Threat Awareness for Critical Infrastructures Resilience

Antonios Gouglidis, Benjamin Green, Jeremy Busby, Mark Rouncefield and David Hutchison
Lancaster University
Lancaster, UK

Stefan Schauer
AIT Austrian Institute of Technology
Vienna, Austria

***Abstract*— Utility networks are part of every nation's critical infrastructure, and their protection is now seen as a high priority objective. In this paper, we propose a threat awareness architecture for critical infrastructures, which we believe will raise security awareness and increase resilience in utility networks. We first describe an investigation of trends and threats that may impose security risks in utility networks. This was performed on the basis of a viewpoint approach that is capable of identifying technical and non-technical issues (e.g., behaviour of humans). The result of our analysis indicated that utility networks are affected strongly by technological trends, but that humans comprise an important threat to them. This provided evidence and confirmed that the protection of utility networks is a multi-variable problem, and thus, requires the examination of information stemming from various viewpoints of a network. In order to accomplish our objective, we propose a systematic threat awareness architecture in the context of a resilience strategy, which ultimately aims at providing and maintaining an acceptable level of security and safety in critical infrastructures. As a proof of concept, we demonstrate partially via a case study the application of the proposed threat awareness architecture, where we examine the potential impact of attacks in the context of social engineering in a European utility company.**

Keywords—critical infrastructures; resilience; threat awareness

I. INTRODUCTION

The protection of critical infrastructures is considered to be essential for the orderly functioning of a society, its economy and national sovereignty [1]: nations are actively looking towards the protection of critical infrastructures. Further, the European Commission and United States Department of Homeland Security both emphasise the importance of critical infrastructures and the need for their protection. Protection is concerned with ensuring the functionality, continuity and integrity of infrastructures to deter, mitigate and neutralise a threat, risk or vulnerability [2]. Research on the emerging area of critical infrastructures has resulted in providing rules, legislation and good practice guidelines towards their protection. Such research is usually funded by the European Commission in Europe, and by the Department of Homeland Security in United States. Specifically, the Council of European Union identified the sectors of energy and transport to be of vital strategic importance [2]. The energy sector includes the subsectors of electricity, oil and gas. Additionally, the transport sector includes the subsectors of road, rail, air, inland waterways transport as well as the ocean and short-sea shipping and ports. Industrial Control Systems (ICS) are used in utility networks for the monitoring, control and automation of operational plants. Due to the importance of critical infrastructures, the European Commission introduced in [2] an action plan where it proposes the development of a framework consisting of five pillars, namely: preparedness and prevention; detection and response; mitigation and recovery; international cooperation; criteria for the ICT sector. Additionally, the U.S. Department of Home Security defined in [3] the need for a resilience framework in critical infrastructures, focused on the abilities of robustness, resourcefulness, rapid recovery, and adaptability. Providing protection in terms of security, safety and resilience in utility networks is inherently considered to be of vital importance. This is also due to the fact that in the past few decades we have experienced a significantly increased demand on utilities resulting in an increased rate of automation in network controls and interconnections. This also resulted in increasing the dependencies amongst various kinds of utility networks.

Having identified the importance of protecting critical infrastructures, we undertook a holistic examination of protective means. Our research was initiated by performing an investigation of trends that bear the potential to become future threats, and propose a future protective mean against them. To the best of our knowledge, such an approach towards the protection of critical infrastructures is absent. Specifically, the former investigation will result in providing proactive knowledge concerning threats mostly in utility networks, and facilitate the identification of risks since threats are an important element in risk assessment [1]. That information will operate as a stepping-stone towards providing resilience in ICS via future protection based on threat awareness [4]. It is noteworthy that in existing approaches technical threats are examined, leaving other threat factors underemphasised (e.g., organisation policies, human behaviour). Yet, in most cases, situation awareness (SA) stages are not clearly defined, and thus they impose a high level of ambiguity with regard to '*situational awareness*', which is often confused with the term '*situation recognition*' (the latter being the first stage towards achieving SA).

The structure of the remainder of this paper is as follows. Section II provides information on related work. Section III clarifies on the methods used for gathering trends and threats. In section IV, we provide prerequisite information on resilience and the fundamentals of SA. In section V, we present our threat

awareness approach for utility networks, and demonstrate the application of the proposed architecture through a case study in section VI. Conclusions are discussed in section VII.

