http://dx.doi.org/10.14236/ewic/ICS2016.5

Ontology and life cycle of knowledge for ICS security assessments

Christopher Tebbe
Faculty I – Electrical Engineering and Information Technology,
University of Applied Sciences and Arts Hannover,
Ricklinger Stadtweg 120,
30459 Hannover, Germany
christopher.tebbe@hs-hannover.de

Karl-Heinz Niemann
Faculty I – Electrical Engineering and Information Technology,
University of Applied Sciences and Arts Hannover,
Ricklinger Stadtweg 120,
30459 Hannover, Germany
karl-heinz.niemann@hs-hannover.de

Alexander Fay
Institute of Automation Technology, Helmut Schmidt University / University of the Federal Armed Forces,
Holstenhofweg 85, 22043 Hamburg, Germany
alexander.fay@hsu-hh.de

Industrial Control Systems (ICS) succumb to an ever evolving variety of threats. Additionally, threats are increasing in number and get more complex. This requires a holistic and up-to-date security concept for ICS as a whole. Usually security concepts are applied and updated based on regularly performed ICS security assessments. Such ICS security assessments require high effort and extensive knowledge about ICS and its security. This is often a problem for small and medium-sized enterprises (SME), which do not have sufficient respective sufficiently skilled human resources. This paper defines in a first step requirements on the knowledge needed to perform an ICS security assessment and the life cycle of this knowledge. Afterwards the ICS security knowledge and its life cycle are developed and discussed considering the requirements and related work.

Keywords: ICS Security, Security Ontology, Security Knowledge, Knowledge Life Cycle.

1. INTRODUCTION

In the last years industrial control systems (ICS) have become a popular aim of attackers of various kinds. Because of the complex infrastructure including many components ICS provide a wide range of targets. This is a major challenge for plant owners and operators. Current trends like office IT adoption, Cyber-Physical-Systems and the Internet of Things aggravate the situation as well, as they ease the access to the ICS from the internet. To improve the security of an ICS, security assessments are a necessity. The execution of such assessments implies a high effort and extensive knowledge. This is challenging, in particular for small and medium-sized enterprises (SME). At this point knowledge based systems (KBS) promise to automate security assesments and to automatically generate security concepts for ICS, although most of them are not mature yet. In this paper the knowledge necessary to determine all kinds of possible threats and necessary measures during ICS security assessments is described. Further the life cycle of the knowledge needed to perform ICS security assessments (called ICS security knowledge in the following) and the influencing entities need to be described. This allows a more efficient maintenance and application of the knowledge, which promises an up-to-date and consistent knowledge and security concept at any time. In addition it might be used for a further automation of the ICS security knowledge handling in the future.

In this paper we first give in section 2 a short overview of related work, followed by a discussion of requirements in section 3. In section 4 a multi-layered approach for representing the ICS security knowledge is presented. The life cycle of the security knowledge, including influencing entities, is discussed in section 5. The paper ends with a conclusion in section 6.

2. RELATED WORK

Security assessments are a vital issue for office IT as well as ICS. There is significant previous work available concerning the security knowledge which is necessary to perform an office IT security assessment (Blanco et al., 2011; Singh and Pandey, 2014; Nguyen, 2011), and in the works of (Fenz and Ekelhart, 2009; Tsoumas and Gritzalis, 2006; Aime and Guasconi, 2010), all required knowledge elements are described.

***Table 1:** Defined content of ICS security knowledge based on requirement sources*

Content	Explanation
Assets	*The term asset outlines all parts of an ICS which have to be examined during a security assessment. The goal is to identify security controls for all assets to reduce their threat level to a tolerable risk. This part of the knowledge can include ICS components, communication relations, software incl. configuration, Know-How, legal claims, etc.. Many of the requirement sources demand asset inventories, which hold all information of ICS, necessary for conducting security assessments.*
Plant Information	*The central part of a plant are its components including media, information systems, control systems and communication solutions on the technical side and the process, know-how, recipes and information on the logical side. All this information is necessary to identify threats and vulnerabilities, assess risks and apply security controls to.*
External Influences	*Because of the surrounding world, external influences like regulations, enterprise requirements and goals need to be considered. Additionally the environment like weather, hazardous zones and the infrastructure like buildings, pipes and wiring need to be considered for a security assessment, too.*
Safety	*A critical item in the operation of an ICS is its safety. Because both security incidents and security controls can harm the function of safety instrumented systems, safety (concepts and requirements) has to be a central element of a security assessment.*
Threat	*The generic item threat includes information covering the threat landscape of an ICS and its assets. Besides describing properties of possible threats and attackers, vulnerabilities and there causes are part of the information, too. Additionally risk needs to be contained in order to assess the security incident likelihood and the threat level which is acceptable in terms to security objectives.*
Security Objective	*The security objective determines which properties of an asset need to be protected by a security control. The central security objects of an ICS are availability, integrity and confidentiality (in this order). Newer publications add safety to the list.*
Security Control	*Security controls are used to reduce possible risks for security incidents to an acceptable level. There are organisational controls like policies or trainings and technical controls like Anti-Malware or installation of patches. Some controls need additional background processes in order to keep them up-to-date like Patch-Management.*
Entity	*This required information represents entities (human or organisations) which need to be represented as part of the security assessment. Possible entities are a person or department responsible for an asset or a security control, a target (person or group) of a security control (e.g. security training, password policy), a vendor or an attacker who tries to compromise an asset, etc..*
Relation	*Relations are a very important part of the knowledge. Relations link the other information in a way that entities like KBS are able to draw conclusions from the knowledge. In case of a security assessment the relations are used to infer which security control has to be applied to which asset.*

However, all these papers do not correlate to the special characteristics of ICS, so they cannot function as a base for the ICS security knowledge alone.

