Practically Formal Development and Assurance of Complex Software-Intensive Safety-Critical Systems

Alan Wassyng
work with Zinovy Diskin, Nicholas Annable, and Mark Lawford

CyPhyAssure, 20 March 2019
GSN-like Assurance Cases

Pros

- Appealingly intuitive
- Does seem to improve safety (for example) by making people examine the “case” more critically

GSN was introduced by Tim Kelly in 1998 [Kelly1998]

He and others have turned it into the most popular notation for assurance cases

GSN-like is meant to include other similar notations such as Claims, Arguments and Evidence (CAE) and tabular approaches
GSN-like Assurance Cases

Cons

- Cases tend to have an ad hoc structure dictated by experience & preference
  - Patterns help but they are not the “solution”

- Cross-cutting concerns abound

- There is an element of confirmation bias

- Provides a false sense of confidence (no matter how we “measure” confidence) since we think our reasoning is rigorous (most never claim formal) – but it is not

- Safety impact analysis is difficult to impossible
  - In general, effective traceability is tough
The actual intent behind GSN was fundamentally flawed in some ways

1. Strategy is optional!
2. The arrows indicate decomposition, not an argument based on premises
3. The promised explicit argument is just not present – if justification was supposed to represent reasoning as some people claim, then why does it support strategy instead of the other way around?
4. GSN/CAE experts say that the only place an explicit argument is necessary is to support evidence, but there is no strategy node even – so, what argument? Better in SACM 2.0
A New Approach

- Before we explore why we came up with a different approach the following slide shows components of the new assurance – as an integral part of the development

- This gives us some idea of where we are headed

- The basis is metamodels and model transformations, refinements and instances
Assurance Case Templates (ACTs)

Describes an assurance case (AC) for a product line or domain.

Needs to be instantiated for a specific product.

Developed BEFORE building products.

Reduces confirmation-bias.

Facilitates incremental assurance.

Could be used to direct development – as a process guide or even as a standard.

[Wassyng2016]

Legend:
- Claim or sub-claim
- Evidence
- A → B - A is claim
- B is premise

acceptance criteria on evidence required specified in the template
Assurance Case Templates (ACTs)

Describes an assurance case (AC) for a product line or domain.

Needs to be instantiated for a specific product.

Developed BEFORE building products.

Reduces confirmation-bias.

Facilitates incremental assurance.

Could be used to direct development – as a process guide or even as a standard.

We have championed “product-focused certification” and we really like ACTs – so why develop workflow+?

Legend:
- Claim or sub-claim
- Evidence
A → B - A is claim
B is premise

acceptance criteria on evidence required specified in the template

[Wassyng2016]
<ADAS> considered as an ISO 26262 item, delivers the behaviour required, and does not adversely affect the safety of the vehicle, over its expected lifetime, in its intended environment.

**Strategy:**
G can be decomposed into
1. Functional safety concept verified. (GS)
2. <ADAS> complies with Functional safety requirements and is released for production (26262). (GR)
3. Production and maintenance processes. (GPM)
4. Configuration management. (GC)
5. Change management. (GCM)
6. <ADAS> not expected to violate documented assumptions (GA)

**Reasoning:**
Premise: GS, GR, GPM, GC, GCM and GA are true. Claim: G is true
i) These 6 premises cover all the major premises in 26262 (See SRi)
ii) GR as in 26262 has been supplemented by our knowledge of SE. Specifically, general functional requirements must not adversely interact with the safety requirements. (See SRii)
iii) Important component is operational assumptions are not so onerous that drivers are likely not to comply with them, and those related to the environment will also be valid. (See SRiii)
Extract from Assurance Case Safety & Security Template

Top Claim, G
<X> considered as an ISO 26262 item/SAE J3061 feature, delivers the behaviour required and does not adversely affect the safety or create security vulnerabilities in the vehicle, over its expected lifetime in its intended environment.

