Situational Awareness for Security Adaptation in Industrial Control Systems

Antti Evesti
VTT Technical Research Centre of Finland, Oulu, Finland
antti.evesti@vtt.fi

Tapio Frantti
University of Oulu, Oulu, Finland,
tfrantti@ee.oulu.fi

Abstract—**Situational Awareness (SA) offers an analysed view of system's security posture. Securing Industrial Control Systems (ICSs) and critical infrastructures requires timely and correct SA. System administrators make decisions and modify security mechanisms based on SA information. In this paper, we envision how security adaptation can facilitate administrators' work in the ICS protection. Security adaptation is not widely applied in ICS context. Moreover, existing security adaptation approaches concentrate on recognition of an adaptation need, *i.e*,. building situational awareness, instead of security decision making. Therefore, we present steps to create a security adaptation plan, and apply fuzzy set theory and linguistic relations for decision making, when SA information indicates that required security is not reached.**

Keywords-critical infrastructure; self-adaptation; self-protection; ICS; decision making.

I. Introduction

A malfunction in a critical infrastructure such as energy and water supply, money transactions, and healthcare can paralyse our daily life, and even operations of the whole society. In this paper we focus on the protection of critical infrastructures that utilise Industrial Control Systems (ICS), *e.g.*, to control power production and to chlorinate water.

Until the present day, ICSs have been closed and static systems, and a threat model has contained only few security threats. At the moment, we are in the face of a new situation. Firstly, new wireless devices appear to industry environments, and secondly, network connections are added to ICSs in order to support remote maintenance and control. Moreover, IP based networks are applied more widely. Thus, the threat landscape is exploding and becoming dynamic, which makes ICSs attractive targets for attackers. The administrator has to be aware of, *e.g.*, network connections, access permissions, and ongoing attack attempts. Situational Awareness (SA) facilitates to gain this information. In a simply form, SA is *being aware of what is happening around you and understanding what that information means for you now and in the future* [1]. For the ICS protection, SA offers the analysed view of system's cyber security posture and administrators perform security decisions, *e.g.,* tune firewall settings and user privileges, based on SA information.

However, humans' decision making capability is limited, and thus, we propose to apply adaptive security to facilitate administrators' decision making. In complex systems, adaptation can be utilised, *e.g.*, to facilitate configuration processes [2]. The MAPE-K (Monitor, Analyse, Plan, Execute and Knowledge) [2] is a common reference model for adaptation, which is also applied for the adaptive security in smart space in [3]. The adaptive security monitors system's security state and modifies security mechanisms to correspond to the dynamic threat landscape.

Survey by Franke *et al.* reveals that cyber situational awareness in ICSs is researched widely [4]. In contrast, the security adaptation in ICS is not researched broadly. The Scopus search (in Nov. 2014) does not find any results with a search string *"security adaptation" AND "industrial control system"* and Google Scholar returns only one result – namely a paper from Salehie *et al.* [5] that envisions research directions of security adaptation in smart grids. Applying security adaptation requires clearly defined decision making. However, a plan phase where a decision for *how to modify security mechanisms for the current threat landscape* is performed, is one of the most uncovered area of the security adaptation [6,7].

The paper describes the decision-making part of the security adaptation process in detail and envisions the use of adaptive security as an addition of situational awareness in ICS context. For the decision-making we introduce fuzzy set theory based technique to select appropriate security mechanisms. The decisions can be used as such or as a complementary part with administrator-based decision making.

The paper is organised as follows. The Section 2 describes background information. Section 3 presents language-oriented approach for decision making. Section 4 envisions the utilisation of security adaptation in ICSs. Steps to produce an adaptation plan are described in Section 5. Section 6 contains discussion and future research ideas, and finally, conclusions are drawn in Section 7.