In the ICS domain, some papers already address the ICS security knowledge. However many of them do not cover the full scope of ICS security assessments (Oates et al., 2013; Schneider, Obermeier and Schlegl, 2015; Lemaire et al., 2015; Lemaire et al., 2014), and others focus on special applications of ICS like smart grids and critical infrastructures (Choraś et al., 2010a; Jarmakiewicz, Maslanka and Parobczak, 2015; Barnett and Crapo, 2011; Koster et al., 2009). Additionally some general papers, dealing with ICS, do not embrace (all) ICS requirements (Bouet and Israel, 2011; Choraś et al., 2010b). Nevertheless many parts of these works can be used as a partial source of the ICS security knowledge content.

Besides the office IT and ICS related papers, which describe the general knowledge for security assessments, there are further papers referring to specific parts of the security knowledge like vulnerabilities or security objectives (Bazaz and Arthur, 2007; Solic, Ocevcic and Golub, 2015) from both office IT and ICS. These works can extend the more general knowledge (e.g. by the specific representation of a vulnerability), mostly represented using ontologies or taxonomies.

During the literature search, no papers referring to the life cycle of security knowledge were identified. However there is general work about knowledge management in place, which describes the life cycle of knowledge in general like (Andriani et al., 2014; Hosseingholizadeh, 2014; Evans, Dalkir and Bidian, 2014). This work can serve as a basis for the ICS security knowledge life cycle design.

The literature search has shown that there is a lack of ICS specific works on ICS security knowledge and its life cycle. This paper strives to close the gap, by developing the ICS security knowledge and its life cycle as a combination and summary of all knowledge necessary for ICS security assessments. In order to represent the characteristics of ICS correctly, the requirements on the ICS security knowledge and its life cycle have to be derived foremost. This is true for the content related coverage as well as acquisition, maintenance and representation.

Table 2: *Requirements on ICS security knowledge and its life cycle*

Requirement	Explanation
Coverage	*The full coverage of ICS security knowledge necessary for a security assessment is essential. The necessary knowledge ranges from identification of assets over risk assessments to identification of security controls. Additionally it must reflect the knowledge needs for the different life cycle stages of an ICS or parts of it. Already existing security controls have to be considered, too.*
Updates	*Because of the ever evolving variety of threats and new security controls as well as new types of assets, the ICS security knowledge needs to be kept up-to-date. It has to be maintained over the complete life cycle of an ICS. In order to deal with future developments the knowledge needs to be extensible, too.*
Acquisition	*There are many different sources for knowledge provided by different entities which have to be considered for knowledge acquisition depending on the type of knowledge (see **Table 1**). During the acquisition the accuracy of the information needs to be ensured (see correctness).*
Generality	*The design and the representation of the ICS security knowledge should be done in a generic way, so it is independent from an individual solution. This enables interoperability between different ICS and allows easy integration of expert knowledge. Additionally the knowledge can be used as a "body-of-knowledge "between different entities. The security knowledge needs to be scalable from small up to complex ICS.*
Correctness	*The correctness of ICS security knowledge is a prerequisite for a successful und correct security assessment. Additionally it accelerates an assessment. Correctness implies that the knowledge is free of inconsistencies, has no duplicates, is syntactically correct and is valid; respectively its integrity is given.*
Evaluation	*During the life cycle of an ICS and its components a continuous monitoring and security control improvement is aspired. This includes reevaluation of the knowledge after update or usage. The former may bring new knowledge which replaces older knowledge, which then has to be archived or excluded. The latter might conclude feedback which knowledge is useful or even new knowledge can be deduced.*
ICS specific Requirements	*In contrast to the office IT, ICS have many diverging requirements which have to be taken into account during the design of the ICS security knowledge and the description of its life cycle. The differing requirements result in diverging knowledge needs and relations (see **Table 1**). See (Stouffer et al., 2015; Larkin et al., 2014) for example.*
Entity	*During the life cycle of the ICS security knowledge many entities influence the knowledge. Entities may be persons, organisations, information systems as wells as components of the ICS. Modelling the life cycle of the ICS security knowledge this has to be considered.*
Usage	*During the life cycle of the ICS security knowledge it is used many times for different purpose. At least it must be usable for on demand and cyclic security assessments, its acquisition and maintenance. Depending on the life cycle stage of an ICS and its components, different parts of the ICS security knowledge may be needed for an ICS security assessment. The life cycle of the knowledge must represent these usage fields in all stages.*

3. KNOWLEDGE REQUIREMENTS

The analysed requirement sources are a selection of relevant international standards, guidelines and other publications from government agencies or operator associations, most of them from the ICS domain. The ones considered most relevant are (Stouffer et al., 2015; ISA, 2015a; ISO and IEC, 2013; VDI, 2011; Bundesamt für Sicherheit in der Informationstechnik [BSI], 2013).

The requirement sources define the content of the ICS security knowledge, as shown in **Table 1** and the requirements regarding the ICS security knowledge and its life cycle are shown in **Table 2**. The requirements mentioned most often in the requirements sources are the ICS specific requirements in comparison with the office IT.

The requirement sources describe the required ICS security knowledge on an abstract level. This is why the profound parts of the ICS security knowledge must be additionally based on specific knowledge described in other office IT and ICS works mentioned in section 2. As a next step the ICS security knowledge is developed.