GS
The safety and cybersecurity concepts of <X> are verified [These include all functional safety and cybersecurity requirements that are derived from a vehicle level combined hazard and threat analysis and risk assessment, and all of these requirements are validated, and non-interfering].

GR
Implementation of <X> complies with its functional safety and cybersecurity requirements within tolerance [The technical requirements are unambiguous and complete on input domain and internally consistent. They include all functional, safety and cybersecurity requirements derived from HARA and TARA respectively].

GPM
Safety and cybersecurity of the vehicle is maintained throughout its operating life [This complies with production requirements, service maintenance requirements and decommissioning requirements in ISO 26262 and SAE J3061].

GC
Configuration management complies with ISO 26262 and SAE J3061 requirements on configuration management.

GCM
Configuration management complies with ISO 26262 and SAE J3061 requirements on change management.

GA
Operation of the vehicle in which <X> is installed is not expected to violate documented operational assumptions [All operational assumptions are adequately documented].

[Chowdhury2018]
We Like the Benefits of ACTs

- They are templates for a product line developed ahead of work on individual products
- They facilitate incremental assurance in the same way that *information hiding* makes software designs robust with respect to *anticipated* changes
- They provide some protection against confirmation bias
- They standardize an approach so that regulators (in particular) can develop expertise in evaluating them
But Could Not Overcome the Flaws in GSN

- GSN is inherently ad hoc – there is no theoretical foundation for its assurance steps

- The “logic” for the explicit argument is either non-existent or hopelessly inadequate to deal with a property like safety
  - We have not managed to define safety semantics for the arrows in GSN – No, SACM does not do this [SACM2.0]
  - Safety or security impact analysis in GSN is fundamentally unsound

- Cross-cutting concerns are unavoidable

- GSN diagrams typically are a mixture of template and instance – see next slide
This is not inherent in GSN – but GSN is so ad hoc in its approach that this is what we see most of the time.
Why workflow+?

- We need process!
  - Even if we want product-focused certification we have always said it has to be based, at the very least, on notions of an idealized process

- We can cope with process, product, people, in much more structured ways

- workflow+ is a formal notation and the inherent assurance steps are not ad hoc

- workflow+ provides a rigorous way of producing and maintaining traceability links providing a method to turn incremental analysis into syntactic checks
Where did it come from?

- Last year we published an early version of the framework in MoDELS [Diskin2018]

These “assurance steps” are suggested by the mathematical structure - no longer ad hoc.
Demonstrate by Way of Example
Example of an Assurance Case Segment

Note: We do realize that this was produced to illustrate GSN constructs not as an example of a safety case, but it is useful for our purpose since it is (sort of) plausible and is simple enough but with some (implicit) detail.
In this metamodel we consider the inference mechanism, i.e., how constraints are derived.

Legend
- **lightGreen** -- Processes
- **Yellow** -- Data
- **Red** -- Constraints
- **Blue** -- Derived elements

To be filled in later
So, where did the assurance steps come from?

There is a constraint that says every hazard must be “dealt with” by a safety requirement

We then have 2 checks on that:
1. semantic – needs people
2. syntactic – can be automated
In this metamodel we consider the inference mechanism, i.e., how constraints are derived.

We have not added all the reviews in the process nor shown how we deal with people in this example.

The framework for each of those can be defined using aspects.

**Workflow representation based on the GSN example**

Number the assurance assets to show the mapping to GSN.
Partial GSN model derived from workflow+ model. Showing only claims and evidence so as not to clutter the diagram. Numbers in node title maps to workflow+ in previous slide.

REQUIRED evidence can be specified in more detail with the aid of the data items in workflow+

This was an assumption in the GSN example but would not be in practice.