II. Related Work

SA has received much attention from researchers and organisations for its application in achieving cyber security and has been lately proposed by ICS-CERT[1] to provide a basic step toward securing critical infrastructures. This statement has been reinforced in a recent systematic literature review performed in [5], where a set of application areas for SA have been identified. These areas include ICS, command and control systems, and operations management. Most of the research using SA has been in the context of ICS. SA is also examined in [6] under the context of critical infrastructures. Specifically, a list of promising approaches for addressing SA in critical infrastructure are examined and compared. In the following, we elaborate on a list of representative work done with regard to achieving cyber security in ICS via SA.

An SA system based on information collected from critical infrastructure is presented in [7]. The authors elaborate on a concept and system that is capable of providing critical infrastructure under a common operating picture. This is done to provide decision-making at different management layers. Their proposed SA for critical infrastructure and networks (SACIN) framework combines existing approaches, i.e., agent-based brokered architecture and data fusion. SACIN has been implemented and evaluated, as well. Nevertheless, topics as dependencies amongst networks and information flow are considered as future research for the project.

A wide-area situational awareness (WASA) framework for the protection of critical infrastructures is proposed in [8]. The WASA framework provides a hybrid solution that includes the presence of humans for the monitoring of emergency situations, and context awareness to protect functional services. The need for monitoring systems in a distributed manner led to the use of existing technologies (i.e., the Internet) as a mean to extend it. Specifically, WASA consists of two phases, viz. setup and commissioning, and development. The former is responsible for configuring and initialising the framework, and the latter provides a set of services (e.g., normalisation of data, prevention and detection, etc.). WASA is considered to be a framework, and therefore, implementation and testing is yet to be confirmed.

A distributed agent-based protection system for smart grids is proposed in [9]. SA was identified as being able to enhance the security and reliability in power transmission systems. Therefore, the use of a distributed protection approach was perceived as a mean to gain SA. The proposed approach included the demonstration of a distributed protection system load shedding strategy, and reputation-based trust and retransmission mechanisms for the detection of cyber-attacks.

An SA architecture for smart grids is proposed in [10]. The authors of the paper propose a system's architecture that provides SA for SCADA devices and their operations in a smart grid environment. This architecture is intended to provide topological and status information of SCADA devices, and information on devices in the smart grid environment. This information will eventually help in detecting security incidents in smart grid environments. Main components of the architecture consist of a set of network sensors; a SCADA gateway; a database, and a control centre. In particular, the gateway is used to collect all data gathered by sensors; information is stored using a schema in the database; the command centre is used as an interface and interprets information provided by the database by performing state based traffic analysis.

In addition to these research approaches there are several other towards achieving SA [5], which mostly make use of anomaly detection algorithms, intrusion detection, identification of networks traffic regularity, etc. Nevertheless, none of them cope with issues stemming from a non-technical point of view, and are based on the fusion of data gathered from various sensors or agents [6]. Furthermore, in the examined approaches there is no explicit reference to information exchange mechanisms amongst other networks to elevate SA (except from SACIN and WASA), which is something that may result in achieving a higher level of security and resilience. Information sharing consist of an important topic, which has been also strongly recommended in the incident handling guidelines provided by the National Institute Standards and Technologies (NIST) in [11], and in European Union's Cyber Incident Reporting System, overviewed by ENISA in [12].

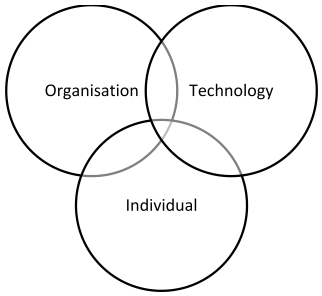

Fig. 1. Viewpoints for utility networks

III. Current and Emerging Trends and Threats

In this section, we provide information on the methods we have used for gathering and analysing trends and threats, as well as, information about their quantification.

A. Methods

The method used for collecting information with regard to technological trends and threats follow the pattern of information collection, analysis and collation. For the analysis of technological trends and future threats, we have used a viewpoint approach. This was applied to enable a broader view of the system, i.e., a representation of the whole system from the perspective of a related set of concerns. The viewpoints we propose for application in utility networks are: Organisation, Technology, and Individual (OTI). OTI is partially derived from IAEA and depicted in Fig. 1. More specifically, the three viewpoints are concerned with: *The organisation viewpoint*, with

[1] https://ics-cert.us-cert.gov/monitors/ICS-MM201404

the groups of people who work together in an organised way for a shared purpose as well as any type of policies, processes and procedures in the organisation; *The technology viewpoint*, with the implemented technologies in a system including the software, hardware and network components, as well as any type of communication amongst them; *The individual viewpoint*, with the way a single person or thing acts or behaves in a particular situation or under particular conditions.