4. ICS SECURITY KNOWLEDGE

Based on the analysed requirement sources and related work we decided to represent the ICS security knowledge in form of an ontology (Obrst, Chase & Markeloff 2012). This allows a generic and implementation-independent representation for humans and machines. Additionally ontologies allow separating the domain class knowledge (e.g. the concept of a vulnerability) from instances of it (e.g. a specific vulnerability). Thereby the ICS security knowledge can easily be combined with knowledge and concepts of other works and can be used in further work as well. Additionally ontologies can be used by KBS for reasoning.

During an assessment different parts of the ICS security knowledge in different levels of tangibility are needed. This means a more general or a more profound respectively detailed knowledge is necessary depending on the task to perform. For example during a high level risk assessment as suggested in (ISA, 2015a) a more general knowledge about the ICS under examination is needed compared to a detailed risk assessment. To address this we decided to use multiple

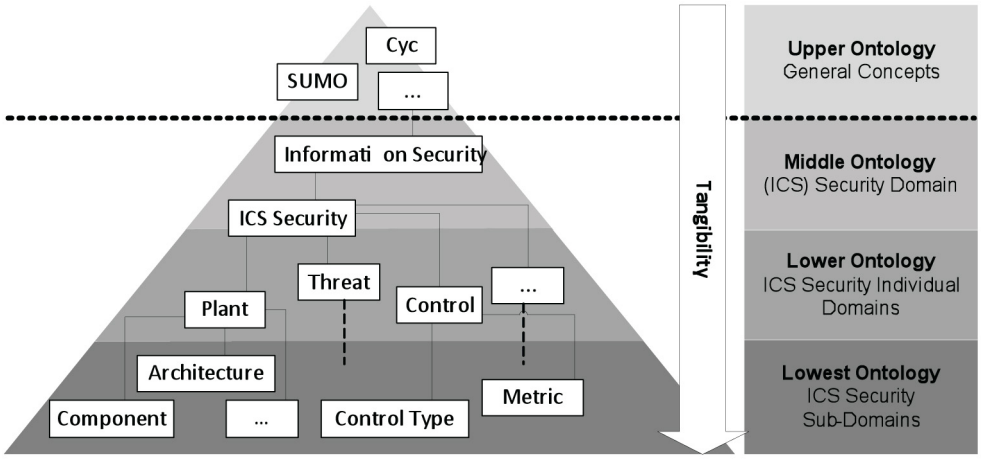

Figure 1: *Overview of different ontology layers in style of (Obrst, 12.01.2006; Obrst, Chase and Markeloff, 2012)*

(Obrst, Chase and Markeloff, 2012). Depending on its tangibility an ontology can be classified into a specific layer (see **Figure 1**). Every layer expands respectively details the concepts of the prior layers.

4.1 Upper Ontology Layer

From a high level of abstraction, information security is a quite specific domain based on more general concepts like part-and-whole relations, locations, time etc. To represent these general concepts, upper ontologies like SUMO (Pease, Niles and Li, 2002) or Cyc (Shepard et al., 2005) exist. The information security specific concepts and relations are part of the middle ontology layer and the ones below, marked by the dashed line in **Figure 1**.

4.2 Middle Ontology Layer

For the middle ontology layer we decided to create two ontologies, shown together in **Figure 2**. The **Information Security** ontology is the most abstract one in the information security domain, which represents the common security knowledge of both office IT and ICS. Hence for this ontology works from the office IT domain and the ICS domain have been considered to identify the common elements. This includes the consideration of the requirement sources described in section 2.

The white boxes in **Figure 2** represent the concepts and the black arrows the relations of the **Information Security** ontology. For complexity reduction reasons, not all elements are shown. An asset is the concept which represents all goods to be protected (Fenz and Ekelhart, 2009; Koster et al., 2009; ISA, 2015a). Assets are owned by an enterprise and represent its resources (Fenz and Ekelhart, 2009; Singhal and Wijesekera, 2010; ISA, 2015a). Not every resource is an asset. Every asset has security objects to achieve (Koster et al., 2009; Miede et al., 2010), which are protected by a control, which itself is an asset, too (Aime and Guasconi, 2010; Souag et al., 2015; Choraś et al., 2010a). Controls can be of different types (Fenz and Ekelhart, 2009) and are generally separated in physical, technical or organisational. Controls are part of a defense strategy (Herzog, Shahmehri and Duma, 2007; Koster et al., 2009). The defense strategy contains all concepts of how to defend an information system. Threat sources mean threats to the assets (Oates et al., 2013; Tsoumas and Gritzalis, 2006; Jarmakiewicz, Maslanka and Parobczak, 2015), whereas a threat is the potential to violate the security of an asset (ISA, 2015a; Bouet and Israel, 2011). Assets have vulnerabilities that can be exploited by a threat (source) to compromise it (Oates et al., 2013; ISA, 2015a). If an asset is affected by a threat, an incident happens (Aime and Guasconi, 2010; Tsoumas and Gritzalis, 2006). Incidents have an unwanted effect on the security objectives and a severity which determines the significance of a security violation (Souag et al., 2015). A control can mitigate incidents, as well as asset vulnerabilities (Aime and Guasconi, 2010).

The **ICS Security** ontology expands the **Information Security** ontology with elements and work of the ICS security domain. Additionally the **ICS Security** ontology has to provide the defined content and to fulfil the derived requirements from section 3.

The grey boxes shown in **Figure 2** represent the concepts and the grey arrows the relations added to the **Information Security** ontology to build the **ICS Security** ontology. During the development of the ICS security ontology, the consideration of ICS requirements is easier presented when using a slightly more detailed ontology. Therefore **Figure 2** shows some concepts of the lower ontology layer marked with the dashed line. Some not so relevant parts are omitted to reduce complexity.