II. Background

A. Security

ISO/IEC [8] defines security as follows: "*The capability of the software product to protect information and data so*

978-1-4799-8993-5/15/$31.00 ©2015 IEEE

that unauthorised persons or systems cannot read or modify them and authorised persons or systems are not denied access to them.“ Accordingly, security is a composition of *security objectives* – including confidentiality, integrity, availability, authentication and authorization. The definition clearly concentrates on information and ICT security. Rossouw *et al.* separate *information*, *ICT* and *cyber security* in [9] as follows: *Information security* refers to security of information based assets, *e.g.,* paper documents; *ICT security* protects information based assets, which are stored and transmitted using ICT; finally, *cyber security* concentrates on non-information based assets, which are vulnerable to threats via ICT, *e.g.,* critical infrastructures and ICSs.

In ICSs, availability and integrity are probably the most important objectives. In ICSs integrity of control information, produced products and manufacturing machines are more valuable than the confidentiality of information delivered in an environment. [10]

B. Security Adaptation

Security adaptation occurs separately for each security objective, *i.e.*, security cannot be adapted as such but individual security objectives and security mechanisms that support these objectives can be adapted. As already said, the MAPE-K is a common reference model for adaptation. The *Monitor*, *Analyse*, *Plan* and *Execute* phases form the adaptation loop supported with the *Knowledge*. The Monitor phase collects input information from the execution environment and system's internal state and behaviour. Afterwards, the Analyse phase recognises the adaptation need by combining monitoring results. The purpose of the Plan phase is to decide how to fulfil required security objectives. Therefore, the Plan decides what and how has to be changed in order to achieve requirements. The output of this phase is called *an adaptation plan*. In the security adaptation, the adaptation plan can be based on two alternatives: i) change the current security mechanism or ii) modify parameters of the current security mechanism. Both alternatives require that the adapted system contains mechanisms to perform required adaptation – in this paper these mechanisms are called *actions to adapt*. Finally, the Execute phase performs the adaptation based on the adaptation plan.

An architecture for the security adaptation that conforms the MAPE-K reference model is defined in [3]. The structural overview of the architecture is presented in Figure 1. The adaptation knowledge is presented by means of Information Security Measuring Ontology (ISMO) [11], which will be also applied here. The ISMO defines *security objectives*, *threats* that threaten objectives, and *security mechanisms* that support objectives. For the adaptation purposes, each security objective has an *indicator* to calculate the current security level for the objective. The indicator is calculated by means of *analysis model*. The analysis model is dependent on the security mechanism, *e.g.*, authentication level indicator is calculated with different analysis model for password authentication and biometric authentication. In this paper, we focus on the Plan phase, *i.e.*, how to create the adaptation plan. Thus, Monitor and Analyse phases form a cyber situational awareness that feeds the Plan phase c.f. Figure 1.

C. Situational Awareness

The formal definition for SA is "*the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future*" [12]. The definition is general – however, it is also applicable for information and cyber security. Cyber security SA can be mapped to the SA as follows: Perception is achieved by utilising monitoring, *e.g.,* traffic monitoring and vulnerability scanners. Comprehension is gained by analysing monitored information, *e.g.,* intrusion detection, correlation and flow analysis. Security visualisation contributes to comprehension and in some extend projection of the future, *e.g.,* by showing trends.

Security measuring is one alternative to produce SA information. Security measures are decomposed to *base measures*, *derived measures* and *indicators*. Base measures are the independent raw measures. Derived measures use simple functions to combine base measures and other derived measures. Indicators use analysis models to combine base measures, derived measures and other indicators. Base measures are perceptions, whereas derived measures and indicators are comprehensions of the current situation.

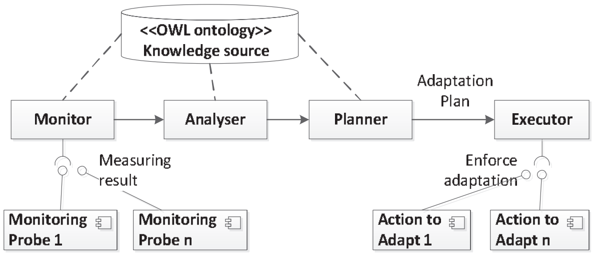


Figure 1. Security adaptation architecture.

