----------------------- REVIEW 1 ---------------------

SUBMISSION: 7555

TITLE: Hierarchical Assurance Patterns for Cyber-Resilient Systems Engineering

AUTHORS: Isaac Amundson, Darren Cofer, David Hardin and John Hatcliff

----------- Overall evaluation -----------

SCORE: -1 (weak reject)

----- TEXT:

In this paper, authors describe hierarchical cyber-resiliency assurance patterns, which can be instantiated within BriefCASE, an open-source model-based engineering environment for cyber-resilient system design. The patterns are represented in GSN.

Strengths

-the topic of assurance patterns is of relevance for SafeComp. The focus is on assurance patterns for ensuring cyber-resiliency only. However, authors mention that the patterns are expected to be integrated within a full system dependability assurance case, when needed.

-The paper is well written.

-The intended contribution is clearly stated.

Weaknesses

The intended contribution is clearly stated. However, the content of the paper seems more to move towards an additional but incomplete demonstration of the potential usage of BriefCASE based on a set of hierarchical but rather weak patterns.

-Novelty.

Related work is discussed in the introduction. However, the discussion shall be expanded to include the discussion of other related work that incorporate a similar workflow (where the proposed patterns could be eventually supported). See for instance:

1) the AMASS platform, hosted by OpenCert https://urldefense.com/v3/\_\_https://www.eclipse.org/community/eclipse\_newsletter/2018/july/amass.php\_\_;!!MvWE!HXnsaFe8GdQstSnFFu6BNz\_QGII6s6X9VhEvEbo8eQVj4pr5gvLE2pdsJnZJgRXU3CHQGUFUXSqCY8fluEWslnU0N3swuA$

https://urldefense.com/v3/\_\_https://www.eclipse.org/community/eclipse\_newsletter/2019/july/amass.php\_\_;!!MvWE!HXnsaFe8GdQstSnFFu6BNz\_QGII6s6X9VhEvEbo8eQVj4pr5gvLE2pdsJnZJgRXU3CHQGUFUXSqCY8fluEWslnVi4f1zkA$

2) I. Šljivo, G. Juez Uriagereka, S. Puri, B. Gallina, Guiding assurance of architectural design patterns for critical applications, Journal of Systems Architecture, Volume 110, 2020, 101765, ISSN 1383-7621,https://urldefense.com/v3/\_\_https://doi.org/10.1016/j.sysarc.2020.101765\_\_;!!MvWE!HXnsaFe8GdQstSnFFu6BNz\_QGII6s6X9VhEvEbo8eQVj4pr5gvLE2pdsJnZJgRXU3CHQGUFUXSqCY8fluEWslnX08o79jw$ .

Add a paragraph for AMASS

In addition, since the core of the contribution is about cyber resiliency patterns, authors shall discuss related work on cyber security/cyber resiliency patterns.

Reference NIST? Research other cyber security patterns?

->the novelty remains arguable.

-Technical soundness of the contribution.

Authors write "We present our assurance patterns as GSN Patterns [13] (with slight abuse of notation for brevity)." However, the abuse is not explained. I could easily detect an abuse of the modelling element "to-be-instantiated" as well as non compliant statements within goals.

Attempt to explain abuse? Redo patterns without abuse?

In addition no IDs are used.

Yes they are. Not sure I understand this comment.

Pattern presented in Fig.4 is rather trivial.

Stupid comment. Add context to top-level goal with reference to guidance. If there’s space, add text with intuition.

For instance, the pattern presented in Fig.5 is rather weak. This pattern contains the goal "security requirements were imported into the model or omitted with rationale". However, the goal is not fully supported by evidence. Where is the evidence for the rationale? This leads to omission of key evidence fallacy.

Update figure to include evidence of import AND omission rationale

Even from a GSN usage perspective the pattern is arguable. Authors do not exploit the pattern-related modelling elements (e.g., the choice). No choice modelling elements is actually used, despite the clear choice represented by the OR.

**Not required, but look into adding choice.**

In addition, as far as I could see, no illustration of the instantiation of the patterns is present in the paper. There is only a discussion that given a system model and given the framework, the instantiation is possible.