An ICS consists of many different resources, which can be separated into human, infrastructure, information, plant and process. Depending on the

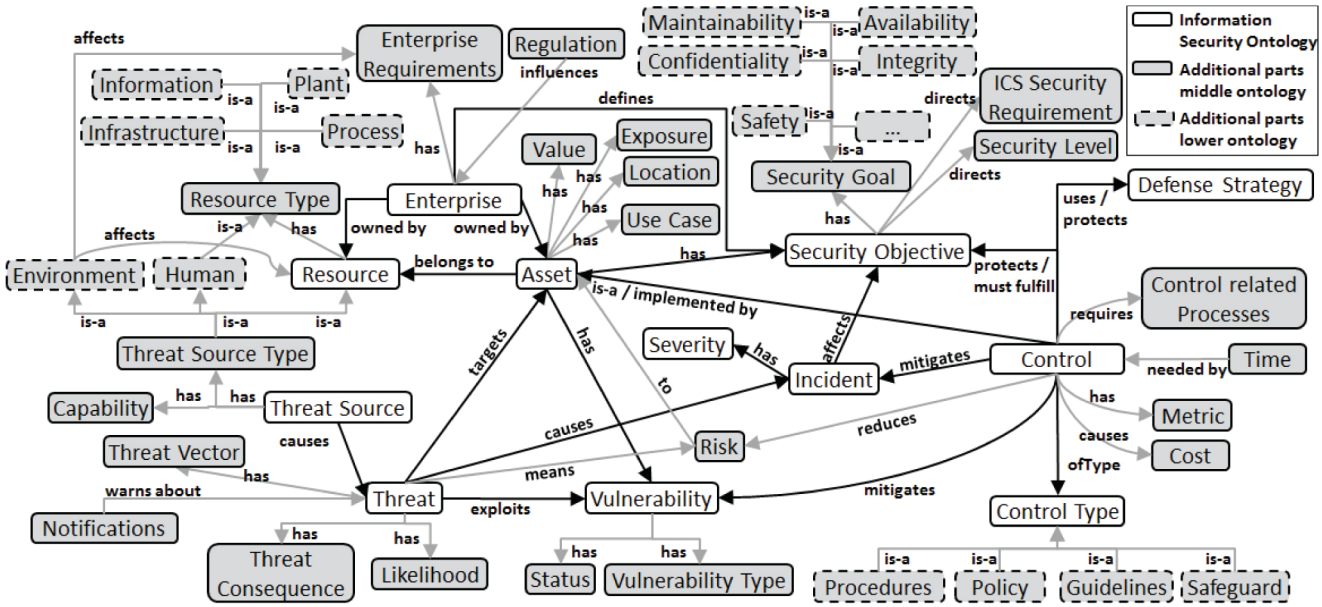

Figure 2: *Information Security ontology and ICS Security ontology of the middle ontology layer*

industry an enterprise has to fulfil different regulations like laws, which can affect the security objectives of an asset (NIST Computer Security Division [CSD], 2013; DIN, 2015). The enterprise requirements like business processes and strategic goals have to be considered, too (VDI, 2011; CSD, 2013; Stouffer et al., 2015). According to an assets exposure, location and its use case different threats and controls exist (Stouffer et al., 2015; ISA, 2015a). Additionally assets have a value to the company which determines the security objectives to achieve (ISA, 2015b; Singhal and Wijesekera, 2010). The Security goals ICS assets have to meet differ from the ones of the office IT (Stouffer et al., 2015; BSI, 2013; ISA, 2015a). The well-known CIA-triad is inverted for ICS, making availability the most important goal, followed by integrity and confidentiality. Additionally safety is an important security goal, too. From an ICS view safety is implicitly contained in many concepts of the ontology. Depending on the asset there are more security goals to fulfil like reliability which covers availability, but contains more requirements like recoverability. The concept of ICS security requirement is a collection of specific ICS requirements which have to be considered when applying controls to an asset (Stouffer et al., 2015; DIN, 2015). For example, many field devices are not capable of running Anti-Malware software because of limited resources. The security level concept was often mentioned in the ICS requirements (ISA, 2015a). Every asset needs to achieve a specific security level, and if the asset itself is not capable to reach it, a compensating control is necessary (e.g. an authentication server) (ISA, 2015a; Stouffer et al., 2015). Additionally the concept risk represents the chance that a threat exploits a vulnerability of an asset (ISA, 2015a; Stouffer et al., 2015). Risk can be reduced via controls.

In order to choose a suitable control, the overall costs have to be known (VDI, 2011; Oleg, Vyacheslav and Andriy, 2013). Besides the initial cost the annual costs have to be considered. For some controls time data like time stamps is critical information (ISA, 2015b). For example it is needed for monitoring purposes. Metrics can be used to measure the effectiveness of controls (DIN, 2015). The types of controls range from procedures, guidelines and policies to safeguards, which can be implemented in the ICS as part of an asset or standalone (ISA, 2015a). For several controls a related process or policy is necessary to support the control (e.g. a Patch-Management or password policy) (Stouffer et al., 2015; ISO and IEC, 2013; ISA, 2015a). All controls applied to an asset need to fulfil security objectives.

The entities of a threat source include a wide range of sources from “script kiddies”, malevolent employees to organised crime and foreign states, all having different intents, capabilities and resources (ISA, 2015a; Jarmakiewicz, Maslanka and Parobczak, 2015; Oates et al., 2013). Notifications are important to be up-to-date with current threats and vulnerabilities. Notifications usually describe the newly emerged vulnerabilities of assets, show the consequences and threat vectors and sometimes even provide information about which control to choose (ISA, 2015b; CSD, 2013). A threat vector describes how a threat source exploits a vulnerability (Homeland Security and CPNI, 2010; ISA, 2015a). Further a vulnerability has a certain likelihood and a consequence which describes the effect if an incident occurs (VDI, 2011; Miede et al., 2010). A vulnerability can be of different type (e.g.

conceptual or a software vulnerability). Additionally the status of a vulnerability can be unknown, unpatched, patched or ignored/accepted (VDI, 2011; ISA, 2015b).

