Current and Necessary Insights into SACM

An Analysis Based on Past Publications

Jose Luis de la Vara
Certus Centre for Software V&V, Simula Research Laboratory
P.O. Box 134, 1325 Lysaker, Norway
jdelavara@simula.no

***Abstract*—SACM (Structured Assurance Case Metamodel) is a standard for assurance case creation and exchange. Although it is a promising initiative towards providing common system assurance practices and improving them, the document of the standard provides little information about how to use SACM, its benefits, and its limitations. Consequently, it is difficult to determine what SACM can be used for and what needs to be investigated about the standard. This position paper aims to address this issue by reviewing 28 publications that have referred to SACM. Based on the insights gained, we propose a set of aspects that need to be further studied. This information can be valuable for anyone interested in the standard.**

***Index Terms*—SACM, Structured Assurance Case Metamodel, assurance case, structured argumentation, evidence management, system assurance, safety assurance, security assurance.**

I. Introduction

SACM (Structured Assurance Case Metamodel; [20]) is an OMG (Object Management Group) standard that specifies a common framework for assurance case development and exchange. It defines assurance case as a collection of auditable claims, arguments, and evidence created to support the contention that a defined system or service will satisfy certain requirements (e.g., regulatory or safety requirements). According to SACM, assurance cases allow system assurance knowledge to be communicated in a clear and defendable way, and support information exchange between suppliers and acquirers, and between operators and regulators.

SACM 1.0 was released in 2013. It consists of an argumentation metamodel and an evidence metamodel, and aims to provide means that facilitate and improve assurance case management. Five companies (Adelard, Benchmark Consulting, Computer Sciences Corporation, KDM Analytics, and Lockheed Martin) and the University of York have contributed to the specification of the standard, all of them with wide experience in system assurance. Therefore, one could expect that SACM fits industry needs for managing assurance cases. However, the document of the standard does not provide many details about how to use it, its benefits, and its possible limitations. Indeed, we have indicated potential issues in SACM in previous publications (e.g., [9]; see Section II.B). It is currently difficult to judge what SACM aspects require further study in order to determine, for instance, how to improve it or facilitate its adoption in industry.

This position paper aims address this issue by analysing the current insights that past publications have provided into SACM. We have reviewed 28 publications that have analysed or implemented SACM, or discussed its possible usage. Most of these publications (26) relate to five main system assurance areas: safety evidence management, safety argumentation, safety compliance, security assurance, and tool support. The other two publications are on system assurance in general.

As a result of the insights gained, we present a set of six aspects that need to be further studied: SACM usage examples, detailed analyses, suitability for assurance of various properties, interest in academia, interest in industry, and details about SACM relationship with other approaches.

To our knowledge, this is the most detailed available analysis of SACM usage possibilities and of SACM aspects to further study. No publication has reviewed the literature on SACM yet. The most similar publication is [17], which presented a systematic review on provision of evidence for safety certification. Unlike this paper, the systematic review did not focus on SACM, only dealt with safety, and did not take grey literature into account. The search for the systematic review was also performed at the beginning of 2012, before SACM 1.0 was released and most of the publications reviewed in this paper (25 out of 28) were published.

The analysis provided in the paper can be very valuable for practitioners assessing SACM adoption, for researchers aiming to determine SACM-related areas for further research, and for the people involved in the specification of the standard as they can identify possible improvements for future versions.

The rest of the paper is organised as follows. Section II reviews the insights provided into SACM in the literature. Section III discusses the SACM aspects to further study. Finally, Section IV presents our conclusions and future work.

II. SACM in the Literature

This section presents the insights provided into SACM in the literature. We outline the research method followed and review the publications selected.