Authors write: "On the DARPA CASE program, BriefCASE was applied to a section of CH-47 mission control software, as well as an AFRL UxAS application. Additional material including videos and code can be found on our BriefCASE project website [5]." But what about the instantiation of the proposed set of patterns?

Look into adding a bit more detail about instantiation

-The background on BriefCase is rather lengthy (3 pages). The majority of the background information including the figure representing the architecture is taken from [3].

Look into shortening if absolutely necessary (but I’m not sure it is)

-Some references are obsolete (see the one for GSN, GSN standard version 3 should have been used). In addition, many of them are related to the BriefCase. Instead I was missing important references in relation to the core of the presented contribution.

Update GSNv3 reference. Not sure what else

Given the above-listed weaknesses, this paper shall not be accepted in its current status.

----------------------- REVIEW 2 ---------------------

SUBMISSION: 7555

TITLE: Hierarchical Assurance Patterns for Cyber-Resilient Systems Engineering

AUTHORS: Isaac Amundson, Darren Cofer, David Hardin and John Hatcliff

----------- Overall evaluation -----------

SCORE: 0 (borderline paper)

----- TEXT:

Hierarchical assurance cases are very important to cope with the ever-increasing complexity of today’s systems. This is even more important for cyber-resilience. Tool support in this area is very appreciated. Security by design is a very important way to tackle cyber threats. The paper thus covers a very relevant topic and fits well with the conference. From my point of view the paper is more a tool paper than a paper on hierarchical assurance patterns.

Is there any way to put more emphasis on the patterns and less on the tooling?

I would like to see more of the patterns. Although it is mentioned in the text that more information can be found on the internet, it would have been nice if the authors would have mentioned, that there are x patterns in the library that covered y% of the vulnerabilities of their example implementations (I guess the library covered 100% - but this remains unclear).

Any way to discuss pattern completeness?

If I understand right, the tools strive to first generate a secure by design product and then generate the assurance cases for it. I would have liked to see some information whether the assurance cases generated are sufficient to be submitted to the authorities or whether there is additional manual rework required.

I thought this was discussed, but maybe in a little more detail. Also add to Conclusion.

I like that it is mentioned that manual input is still required. Unfortunately, this is more or less only the case in the summary. In most cases including such artifacts will require quite some extra effort. It would have been a plus if this had been mentioned.

Describe in more detail how manual specification of additional assurance goals and evidence is accomplished in the tool.

----------------------- REVIEW 3 ---------------------

SUBMISSION: 7555

TITLE: Hierarchical Assurance Patterns for Cyber-Resilient Systems Engineering

AUTHORS: Isaac Amundson, Darren Cofer, David Hardin and John Hatcliff

----------- Overall evaluation -----------

SCORE: -2 (reject)

----- TEXT:

The paper presents BriefCASE, which is an open-source tooling platform for assurance of cyber-resilient systems. The paper presents the architecture of the software tooling as well as a number of patterns for reasoning about security requirements, with a focus on AADL programs.

Comments/questions:

- The title mentions Hierarchical Assurance Patterns, though this issue is not covered clearly in the paper.

- In the Introduction, you write "The assurance patterns are hierarchical in that they are represented as modules that can be composed into a comprehensive pattern for addressing specific dependability concerns". In what sense are hierarchical structures also modular?

A bit more explanation here I guess

- You compare your work with the work of Hawkins et al on model weaving. You describe your work as not need model weaving "due to the tight coupling between the modeling environment and assurance tool". Is that a good thing? If so, how?

Do not address, it should be obvious

- The paper looks more like a tooling paper than a regular research paper.

- The paper lacks evaluation. It's unclear to the reader if the approach works, when and how.

Discuss evaluation somehow.

- Your GSN patterns would benefit from more strategy elements to explain the reasoning stepping stones between the goals and their decomposition. Otherwise, it's hard to follow the argument (e.g. Figure 5).

**Look into this**

- More context elements in GSN would also help, e.g. defining 'filer' in the argument.

**Look into this**