Application of assurance cases in arguing EM resilience

Mohammad Tishehzan

PhD student

University of York

Mohammad.Tishehzan@york.ac.uk

This project has received funding from the European Union's EU Framework Programme for Research and Innovation Horizon 2020 under Grant Agreement No. 812.790.

About the presenter

Mohammad Tishehzan is an Early Stage Researcher in the EU-funded MSCA PETER Project and PhD student in the department of computer science at the University of York since 2020. He is carrying out research on "*Modelling and Reasoning about EMI Interactions in Autonomous and Complex Vessel*". His primary goal is to develop a through-life EMI risk-based modular safety case approach in a form suitable for all of the stakeholders in the marine industry. He completed his B.Sc. and M.Sc. programs in electrical engineering in 2015 and 2019, respectively, from Shahid Beheshti University and Amirkabir University of technology. He also worked as an EMC test engineer at the EMC type approval laboratory of Amirkabir University for two years before joining the PETER project.

Pan-European Training, research and education network on ElectroMagnetic Risk management.

This project has received funding from the European Union's EU Framework Programme for Research and Innovation Horizon 2020 under Grant Agreement No. 812.790.

Outline

- Evolution of EM Risk Management
- Demonstration of Systems' properties
- Goal-Based Demonstration
- Assurance Case and its structure
- Goal Structuring Notation (GSN)
- Application of Assurance Case in EMC

Evolution of EM Risk Management

UNIVERSITY of York

EMC & COMPLIANCE INTERNATIONAL

Rule-Based → Urging elements for a change → **Risk-Based**

- Achieving compliance with EMC Directive
- Physical immunity and emission testing

Risk of having EMI

- Lag of the standards development from technology evolution
- The Shortage of compliant COTS equipment in some industries e.g. maritime
- Increase of certification costs in modular and complex systems
- Increase of EMI risks in safety critical applications

- considering the actual intended electromagnetic environment
- Considering the actual intrinsic immunity

Having Safety, security… risks emerged from EMI

Demonstration of Systems properties

Prescriptive Approach

- standards and guidelines provide rules that must be followed for a product or a process to achieve certification

Main Argument: passing EMC tests in specific scenarios defined in the standards

The need for a tool to formalize the argument has not been extensively noticed

Goal- Based Approach

- Achievement of the required outcome by identifying a set of criteria for certification and demonstrations of the means and the validity of the means used to meet the criteria originated from safety critical systems approach

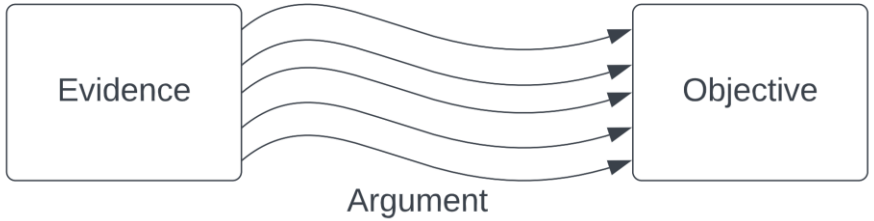
Main Argument: achieving goals regarding various system properties by providing arguments related to scenarios which might not be anticipated in EMC standards

Requires a proper way to communicate the argument with other parties

Goal-Based Demonstration: Assurance Case

Assurance Case

A reasoned, audit-able artefact that supports the contention that its top-level claim (or set of claims), is satisfied, including systematic argumentation, its underlying evidence, and explicit assumptions that support the claim(s)



Assurance case main Elements:

- **Objective (Goal)** – what we want to show
- **Argument** – explanation of why we believe the claim is met…
- **Evidence** – test results, analysis results, etc.