Regarding the analysis of gathered information, we applied a basic qualitative research analysis. This approach suits for research problems characterised by the following: the sample size of data can be relatively small; the collection of data can be based on that of OSINT; the interpretation of data can be based on a combination of researchers' perspective and data collected. Specifically, in this paper, the classification of data was performed on the basis of the proposed OTI viewpoints, which involved the use of an eclectic approach to match the examined data. During this process, the identified trend or threat is mapped onto one of the viewpoints. This is done by forming a series of questions to identify the source of each trend/threat. Examples of questions are: Is the trend in conflict with any of the organisation's policies? Does the threat stem from a hardware fault? Is the threat a result of employees' behaviour? (… etc.). In case the categorisation is not clear, the definition of the threat/trend has to be refined and re-examined on the basis of the defined questions.

In order to identify the emerging technological trends and threats, we conducted a review of the latest information provided by major consulting firms and organisations. The information refer to both ICS and IT systems since there is increasing integration between them. Being aware of the latest information not only helps in achieving a better view of the trends and threats for utility networks but will also provide hints towards achieving appropriate SA.

B. Trends and threats

A trend can be defined as a general development or change in a situation or in the way that people behave. A technological trend consists of a trend relating to, or involving technology. An example of a technological trend could be that of '*Bring Your Own Device*' (BYOD) policy, which many organisations are pursuing to support. In the following, we provide quantitative information on technological trends, as identified by major consulting firms and organisations. Regarding the analysis of trends, we gathered information from reports provided by Deloitte; PriceWaterhouseCoopers; Ernst & Young; KPMG; Gartner; Computer Economics and Accenture. Exploring in more detail the various technological trend lists provided by these firms, we extracted many similarities amongst them. This is something to be expected since all trends stem from the latest individuals', organisations' and technological need, and also helps in identifying the main areas that the majority of businesses are focusing on for the next three years. Table I (middle column) shows the number of trends categorised in each viewpoint. Specifically, the results imply that the majority of trends fall into the '*technology*' area; '*organisation*' comes second and '*individual*' follows in third place.

Regarding the analysis of trends, they were examined in the context of business and IT systems since none of the reports refer explicitly to ICS. On the contrary, governments and organisations have already identified the need for examining threats in ICS. Specifically, information regarding threats in ICS was extracted from reports by ENISA [1, 13], NIST [14] and ISO/IEC PDTR 13335-1[2]. It is noteworthy that the human factor (conceived as '*individual*' in OTI) has been characterised as a challenge due to humans' lack of interest and/or understanding of security issues in ICS. Therefore, having examined the threats identified in ICS by the above mentioned reports, we also categorised them according to the OTI viewpoints. The number of threats in each viewpoint is depicted in Table I (last column). Specifically, it is shown that the human factor consists of a major threat for ICS; technology turns out to be the second most important source of threat, followed by organisational issues. Our results appear to be in line with recent major security incidents such as the attack on the German steel mill and the attack on the Ukrainian electric power industry occurred in late 2014 and 2015, respectively. In both cases, the attackers initiated spear phishing attacks to gain access to the production networks, something that indicates the importance of human behaviour in critical infrastructures.

TABLE I. OTI BASED CLASSIFICATION OF TRENDS AND THREATS

Viewpoint	*Num. of trends*	*Num. of threats*
Organisation	35	10
Technology	**37**	21
Individual	17	**25**

IV. PREREQUISITE INFORMATION

This section provides prerequisite information with regard to our approach towards achieving resilience in critical infrastructures. Specifically, we consider a resilience strategy in place to cope with the emerging challenges in critical infrastructures. Our resilience strategy is capable of embracing (cyber) situational awareness. The latter sets its own processes, in order for a threat awareness architecture to be based on solid and concrete phases and to provide eventually the adequate level of security and safety required by critical infrastructures. In the following, we elaborate on resilience and our resilience strategy, provide information about (cyber) situational awareness and its main phases. This information set the basis for the threat awareness architecture proposed in section V.

