An Assessment Model for Continuous Security Compliance in Large Scale Agile Environments

Exploratory Paper

Sebastian Dännart[1,2(✉)], Fabiola Moyón Constante[2], and Kristian Beckers[2]

[1] Infodas GmbH, Cologne, Germany
s.daennart@infodas.de
[2] Siemens Corporate Technology, Munich, Germany
{fabiola.moyon,kristian.beckers}@siemens.com

Abstract. Compliance to security-standards for engineering secure software and hardware products is essential to gain and keep customers trust. In particular, industrial control systems (ICS) have a significant need for secure development activities. The standard IEC 62443-4-1 (4-1) is a novel norm that describes activities required to engineer secure products. However, assessing if the norm is still fulfilled in continuous agile software engineering environments is difficult. It often remains unclear how the agile and the secure development process have to intertwine. This is even more problematic when changes on the basis of assessment results of 4-1 or other secure development activities have to be applied. We contribute a novel assessment model that contains a baseline process for secure agile software engineering compliant to 4-1. Our assessment results show precisely where in the development process activities or artifacts have to be applied. Moreover, it contains a refinement into goals and metrics that allow the evaluator to present the evaluate with a precise 'shopping list' of where to invest to achieve compliance. Afterwards, management can include precise compliance expenditure estimates in their business models.

Keywords: IT security · Agile development · Compliance assessment · Security standard

1 Introduction

Agile software engineering provides the basis for faster software development aligned with a close cooperation with the customer and is a de-facto standard for software engineering in numerous domains [18]. Nevertheless, software engineering for domains with a high demand for security, such as industrial control systems (ICS), has several obstacles to overcome before agile methodologies can be largely applied. In particular, software for security critical systems often has to

P. Giorgini and B. Weber (Eds.): CAiSE 2019, LNCS 11483, pp. 529–544, 2019.
https://doi.org/10.1007/978-3-030-21290-2_33

be engineered compliant to security standards, which demand numerous security analysis and risk management activities, as well as strict documentation. Today software engineering methods are missing to provide compliance to these standards and large scale agile methodologies, e.g. the Scaled Agile Framework (SAFe) [16]. The ICS domain is regulated by security-standard family IEC 62443 and the secure software engineering process by IEC 62443-4-1 [5] (4-1) in terms of cybersecurity. Current research [14] contains an approach that analyzed and modeled this standard and the agile software engineering processes SAFe. The result is a set of BPMN processes that shows the activities and artifacts required to fulfill both standards. Furthermore, some proposals were made how to merge the 4-1 standard and SAFe. To meet specific agile requirements, such as lean processes with high flexibility, all conformance actions are consequently integrated in the existing agile development cycle without bloating processes.

Our contribution is an assessment methodology for agile security compliant processes based on the SAFe and 4-1 models. Process maturity assessment can answer the question, how repeatable and optimized the agile development process is, while security-standard assessment methods provide details of non-conformance with the norms. Transferring the agile mindset into the assessment, not only the process is measured, but conformance can be monitored during repeated agile-specific characteristics, such as sprints. Currently, these assessments have to be done separately. We propose to combine these assessments into one method provides both answers. For that end, we re-use the established Capability Maturity Model Integration for development (CMMI-dev) to assess process maturity and we add a model for measuring artifact quality because security standard compliance assessments are largely based on documentation. Furthermore, we designed this tool to support security compliant management decisions. Therefore, we provide the means to create a detailed 'shopping list' of which activities and artifacts need to be created to achieve security compliance. This list can be enhanced with costs so the management can weight the cost of security compliance versus the expected revenue it generates.

We evaluated our exploratory approach with one of Germany's largest industrial actors in the field of ICS. For that purpose, we interviewed in total 21 senior industrial experts from the fields of software development, security engineering and security management. Interviews with those experts were used to evaluate practical applicability and the utility of our work.

2 Background and Related Work

Security-Standard Compliant SAFe. *IEC 62443* constitutes a series of standards for network and system security published by the International Electrotechnical Commission (IEC). Group 4 focuses on requirements for component providers for industrial automation and control systems, part 4-1 describes process requirements for secure product development [5]. We refer to this part of the standard as "4-1" or"4-1 standard". The *Scaled Agile Framework (SAFe)* is a widely used process framework that scales lean and agile development to large

organizations with multiple levels and that defines corresponding roles, responsibilities, activities, and artifacts [10]. For such environments Security-standard compliant SAFe (S^2C-SAFe) aims to bridge the gap between lean and agile development, practical security, and compliance [14]. S^2C-SAFe is one solution for the well-known research problem of integrating security into lean and agile methods [1,3,19] and the only solution for integrating 4-1 and SAFe.