Evidence without Argument is unexplained
Argument without Evidence is unfounded

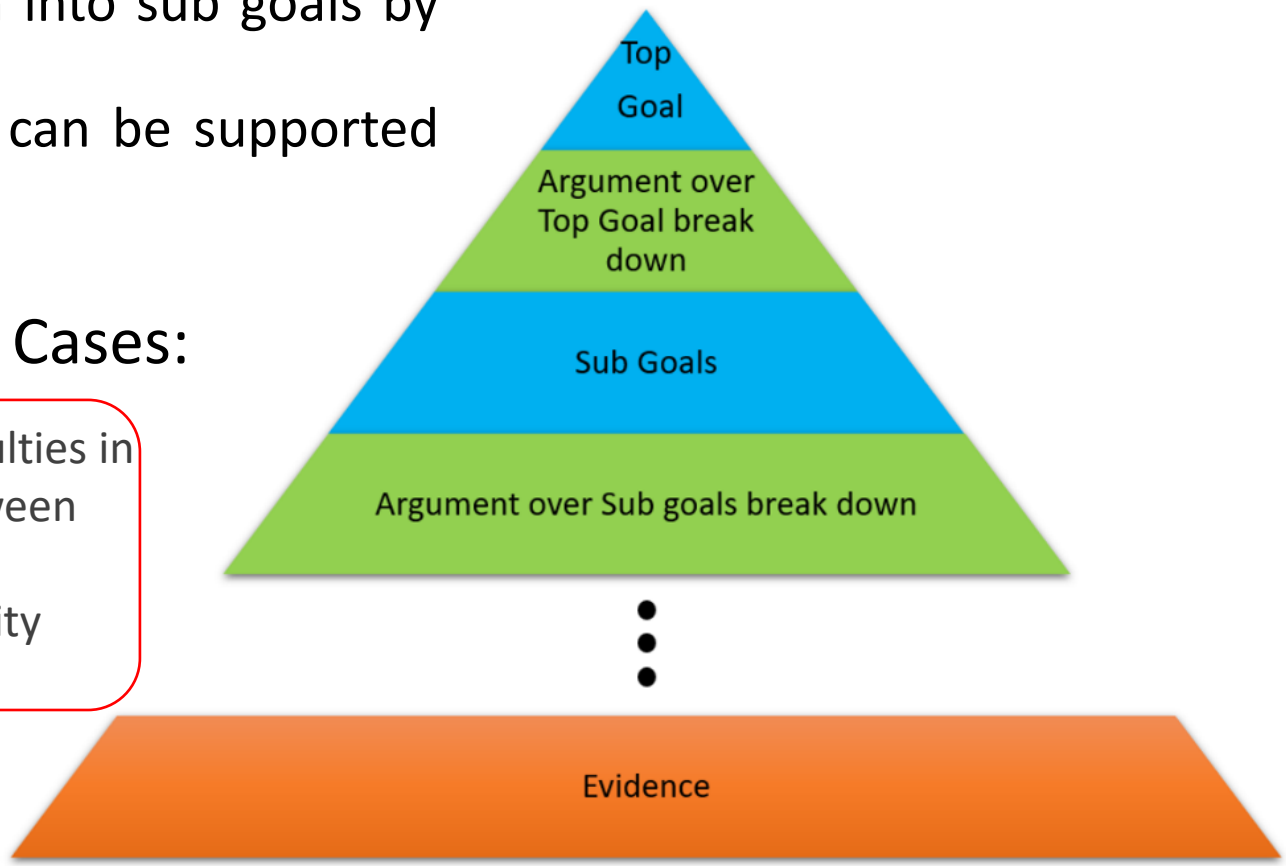
Assurance Case Structure

- An Assurance Case has a hierarchical structure
  - The defined top-level goal is broken down into sub goals by appropriate arguments
  - This process continues until the sub-goals can be supported by evidence directly

- Various ways to demonstrate Assurance Cases:
  - Free Text
  - Tabular Structure

  →
  - Ambiguity and difficulties in communication between engaged parties
  - Difficulty in traceability between elements

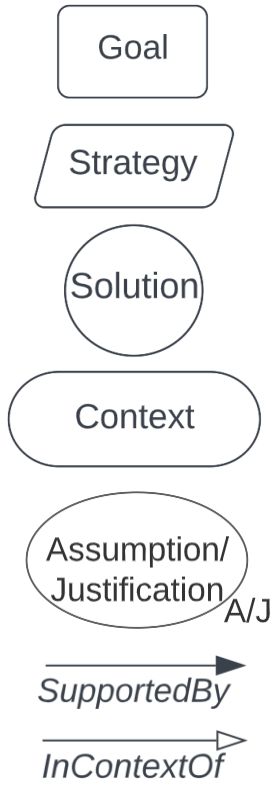
  - Graphical methods
    - Goal Structuring Notation (GSN)