A. Resilience strategy

The term '*resilience*' has been used in the past several decades in different ways to describe the ability of materials, engineered artefacts, ecosystems, communities, etc., to adapt to changes, and is also adopted by sciences (e.g., psychology) and organisations (e.g., business continuity lifecycles) [15]. Although the etymology of resilience clearly refers to the capacity to recover from difficulties, a single agreed definition is currently elusive. This is mostly because of the complexity and diversity of contemporary socio-technical systems, which eventually resulted in the many definitions of resilience. Our resilience strategy,

[2] http://www.iso.org/iso/catalogue_detail.htm?csnumber=39066

entitled D^2R^2+DR (Defend, Detect, Remediate, Recover, and Diagnose and Refine), defines resilience as *'the ability of a network or system to provide and maintain an acceptable level of service in the face of various faults and challenges to normal operation'* [16]. Defend, Detect, Remediate, and Recover consist processes of an internal loop process and Diagnose and Refine processes of an outer loop. In more detail, it is: Defend against challenges and threats to normal operation; Detect when an adverse event or condition has occurred; Remediate the effects of the adverse event or condition; Recover to original and normal operations; Diagnose the fault that was the root cause; and Refine behaviour for the future based on past D^2R^2+DR cycles.

B. Situational awareness

SA is defined by the Committee on National Security Systems as '*within a volume of time and space, the perception of an enterprise's security posture and its threat environment; the comprehension/meaning of both taken together (risk); and the projection of their status into the near future*'. Cyber SA can be defined as the part of SA that is concerned with cyber environments [5]. Following, we elaborate on cyber SA in utility networks, and further continue with the introduction of threat awareness (TA) architecture in the context of cyber SA. The latter is able to identify and assess threats; exchange threat information; and help in decision-making with regard to risks. To the best of our knowledge, none of the existing approaches in SA and ICS are coping with the incorporation of non-technical information, i.e., threat information that may stem also from an organisational or individual's perspective. SA and resilience are examined in [4, 17] as a mean towards providing proactive network resilience management. In this paper, we examine SA in the context of our resilience strategy as a mean towards providing threat awareness in critical infrastructures.

C. Cyber situational awareness

Utility networks operate in complex environments where interactions take place amongst the assets of the network, the participating people and the ICS. Any of these might be vulnerable to various types of threats, and therefore, become a risk for the network. ENISA identified in [1] a list of 15 threats in the emerging technology area of critical infrastructures. Although this information is valuable in terms of current and emerging threats in ICS, it is not possible to fully cover the wide variety of ICS systems and their evolving environment. Therefore, in the context of providing a holistic approach towards protecting utility networks, we propose the application of the OTI viewpoint-based approach as a first step towards achieving cyber SA in utility networks. Cyber SA is crucial to apply in networks in order to safeguard sensitive data, sustain fundamental operations, and protect infrastructures. Furthermore, cyber SA was identified as an attractive approach by the FOI Swedish Defence Research Agency, which is capable of copying with the complexity provided by ICS [5]. Cyber SA can be applied as a three-phase process [18, 19]. The main phases are: situation recognition, situation comprehension and situation projection. Each one of these phases consists of several aspects [19]. More specifically, situation recognition includes the aspects of being aware of the current situation and of the quality of the collected situation aware information items, as well as, the knowledge, intelligence and decisions that are derived from these information items. Situation comprehension includes the aspects of being aware of the impact of an attack, the adversary behaviour and of why and how the current situation is caused. Lastly, situation projection includes the aspects of being aware of how situations evolve and assesses plausible futures of the current situation. The application of cyber SA in utility networks will help in achieving an accurate awareness of these networks and a complete understanding of the operations that can take place in them. Performing a proper assessment of the operations in utility networks will also help to discover potential weak areas and vulnerabilities, and to assess potential threats to prevent them in their early stage of dispersion.

V. Threat Awareness Architecture

Threat Awareness (TA) is considered to be an essential component of a security programme. Symantec defines it as '*the monitoring, identification, analysis, and notification of potential threats or vulnerabilities that can cause harm to system and network environments*'. The term is enriched by MITRE, stating that TA needs also to incorporate knowledge of external threat