III. LINGUISTIC EQUATIONS

Here we envision to use fuzzy set theory on embedded decision making system to reason with uncertain and vague information. A fuzzy approach was originally developed to include a human operator's or system engineer's expertise, which does not lend itself to being easily expressed in differential equations but rather in situation/action rules. In the fuzzy reasoning system, the input and output variables are represented in linguistic form after fuzzyfication of physical values into linguistic form. The fuzzyfication procedure is illustrated in detail, *e.g.*, in [13].

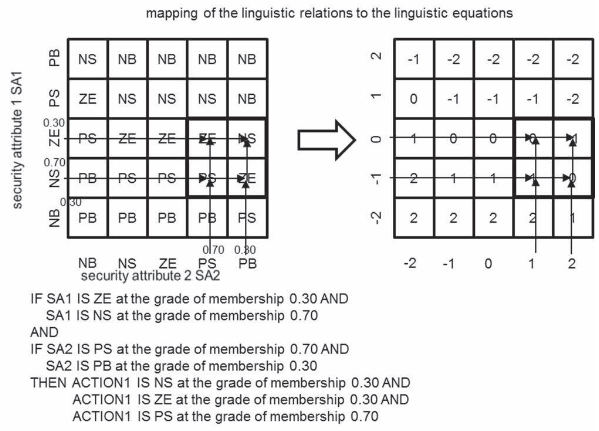
In the systems, where the knowledge would be expressed in a linguistic or verbal form, a language-oriented approach can be used in a model generation (linguistic model). In the language oriented approach we encounter a concept of linguistic relations, which describes the degree of associations between fuzzy sets given in a linguistic form. In this application, a linguistic model of a system is described by linguistic relations. The linguistic relations form a rule base (see Figure 2) of the system that can be converted into numerical equations. Suppose, as an example, that X_{ij}, *i=1,2; j = 1,..., m* (*j* is uneven number), is a linguistic level (*e.g., negative big (NB), negative small (NS), zero (ZE), positive small (PS), and positive big (PB)*) for a variable X_i. The linguistic levels are replaced by integers *–(j-1)/2, ... , -2, -1, 0, 1, 2, ... , (j-1)/2*. The direction of the interaction between fuzzy sets is presented by coefficients $A_{ij}=\{-1, 0, 1\}$, *i=1,2; j = 1,..., m*. This means that the directions of the changes in the output variable decrease or increase depending on the directions of the changes in the input variables. Thus, a compact equation for the output Z_{ij} is:

$$\sum_{j=1,m}\sum_{i=1,2} A_{ij}\, X_{ij} = Z_{ij} \ .$$

The mapping of linguistic relations to linguistic equations (LE) for two input variables is described in Figure 2. For example, we can read from Figure 2 that *IF SA1 IS negative small AND SA2 IS positive small THEN the ACTION IS positive small*. In linguistic equations this can be presented as

$$\left\lceil \frac{-1*-1+1*1}{2} \right\rceil = 1 \ .$$

The advantage of LE approach is that we can rather easily manage numerous input variables with multidimensional rule base that would not easily be possible with *IF-THEN-ELSE* rules.


mapping of the linguistic relations to the linguistic equations

security attribute 1 SA1 \ security attribute 2 SA2	NB	NS	ZE	PS	PB
PB	NS	NB	NB	NB	NB
PS	ZE	NS	NS	NS	NB
ZE	PS	ZE	ZE	ZE	NS
NS	PB	PS	PS	PS	ZE
NB	PB	PB	PB	PB	PS

	-2	-1	0	1	2
2	-1	-2	-2	-2	-2
1	0	-1	-1	-1	-2
0	1	0	0	0	1
-1	2	1	1	1	0
-2	2	2	2	2	1

IF SA1 IS ZE at the grade of membership 0.30 AND
SA1 IS NS at the grade of membership 0.70
AND
IF SA2 IS PS at the grade of membership 0.70 AND
SA2 IS PB at the grade of membership 0.30
THEN ACTION1 IS NS at the grade of membership 0.30 AND
ACTION1 IS ZE at the grade of membership 0.30 AND
ACTION1 IS PS at the grade of membership 0.70

Figure 2. Mapping of the linguistic relations to linguistic equations.