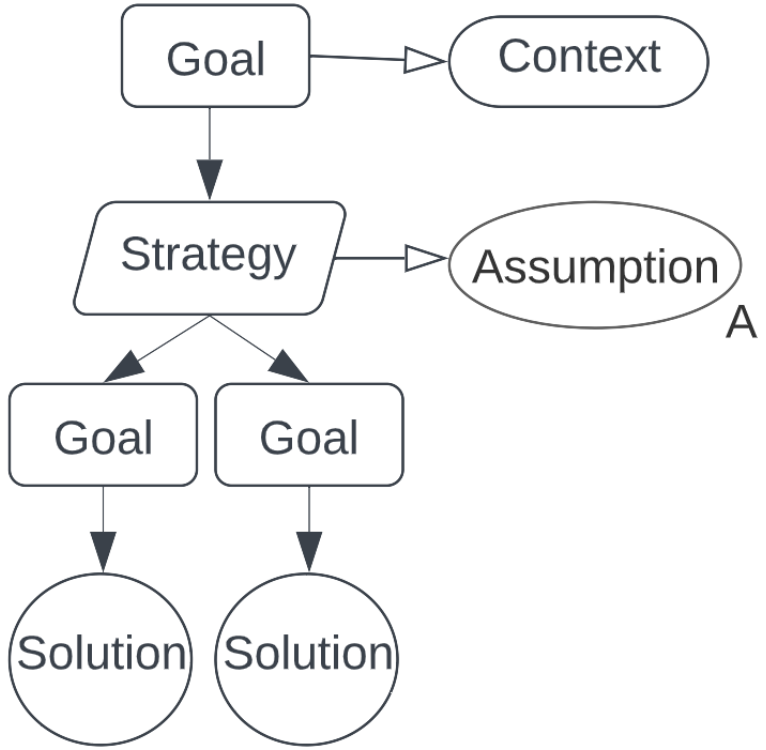


Goal Structuring Notation (GSN)

- GSN facilitates demonstrating the interaction between objectives, arguments, and evidence through a set of graphical elements to achieve a better projection of argumentation

- GSN Elements:
  - **Goal**: A claim about the system that needs to be supported e.g. a requirement, target or constraint
  - **Strategy**: The reasoning behind how goals break down into sub goals
  - **Solution**: The items of evidence provided to support claims
  - **Context**: The contextual information about a goal, strategy, or solution essential to be considered is presented as a context in GSN
  - **Assumptions, Justifications**: Additional information about reasoning behind defined elements
  - ***SupportedBy***: Causal link between elements
  - ***InContextOf***: contextual link between elements





