Safety Cases: A Review of Challenges

Zarrin Langari and Tom Maibaum

McMaster University, Canada

May 2013

Safety Cases are Not New but…

- Still immature
- Confront challenges in
  - Development
  - Use
  - Maintenance
- Their effectiveness should be evaluated
- Their assessment is not straightforward

Challenges

Report and Presentation

- Size and complexity
- Readability
- Graphical Notation

Content and Structure

- Variety of evidence
- Challenges with context and assumptions
- Challenges with arguments

General

- Confirmation Bias
- Challenges of process- and product-based approaches
- Challenges with safety cases for product lines
- Safety Cases in the SDLC

- Assessment of safety cases by regulators

Challenges

Report and Presentation

- Size and complexity
- Readability
- ***Graphical Notation***

Content and Structure

- Variety of evidence
- Challenges with context and assumptions
- ***Challenges with arguments***

General

- Confirmation Bias
- ***Challenges of*** process- and ***product-based approaches***
- Challenges with safety cases for product lines
- Safety Cases in the SDLC

- ***Assessment of safety cases by regulators***

Graphical Notation

+ Graphical notation facilitates presentation of a large and complex safety case

+ It is convenient to use graphical notation for referencing

+ Templates and patterns simplify the construction of a case

- It may create illusion that safety claim is met due to this sophisticated presentation

- With good references to a hazard log we cannot assure all hazards are really mitigated.

- Important differences of individual products may be ignored

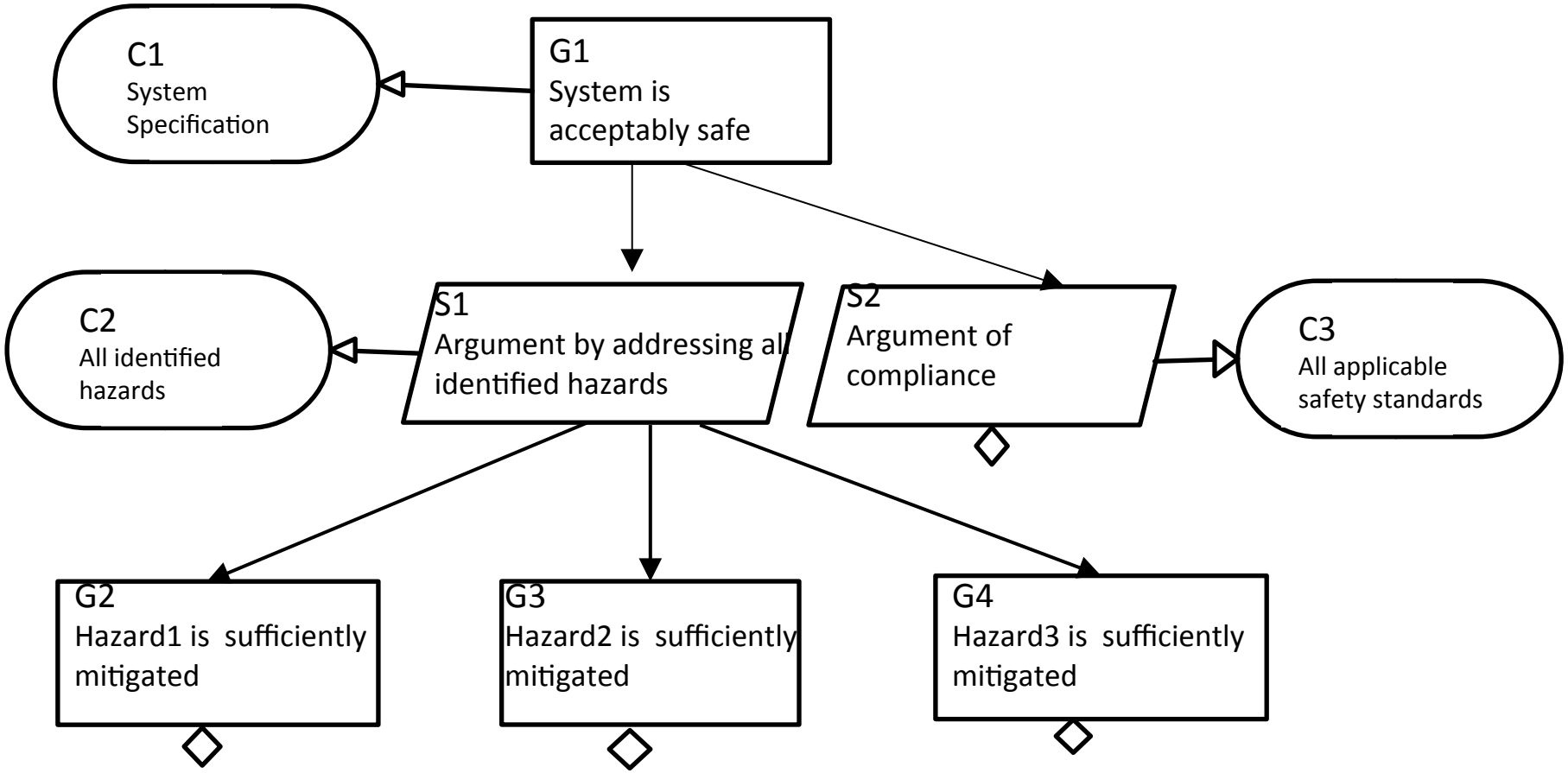
Challenges with arguments

1. Completeness

Considerations:

- All elements of an argument required to make a convincing case should be present
- Using and developing patterns should be handled with care
  - Patterns should be validated