4.3 Lower and Lowest Ontology Layer

Ontologies of the lower layer describe a specific knowledge domain of one (or more) concepts of the middle layer in more detail. An example is the plant concept (see **Figure 2**). The plant ontology contains all concepts of its domain like architecture, network, component and their configuration. The lowest ontology layer contains the most specific ontologies mostly describing ICS security sub-domains of the lower ontology layer (see **Figure 1**). Concerning the plant ontology example one of the lowest layer ontologies describes the physical part of components, which includes the electrical interfaces, its hardware, its enclosure, etc..

The works referring to specific parts of the security knowledge mentioned in section 2 can be classified into one of these ontology layers. Eventually a mapping of ontological concepts and relations is necessary. The ICS requirements identified in section 3 have to be considered as well.

By describing the ICS security knowledge, a simplification of security assessments in the ICS domain especially for SME can be achieved. But for easier management and more efficient usage of the ICS security knowledge, its life cycle has to be considered as well.

5. KNOWLEDGE LIFE CYCLE

This section describes the phases of the general life cycle of the ICS security knowledge so it applies to the application on most ICS. Nonetheless depending on the industry sector there might be necessary adjustments to fulfil specific requirements. The life cycle of the ICS security knowledge is based on the requirements from section 3 including input from the requirement sources and general work on knowledge life cycles already mentioned in section 2. Generally speaking all general work bases on quite similar approaches, which usually contains phases like acquisition, store, organise, use and evolve.

Figure 3 shows the ICS security knowledge life cycle and the entity groups which influence the ICS security knowledge, either as a knowledge source or sink, depending on the life cycle phase. The entities are based on the requirement sources like (ISA, 2015a; VDI, 2011; Stouffer et al., 2015; BSI, 2013). However not all parts of the ICS security knowledge might be processed in the same phase at the same time. The tasks of every phase are performed by the entity groups **ICS Security Experts** and/or **Applications**, except the **Creation Phase** which is performed by ICS Security Experts only. As a continuous example, the life cycle of a vulnerability is described throughout the phases here. The life cycle of new ICS security knowledge starts with an **Update / Expansion required event**, which can be triggered from an entity group or some life cycle phases.

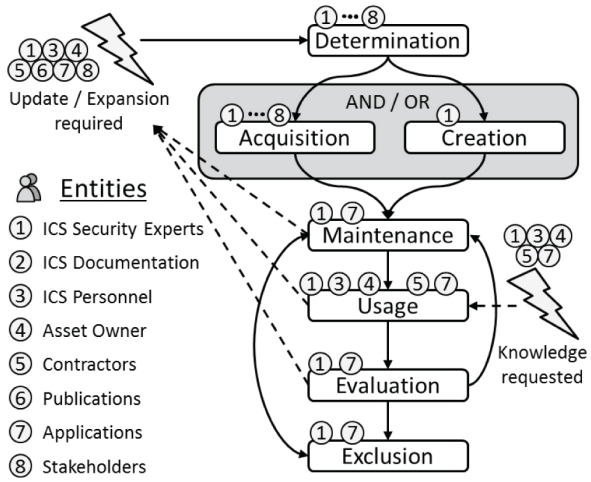

Figure 3: *Life cycle of the ICS security knowledge*

The main tasks to be carried out in the **Determination Phase** are to identify all new ICS security knowledge necessary (e.g. update of vulnerabilities); to search for high quality and trustworthy sources and to analyse the knowledge gap between the sources and the ICS security ontology. Different sources and the attributes are partly mentioned in (Stouffer et al., 2015; ISA, 2015b; ISA, 2015c), for example. The type of a source depends on the ICS security knowledge needed. **Table 3** shows a brief correlation. In most cases ICS security experts choose new knowledge sources. Additionally the type of the ICS security knowledge determines the update rate needed to keep the ontology up-to-date (ISA, 2015b; Stouffer et al., 2015; CSD, 2013; NAMUR, 2015). This can differ between the ICS security knowledge types.

Example: For a vulnerability there are different sources like advisories, manufacturer notifications or internet forums. Depending on the source, the quality and correctness differs. Generally advisories are a good and trustable source. Regular updates in short intervals are necessary, since new vulnerabilities appear often.

The **Acquisition and Creation Phases** follow the determination phase. Both phases can be performed independent of each other by using the results of the knowledge sources determination. The acquisition phase focusses on ICS security knowledge already available somewhere, whereas the creation phase assumes the creation of new ICS security knowledge. The acquisition of knowledge is mentioned in some requirements sources like

(Stouffer et al., 2015; ISA, 2015c; ISA, 2015b; Homeland Security and CPNI, 2010), whereas the creation is not mentioned directly. The tasks of the acquisition phase are to retrieve the ICS security knowledge from possible sources (see Table 3); to formalize it according to the ICS security knowledge format and to integrate it into the knowledge. Depending on the knowledge type and source, different approaches have to be used for acquisition (ISA, 2015b). Usually the acquired ICS security knowledge is stored as instances of the domain knowledge, but could be stored as concepts and relations, too. During the creation phase, mainly domain knowledge, including concepts and relations, is considered. The tasks performed in the creation phase are: to analyse the existing ICS security ontology to find links; to create the ICS security knowledge and to integrate it, using the found links. The usual source of the ICS security knowledge is the ICS Security Experts group. During both phases, meta data like the name of the knowledge source and a timestamp need to be added to enable traceability and evaluation of the ICS security knowledge (Stouffer et al., 2015; BSI, 2013; ISA, 2015b; ISO and IEC, 2013).