Maturity Models for Security and Agile. Measuring maturity of development processes is a well-known field that contains common frameworks like the Capability Maturity Model Integration for development (CMMI-dev) [2], the ISO/IEC 15504 SPICE-framework [15], or the COBIT5 Process assessment model [6]. All of them focus on processes and define several maturity levels for assessing the processes maturity. Concerning agile development, current models do not focus on security but aspects like velocity, estimated effort, or sprint planning [8]. Furthermore, security requirements are hard to measure and very specific for each case, the range of assessment models in this field is narrow [7]. Considering the individual requirements of assessment of the combination of both, security and agile development, there are no common models.

Related Work. A common theme in security requirements engineering is modeling aspects of socio technical systems (STS). For example, Lamsweerde [9] investigates security requirements for software, Mouratidis [13] and Liu [12] analyze organizational security issues, and Herrmann [4] focuses on business processes. The work of Li [11] considers all aspects of STS in one holistic model. These approaches have in common that they often analyze security concerns in separate models. This leads to a gap in knowing where to conduct which security activity in a large scale agile process.

3 Security-Standard Compliance Assessment Model

As a first step, we set up on Moyons [14] work and completed S^2C-SAFe by injecting requirements of all practices of the 4-1 standards into the agile development processes of SAFe; a framework of about 80 single models arose. Of course, by just merging all the processes there is no evidence of compliance until particular implementation has been reviewed. For stating compliance with the requirements of 4-1, the norm demands one or more of the following conditions per requirement:

1. processes named by the requirement shall be specified, employed or enforced
2. certain aspects shall be defined, identified, characterized, tracked or documentation shall be created.

Following this segmentation, 4-1 requirements can be divided into two dimensions of requirements - *processes* and *artifacts*. Within the processes certain IT

security measures shall be implemented within the development process. Artifacts represent outputs and deliverables needed to prove compliance. Those can be embodied as code snippets, log files or other sort of documentation. Hence a model which aims to assess compliance has to factor both, *process maturity* and *artifact quality*, in.

The Security-standard Compliance Assessment Model (S^2C-AM) presented in this paper combines both dimensions to deliver a consolidated state of compliance for each requirement of the 4-1 standard.

3.1 Process Maturity

There are several models to assist assessing the maturity of processes (see Sect. 2). The 4-1 itself proposes CMMI-dev [2] to measure maturity of required processes. Moreover, the 4-1 [5] delivers a mapping between CMMI-devs maturity levels and the expectations on processes by the 4-1 standard itself. S^2C-AM utilizes this mapping for the process dimension of compliance assessment.

Furthermore, the proposed approach delivers specific metrics for every process the 4-1 requires. Due to the major focus of agile development on processes and the ability of S^2C-SAFe to keep processes lean in spite of additional security tasks, the proposed approach delivers metrics for those goals as well. Those metrics are part of the requirement cards described in Sect. 3.4 of this paper.

3.2 Artifact Quality

In contrast to process maturity methods for measurement of artifact quality is hardly prevalent. Therefore, we propose a new model based on maturity levels as well to keep needed skill adaption down.

Basically, two aspects describe the quality of artifacts: completeness and timeliness. The quality of an artifact arises of the combination of both (Table 1).

Levels and descriptions have been designed iteratively and were discussed and optimized in cooperation with process and security experts.

As mentioned above the quality of artifacts is based on the two aspects of completeness and timeliness. To support decision making on which level fits best, we deliver a support matrix (shown in Fig. 1) which combines both aspects to a certain artifact quality level. Basically, the single aspect has to be rated from 0 - none/worst to 2 - complete/best. The two grey fields logically can not be true: if there is no documentation, it cannot be up-to-date.

3.3 Compliance Matrix

After process maturity and artifact quality for a single requirement have been elicited, the requirement can be placed in the compliance matrix as shown in Fig. 2. The vertical axis displays the level of process maturity described in Sect. 3.1, the horizontal one covers the level of artifact quality in Sect. 3.2.

Four example requirements have been placed in Fig. 2 representing the requirements of 4-1 standards *Practice 3 Secure Design*. Focusing on displayed

Table 1. Profile groups and count of interviewees each.