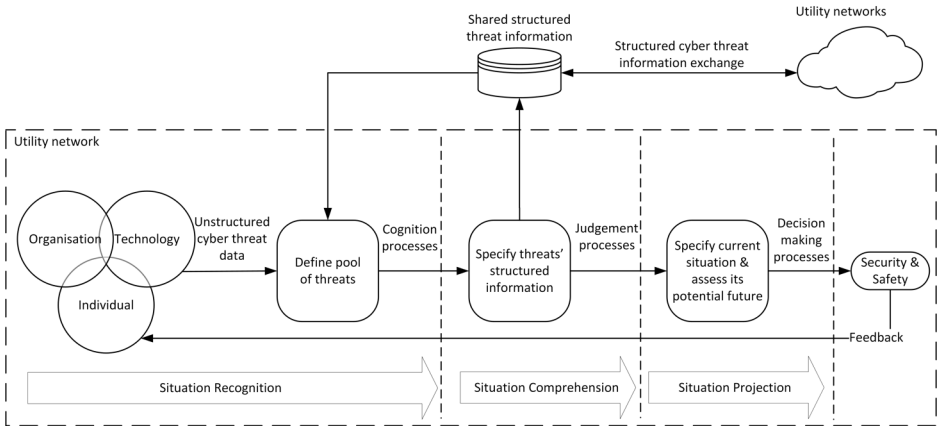

Fig. 2. Threat awareness for utility networks

information, and to participate in cross-industry or cross-government communities to share information regarding threats' possible indicators and warnings. In this section, we further elaborate on a TA architecture that is able to incorporate all the above characteristics. The architecture is based on the SA stages described in [19]. Therefore, the distinct stages for TA are divided into those of situation recognition, situation comprehension and situation projection. The proposed TA architecture for application in ICS is depicted in Fig. 2.

The first stage consists that of situation recognition. During this stage, two requirements are fulfilled, i.e., being aware of the current situation, and ensure the quality of the collected situation aware items [19]. These items should be characterised by truthfulness, completeness and freshness. In order for the requirements to be accomplished, we propose to initially apply the OTI viewpoints to be aware of the current trends that will lead to the exposure of emerging threats within the examined utility network. This step requires a high cognitive knowledge level of the organisation's procedures, technical infrastructure and individuals. Our research work under this stage includes, amongst other, the implementation of a framework that supports the detection of anomalies by using appropriate techniques at the different levels of critical infrastructure and service [20]. At this stage, it is possible to incorporate threat information from other utility networks. This consists of an operation that could be automated and will provide better protection due to the existence of a collectively stronger cyber-security ecosystem. Exchange of threat information should be based on existing data exchange formats for the sharing of threat intelligence. Such solutions are OpenIOC, TAXII™, and RID. More information on existing solutions can be found in [21]. Existing threat catalogues can be incorporated, nevertheless, the complexity of this type of socio-technical systems may require additional processes such as the performance of interviews with the operators or ethnographic studies to populate custom threat catalogues per case. These steps may help in the creation of a threats pool. The latter could have two different sources of input. The first consists of threats identified within the utility network using the OTI viewpoint approach. The second source of input contains threats retrieved from other networks. The next step includes the use of a set of cognition processes to transit to the second stage of situation comprehension. The cognition processes in this stage will try to describe the type of the identified threats; their source, target, etc., that is information required for providing structured information for newly identified threats.

In the second stage of the TA architecture, we work towards achieving situation comprehension. As input to this stage, we assume the knowledge information created from its prior stage. The importance of this information is two-fold; firstly, newly defined threats are pushed to a central threat repository in order to share threat knowledge. For the definition of the structured threat information existing languages could be used, such as STIX™ and IODEF. Secondly, the structured threat information is used in a series of judgement processes. The latter aim to facilitate threat assessment, which includes analysing their behaviour and helping to resolve questions with regard to the threats' origin and purpose. Such judgement processes include, but are not limited to, vulnerability analysis and threat assessment; attack trend and intent analysis; causality analysis, and forensics [19]. These judgement processes can result in gradually increasing the awareness of a situation in utility networks. For instance, not all of the defined threats might be exploitable in the infrastructure of a utility network. That will be the case if the vulnerability for exploiting a specific threat is absent. This inputs valuable information to the next phase of the threat awareness architecture. It is worthy to note that during the phase of situation comprehension, various types of security information, not only related to threats, but also related to vulnerabilities, can be identified and described in existing formats (e.g., CVE, OSVDB, CVRF). This information can be examined on the basis of the infrastructures, and therefore, could also be collected by applying the OTI approach. The latter will result in the collection of vulnerabilities not only restricted to the technical aspects of an infrastructure (e.g., technical vulnerability, or misconfiguration in software, systems, or networks), but instead will additionally expose, include and convey organisational and individual based vulnerabilities.

The phase of situation projection is concerned with being aware of how a threat might evolve to assess plausible futures. This information helps in decision-making, i.e., a cognitive process in selecting an action that will eventually lead the system in a secure and safe state. Security and safety consist of the main objectives of the decision making process. For instance, if during the previous phase an exploitable threat is identified in an infrastructure, it will require from the current phase to assess plausible futures of it, and also to get a decision with regard to its mitigation. The latter is required for reaching a secure and safe state. If a threat is not exploitable in an infrastructure, the thread can be considered as not real, and therefore, assume that the system is in a secure and safe state. Consequently, after ensuring the secure and safe state of the system, the new state operates as a feedback for the threat awareness process. Within this feedback, it also has to be ensured that the infrastructure does not evolve into a state, in which some threats become exploitable again due to mitigation actions taken in this phase. The proposed architecture is different from existing solutions since it is not bounded only to information sharing, but instead is looking towards providing a holistic approach to gain threat awareness. Therefore, solutions such as the Malware Information Sharing Platform and Microsoft's Interflow could be incorporated to provide a concrete threat awareness platform.