No check for bad emergent behaviour
Expansion of the module on the previous slide

C1.2.3 [6]
All protection systems verifiably satisfy all their safety requirements

C1.2.3.1 [19]
All safety requirements in each protection system are implemented

C1.2.3.2 [10]
Each protection system satisfies all its requirements

C1.2.3.3 [11]
Each protection system mitigates the hazards it is intended to mitigate

C1.2.3.4 [12]
Each protection system eliminates the hazards it is intended to eliminate

E1.2.3.1.1 [19e]
Syntactic check that each safety requirement in the protection system is implemented

E1.2.3.1.2 [20e]
Review: Each safety requirement in the protection system is effectively implemented

E1.2.3.2 [10e]
Verification: All safety requirements in each protection system are verified to be implemented correctly

E1.2.3.3 [11e]
Verification: Each mitigated hazard in all protections systems is shown to be mitigated adequately

E1.2.3.4 [12e]
Verification: Each eliminated hazard in all protections systems is shown to be eliminated
Partial GSN model derived from workflow+ model. Showing only claims and evidence so as not to clutter the diagram. Numbers in node title maps to workflow+ in previous slide.

REQUIRED evidence can be specified in more detail with the aid of the data items in workflow+

AND – this is an Assurance Case Template! It is at the level of a metamodel, not an instance. The evidence nodes are very similar to what we wanted in the Assurance Case Template.
Benefit 1

- **Traceability**
  - Have a look at the GSN view
  - Now consider traceability – remember our discussion on traceability between artifacts (development, assurance etc) and the problem of granularity of evidence
  - If we look at the workflow+ example, the traceability links are obvious and they link between artifacts in all components of the model(s)
    - They can extend into the environment as well!
  - This will become important when we extend this to incremental assurance
Benefit 2

- workflow+ is a metamodel – it is automatically a template for all products produced using the same processes, etc
  - Yes, it is a lot of work, but it is done once used many times. Also, a lot of the work has to be done anyway
  - It is developed before you build the products and thus reduces confirmation-bias
  - The evidence at this level (like in ACTs) describes what evidence must be produced for a product, and should be linked to the appropriate data items in the model. This will provide definitive acceptance criteria
  - This approach satisfies both process and product assurance – and the product assurance is much more specific than competing methods (see the previous bullet)
Benefit 3

- With appropriate tooling, workflow+ facilitates many automatic checks – aids in development as well as assurance

- The technology is pretty standard and commercial tool vendors are starting to produce tools based on very similar notations (not for assurance cases etc – I was thinking of tools like Medini Analyze when I wrote that, it aids safety analysis)
Benefit 4

- Compared with something like GSN, workflow+ is much closer to the way in which many companies have built safety-critical systems in the past.
Benefit 5

- workflow+ facilitates separating process, product and people – intuitively what many people would prefer. Our experience is that this is fundamentally difficult in GSN
  - We often need a combination of these as premises for a claim
  - And need the same premises elsewhere in the GSN graph
  - That means we either have to resort to duplication, or we have links stretching across different slices of the graph
Benefit 6

- Current standards such as ISO 26262 can be modeled using workflow+ and could be used as normative models for conformance checks of internal company processes
  - We have experience of constructing UML models of ISO 26262 – before we defined workflow+
  - workflow+ models would be very similar
What is missing?

- The explicit demonstration that the system is safe!!!!

- We are working on that

- There are various options
  - Best I think is to do what we have always done – demonstrate that
    - The requirements will result in a safe system
    - The system as implemented complies with its requirements
What is missing?

- The explicit demonstration that the system is safe!!!!
- We are working on that
- There are various options
  - Best I think is to do what we have always done – demonstrate that
    - The requirements will result in a safe system
    - The system as implemented complies with its requirements

Actually, also show that (all) obstacles to achieving these 2 results have been overcome
What is missing?

- The explicit demonstration that the system is safe!!!

- We are working on that

- There are various options
  - Best I think is to do what we have always done – demonstrate that
    - The requirements will result in a safe system
    - The system as implemented complies with its requirements
    - These are already process steps so it should not be difficult to augment them appropriately in workflow

Actually, also show that (all) obstacles to achieving these 2 results have been overcome
References