Level	Quality level	Description
1	None	There is no documentation available
2	Partial	Documents and output of processes comply to certain requirements of 4-1 standard. Possibly information is available in different sources but has to be consolidated to meet requirements completely. Potentially some artifacts are not up-to-date
3	Complete	All necessary artifacts to proof compliance are available in a structured form. Potentially some artifacts are not up-to-date
4	Up-to-date	To reach this level, creation and update of artifacts are fully integrated in the employed S^2C-SAFe processes. Processes are lived and updates on a regular basis are verifiably warranted Note: To reach this level, usually there is a process maturity of level 3 necessary

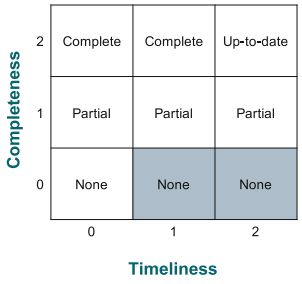


Fig. 1. Support matrix for categorization of artifacts

requirement *SD-1* it seems that the required process has a process maturity of "2 - Managed" and the artifact quality of the artifacts demanded by 4-1 in this single requirement is "2 - partial".

During workshops with 4-1 experts they pointed out that an auditor or evaluator would expect certain minimum process maturity and artifact quality to see the 4-1 requirements as fulfilled: a minimum of level 3 for each of the compliance dimensions is necessary. Therefore, the green coloured area of the matrix in Fig. 2 represents 4-1 standard compliance. The orange area is not completely compliant and has some specific deficits. The red area is not compliant, while

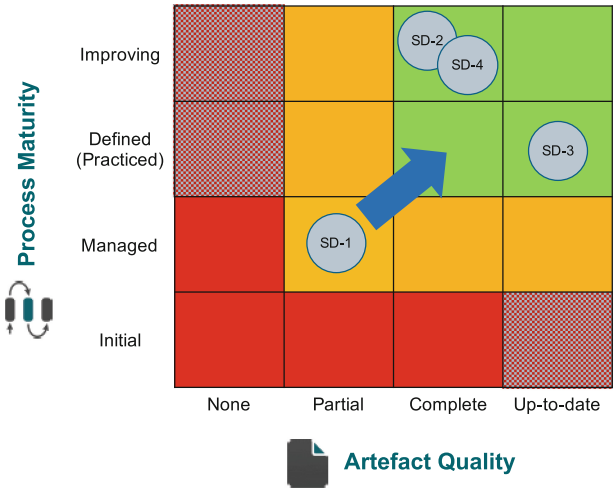


Fig. 2. Compliance matrix with exemplary requirements

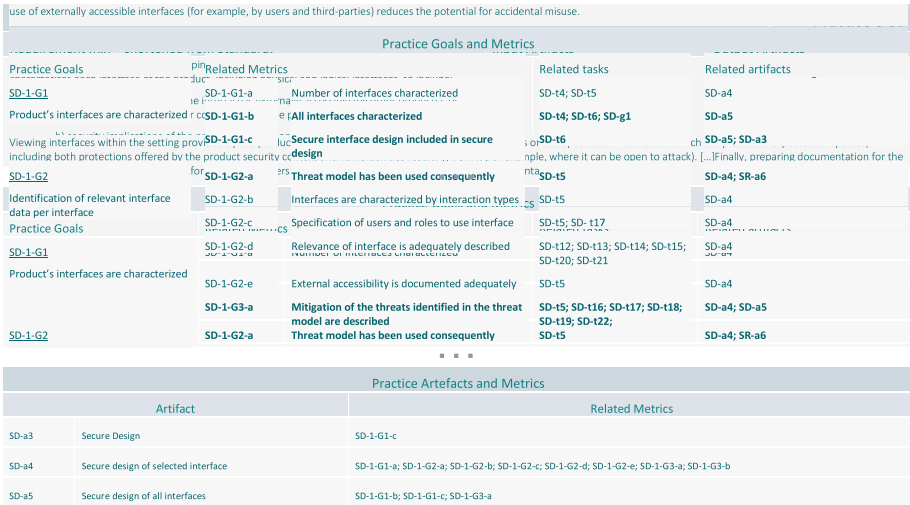
the shaded area is logically not possible: if there is a defined process according to S^{2}C-SAFe, there cannot be no artifact, as well as an up-to-date artifact is impossible with just having an initial process.

3.4 Requirement Cards

Before the level of compliance can be displayed in the proposed model, the compliance to a certain 4-1 requirement has to be assessed. Therefore, we designed requirement cards as shown exemplarily in Fig. 3. Besides a summary of the original text from the 4-1 standard, we added expected input artifacts and expected output artifacts. To facilitate compliance assessment we derived particular practice goals from the 4-1 requirements and enriched them with related metrics to enable precise assessment of achievements. The subsumption of those assessments allows a placement of the requirement in the S^{2}C-AM matrix.