After elaborating on the type of processes that can take place within each of the main phases of TA, we provide a mapping between the latter and our resilience strategy. TA provides a solution for some of the steps of D^2R^2+DR, and therefore, a complete resilience solution may require the existence of additional components to introduce functionalities as defend measures (e.g., by setting in place security controls), remediation and recovery. Hence, the capabilities of the TA architecture are mainly concentrated on the detection of challenges and threats via situation recognition; the provision of diagnostic information through situation comprehension; and, the refinement of future behaviours of systems via situation projection. Nevertheless, we have presented in [17], how the remaining steps of the resilience

strategy can be covered in an overall resilience architecture by using external components to provide the additional set of services.

VI. Case Study

In [22] we elaborated on a case study where we examined and analysed the potential impact of attacks in the context of social engineering in a European utility company. In this paper, we map the processes we followed in [22] with the stages in the proposed TA architecture. Nevertheless, detailed information about the assurance techniques used and qualitative metrics evaluated in the case study are available in [22].

Since the TA architecture considers issues across each OTI viewpoint, the inclusion or adaptation of any method that could support them was vital. While existing methods [23-27] provide interesting insight into the assessment of security, it appears some may face challenges when considering multiple OTI viewpoints. Through basic adaptation, the method in [28] appears to provide a good starting point. Specifically, that includes the application of the Mean Time-to-Compromise (MTTC) metric [28], i.e., an attack graph that highlights nodes within the ICS, and their accompanying MTTC. Attack paths can then be generated, including also the total time to compromise target nodes. Following a holistic view of ICS security [29], it is possible also to cover systems/devices residing in levels 0-5 of the Purdue model [30]. Considering the MTTC metric for our assessment, we applied the following steps to perform an assessment of a utility company: (1) system architecture review; (2) shared threat information review; (3) e-mail access review; (4) conceptual social engineering (malicious e-mails) review; (5) technical vulnerability assessment; (6) calculation of MTTC for each system node; (7) attack graph generation based on specified target node (Supervisory Control and Data Acquisition (SCADA) workstation); (8) overlay of ICS levels (0-5) onto the attack graph; and (9) highlighting the nodes susceptible to selected social engineering attack vectors (malicious e-mails). With regard to the mapping of the previous steps into the TA architecture: steps 1-3 map to the phase of situational recognition and steps 4-9 map to the phase of situation comprehension. Once completed, the outputs can be used during the situation projection stage as a baseline on which to review any prospective changes. This includes the addition/removal of nodes, security controls, etc. In overlaying all applicable ICS levels (step 7), we extend on the work by [31], providing further granularity as discussed in [29]. Applying the results from step 3 in step 9, demonstrates the flexibility of the proposed approach to include non-technical challenges. Steps 3, 4 and 9 were an output of step 2 in which shared threat information suggests ICS could become targeted via e-mail based attacks.

The result of the assessment process was the generation of a MTTC attack, as depicted Fig. 3. The shortest MTTC path is highlighted with blue arrows, in both a penetrative and destructive context (i.e., take control of the system, or cause it to fail). The oval nodes represent the nodes capability to receive e-mails. Via the performance of interviews with individuals in the examined organisation, we identified that 41% of users would action the malicious e-mail (i.e., phishing and spear-phishing) content. This increased to 50% when the sender of the e-mail was a colleague. In the case of a successful attack, the perimeter breach could be bypassed, providing direct internal system access, and thus, reducing the shortest attack path by approximately 47%.