Example: A particular vulnerability described in an advisory represents an instance of the ICS security concept vulnerability, so it is added to the knowledge during the acquisition phase. Because advisories are written in text, the necessary information has to be extracted and converted to a new instance of the ICS security ontology. Additionally multiple sources could hold information about a vulnerability. In this case the information has to be compared and merged. Possible meta data includes: knowledge source(s), discrepancy information, quality/accuracy rating, creation date.

Table 3: *Knowledge types and their sources*

Knowledge Type	Entity groups
Threats, Vulnerabilities, Incident	*ICS Security Experts (cyber security team, external security experts, …), ICS Personnel (operations team, …), Publications (alerts, reports, catalogues, …), …*
Controls	*ICS Security Experts, Publications (guidelines, catalogues, …), Stakeholders (User/Vendor Associations, …)*
Security Objectives	*ICS Security Experts, ICS Documentation, Contractors (Vendor, Integrator, …), ICS Personnel, Asset Owner (Manager, office IT, …), Stakeholder (Regulatory Authorities, States, …)*
Assets, Resources	*ICS Documentation, ICS Personnel, Asset Owner (Service Personnel, …), Contractors (Vendor, Supplier, Service Provider, …), Applications (Asset Inventory, …)*
Relations	*ICS Security Experts*

After the new ICS security knowledge has been gathered, the **Maintenance Phase** follows. In this phase ICS security knowledge and its meta data is searched for problems like conflicts, inconsistencies, semantic and syntactic faults (CSD, 2013; NAMUR, 2015). Afterwards the problems are analysed and solved, if possible. This may lead to the exclusion of knowledge or enforce an update event (ISA, 2015b; BSI, 2013). Depending on the knowledge type, different mechanisms might be necessary for maintenance. In this phase neither ICS security knowledge sources nor sinks are involved. Additionally a copy of all ICS security knowledge needs to be stored in a usable condition (Stouffer et al., 2015). This allows the usage of ICS security knowledge whenever it is needed (e.g. when an incident happens), although some parts of the ICS security knowledge might be processed in another phase.

Example: In this phase the new acquired and stored vulnerability instance is checked for its correctness. For example it is checked for double or contradictory instances of vulnerabilities or the correctness of given vulnerability data, which may be corrected by an ICS security expert. Additionally a usable copy of all vulnerabilities is stored, to be able to share vulnerability information although it is processed in another phase at the same time.

After maintenance is completed, the ICS security knowledge is ready for usage. During the **Usage Phase** (Stouffer et al., 2015; ISA, 2015a; VDI, 2011) the ICS security knowledge is first prepared. This involves the selection of the ICS security knowledge parts needed and to represent it in a form that is suitable for its application and the demanding entity group This is demanded by (Stouffer et al., 2015), for example. Additionally access rights of the entity group may be checked, since the ICS security knowledge or parts of it might be an asset itself. Because it is not foreseeable when ICS security knowledge is needed, a **Knowledge requested event** is introduced, which can be triggered by demanding entity groups. After the usage the meta data is updated to reflect the last usage time, for example. Additionally the using entity can provide feedback about the ICS security knowledge used (Stouffer et al., 2015; ISA, 2015b).

Example: If an entity demands vulnerability information, the instances of the concept vulnerability are selected and converted into a representation corresponding to the questioner's needs. For example it could be a list of all vulnerabilities of an ICS for management purposes. This demands a more abstract description compared to the needs of a security auditor. Feedback could be added by the using entity by answering some questions or by directly editing meta data of the vulnerability knowledge.

The feedback of the usage phase is evaluated together with the meta data and the (used) ICS security knowledge in the **Evaluation Phase** (Stouffer et al., 2015; ISA, 2015b). Here the ICS security knowledge is rated, and its meta data is updated. Depending on the evaluation result, ICS security knowledge might have to be excluded, or an update event is triggered (VDI, 2011; CSD, 2013), thus the ICS security knowledge changes back to the maintenance phase.

Example: The evaluation of a vulnerability could be based on its age (meta data) for example. If the vulnerability is old or has been fixed, it could be marked for exclusion. If the feedback from an entity like management states that a vulnerability is acceptable or can be ignored, it is marked in its meta data, and the vulnerability either remains in the knowledge or is excluded.

In the **Exclusion Phase** the evaluated ICS security knowledge is checked for obsolete knowledge (ISA, 2015b). For example contradictory ICS security knowledge can be deleted whereas other ICS security knowledge, which may be needed later, is archived. Again the knowledge type might give a clue when exclusion or archiving is necessary. If ICS security knowledge is reactivated it changes back to maintenance phase, where the compatibility with the rest of the ICS security knowledge is checked.

Example: Old vulnerabilities may be archived for later use. If a patch for a vulnerability was released and installed, it might happen that the patch did not close the vulnerability, what might become generally known at a later point in time. Vulnerability instances which are malformed or corrupted can be deleted.

6. CONCLUSION

In this paper, requirements of ICS concerning the knowledge needed to perform an ICS security assessment and its life cycle have been derived. Based on the requirements and work of the office IT and ICS domain, an ICS security ontology, consisting of different layers of tangibility, has been developed. Additionally the life cycle of the ICS security knowledge, its usage and the entity groups influencing it have been discussed.