Using the same identifiers as used in S^{2}C-SAFe a direct link into the agile processes is possible. Thereby, input and output artifacts can be determined precisely and for every metric relevant tasks and artifacts are assigned. With this, both, product supplier and auditors, for instance can easily identify where in the agile development process improvements have to take place and which processes struggle. Focusing on artifacts, a cross-reference for related metrics to every output artifact was added.

As the arrow in Fig. 2 indicates, for requirement *SD-1* process maturity as well as artifact quality have to be improved to become compliant. To identify potential improvements the requirements card points on possible weak points and proposes tasks and artifacts to focus on to expunge them.



use of externally accessible interfaces (for example, by users and third-parties) reduces the potential for accidental misuse.

Practice Goals and Metrics

Practice Goals	Related Metrics		Related tasks	Related artifacts
SD-1-G1	SD-1-G1-a	Number of interfaces characterized	SD-t4; SD-t5	SD-a4
Product's interfaces are characterized r	**SD-1-G1-b**	**All interfaces characterized**	**SD-t4; SD-t6; SD-g1**	**SD-a5**
Viewing interfaces within the setting prov	**SD-1-G1-c**	**Secure interface design included in secure design**	**SD-t6**	**SD-a5; SD-a3**
including both protections offered by the product security c			nple, where it can be open to attack). [...]Finally, preparing documentation for the	
SD-1-G2	**SD-1-G2-a**	**Threat model has been used consequently**	**SD-t5**	**SD-a4; SR-a6**
Identification of relevant interface data per interface	SD-1-G2-b	Interfaces are characterized by interaction types	SD-t5	SD-a4
Practice Goals	SD-1-G2-c	Specification of users and roles to use interface	SD-t5; SD- t17	SD-a4
SD-1-G1	SD-1-G2-d	Relevance of interface is adequately described	SD-t12; SD-t13; SD-t14; SD-t15; SD-t20; SD-t21	SD-a4
Product's interfaces are characterized	SD-1-G2-e	External accessibility is documented adequately	SD-t5	SD-a4
	SD-1-G3-a	**Mitigation of the threats identified in the threat model are described**	**SD-t5; SD-t16; SD-t17; SD-t18; SD-t19; SD-t22;**	**SD-a4; SD-a5**
SD-1-G2	**SD-1-G2-a**	**Threat model has been used consequently**	**SD-t5**	**SD-a4; SR-a6**

Practice Artefacts and Metrics

Artifact		Related Metrics
SD-a3	Secure Design	SD-1-G1-c
SD-a4	Secure design of selected interface	SD-1-G1-a; SD-1-G2-a; SD-1-G2-b; SD-1-G2-c; SD-1-G2-d; SD-1-G2-e; SD-1-G3-a; SD-1-G3-b
SD-a5	Secure design of all interfaces	SD-1-G1-b; SD-1-G1-c; SD-1-G3-a

Fig. 3. Excerpts of the requirement card for the *Secure Design* requirement *SD-1 Secure design principles*

3.5 From Assessment to Process Improvement

Combining the components, namely the S^{2}C-SAFe, the bi-dimensional compliance matrix and the requirement cards as well as the method to use them, there appears a direct path to particular improvement of certain practice goals. Figure 4 drafts this process. Sticking to the same example as in Sect. 3.3 and Fig. 2 Requirement *SD-1* is still in deficit. As shown in Fig. 4 the requirement card of *SD-1* suggests metrics for the practice goal and points on related tasks and artifacts responsible for the performance concerning this metric. The next step leads directly into the S^{2}C-SAFe development process as shown in the process excerpt in Fig. 4. Thus, the highlighted elements of the process model have a direct impact on the compliance.

4 Support of Business-Relevant Security Choice

One major goal, besides the pure assessment of security-standard compliance, was the ability to integrate the S^{2}C-AM results in common management frameworks. Delivering security demands through well-known methods will make it easier for management to include security in their daily thoughts. Enabled through the design of the requirement cards this component of the proposed approach facilitates refinement of business goals, justification of security spendings and a steering tool.