Application of Assurance Case in EMC

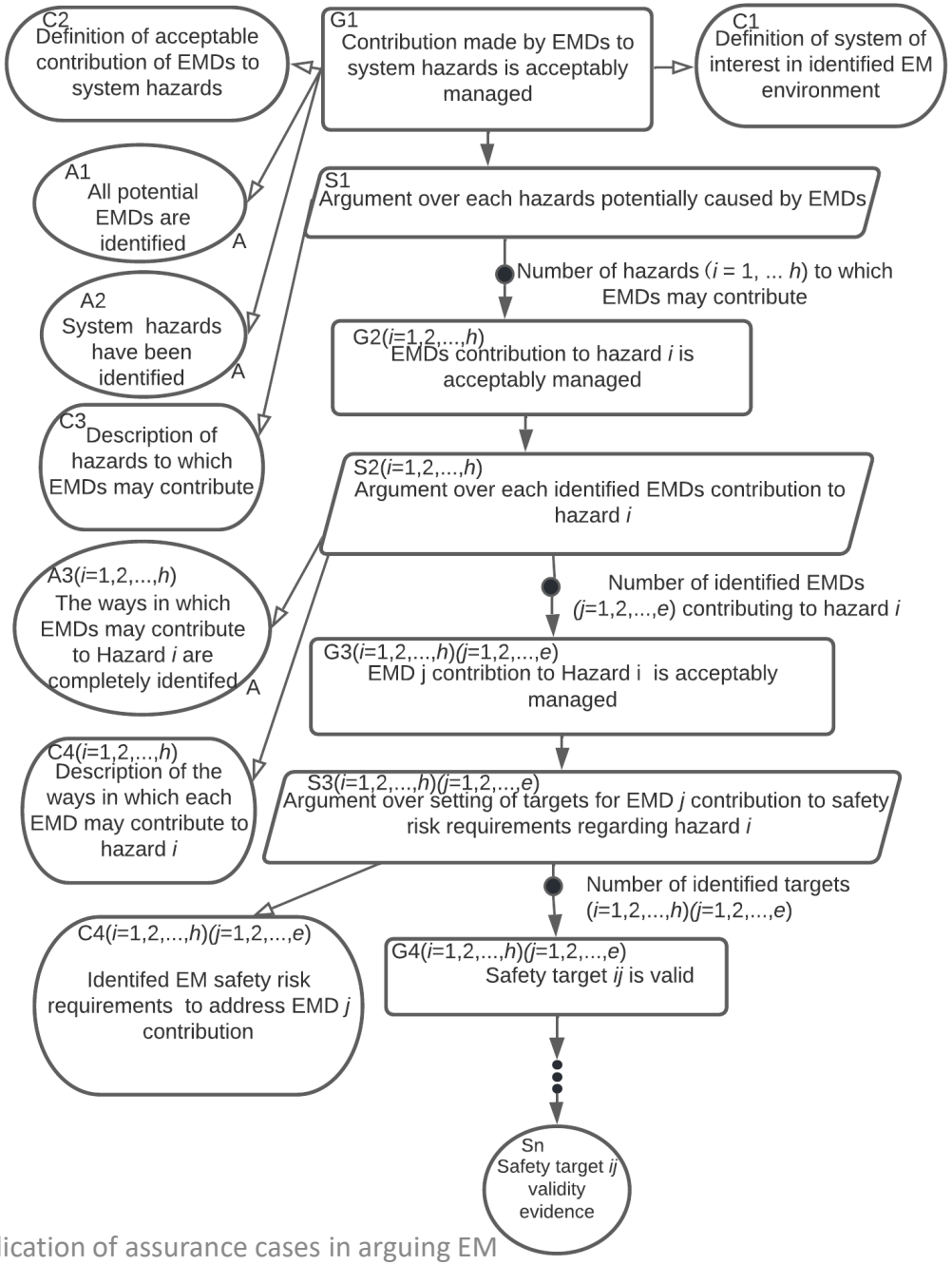
- Its application for assuring compliance with EMC standard has been recently investigated
- Employing assurance cases for argumentation about achieving EMC goals has not been a common practice so far
- Its application in argumentation about safety goals regarding EM disturbances has not been examined
- The Application of GSN in demonstrating principles 1 and 3 of 4+1 Principles of EM Risk Management is addressed

Derived from 4+1 principles of software safety

Principle 1	EM risk requirements shall be defined to address the contribution of EMDs to system hazards
Principle 2	The intent of the EM risk requirements shall be maintained throughout requirements decomposition
Principle 3	EM risk requirements shall be satisfied
Principle 4	Emergent hazardous behavior of the system due to EMDs shall be identified and mitigated
Principle 4+1	The confidence established in addressing the EM risk principles shall be commensurate to the contribution of the EMD to the system risk