IV. The Vision of SA Based Security Adaptation

In order to facilitate administrators' work, we propose a shift from manual modifications towards security adaptation. Figure 3 depicts the vision of an intended approach. In the current practice (c.f. upper part of Figure 3), situational awareness offers input for the human decision making. However, we argue that at least part of decisions can be performed automatically. Thus, a set of SA information is fed into an adaptation part, see Figure 3. Thus, security management is divided in conventional human-based decision making and automatic adaptation-based decision making. The division still leaves freedom for an administrator to intervene security decisions. In the same time, the approach saves administrators' resources for the most important tasks. Moreover, it is possible to build an interaction between manual and automatic decision making, *i.e.*, the administrator is able to utilise information produced by adaptation to support his own decision making. Or alternatively, the adaptation part can monitor decisions made by the administrator and note if a decision is going to violate other qualities for instance.

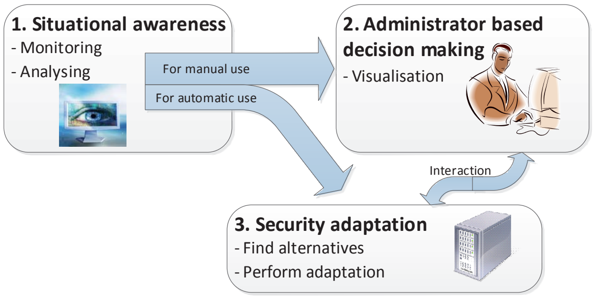


Figure 3. Paradigm Change for ICS protection.

Security controls are either management, operational, or technical controls [10]. The efficient protection of ICS has to cover all of these areas. However, from the adaptation perspective the focus is on technical controls.

SA is based on perceptions from various sources, which we call factors of cyber situational awareness. In Table II SA factors are categorised into two level hierarchy, *i.e.*, the main- (bold font) and sub-factors The list is not intended to be exhaustive – instead the purpose is to present the diversity of factors affecting to the SA. It is notable that from the SA perspective, the attainability of factors is a fundamental aspect and a system has to contain a monitoring probe to retrieve particular information. Some factors can be adapted as such, *i.e.*, it is possible to find mapping from perception to adaptation. Thus, the list categorises adaptation possibilities of each factor. Some factors, such as an operating system, are design decisions that affect to the achieved security level but cannot be adapted at runtime. However, the parameters of operating system can be adapted. We have evaluated adaptation possibilities of factors by using categories defined in Table I.

TABLE I. ADAPTATION (AD) CATEGORY DEFINITIONS

Ad Category	Definition
No (N)	the factor cannot be adapted autonomously at runtime
Partially (P)	some aspects of the factor can be adapted
Yes (Y)	the factor can be adapted at runtime

TABLE II. EXAMPLE FACTORS OF CYBER SITUATIONAL AWARENESS

Factor	Ad	Adaptation possibilities
Vulnerabilities	N	
CVSS score	N	
Finding date	N	
Firewall (FW)	Y	Adapting firewall's settings
IP address	P	Deny traffic to/from particular address.
Port	P	Deny traffic to/from particular port.
Protocol	P	Deny particular protocol.
FW logs	P	Adapting the amount of logging.
FW rules	Y	Modify / create new rules.
Network (net)	n/a	
Net topology	Y	Source routing to avoid some nodes.
Subnetwork	P	Isolation of network parts.
FW location	P	Define new routing
DMZ location	P	Define new routing
System param.	n/a	
OS	N	
Net type	N	
Resource type	N	
Provided serv.	N	
Host activities	P	Move critical activities to another host.
Wireless com.	P	Deny / Enforce security controls.
Remote access	P	Deny / Restric remote accesses.
App. logs	N	
IDS alerts	N	
W/R of crit. files	P	Limit write / read access to critical files.
Incr. privileges	N	
Sec controls	n/a	Sub-factors can be adapted.
User auth (UA)	Y	Adapt. mechanism / parameters.
UA key lenght	Y	Enforce new key.
UA pwd length	Y	Enforce password change.
UA pwd age	Y	Enforce password change.
UA sess. dur.	P	Enforce reauthentication.
UA no. of failures	P	Limit no. of allowed login failures.
UA login delay	Y	Add delay after a login failure.
AC policy	Y	Modify access control policy
Physical AC	N	