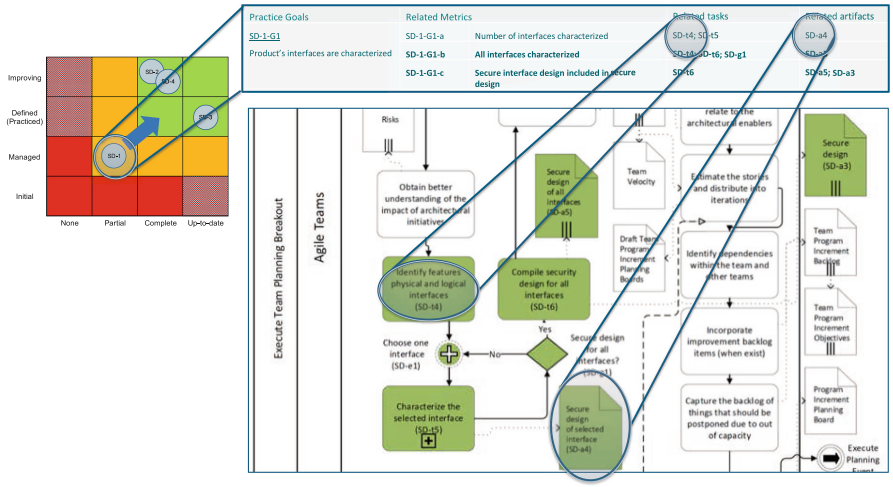


Fig. 4. Connection of multiple elements: compliance matrix (top left); excerpt of the *SD-1* requirement card (top right); excerpt of S^{2}C-SAFe (bottom right), showing parts of *SD-1* integration.

4.1 Refinement of Business Goals

COBIT5 derives its processes from IT-related goals which cascade from enterprise goals and stakeholder needs [6]. Following this method, the design of the requirement cards is based on process description in COBIT5. Moreover, COBIT5s goal cascade can be extended by the requirements of the 4-1 standard. As shown in Table 2 we developed cross-reference tables, which assign the practice goals, introduced in Sect. 3.4, to COBIT5s IT-related goals. Just as in COBIT5, the practice goals are marked as primary (P) or secondary (S) influencing the referenced IT-related goal.

Via this reference, practice goals can be connected directly to IT-related goals and their reference to enterprise or business goals, thus, their business relevance can be illustrated. Vice versa business goals can be refined down to the level of practice goals for secure development and - in connection with the requirement cards - down to security tasks in the agile development process.

4.2 Justification of Security Spendings

Security spendings are hard to justify because measures and projects often do not offer a clear return on investment (ROI) and so security budgets stay narrow. By building a causal chain between enterprise goals and particular security processes, investments can be linked up to actual business strategies.

As process tasks and creation of artifacts need a certain amount of time and money, a particular assumption of costs for improvement of the identified process parts. Therefore, through the proposed approach, not only a assessment of compliance can be made but costs for compliance improvement can be specifically

Table 2. Example of COBIT5 IT-related goals cross-reference matrix for practice goals of 4-1 requirement *SD-1 Secure design principles*. (P = primary influence; S = secondary influence)

Practice 3 Secure Design SD-1 Secure Design Principles		IT compliance	IT-related risk	Transparency of IT costs	Security of information	Secure IT product development
		02	04	06	10	18
SD-1-G1	Products interfaces are characterized	P	S	P	P	P
SD-1-G2	Identification of relevant interface data	P	S		S	P
SD-1-G3	Mitigation of vulnerability of interfaces	P	S		S	P

calculated. By utilizing the connection to the COBIT5 goal cascade (see Fig. 2) those costs can be assigned to certain enterprise goals and strategic alignment.

With this approach, management can decide which costs the more of compliance causes and if adjustments are worth it.

4.3 Management Steering Tool

While the proposed metrics help to assess compliance, process maturity and artifact quality, they are an opportunity to enable managers fine-tune their processes. Having a look at the compliance matrix of Sect. 3.3, it shows not only the compliance level but offer starting points for improvement or change processes. Taking a look on a special goal from a certain practice goal, particular tasks can be identified in the agile development process and chosen for improvement projects. While a certain objective should be reached with those projects, possible consequences for other IT-related, and enterprise goals can be derived from the cross-reference tables. This enables managers to choose whether to improve a single requirement with a single focus or to earn low hanging fruits by improving requirements with multiple effects.

5 Evaluation

To evaluate the proposed assessment model and the method to use it, we conducted a qualitative expert interview series. During 21 semi-structured interviews with experts, working as cybersecurity specialists and managers at one of Germany's largest industrial actors, our main focuses were the needs of practitioners and how the S2C-AM can solve them. Moreover, we asked for practical benefits the S2C-AM delivers and the potential limitations of the approach. After all, we tried to figure out if the experts would use the model in there daily

work. Therefore, the following research questions (RQ) guided our evaluation and where asked among others during the interviews[1]:

RQ 1 Does S²C-AM cover all relevant aspects for compliance assessments?
RQ 2 From management perspective, does the model deliver the information managers demand for?
RQ 3 Which challenges exist when assessing security-standard compliance in this way?

