MASCA 2023

Workshop on Modular Argumentation to Support Device Conformity Assessment

(Abstract)

Uwe Becker (Draeger), Germany
Frederic Courivaud, Dag McGeorge (DNV), Norway
Janusz Górski, (GUT, Argevide), Poland

Certification of critical systems is based on an explained and well-founded body of evidence which shows that the system acceptably meets the assurance objectives. This system assurance is one of the most expensive and time-consuming tasks during development of critical systems. With growing complexity of the systems and the growing regulatory complexity, the related assurance tasks become even more complex and time-consuming. Currently, conformity assessment relies mostly on audit, testing and document review by experts.

Structuring explicit assurance claims into digital and reusable arguments has the potential to dramatically improve the conformity management process, ultimately leading to shorter time-to-market. Moreover, arguments are reusable for other similar products or systems, or they can be modified and reused according to periodic reassessment needs.

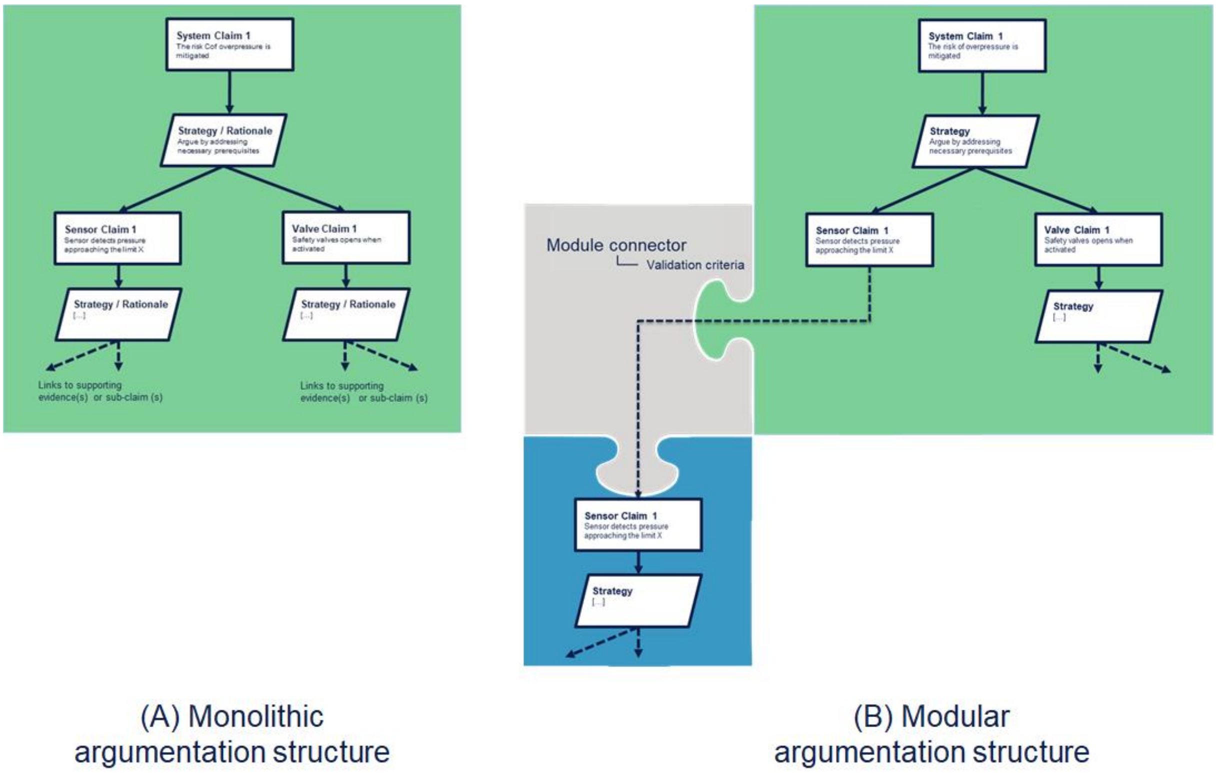
However, practical use of explicit assurance arguments raises several challenges, some of them are listed below.

- Complex systems may require long chains of argumentation supported by many pieces of evidence, resulting in a large and complex monolithic arborescence or *assurance case*, which can be difficult to develop, maintain and assess.
- Complexity here also arises from updates of the system sub-components (e.g., such as a sensor or firmware) typical of cyber-physical systems. These updates impact on the validity of the system's overall assurance case validity resulting in frequent updates of the assurance case.
- In many situations a critical system is integrated of components manufactured by different (external) suppliers rather than developed by a single manufacturer. In such situation the question arises if and how it is possible to assure the component and the integrated system separately and whether assurance arguments of components can be reused in different target systems.
- There may be multiple assurance objectives subjected to certification, like safety, security, effectiveness and accuracy, robustness, and others. They represent different concerns and although they may overlap, separation of

such concerns may be an attractive way of addressing the complexity of large assurance argumentation.

- In many industrial domains certifications are renewed periodically. In a more rapidly changing world, where the context of use of the system can change frequently and the system itself may be updated, often in unpredictable ways, this may compromise the consistency between the certificate and the object being certified. This increases the pressure towards some forms of ‘continuous’ assessment and certification. An example could be a rapidly changing landscape of security threats and the resulting risks which can undermine the validity of security certificates.

One way to tackle these challenges is to modularize the assurance cases as shown in the figure below.


System Claim 1
The risk Cof overpressure is mitigated
Strategy / Rationale
Argue by addressing necessary prerequisites
Sensor Claim 1
Sensor detects pressure approaching the limit X
Valve Claim 1
Safety valves opens when activated
Strategy / Rationale
[...]
Strategy / Rationale
[...]
Links to supporting evidence(s) or sub-claim (s)
Links to supporting evidence(s) or sub-claim (s)
Module connector
Validation criteria
System Claim 1
The risk of overpressure is mitigated
Strategy
Argue by addressing necessary prerequisites
Sensor Claim 1
Sensor detects pressure approaching the limit X
Valve Claim 1
Safety valves opens when activated
Strategy
[...]
Sensor Claim 1
Sensor detects pressure approaching the limit X
Strategy
[...]

(A) Monolithic argumentation structure

(B) Modular argumentation structure

Figure 1 A: Illustration of a monolithic assurance case argumentation at the left, and B: a modular assurance case at the right, in which part of the safety argumentation, i.e. argumentation provided by the sensor supplier of the considered system, is connected to the overall system assurance case argumentation through a modular connection.

In this sense modular assurance is the connection of an argumentation arborescence (e.g., the conformity demonstration of a sub-component of a device or software) to the assurance case of the overall system or product it belongs to.

The MASCA workshop aims to

- Foster a shared understanding of key challenges from various industrial sectors where modular assurance has the potential to simplify conformity management.
- Present at least two practical examples, from the medical device sector and autonomous transportation, as reference use cases.
- Discuss, summarize, and share specificities and commonalities of modular assurance requirements among participants.
- Provide an opportunity for participants to test modular assurance concepts “live” using a demonstrator that will be made available during and after the workshop.
- Finally, provide an opportunity for participants to join a dedicated modular assurance working group with the aim to promote the use of modular, digital and reusable assurance arguments to improve compliance processes in various industrial sectors.