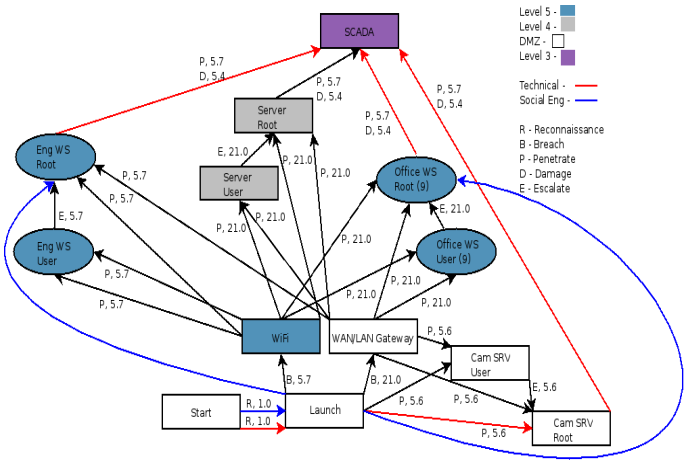

Fig. 3. Compromise graph [22]

In Table II, we provide a short threat catalogue in the context of the OTI viewpoints, prepared as an output of the assurance techniques applied in the case study. For privacy and safety reasons, a number of threats and their detail have been omitted or simplified. Specifically, the information includes some of the assets in the utility network; threats to them; identified vulnerabilities and the potential impact of successfully exploiting a vulnerability. Assets are mapped with only few of the components referred to in Fig. 3 for the reasons stated above.

VII. Conclusion

Investigating the nature and diversity of trends and threats in utility networks has amplified our understanding of the potential

TABLE II. Threat Catalogue

Viewpoint	*Asset*	*Threat*	*Vulnerability*	*Impact*
Organisation	Network component	Missing password policy	Access to network component's control panel using default credentials	Reconfiguration of component
Technology	SCADA workstation	Software vulnerabilities or errors	Prone to multiple vulnerabilities	Disclosure of information; privilege escalation; DoS conditions
	Camera server	Software vulnerabilities or errors	Prone to remote code execution vulnerability	Execution of arbitrary code; DoS conditions
Individual	Operators	Social engineering	Prone to spear-phishing attacks	Provide access to internal network components

dangers these may introduce in critical infrastructures. The application of Organisation, Technology, and Individual (OTI) viewpoints has shown that the majority of trends fall under the category of *'technology'*, but *'individuals'* clearly pose a significant threat to utility networks. Although this might be expected, its confirmation via OTI indicates that their identification could potentially be systematised. Additionally, the proposed Threat Awareness (TA) architecture may operate as a future protective means in the context of a resilience strategy. Overall, we have shown that the protection of critical infrastructures is not a single but rather a multi-variable problem, which requires the incorporation of information stemming from various viewpoints of a networked system. Furthermore, the identification and assessment of threats would not be sufficient to introduce the appropriate level of resilience in utility networks. The proposed TA architecture embraces existing technologies and processes in the context of our resilience strategy to fulfil that objective. Through a case study, we demonstrated the use of the TA architecture as an orchestration architecture for existing risk assessment methods, which could provide meaningful and easy-to-understand results to industrial control systems operators. Finally, we have already engaged in research towards the automation of some of the TA processes [20], which we anticipate will result in improving the overall efficiency and effectiveness of our approach.

ACKNOWLEDGMENT

The research leading to these results has received funding from the European Union Seventh Framework Programme under grant agreement no. 608090, Project HyRiM (Hybrid Risk Management for Utility Networks).

REFERENCES

[1] ENISA, "ENISA Threat Landscape 2013 - Overview of current and emerging cyber-threats," 2013.

[2] E. Commission, "Council Directive 2008/114/EC," Official Journal of the European Union, vol. L345, p. 8, 2008.

[3] A. R. Berkeley III, M. Wallace, and C. COO, "A framework for establishing critical infrastructure resilience goals," Final Report and Recommendations by the Council, National Infrastructure Advisory Council, 2010.

[4] M. Liu, T. Feng, P. Smith, and D. Hutchison, "Situational Awareness for Improving Network Resilience Management," in Information Security Practice and Experience, ed: Springer, 2013, pp. 31-43.

[5] U. Franke and J. Brynielsson, "Cyber situational awareness – A systematic review of the literature," Computers & Security, vol. 46, pp. 18-31, 2014.

[6] V. Abate, L. Adacher, and F. Pascucci, "Situation awareness in critical infrastructures," International Journal of Simulation and Process Modelling, vol. 9, pp. 92-103, 2014.

[7] J. Timonen, L. Laaperi, L. Rummukainen, S. Puuska, and J. Vankka, "Situational awareness and information collection from critical infrastructure," in Cyber Conflict (CyCon 2014), 2014 6th International Conference On, 2014, pp. 157-173.

[8] C. Alcaraz and J. Lopez, "Wide-area situational awareness for critical infrastructure protection," Computer, vol. 46, pp. 30-37, 2013.