5.1 Subject Selection

The S²C-AM will mainly touch three different fields in practice: security, agile development and management. The model can potentially either bring benefits or barriers for players in all three areas.

To collect necessary needs and opinions from all the necessary fields, connected with security compliance, we asked security experts and agile development experts as well as governance and management experts. They cover for instance internal security process consultants, IT-infrastructure security specialists, developers and project leaders in agile environments, security governance consultants as well as managers from different business units. Additionally, among our interviewees there were IEC committee members for the IEC 62443 standard and an active contributor to SAFe.

Table 3 lists expert profiles, characterizes them and shows the number of interviewees associated with that group. Each interviewee was associated to only one group. We distinguish between different senior security experts, according to their main expertise and current area of responsibility.

5.2 Survey Instrument

Due to our goal to receive new ideas, valuable input and important expertise besides the singular appraisal of our method, we selected semi-structured interviews as the technique to conduct the interviews [17]. Meeting the interviewees in insulated environments, the interviews lasted between 60 and 90 min. One or two interviewers conducted the interviews with one to a maximum of two experts.

Each interview started with a quick briefing of the interview flow, followed by of a short explanation of the subjacent S²C-SAFe and a detailed introduction in the S²C-AM, containing the models elements, its possible application and the management integration approach. Afterwards the semi-structured interview was based on an interview guideline which consisted of five areas based on the research questions defined above.

[1] For the complete interview questionnaire visit https://sites.google.com/view/s2c-am-evaluation.

Table 3. Profile groups and count of interviewees each.

Profile	Characterization	Interviews	Count
SAFe Contributors	Contribute to improve SAFe. Companies ultimate experts concerning scaled agile	#8	1
IEC 62443 Contributors	Contributed to and evaluated the IEC 62443 norm for the IEC. Companies ultimate experts concerning for IEC 62443	#16, #17	2
Senior experts for IT security (management position)	Experienced and accepted experts for IT security. Holding a management position in the company	#9, #10, #13, #18, #21	5
Senior experts for security in IT infrastructure	Experienced and accepted experts for IT security. Responsible for IT security concerning IT infrastructure in their company	#14, #15	2
Senior experts for IT security governance	Experienced and accepted experts for IT security governance in their company, including IT governance, maturity models and frameworks	#1, #2 #20	3
Senior experts for IT security processes	Experienced and accepted experts for IT security processes. Responsible for IT security process assessment in their company	#4, #5 #19	3
Senior experts for agile development	Experienced and accepted experts for agile methodology and development. Responsible for agile development processes in their company	#3, #7 #11, #12	4
Experts for IT security	Experts for IT security in others than the areas above	#6	1
Overall count			21

5.3 Evaluation Results

As we analyzed the opinions of all experts in a qualitative manner, the following section summarizes all answers and interprets the results according to our research questions. Answers of particular interviewees will be pointed out by referencing the interview number (e.g. #13).

Section 5.3 Process maturity model, 5.3 Artifact quality model and 5.3 Compliance matrix discuss the basic elements of the model and answer on research question 1 (RQ1). Section 5.3 Management deals with RQ2 and Sect. 5.3 Practical use answers RQ3.

In addition, we asked if process maturity and artifact quality level description as well as the compliance matrix is intuitive and easy to understand. As Fig. 5 shows, the opinion of the interviewees is for all three aspects satisfying. The newly developed levels of the artifact quality are for 85 percent of the inter-

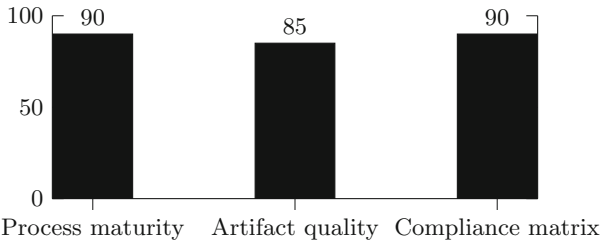


Fig. 5. Percentage of interviewed experts, who find the mentioned elements of the model intuitive and easy to understand.

viewees intuitive and easy to understand. 90 percent described the combined representation of both dimensions in the compliance matrix like this as well.

Process Maturity Model. For the design of the process maturity dimension we adopted the CMMI-dev-based model the 4-1 proposes. Interviewees encouraged us to do so and titled this as a good basis for acceptance in practice.