The list above contains 36 factors of SA – as an example. The abstraction level of factors varies from high level factors to in detail technical factors. From SA point of view both high level and technical factors are relevant. On the other hand, it is visible from the list that security adaptation is mostly applicable only for more detailed factors. From the list it is clear that a huge amount of factors can be listed, and thus, achieving an exhaustive list requires extensions from various perspectives. For instance, the main factor, *Sec. controls*, contains only password authentication. It is common to think SA from a network perspective – containing, *e.g*., IDSs and firewalls. However, the list shows that the extensive SA is more than network traffic. Finally, the list also reveals that extensive SA cannot be achieved only with automatic monitoring and analysing. Human interpretation is needed especially when the implications of higher level factors for SA are analysed.

V. CREATING THE ADAPTATION PLAN

In our proposal, the adaptation plan is created in two parts. The first part produces a list of possible adaptation alternatives. The second part evaluates the security of alternatives, and finally the security actions of the adaptation plan are reasoned from security attributes by means of a fuzzy set theory and linguistic algorithm. Figure 4. presents steps to produce the adaptation plan. The rounded rectangles indicate steps and rectangles present produced / consumed information.

Input knowledge for *Retrieve alternatives to adapt* step is the required security objective and level, the currently achieved security objective and level, and the security mechanism currently in use. In ICSs, required security objective and level can be defined at the system design phase, or alternatively, those can be reasoned from SA information. For instance, if authentication level 2 is required but only level 1 is currently achieved, it is required to find means to increase the authentication level from 1 to 2. This can be achieved by changing security mechanism or tuning the parameters of the current security mechanism. It is possible to find both, alternative mechanisms and parameters, from the ISMO (Information Security Measuring Ontology). The ISMO describes security objectives and supporting security mechanisms. Hence, it is straightforward to search mechanisms that support the required security objective. This is visible in Figure 5, where *authentication security objective* (on the top of figure) and supporting *security mechanisms* are connected with the *supports* property.

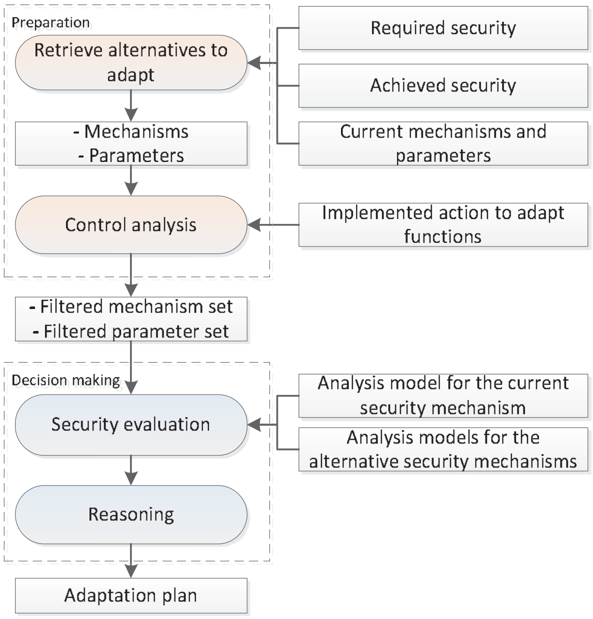

Preparation
Retrieve alternatives to adapt
Required security
Achieved security
Current mechanisms and parameters
- Mechanisms
- Parameters
Control analysis
Implemented action to adapt functions
- Filtered mechanism set
- Filtered parameter set
Decision making
Security evaluation
Analysis model for the current security mechanism
Analysis models for the alternative security mechanisms
Reasoning
Adaptation plan

Figure 4. Steps to produce an adaptation plan.