The requirement to cover all knowledge necessary for ICS security assessments (see **coverage** in Table 2) can be achieved by using a layered approach, where the ICS security ontology is used as a base to add ontologies describing specific domains in more detail. In this way other work can be included, too. However a mapping might be necessary. Keeping the ICS security knowledge up-to-date (**updates**) was another requirement, which is fulfilled by describing the life cycle of the ICS security knowledge including influencing entities and the layered approach. The **acquisition** of the ICS security knowledge is possible, because using an ontology allows the interpretation by humans and machines, as well as mappings from different knowledge sources. The requirement **generality** can be achieved by using ontologies as ICS security knowledge representation, too. It provides the separation of domain knowledge and instances of it, making it easier to represent new ICS security knowledge like vulnerabilities and controls without changes on the domain knowledge. Only changes in the domain demand a change of the domain knowledge. The **correctness** of the ICS security knowledge can be assured using applications like reasoners for validation. Additional meta data checks and human interaction might be necessary. The **evaluation** requirement is fulfilled in the corresponding life cycle phase, where evaluation of the ICS security knowledge based on applicability, meta data and feedback is performed. The **ICS specific requirements** have been considered during the design of the ICS security knowledge and the life cycle definition including the influencing **entities**. The requirement **usage** demands the examination of which ICS security knowledge part is needed by whom and in which extent. This is done during the discussion of the life cycle and entity groups. Additionally the layered approach of ontologies with ascending tangibility allows the detailed consideration of the ICS security knowledge parts necessary depending on its application and addressee.

The ICS security knowledge and its life cycle fulfil the gathered requirements and join the existing works into one approach. Until now the ICS security ontology and its life cycle are concepts. However they will be advanced in future, including tools for knowledge management, like maintenance and evaluation, as part of the ICS security life cycle. They can already be used as a good base for holistic, up-to-date ICS security assessments for SMEs. This increases the dependability of an ICS, protecting its know-how and reducing its downtimes. Additionally the consideration of the life cycle and the ICS security knowledge itself can be beneficial for other entities as well as serving as a common Body-of-Knowledge. Considering KBS this is a good starting point.

REFERENCES

Aime, M. D. and Guasconi, F. (2010). Enhanced Vulnerability Ontology for Information Risk Assessment and Dependability Management. In: *Third International Conference on Dependability (DEPEND)*, Venice, Italy, (18.-25.07.2010). 92–97.

Andriani, M. et al. (2014). Theoretical model of knowledge management in SMEs life cycle: (A literature study). In: *2nd International Conference on Technology, Informatics, Management, Engineering & Environment*, Bandung, Indonesia, (19.-21.08.2014). 351–356.

Barnett, B. and Crapo, A. (2011). A Semantic Model for Cyber Security. In: *Grid-Interop Proceedings: Implementing Interoperability, Advancing Smart Grid Standards, Architecture and Community*, Phoenix, AZ, USA, (05.-08.12.2011).

Bazaz, A. and Arthur, J. (2007). Towards a Taxonomy of Vulnerabilities. In: *40th Annual Hawaii International Conference on System Sciences (HICSS)*, Waikoloa, Hawaii, USA, (Jan. 2007).

Blanco, C. et al. (2011). Basis for an integrated security ontology according to a systematic review of existing proposals. *Computer Standards & Interfaces* 33(4). 372–388.

Bouet, M. and Israel, M. (2011). INSPIRE Ontology Handler: Automatically building and managing a knowledge base for Critical Information Infrastructure protection. In: *Integrated Network Management (IM), 2011 IFIP/IEEE International Symposium on*, Dublin, Ireland, (23.-27.05.2011). 694–697.

Bundesamt für Sicherheit in der Informations-technik (BSI) (2013). ICS-Security-Kompendium.

Choraś, M. et al. (2010a). Decision Aid Tool and Ontology-Based Reasoning for Critical Infrastructure Vulnerabilities and Threats Analysis. In: *Critical Information Infrastructures Security: Revised Papers of 4th International Workshop*, Bonn, Germany, (30.09.-02.10.2009). 98–110.

Choraś, M. et al. (2010b). Ontology Applied in Decision Support System for Critical Infrastructures Protection. In: *Trends in applied intelligent systems: 23rd International Conference on Industrial Engineering and Other Applications of Applied Intelligent Systems, Proceedings part 1*, Cordoba, Spain, (01.-06.2010). 671–680.

DIN ISO/IEC TR 27019 (2015). Informationstechnik - Sicherheitsverfahren - Leitfaden für das Informationssicherheitsmanagement von Steuerungssystemen der Energieversorgung auf Grundlage der ISO/IEC 27002 (ISO/IEC TR 27019:2014). Berlin: Beuth Verlag GmbH.

Evans, M. et al. (2014). A Holistic View of the Knowledge Life Cycle: The Knowledge Management Cycle (KMC) Model. *Electronic Journal of Knowledge Management*, 12(2). 85–97.

Fenz, S. and Ekelhart, A. (2009). Formalizing information security knowledge. In: *4th International Symposium on Information, Computer, and Communications Security: Proceedings*, Sydney, NSW, Australia, (10.-12.03.2009). 183–194.

Herzog, A., Shahmehri, N. and Duma, C. (2007). An Ontology of Information Security. *International Journal of Information Security and Privacy*, 1(4). 1–23.

Homeland Security and CPNI (2010). Cyber Security Assessments of Industrial Control Systems: Good Practice Guide.

Hosseingholizadeh, R. (2014). Managing the knowledge lifecycle: A integrated knowledge management process model. In: *4th International eConference on Computer and Knowledge Engineering (ICCKE)*, Mashhad, Iran, (29.-30.08.2014). 102–110.

ISA 62443-1-1 (2015a). *Security for Industrial Automation and Control Systems - Models and Concepts. Draft 5, Edit 5*.