"Applying this, we would be way ahead." - *IEC 62443 Contributor (#16)*

Three interviewees (*#8, #18, #21*) mentioned using CMMI-dev as a baseline means a lack of agile aspects. The levels adopted from 4-1 standard do not clearly require the process to be lived, four of the interviewees (#1, #5, #7, #10) pointed out. Finally three experts (#12, #13, #14) mentioned that a questionnaire or any other support for conduction the assessment might be helpful.

Artifact Quality Model. While most experts (17 out of 21) agree that the two major aspects for a good artifact are completeness and timeliness, a few more aspects to consider were named: for instance correctness of content *(#7, #8)*, traceability *(#18)* and understandability *(#10)*. Moreover, four interviewees *(#4, #12, #14, #20)* demanded templates for each required artifact, to deliver precise information on required structure and content. Only one participant *(#19)* called the artifact dimension "understandable but unnecessary".

"This seems to be a very good method." - *IEC 62443 Contributor (#17)*

Although one interviewee (*#2*) was in doubt if timeliness is really measurable, another expert *(#6)* said that "the use of the support matrix illustrates the path to certain levels very comprehensible". Finally, an *IT infrastructure expert (#14)* presumed that "the model might be much more valuable than just to use it for agile development."

Compliance Matrix.

"If we only get those two dimensions under control, we are fine!" - *Agile development expert (#7)*

The conjunction of process maturity and artifact quality was appreciated by all experts but one (*#19*) who thought it was too complex. Two interviewees (*#12, #18*) missed roles and responsibilities in this representation and another one (*#17*) supposed to put in a third dimension of "multiple projects in a row". First and foremost the simplicity of this representation and the good level of abstraction for the management is emphasized by the interviewed experts.

> "Especially for representing conformity, that model is perfectly comprehensible." - *Senior expert IT security in management position (#18)*

Management Focus.

> "The matrix is a really good representation, this is exactly what they want." - *IEC 62443 Contributor (#16)*

Regarding RQ1, we asked all experts, if the model delivers all necessary information demanded by the management for compliance insights and control decisions - 95 percent agreed completely. Although some raised that only the matrix should find its way into management summaries due to complexity of the requirement cards. Their granularity might be to detailed but could be abstracted.

Moreover, one *IEC 62443 contributor* mentioned (*#16*) that the complete model might be a enormous help for auditors as well. An *IT security expert in management position* highlighted the expedient value of cascading from enterprise goals down to practice goals and vice versa. Two-thirds appreciate the link-ability to COBIT5s goal cascade and the adoption of its process description for the requirement cards, as it is a well known IT government framework.

> "Until now we did not find an appropriate bridging between business an IT - this seems to be a good one." - *Senior expert IT security in management position (#18)*

Practical Use.

> "This approach perfectly fits to our manner of depicting and living processes." - *IEC 62443 Contributor (#16)*

About 80% of the experts would like to try the approach directly in their division. The others concerned that it might be to heavy to integrate ad hoc and would wait until pilot projects worked out. Regarding RQ2 the main challenges the participants see are the regulation of process overhead and therefore the acceptance of the higher workload for development teams. Moreover, some demand for a road map and trainings for developers as well as project leaders to introduce the model.

The rising relevance of compliance and its verification in the future makes this model a valuable asset, a *senior expert IT security in management position (#21)* stated. Some experts see more than an assessment tool in this approach

by now. Although an *expert for security in IT infrastructure (#15)* complained that in his sense most managers trust their guts instead of rational criteria.

Finally, the concluding tenor of almost all interviews was: "please, can we give it a try?"

6 Conclusion and Future Work

Our contribution provides a foundation for business-driven security compliance management. It is currently tailored to the security-standard IEC 62443-4-1 (4-1) for secure product development in the industrial control system (ICS) domain and the Scaled Agile Framework (SAFe). However, they are currently provided in BPMN models, these can be exchanged with little effort and therefore allow our approach to be used with other standards and frameworks as well.

In particular, we showed how the precision of process models in combination with security maturity assessment based on the 4-1 standard can be utilized to detect non-conformance, precisely describe what activities and artifacts have to be improved or introduced. By this, our method delivers compliance by default. Moreover, it enables to estimate the costs of security compliance. Note that costs can be expressed in time, which the activities add to the overall development effort, in the amount of money these extra hours cost, and in the costs for creating and maintaining the additional artifacts. These numbers provide management with an estimation of how much they have to spend for security compliance. Therefore, management can decide if the costs for compliance justifies the improvement in product quality.