In contrast, searching parameters to adapt requires that attributes that affect to the current security level are searched, *i.e.*, a root cause analysis is needed. *Analysis models* are defined for each security mechanisms, *e.g.*, a security level for password and fingerprint authentication are calculated with different *analysis models*, see Figure 5. The analysis model points to the security mechanism, which in turn has various attributes. These attributes are possible parameters for the adaptation. Example in Figure 5. contains *password length*, *usage time* and *session duration* attributes for the password authentication mechanism. The usage time is time from the latest password change, whereas the session duration is time from the last authentication. In contrast, attributes for the fingerprint authentication are *session duration*, *image resolution* and *number of scanned fingers*. The session duration attribute is mutual to password and fingerprint authentication alike. The values of attributes are the basis for the current user authentication level and parameter adaptation change some of these attributes. The final output of the first step is the list of alternative security mechanisms and parameters to adapt.

The mechanism and parameter lists from the previous step contain all mechanisms and parameters described in the ISMO. However, all of these alternatives are not applicable adaptations, and thus, the *control analysis* step filters mechanisms and parameters. Security mechanisms, which are not supported in the adapted device, are filtered out. For instance, fingerprint authentication mechanism is filtered out if the adapted device does not contain a fingerprint reader.

Similarly, it is not possible to change all the parameters. In the ISMO attributes, which can be adapted has an *adaptableWith* property that point to the adaptation action – it is notable, that in the ISMO security mechanisms have attributes, which are called parameters in the adaptation terminology. In Figure 5 two *action to adapt* alternatives are included; the *re-authentication function* is an action to adapt that is able to affect both fingerprint and password authentication. Re-authenticating a user ensures that the user has not forgotten to sign-out and another user starts to use device or service without a permission. In contrast, the *password change function* affects only to password authentication. There is not action to adapt descriptions for *image resolution* and *number of scanned fingers* attributes, *i.e,.* these attributes cannot be adapted. Consequently, the final output of the second step is a list of mechanisms and parameter that the device is able to adapt.

The adaptation alternatives have distinct effects for security – from minor change to significant security improvement. In the *Security Evaluation* step, the purpose is to evaluate adaptation alternatives and filter out alternatives that are not able to offer required security level. If the parameter set contains parameters *usage time*, *password length* and *session duration* the security evaluation evaluates how the adaptation of each parameter affects to achieved security level. For the parameters the security evaluation is made by utilising the analysis model. The evaluation goes through the analysis model and searches parameter values, which produce the required security level. For instance, if the current authentication level is 1 and level 3 is required the analysis model for password authentication shows parameter values to achieve the required level. Thus, the analysis model contains knowledge required to find acceptable parameters.