A. Research Method

The overall goal of the literature review was to compile information about how to use SACM, its benefits, and its limitations. Firstly, we performed automatic searches in Google and Google Scholar. The final search string was: *("SACM" OR "structured assurance case metamodel" OR "SAEM" OR "software assurance evidence metamodel" OR ("ARM" AND*

"argumentation") OR "argumentation metamodel") AND ("OMG" OR "Object Management Group"). This string refers to both the current SACM version and previous ones. For example, SAEM corresponds to a former acronym of the evidence metamodel. For inclusion, a publication had to (1) be written in English and (2) have analysed or implemented SACM, or discussed its possible usage. Presentations and OMG documents were excluded. When a tool was referred to in a publication, we searched its website (e.g., [5]).

After selecting an initial set of 44 publications, we searched where SACM was mentioned in each publication in order to determine the insights provided. Publications that simply acknowledged SACM existence and duplicates (i.e., publications with at least one author in common that provided the same insights) were excluded (19 publications). We then added other publications of which we were aware and that had not been identified with the automatic search. We included the Astah tool [2] and two deliverables from OPENCOSS, a research project on safety certification for automotive, avionics, and railway. The final set of selected publications consisted of 28 items. No further data was extracted from the publications beyond the information presented below.

Regarding the limitations of the process, the involvement of more researchers might have mitigated threats to validity related to the possibility of missing some publication or insight. Nonetheless, we do not regard this as an important weakness. This paper mainly corresponds to exploratory research, and aims to provide general insights into SACM and its needs.

B. Literature Review

This section summarises the insights provided into SACM in past publications. Most of the publications (15 out of 28) have indicated the possible relationship of the results presented with SACM, or the possibility of further investigating this relationship. Fig. 1 shows the six categories of publications defined, indicating the percentage of publications in each category and their number (in brackets).

Safety evidence management. The publications that have probably provided more insights into SACM usage for safety evidence management are [9][18]. The former indicates possible redundant classes in the evidence metamodel, possible overlaps between the classes, and implementation decisions that might have been included. It also recommends carefully analysing SACM before deciding to use it as basis for another metamodel. Both publications indicate that the notion of evidence in SACM is unclear. In summary, these publications highlight parts of SACM that should be clarified. Other authors have indicated the potential relationship of SACM with their proposals for safety evidence lifecycle [8], for characterising safety evidence assessment [34], and for characterising safety evidence in general [21][23]. According to [17], SACM does not provide a thorough and sufficiently detailed analysis of the possible evidence types to provide for safety certification and of how to structure and assess evidence.

Safety argumentation. Six publications on safety argumentation have referred to SACM. They have investigated areas such as the formalization of safety case patterns [7], safety argumentation for unmanned avionics product lines [19], and Toulmin model-based argumentation [35]. In [13], the authors compare goal-based and process-based safety assurance and certification, and suggest that SACM can facilitate the sharing of experience and expertise on assurance cases among different application domains. An extension to SACM for compositional safety argumentation has been proposed in [22], taking also into account the possibility of specifying safety argument patterns. The approach for goal-based technology qualification presented in [29] uses KAOS models, and the authors indicate that the transformation from KAOS to SACM models, and vice-versa, could be studied.

Safety compliance. Three approaches for compliance with safety standards have referred to SACM. The model-based approach for verifying compliance with IEC61508 presented in [26] proposes the use of UML profiles, outlining how the approach could be linked to SACM. In [30], the authors indicate that concepts of their approach for analysing safety standards in the nuclear domain (e.g., justification) are related to SACM. Finally, a generic metamodel for safety standards, and more specifically for modelling how to comply with them, is proposed in [10]. The authors acknowledge that its relationship with SACM should be further investigated.

Security assurance. Four publications on how to ensure and show system security have provided insights into SACM. Its possible relation with Common Weakness Enumeration is discussed in [3], and its usage for cloud computing and the future Internet in [12]. More details about SACM usage for security assurance are presented in [15][33]. The former includes a case study in which SACM is used for assurance case specification. The latter presents a proposal for using the standard in the scope of cloud security, linking it with other approaches for governance, risk, and compliance management.

Tool support. SACM has been implemented in the CertWare tool [5]. AdvoCATE [6] claims to be compliant with SACM, and ACedit [1], Astah [2], and D-Case [11] with its argumentation metamodel. However, it seems that the SACM version taken into account in these tools is not the latest one. It is also not clear if the standard has been implemented completely or partially. The need for updating the ASCE tool so that it complies with SACM is discussed in [25].