[9] K. J. Ross, K. M. Hopkinson, and M. Pachter, "Using a distributed agent-based communication enabled special protection system to enhance smart grid security," Smart Grid, IEEE Transactions on, vol. 4, 2013.

[10] A. Mavridou and M. Papa, "A situational awareness architecture for the smart grid," in Global Security, Safety and Sustainability & e-Democracy, 2012, pp. 229-236.

[11] P. Cichonski, T. Millar, T. Grance, and K. Scarfone, "Computer Security Incident Handling Guide. Recommendations of the Natioanl Institue of Standards and Technology," 2012.

[12] M. Dekker, C. Karsberg, and B. Daskala, "Cyber Incident Reporting in the EU. An overview of security articles in EU legislation," 2012.

[13] ENISA, "Smart Grid Threat Landscape and Good Practice Guide," 2013.

[14] NIST, "Guide to Industrial Control Systems (ICS) Security," 2014.

[15] E. Hollnagel, D. D. Woods, and N. Leveson, Resilience engineering: Concepts and precepts: Ashgate Publishing, Ltd., 2007.

[16] J. P. Sterbenz, D. Hutchison, E. K. Çetinkaya, A. Jabbar, J. P. Rohrer, M. Schöller, et al., "Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines," Computer Networks, vol. 54, pp. 1245-1265, 2010.

[17] M. Liu and D. Hutchison, "Towards Resilient Networks Using Situation Awareness," in 12th Annual Postgraduate Symposium on Convergence of Telecommunications, Networking and Broadcasting (PGNet 2011), 2011.

[18] G. Tadda, J. J. Salerno, D. Boulware, M. Hinman, and S. Gorton, "Realizing situation awareness within a cyber environment," in Defense and Security Symposium, 2006, pp. 624204-624204-8.

[19] P. Barford, M. Dacier, T. G. Dietterich, M. Fredrikson, J. Giffin, S. Jajodia, et al., "Cyber SA: Situational awareness for cyber defense," in Cyber Situational Awareness, 2010, pp. 3-13.

[20] A. Gouglidis, S. N. Shirazi, S. Simpson, P. Smith, and D. Hutchison, "A Multi-Level Approach to Resilience of Critical Infrastructures and Services," in International Conference on Telecommunications, 2016.

[21] ENISA, "Detect, SHARE, Protect. Solutions for Improving Threat Data Exchange among CERTs," 2013.

[22] B. Green, D. Prince, J. Busby, and D. Hutchison, "The impact of social engineering on Industrial Control System security," in ACM Workshop on Cyber-Physical Systems Security & Privacy (CPS-SPC), 2015.

[23] L. Pièrre-Cambacédès and M. Bouissou, "Beyond attack trees: dynamic security modeling with Boolean logic Driven Markov Processes (BDMP)," in Dependable Computing Conference, 2010 European, 2010, pp. 199-208.

[24] P. Ralston, J. Graham, and J. Hieb, "Cyber security risk assessment for SCADA and DCS networks," ISA transactions, vol. 46, pp. 583-594, 2007.

[25] D. Kundur, X. Feng, S. Liu, T. Zourntos, and K. L. Butler-Purry, "Towards a framework for cyber attack impact analysis of the electric smart grid," in Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on, 2010, pp. 244-249.

[26] D. Kundur, X. Feng, S. Mashayekh, S. Liu, T. Zourntos, and K. L. Butler-Purry, "Towards modelling the impact of cyber attacks on a smart grid," International Journal of Security and Networks, vol. 6, pp. 2-13, 2011.

[27] W. Boyer and M. McQueen, "Ideal based cyber security technical metrics for control systems," in Critical Information Infrastructures Security, 2008, pp. 246-260.

[28] M. A. McQueen, W. F. Boyer, M. A. Flynn, and G. A. Beitel, "Time-to-compromise model for cyber risk reduction estimation," in Quality of Protection, 2006, pp. 49-64.

[29] B. Green, D. Prince, D. Hutchison, U. Roedig, and J. Busby, "Socio-technical security analysis of industrial control systems (ICS)," in International Symposium for ICS&SCADA Cyber Security Research, 2014.

[30] P. Didier, F. Macias, J. Harstad, R. Antholine, S. A. Johnston, S. Piyevsky, et al., "Converged Plantwide Ethernet (CPwE) Design and Implementation Guide," CISCO Systems and Rockwell Automation, pp. 252-253, 2011.

[31] D. J. Leversage and E. J. Byres, "Comparing electronic battlefields: Using mean time-to-compromise as a comparative security metric," in Computer Network Security, 2007, pp. 213-227.