Results of our evaluation with numerous key stakeholder of a major industry player in the field of ICS confirm the usefulness and applicability of our work.

6.1 Limitations and Threats to Validity

We discuss the threats to validity using the four validity classes proposed by Wohlin et al. [20].

Construct Validity. The measurements of the experiment include the process maturity standard CMMI-dev, which is an internationally established method to assess process quality. Therefore, we believe this measure to be appropriate for our study. The artifact quality approach adopts the same method. Combination of two dimensions in a matrix is a common, intuitive method to aggregate. However, findings are based on opinions of experts, which did neither have hands-on experience with the model nor the method.

Conclusion Validity. The experiment was conducted by using one particular part of the security standard IEC 62443-4-1 and SAFe. We decided not to show the entire models and assessment tool in order to avoid lengthy processes and too much complexity. Moreover, the participants were interviewed individually, to avoid that they talk to each other.

Internal Validity. We selected practitioners in this experiment who hold leading positions in software engineering and security engineering in a large German company, active in the field of ICS. To assess expert status, we asked the participants for a self-assessment of their knowledge and skills in the knowledge areas of security and software engineering.

References

1. Ahola, J., et al.: Handbook of the Secure Agile Software Development Life Cycle. University of Oulu, Finland (2014)
2. CMMI Product Team: CMMI for Development, version 1.2 (2006)
3. Fitzgerald, B., Stol, K.J.: Continuous software engineering: a roadmap and agenda. J. Syst. Softw. **123**, 176–189 (2017)
4. Herrmann, P., Herrmann, G.: Security requirement analysis of business processes. Electron. Commer. Res. **6**(3), 305–335 (2006)
5. IEC: 62443-4-1 Security for industrial automation and control systems Part 4–1 Secure product development life-cycle requirements. IEC (2016)
6. Isaca, P.A.M.: Using COBIT 5. ISACA, Rolling Meadows (2013)
7. Jaquith, A.: Security Metrics: Replacing Fear, Uncertainty, and Doubt. Pearson Education, London (2007)
8. Kupiainen, E., Mäntylä, M.V., Itkonen, J.: Using metrics in agile and lean software development - a systematic literature review of industrial studies. Inf. Softw. Technol. **62**, 143–163 (2015)
9. van Lamsweerde, A., Letier, E.: Handling obstacles in goal-oriented requirements engineering. IEEE Trans. Softw. Eng. **26**(10), 978–1005 (2000)
10. Leffingwell, D., Yakyma, A., Jemilo, D., Oren, I.: SAFe Reference Guide. Pearson, London (2017). (2017 edn.)
11. Li, T., Horkoff, J.: Dealing with security requirements for socio-technical systems: a holistic approach. In: Jarke, M., et al. (eds.) CAiSE 2014. LNCS, vol. 8484, pp. 285–300. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-07881-6_20
12. Liu, L., Yu, E., Mylopoulos, J.: Security and privacy requirements analysis within a social setting. In: Proceedings of the 11th IEEE International Conference on Requirements Engineering, RE 2003, Washington, DC, USA, pp. 151. IEEE Computer Society (2003)
13. Mouratidis, H., Giorgini, P.: Secure Tropos: a security-oriented extension of the Tropos methodology. J. Auton. Agents Multi-Agent Syst. (2005)
14. Moyon, F., Beckers, K., Klepper, S., Lachberger, P., Bruegge, B.: Towards continuous security compliance in agile software development at scale. In: Proceedings of RCoSE. ACM (2018)
15. Pino, F.J., Baldassarre, M.T., Piattini, M., Visaggio, G.: Harmonizing maturity levels from CMMI-DEV and ISO/IEC 15504. J. Softw. Maintenance Evol.: Res. Pract. **22**(4), 279–296 (2010)
16. Scaled Agile Inc.: Safe reference guide (2017). http://www.scaledagileframework.com/
17. Shull, F., Singer, J., Sjøberg, D.I.: Guide to Advanced Empirical Software Engineering. Springer, London (2007). https://doi.org/10.1007/978-1-84800-044-5
18. TechBeacon: Survey: is agile the new norm? (2017). https://techbeacon.com/survey-agile-new-norm

19. Turpe, S., Poller, A.: Managing security work in scrum: tensions and challenges. In: Proceedings of SecSE (2017)
20. Wohlin, C., Runeson, P., Höst, M., Ohlsson, M.C., Regnell, B., Wesslén, A.: Experimentation in Software Engineering. Springer, Berlin (2012). https://doi.org/10.1007/978-3-642-29044-2