Other insights. Other authors have indicated that SACM should be based on work conducted in linguistics and law [27], and that it can be useful for software assurance measurement [31]. These publications studied system assurance in general.

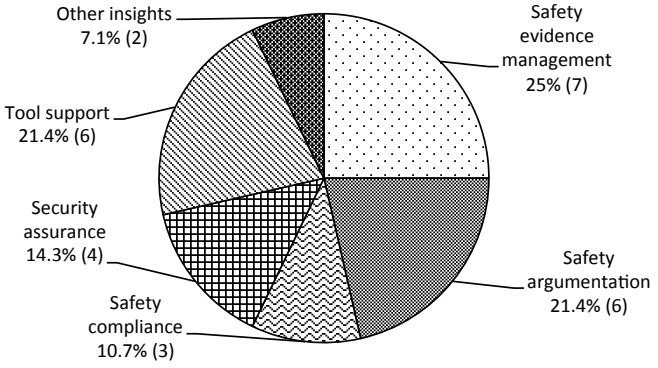

Fig. 1. Ratio of publications in each category

III. SACM Aspects to Further Study

Based on the insights gained from reviewing the literature, we propose the following six areas as the main SACM aspects that require further study. New insights into these areas would help in determining how to use SACM, how to improve or extend it, and how to facilitate its adoption in industry.

A. SACM Usage Examples

In our opinion, the main weakness of SACM currently is the extremely low number of usage examples. The document of the standard just provides two small examples about an industrial press safety argument and a Bluetooth security case. In the literature, only [15] provides a realistic and relatively elaborated usage example. In both cases, instances of the vast majority of SACM classes and associations are not shown.

The new examples must be larger, showing real-scale SACM applications. The examples are also essential to better understand the standard and its usage. In this sense, some of the possible issues identified in SACM (e.g., in [9]) might have happened because of a misinterpretation of its text. This could be mitigated with more usage examples.

Furthermore, the need for and importance of most SACM classes and association has not been shown. No example about them has been provided, thus it can be argued that no evidence of their need exists.

B. Detailed SACM Analyses

Several potential issues in SACM have been indicated in the literature. Therefore, SACM quality should be further investigated. As for other OMG standards, SACM could be analysed in relation to, for instance, its ontological foundations (as BPMN in [28]) and its complexity (as UML in [32]).

Another type of analysis that could be performed is on SACM suitability for specific purposes. For example, we are interested in further analysing SACM support for safety evidence management. To this end, we want to analyse if SACM meets the requirements for this activity that we have identified in previous studies on the state of the art [17] and on the state of the practice [16], as well as the requirements specified, for instance, in the OPENCOSS project [24].

In line with the validation conducted for the safety evidence traceability model proposed in [18], it would also be useful to analyse how assurance information of past projects could be specified with SACM. This could facilitate the determination of SACM classes and associations that might be redundant or might overlap. This would be based, for instance, on the identification of a piece of information in a past project that could be specified in two different ways with SACM.

C. SACM Suitability for Assurance of Various Quality Properties

The possible use of SACM has only been indicated for two specific system quality properties: safety and security. Furthermore, most of the publications reviewed (22 out of 28) are explicitly on or related to safety assurance. Therefore, assurance of many other quality properties with SACM needs to be studied. For example, a railway system needs to also take into account reliability, availability, and maintainability [4].

The need for assurance of various quality properties in many application domains also implies that the creation of multi-concern assurance cases with SACM should be investigated. It is not enough anymore to simply assure, for instance, safety or security requirements, as an assurance case for a system might have to justify how the system satisfies both requirements types. A comparison of the insights provided into SACM for security assurance and of those for safety assurance would also be very interesting. There is an increasing interest in the relationship between safety and security, especially in how security vulnerabilities can raise safety risks [14].