ISA-62443-2-1 (2015b). *Security for industrial automation and control systems - Part 2-1: Industrial automation and control system security management system. Draft 7, Edit 5*.

ISA-62443-3-2 (2015c). *Industrial communication networks - Network and system security - Part 3-2: Security risk assessment and system design. Draft 6, Edit 3*.

ISO/IEC 27001 (2013). *Information technology - Security techniques - Information security management systems - Requirements*. Second Edition.

Jarmakiewicz, J., Maslanka, K., and Parobczak, K. (2015). Development of cyber security testbed for critical infrastructure. In: *International Conference on Military Communications and Information Systems (ICMCIS)*, Cracow, Poland, (18.-19.05.2015). 1–10.

Koster, F. et al. (2009). Collaboration in security assessments for critical infrastructures. In: *Fourth International Conference on Critical Infrastructures (CRIS)*, Linköping, Sweden, (28.-30.04.2009). 1–7.

Larkin, R. D. et al. (2014). Evaluation of security solutions in the SCADA environment. *SIGMIS Database*, 45(1). 38–53.

Lemaire, L. et al. (2014). A SysML Extension for Security Analysis of Industrial Control Systems. In: *2nd International Symposium for ICS & SCADA Cyber Security Research 2014: Proceedings* : St. Pölten, Austria, (11-12 Sep. 2014).

Lemaire, L. et al. (2015). Extracting Vulnerabilities in Industrial Control Systems using a Knowledge-Based System. In: *3rd International Symposium for ICS & SCADA Cyber Security Research: Proceedings*, Ingolstadt, Deutschland, (17-18 Sep.~2015).

Miede, A. et al. (2010). A Generic Metamodel for IT Security Attack Modeling for Distributed Systems. In: *10th International Conference on Availability, Reliability, and Security*, Krakau, Poland, (15.–18.02.2010). 430–437.

NE 153 (2015). *Automation Security 2020 - Design, Implementierung und Betrieb industrieller Automatisierungssysteme*.

Nguyen, Van (2011). *Ontologies and Information Systems: A Literature Survey, DSTO-TN-1002*. Edinburgh, South Australia 5111, Australia.

NIST Computer Security Division (CSD) (2013). NIST SP 800-53 Revision 4: Security and Privacy Controls for Federal Information Systems and Organizations: National Institute of Standards and Technology.

Oates, R. et al. (2013). Practical Extensions of Safety Critical Engineering Processes for Securing Industrial Control Systems. In: *8th IET International System Safety Conference incorporating the Cyber Security Conference 2013*, Cardiff, UK, (16.–17.10.2013). 2.

Obrst, L. et al. (2012). Developing an Ontology of the Cyber Security Domain. In: *Proceedings of the Seventh International Conference on Semantic Technologies for Intelligence, Defense, and Security*, Fairfax, VA, USA, (23–26.10.2012).

Obrst, Leo (2006). The Ontology Spectrum Semantic Models 12. Januar. MITRE Corporation - Information Semantics Group. Available from http://ontolog.cim3.net/file/resource/presentation/LeoObrst_20060112/OntologySpectrumSemanticModels–LeoObrst_20060112.ppt . (21 Apr. 2016).

Oleg, I. et al. (2013). Cyber security lifecycle and assessment technique for FPGA-based I&C systems. In: *11th East-West Design and Test Symposium*, Rostov-on-Don, Russia, (27.–30.09.2013). 1–5.

Pease, A. et al. (2002). The Suggested Upper Merged Ontology: A Large Ontology for the Semantic Web and its Applications. In: *Proceedings of the Eighteenth National Conference on Artificial Intelligence*, Edmonton, Alberta, USA, (28.07.-01.08.2002).

Schneider, J. et al. (2015). Cyber Security Maintenance for SCADA Systems. In: *Proceedings of the 3rd International Symposium for ICS & SCADA Cyber Security Research*, Ingolstadt, Germany, (17.-18.09.2015).

Shepard, B. et al. (2005). A knowledge-based approach to network security: applying Cyc in the domain of network risk assessment. In: *Proceedings of the Seventeenth Conference on innovative applications of Artificial Intelligence*, Edmonton, Alberta, USA, (09.–13.07.2005). 1563–1568.

Singh, V. and Pandey, S. K. (2014). Revisiting Security Ontologies. *IJCSI International Journal of Computer Science Issues*, 11(6). 150–159.

Singhal, A. and Wijesekera, D. (2010). Ontologies for modeling enterprise level security metrics. In: *Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research*, Oak Ridge, Tennessee, USA, (21.-23.04.2010).

Solic, K. et al. (2015). The information systems' security level assessment model based on an ontology and evidential reasoning approach. *Computers & Security*, 55. 100–112.

Souag, A. et al. (2015). A Security Ontology for Security Requirements Elicitation. In: *Engineering Secure Software and Systems: Proceedings of 7th International Symposium*, Milan, Italy, (04.-06.03.2015). 157–177.

Stouffer, K. et al. (2015). Guide to Industrial Control Systems (ICS) Security: Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), and Other Control System Configurations such as Programmable Logic Controllers (PLC). Special Publication 800-82. Revision 2: National Institute of Standards and Technology.

Tsoumas, B. and Gritzalis, D. (2006). Towards an Ontology-based Security Management. In: *20th International Conference on Advanced Information Networking and Applications - Volume 1 (AINA'06)*, Vienna, Austria, (18.-20.2006). 985–992.

VDI/VDE 2182 Blatt 1 (2011). *Informationssicherheit in der industriellen Automatisierung - Allgemeines Vorgehensmodell. Edit 3*. Berlin: Beuth Verlag GmbH.