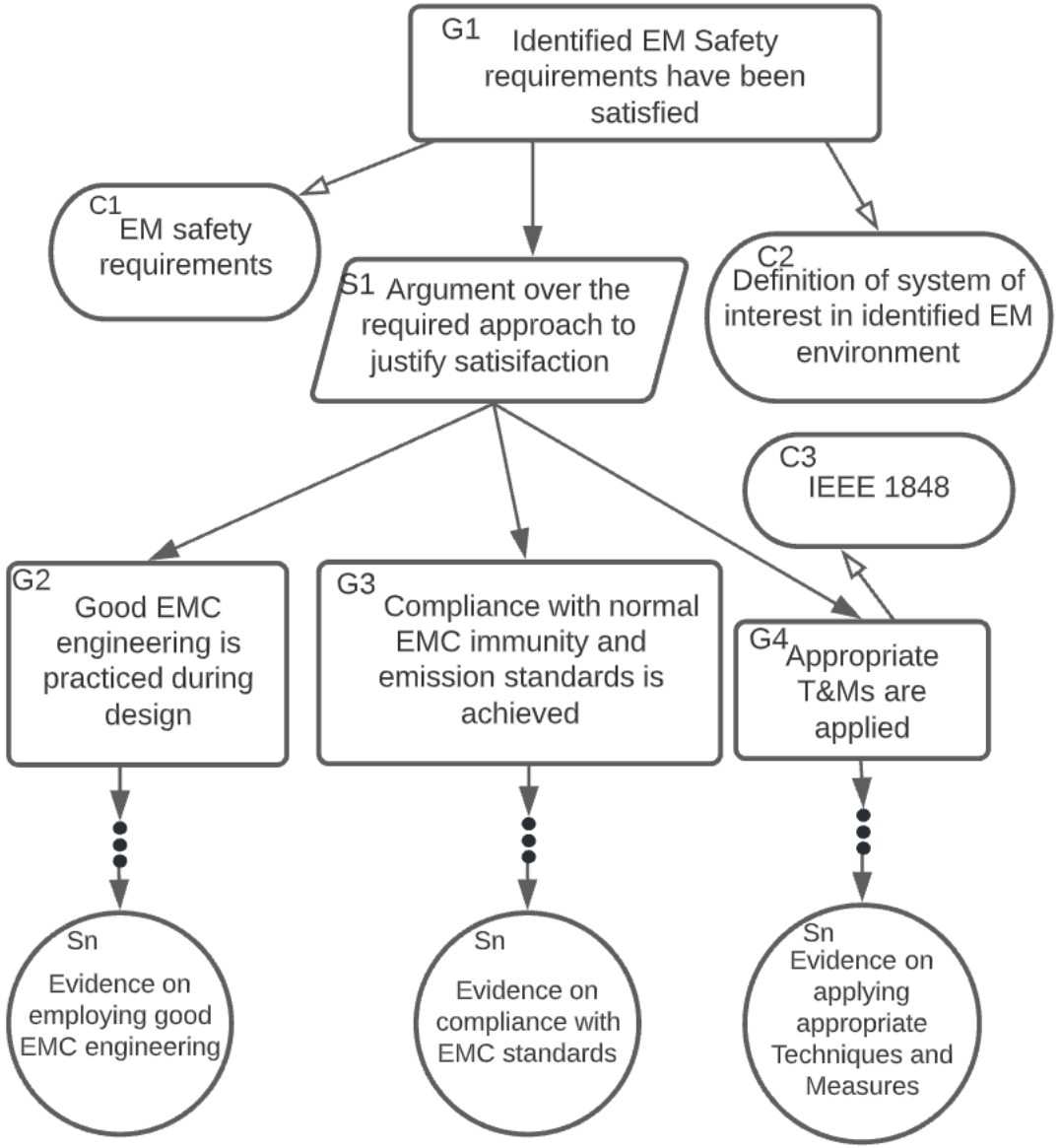
GSN Illustration of Principle 1

- Principle 1: EM risk requirements shall be defined to address the contribution of EMDs to system hazards
- This principle requires that all risks relating to the property of interest (e.g. Safety) arising from all possible EMDs be identified and appropriate requirements for managing those risks be defined
- For safety, it argues that the contribution of each EMD to any known hazard is identified



GSN Illustration of Principle 3

- **Principle 3**: EM risk requirements shall be satisfied
- It focuses on the verification of the satisfaction of EM requirements
- For illustration of the third principle, the recommended approach in IEEE 1848 standard is considered
- IEEE 1848 addresses the management of functional safety and other risks with regards to EM disturbances



Conclusions

- Argumentation in risk-based EMC is not as straightforward as argumentation about rule-based approach
- Using assurance cases as an argumentation tool facilitates certification and communication with engaged parties
- GSN can be used to argue about Safety, security, reliability, … claims
- Appropriate activities during development lifecycle and operation of systems required for developing assurance case
- This research aims to develop a process for producing safety cases in regards to EMI in complex platforms

Thank You!