D. Interest in SACM in Academia

Another general conclusion after reviewing the literature is that the interest in SACM seems to be growing in academia. However, the set of authors that have provided insights into SACM is limited. For example, people involved in or related to OPENCOSS have participated in 12 out of the 22 publications found on safety assurance. Consequently, it is not clear yet the general interest in SACM in the research community.

E. Interest in SACM in Industry

Although past research has shown that models are used in industry for system assurance [16], five companies have contributed to SACM, practitioners have co-authored publications referring to the standard (e.g., [3][8][15][18][25][29]), and several tools support it, we think that it needs to be further investigated if industry is really interested in the standard. Based on [16], the number of companies using structured argumentation-based assurance approaches is for sure larger, but no information about their interest in and need for SACM is available. In addition, the benefits of using SACM should probably be more clearly presented, justified, and quantified for adoption in industry.

F. Details about SACM Relationships with other Approaches

Last but not least, most of the publications reviewed have acknowledged the existence of a relationship between their system assurance approaches and SACM, or the possibility of its existence. However, very few details have been provided about these relationships. Without this information, it is very difficult to determine the extent to which the approaches actually relate to SACM, or to find improvement opportunities and extension possibilities in SACM based on the publications.

IV. Conclusion

This paper has proposed six areas on which further research on SACM (Structured Assurance Case Metamodel) should be conducted in order to provide new, necessary insights into the standard. The areas are based on the results of a literature review, which corresponds to the largest collection of available information about SACM. The review shows that SACM has been referred to mainly regarding safety assurance, and that it has mostly been mentioned in past publications as a standard whose relationship with other approaches could be studied. The insights provided in the review can also be very valuable for those analysing SACM improvement or adoption, since they indicate possible issues and potential needs to address.

Studying the six areas can clearly lead to the identification of improvement opportunities in SACM. In our opinion, the issues that require immediate attention are the need for further SACM usage examples and the need for detailed analyses. Firstly, they will help researchers and practitioners to better understand SACM, its usage, its benefits, and its possible limitations. Secondly, these aspects can impact all the other areas and contribute to addressing them. A better understanding of SACM will facilitate the analysis of its suitability for various quality properties and of its relationship with other approaches, and that academia and industry gain interest in the standard.

We plan to continue analysing SACM in the future, especially its usage for safety evidence management. We would also like to study other aspects presented in Section III.

ACKNOWLEDGMENT

The research leading to this paper has received funding from the FP7 programme under the grant agreement n° 289011 (OPENCOSS) and from the Research Council of Norway under the project Certus-SFI.

REFERENCES

[1] ACedit, http://acedit.googlecode.com (Accessed May 28, 2014)

[2] Astah, http://astah.net/editions/gsn (Accessed May 28, 2014)

[3] B. Badillo, and M. Abrams, "Defining Proactive Software Practices for Healthier Cyber Ecosystems", CrossTalk Sep/Oct 2012, pp. 20-14, 2012

[4] CENELEC: EN50126-1: Railway applications - The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS), 2005

[5] CertWare, http://nasa.github.io/CertWare/ (Accessed May 28, 2014)

[6] E. Denney, G. Pai, and J. Pohl, "AdvoCATE: An Assurance Case Automation Toolset", SAFECOMP 2012 Workshops, pp. 8-21

[7] E. Denney and G. Pai, "Formal Basis for Safety Case Patterns", SAFECOMP 2013, pp. 21-32

[8] J.L. de la Vara, et al., "Towards a Model-Based Evolutionary Chain of Evidence for Compliance with Safety Standards", SAFECOMP 2012 Workshops, pp. 63-78

[9] J.L. de la Vara and H. Espinoza, "Dealing with Software Model Quality in Practice: Experience in a Research Project", QSIC 2013, 396-405

[10] J.L. de la Vara and R.K. Panesar-Walawege, "SafetyMet: A Metamodel for Safety Standards", MODELS 2013, pp. 69-86

[11] D-Case, http://dcase.jp/index_en.html (Accessed May 28, 2014)

[12] R. Goyette and A. Karmouch, "Toward Assurance in Cloud Computing and the Future Internet", http://www.richardgoyette.com, 2012 (Accessed May 28, 2014)