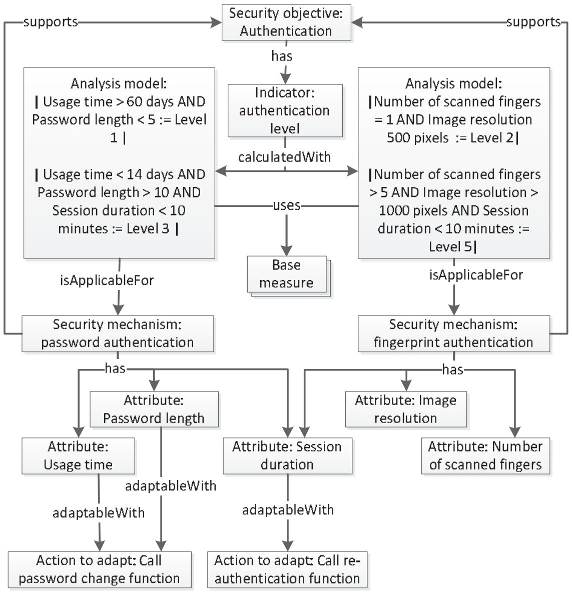

Security objective: Authentication
supports
supports
has
Indicator: authentication level
calculatedWith
uses
Base measure
Analysis model: | Usage time > 60 days AND Password length < 5 := Level 1 |
| Usage time < 14 days AND Password length > 10 AND Session duration < 10 minutes := Level 3 |
Analysis model: |Number of scanned fingers = 1 AND Image resolution 500 pixels := Level 2|
|Number of scanned fingers > 5 AND Image resolution > 1000 pixels AND Session duration < 10 minutes := Level 5|
isApplicableFor
isApplicableFor
Security mechanism: password authentication
Security mechanism: fingerprint authentication
has
has
Attribute: Password length
Attribute: Usage time
Attribute: Session duration
Attribute: Image resolution
Attribute: Number of scanned fingers
adaptableWith
adaptableWith
adaptableWith
Action to adapt: Call password change function
Action to adapt: Call re-authentication function

Figure 5. Example knowledge from ISMO.

Next, alternative security mechanisms are evaluated to find mechanisms, which are able to produce required security level. For this purpose, achievable security levels of security mechanisms are compared to the required security level. This requires that the analysis model for each alternative mechanism is retrieved from the ISMO – analysis models contain the levels that the mechanism is able to produce. For instance, the highest authentication level achievable with the fingerprint authentication is level 5, *c.f.*, analysis model example in Figure 5.

As the final output, the security evaluation step produces a list of parameters and mechanisms, which are able to produce the required security level. The Reasoning step produces the adaptation plan by applying fuzzy set theory and linguistic algorithms. Consider as an example, that security attribute 1 (SA1) and security attribute 2 (SA2) and desired action are divided to 5 linguistic levels (negative big, negative small, zero, positive small, positive big). The number of input variables is not limited to two but can be an arbitrary number. The number of linguistic levels can be arbitrary odd number. The rule base that defines the linguistic relations is presented in Figure 2. Now we can read, as an example, from the Figure 2 that IF *SA1 IS negative small AND SA2 IS positive small THEN the ACTION IS positive small.* Security attribute 1 may be *session duration* and security attribute 2 may be *sensitivity of data*. An action could be that *increase the password length* to the amount of *positive small*. It is notable that the linguistic equations approach is intended for quantitative attributes. However, security metrics can be applied to express security attributes in a required quantitative form.

VI. Discussion and Future Work

Here, we have envisioned how to exploit situational awareness for security adaptation in an ICS environment by defining related concept and listing example factors that build up SA. We defined steps to produce the adaptation plan for security. Firstly, adaptation alternatives are filtered, and finally, fuzzy set theory and linguistic relations are applied to select the best alternative.

The proposed steps take into account the supported security mechanisms and the security level each mechanism is able to offer. Moreover, it is possible to develop each step further without affects to other steps. Knowledge for adaptation is retrieved from the ISMO ontology, which offers a significant advantage because knowledge is not hard-coded and it can be updated. The proposed steps are similar for each device and situation but input knowledge ensures that different adaptation plans are produced in each situation. The steps (*c.f.* Figure 4) conform the pipes and filters architecture pattern, *i.e.*, output from one step is an input for the next step [14]. The pipes and filters pattern can support multitasking and continuous execution of steps, or alternatively, steps can be executed one by one. Multitasking offers performance advantage when the purpose is to find the first acceptable adaptation from the huge set of alternatives.

Although, the proposal is on the conceptual level and it is not yet experimentally evaluated, we see it as a promising approach. Therefore, we are implementing it to our Cyber Laboratory to build an evaluation case to achieve concrete evidences and experiences from the approach. After that, it is possible to recognise missing steps and knowledge. Clearly, steps for matchmaking and trade-offs are needed in the future. Matchmaking is needed when the adaptation affects the whole environment, whereas trade-off analysis can be utilised to reveal violations for other qualities, *e.g.*, performance. Both are challenging areas but not only related to security adaptation, and thus, applicable solutions can be also found from other research areas.