Challenges with arguments



Challenges with arguments

2. dependency between different parts of an argument
   - A defect in a sub-argument will affect the whole argument

Possible resolution

- Developing independent arguments or pieces of evidence, e.g. by using choice connectors

Challenges with arguments

3. No formal semantics to support correct decisions about soundness of arguments
   - Combining two sequences of reasoning is not straightforward and should be done with care

Possible resolution

- Providing semantics for safety cases ☺

Challenges with arguments

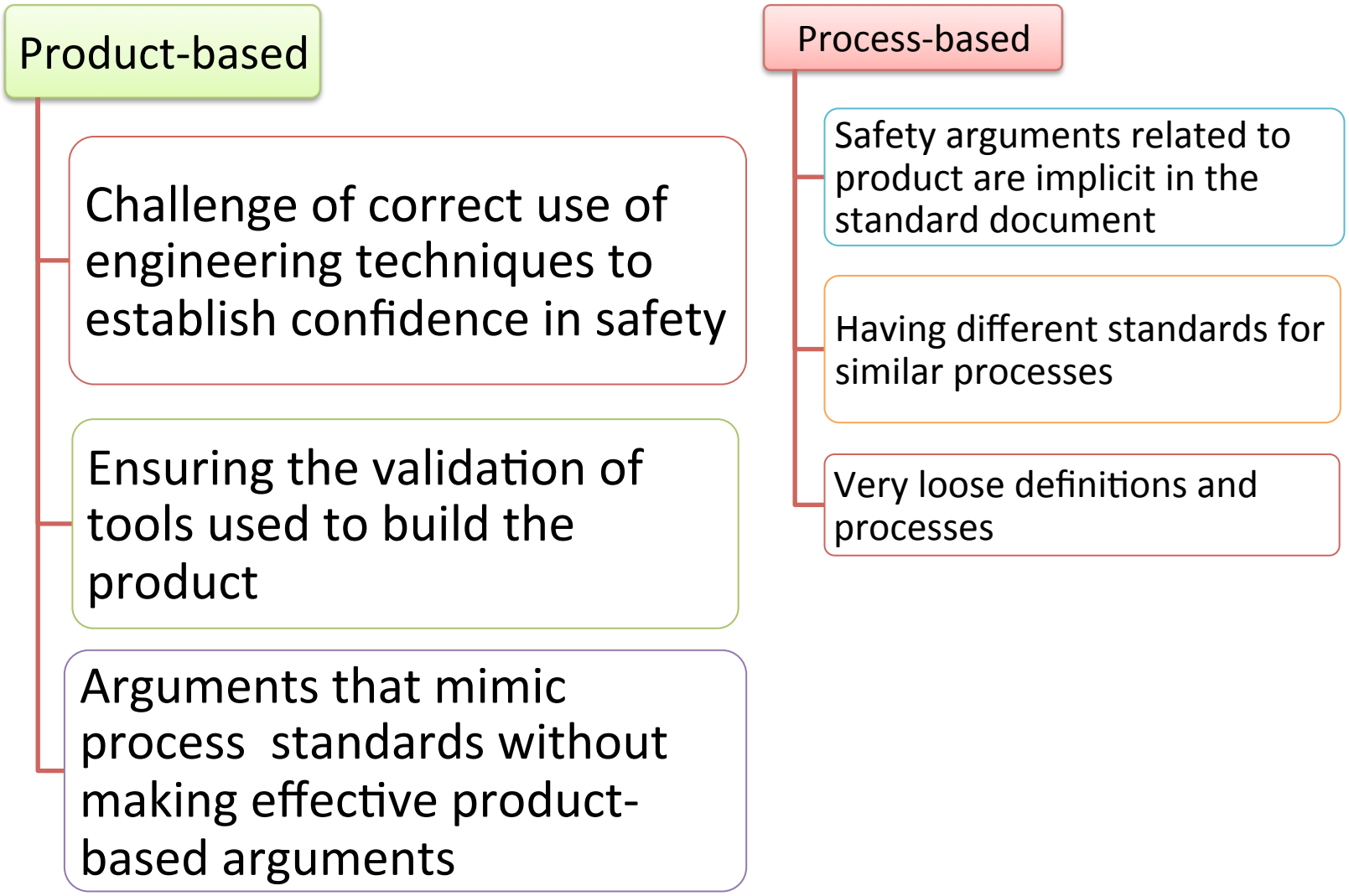
4. Argument fallacies[1]
   – Reliance on common practice

Possible resolution

- Inspecting the safety case thoroughly

[1] W. S. Greenwell, J. C. Knight, C. M. Holloway, and J. J. Pease, "A taxonomy of fallacies in system safety arguments," in Proceedings of the 2006 International System Safety Conference, 2006.

Challenges of product-based approaches



Assessment of Safety Cases by Regulators

Prerequisites of Assessment

Establishing acceptance criteria to approve the case

- Should be repeatable
- Should be publicly available

Establishing a rigorous approach for assessment

- Human inspections, e.g. active reviews and SW Engineering techniques
- Mechanical analysis, e.g. model checking

Assessment of Safety Cases by Regulators

Aspects related to Assessment

- Assessing content and structure
  - With no semantics for safety case, structure review is difficult
- Domain-specific expertise is expected
- Exploiting commonalities yields better reviews
- Soundness and completeness of a safety case should be checked

Assessment of Safety Cases by Regulators

Aspects related to Assessment

- With no semantics for safety case, review is difficult
- Domain-specific expertise is expected
- Exploiting commonalities yields better reviews
- **Soundness** and **completeness** of a safety case should be checked

Questions?