[13] R. Hawkins, et al., "Assurance cases and prescriptive software safety certification: A comparative study", Safety Science, vol. 59, pp. 55-71, 2013

[14] Lee, I., et al., "Challenges and Research Directions in Medical Cyber-Physical Systems", Proceedings of the IEEE, vol. 100(1), pp. 75-90, 2012

[15] N. Mansourov and D. Campara, System Assurance: Beyond Detecting Vulnerabilities, Morgan Kaufmann, 2011

[16] S. Nair, et al., "Management of Evidence for Compliance with Safety Standards: A Survey on the State of Practice", Simula Research Laboratory, Technical Report, 2013

[17] S. Nair, et al., "An Extended Systematic Literature Review on Provision of Evidence for Safety Certification", Information and Software Technology, vol. 56(7), pp. 689-717, 2014

[18] S. Nair, et al., "Safety Evidence Traceability: Problem Analysis and Model", REFSQ 2014, pp. 309-324

[19] A. Oliveira, et al., "Impact of Feature Interaction on the Safety Analysis for Unmanned Avionics Product Lines", SAFECOMP 2013 Fas Abstracts

[20] OMG, Structured Assurance Case Metamodel (SACM), Version 1.0, http://www.omg.org/spec/SACM/, 2013 (Accessed May 28, 2014)

[21] OPENCOSS, D4.1 - Baseline for the Common Certification Language, Version 1.1, http://www.opencoss-project.eu/node/7, 2013 (Accessed May 28, 2014)

[22] OPENCOSS, D4.4 - Common Certification Language: Implementation, Version 1.1, http://www.opencoss-project.eu/node/7, 2013 (Accessed May 28, 2014)

[23] OPENCOSS, D6.1 - Baseline for the evidence management needs of the OPENCOSS platform, http://www.opencoss-project.eu/node/7, 2012 (Accessed May 28, 2014)

[24] OPENCOSS, D6.2 - Detailed requirements for evidence management of the OPENCOSS platform, http://www.opencoss-project.eu/node/7, 2012 (Accessed May 28, 2014)

[25] R.L., Pancotti, et al., "Governance of Composable Capability on Demand (CCOD)", MITRE, Technical Report, 2010

[26] R.K. Panesar-Walawege, M. Sabetzadeh, and L. Briand, "Supporting the verification of compliance to safety standards via model-driven engineering: Approach, tool-support and empirical validation", Information and Software Technology, vol 55(5), pp. 836-864, 2013

[27] T. Polacsek, "Argumentation and V&V", http://ftp.rta.nato.int/public/PubFullText/RTO/EN/STO-EN-MSG-123/EN-MSG-123-05.pdf, 2014 (Accessed May 28, 2014)

[28] J. Recker, Evaluations of Process Modeling Grammars - Ontological, Qualitative and Quantitative Analyses Using the Example of BPMN, Springer, 2011

[29] M. Sabetzadeh, et al., "A goal-based approach for qualification of new technologies: Foundations, tool support, and industrial validation", Reliability Engineering & System Safety, vol. 119, pp. 52-66, 2013

[30] N. Sannier and B. Baudry, "INCREMENT: A Mixed MDE-IR Approach for Regulatory Requirements Modeling and Analysis", REFSQ 2014, pp. 135-151

[31] D. Shoemaker and N.R. Mead, "Software Assurance Measurement - State of the Practice", Software Engineering Institute, Technical Note, 2013

[32] K. Siau and Q. Cao, "Unified Modeling Language: A Complexity Analysis", Journal of Database Management, vol. 12(1), pp. 26-34, 2001

[33] M. Spies, "A software assurance evidence approach to cloud security", DEXA 2011, pp. 39-43

[34] L. Sun, "Establishing Confidence in Safety Assessment Evidence", PhD Thesis, University of York, 2013

[35] X. Zhao, et al., "A New Approach to Assessment of Confidence in Assurance Cases", SAFECOMP 2012 Workshops, pp. 79-91