/organisation-wide perspective of security postures and vulnerabilities?

- ❍ Strongly Appropriate
- ❍ Appropriate
- ❍ Inappropriate
- ❍ Strongly Inappropriate
- ❍ No Opinion / Don't Know

Q8 Each Phase and attribute-decomposition in the OSMD framework relates to a relevant security requirement, standard or best practice guide.

- ❍ Strongly Agree
- ❍ Agree
- ❍ Disagree
- ❍ Strongly Disagree
- ❍ No Opinion / Don't Know

Q9 Each Phase and sub-phase of the OSMD framework is easy to understand (i.e., clearly defined and unambiguous).

- ❍ Strongly Agree
- ❍ Agree
- ❍ Disagree
- ❍ Strongly Disagree
- ❍ No Opinion / Don't Know

Section C: Framework Feasibility Evaluation

Q10 How realistic is it for industrial organisations to use this OSMD framework to view their security requirements, generate and use security metrics to understand organisational security capabilities (postures or vulnerabilities)?

- ❍ Strongly Realistic
- ❍ Reaslistic
- ❍ unrealistic
- ❍ Strongly Unrealistic
- ❍ No Opinion / Don't Know

Q11 How easy would it be to adapt (add/remove/amend) this proposed OSMD framework to meet individual and varied industrial operational environments?

- ❍ Strongly Easy
- ❍ Easy
- ❍ Uneasy
- ❍ Strongly Uneasy
- ❍ No Opinion / Don't Know

Q12 How useful would this framework be to the industrial community in the pursuit of operational security assurance?

- ❍ Strongly Useful
- ❍ Useful
- ❍ Not Useful
- ❍ Strongly Not Useful
- ❍ No Opinion / Don't Know

Q13 How useful would this framework be to the academic and research community to guide further developments towards effective operational security assurance?

- ❍ Strongly Useful
- ❍ Useful
- ❍ Not Useful
- ❍ Strongly Not Useful
- ❍ No Opinion / Don't Know

Q14 To what extent do you think the proposed OSMD framework is applicable for yielding desirable security metrics relative to industrial operations scenarios?

- ❍ Strongly Applicability
- ❍ Applicable
- ❍ Not Applicable
- ❍ Strongly Not Applicable
- ❍ No Opinion / Don't Know

A framework for operational security metrics development for industrial control environment

Daniel Ani, Uchenna P.

2018-12-13

Ani UPD, He H, Tiwari A. A framework for operational security metrics development for industrial control environment. Journal of Cyber Security Technology, Volume 2, Issue 3-4, 2018, pp. 201-237

https://doi.org/10.1080/23742917.2018.1554986