We would like to note that for humans, SA can produce information in different abstraction levels and formats, but the automatic adaptation needs uniform, comparable, and well-formed SA information. Hence, the current SA solutions have to be also developed further to support machine-based decision making, *e.g.*, by providing uniform analysis techniques and formats for SA information.

Testing is a big challenge in the adaptation of ICSs. Thus, it is mandatory to take testing practices into account in the future research. We anticipate that, as high amount of false positives in the existing Intrusion Detection Systems (IDS) [15], false positives might cause challenges for situational awareness and security adaptations and the autonomic response for the incidents may be a challenge.

VII. Conclusions

This paper concentrated on the situational awareness and security adaptation. Currently, security adaptation is not applied in ICSs and the existing security adaptation approaches do not describe the creation of adaptation plan in detail. Hence, we proposed steps to create the adaptation plan by filtering adaptation alternatives and performing selection with the fuzzy set theory and linguistic models. The proposed steps utilise ontology-based knowledge base to present adaptation knowledge in an extensible form.

Acknowledgment

The work was financially supported by Academy of Finland SAICS and SASER-Siegfried Celtic-Plus projects.

References

[1] M. R. Endsley, "Designing for situation awareness: An approach to user-centered design" 2nd ed., CRC Press, Boca Raton, 2011.

[2] J. O. Kephart, D. M. Chess, "The vision of autonomic computing", vol. 36, Computer, 2003, pp. 41-50.

[3] A. Evesti, J. Suomalainen, E. Ovaska, "Architecture and Knowledge-driven Self-adaptive Security in Smart Spaces", vol. 2, Computers 2013, pp. 34-66.

[4] U. Franke, J. Brynielsson, "Cyber situational awareness – A systematic review of the literature", vol 46, Comput.Secur. 2014, pp. 18-31.

[5] M. Salehie, L. Pasquale, I. Omoronyia, B. Nuseibeh, "Adaptive security and privacy in smart grids: A software engineering vision", In Proceedings of the International Workshop on Software Engineering for the Smart Grid, 2012, pp. 46-49.

[6] E. Yuan, S. Malek, "A taxonomy and survey of self-protecting software systems", In Proceedings of the Software Engineering for Adaptive and Self-Managing Systems, 2012, pp. 109-118.

[7] A. Evesti, E. Ovaska, "Comparison of Adaptive Information Security Approaches", ISRN Artificial Intelligence, 2013, pp. 1-18.

[8] ISO/IEC 9126-1:2001 Software Engineering - Product Quality - Part 1: Quality Model, International Organization of Standardization 2001.

[9] R. von Solms, J. van Niekerk, "From information security to cyber security", vol. 38, Comput.Secur., 2013, pp. 97-102.

[10] K. Stouffer, J. Falco, K. Scarfone, "Guide to Industrial Control Systems (ICS) Security", NIST Special publication 800-82, 2011.

[11] A. Evesti, R. Savola, E. Ovaska, J. Kuusijärvi, "The Design, Instantiation, and Usage of Information Security Measuring Ontology", In Proceedings of the 2nd International Conference on Models and Ontology-based Design of Protocols, Architectures and Services, 2011, pp. 1-9.

[12] M. R. Endsley, "Design and evaluation for situation awareness enhancement", In Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 1988, pp. 97-101.

[13] T. Frantti, M. Majanen, "An expert system for real-time traffic management in wireless local area networks", vol. 41, Expert Syst.Appl. 2014, pp. 4996-5008.

[14] F. Buschmann, R. Meunier, H. Rohnert, P. Sommerlad, M. Stal, "Pattern-oriented software architecture - A system of patterns", John Wiley, 1996.

[15] E. Cole, R. Krutz, J. W. Conley, "Network Security Bible", 2nd ed., Wiley 2009.