SAFETY CASES WITH THE HELP OF GSN

Tutorial at the
International System Safety Conference 2015
San Diego, California, USA
→ Your competences after the workshop

→ Understanding of the concept of safety cases

→ Understanding of the benefits and potential pitfalls of safety cases

→ Knowledge of the Goal Structuring Notation (GSN)

→ Ability to read GSN

→ Ability to create simple arguments in GSN
Agenda

What are Safety Cases?

The Goal Structuring Notation (GSN)

Common Errors in GSN arguments

Case Study

Concluding Remarks
→ Acknowledgements

→ The original work on GSN is Tim Kelly's doctoral thesis [Kel98]

→ The GSN slides in this presentation are heavily based on [Spr12], which we highly recommend as a very readable introduction to safety arguments and GSN

→ A useful web resource is http://www.goalstructuringnotation.info
Literature


3 publicly available Safety Cases:


INTRODUCTION TO SAFETY CASES
What is a "Safety Case"?

- The "Robens Report" (1972)
  - Balance between “prescriptive” and “goal setting” legislation needed to shift towards the latter

- Piper Alpha Accident (1988)
  - Conclusion that compliance with detailed prescriptive regulations was not sufficient to ensure safety

- It is necessary to "make a case" for safety!

- "Make a case": to show that what you say is true
- Safety Case: shows that sufficient safety is given
- Term "safety case" has a legal origin
Prescriptive vs. Goal-based Standards

**Prescriptive**
- Describes what to do (way)
- Process-focus
- Requires the application of specific techniques and methods
- Less freedom, less responsibility
- Based on the assumption: "good process leads to good product"
- (Generally) does not require a safety case

**Goal-Based**
- Describes what to achieve (goal)
- Product-focus
- Requires certain product characteristics
- More freedom, more responsibility
- Based on the general approach:
  - Determine hazards and safety requirements
  - Design and implement them
  - Demonstrate achievement
- (Generally) requires a safety case
IEC 61508 (2010)

- No safety case required

- Requires processes, documents, verification, validation and functional safety assessment

- Requires detailed techniques and measures based on required safety integrity

- Very prescriptive
→ **DO-178C (2012)**

- No safety case required
- A "software accomplishment summary" is required, which shows compliance to the planned lifecycle
- Detailed documentation and processes required
- Very prescriptive
Safety Case required: "A structured argument, supported by a body of evidence that provides a compelling, comprehensible and valid case that a system is safe for a given application in a given operating environment."

Safety Management Requirements for Defence Systems

Strongly goal-based

No specific processes or documentation structure suggested

Safety Case is a major requirement
→ CENELEC EN 50129 (2003)

→ Safety Case required: "the documented demonstration that the product complies with the specified safety requirements"

→ Although detailed processes, documents, techniques and measures are required, a safety case is also required

→ But: A very prescriptive description of how a safety case shall be structured, containing even the parts, sections and subsections of the complete safety case

→ Practically no freedom how to argue safety
Safety Case: "argument that the safety goals for an item are complete and satisfied by evidence compiled from work products of the safety activities during development"

Required for ASILs B, C, D

No detailed requirements on structure of safety case, but "the safety case shall be sufficiently complete to evaluate the achievement of functional safety of the item."

Processes, documents, techniques and measures are nevertheless required in detail

Safety Case is a prerequisite for assessment
<table>
<thead>
<tr>
<th>Standard</th>
<th>Safety Case</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEC 61508</td>
<td>No</td>
<td>-</td>
</tr>
<tr>
<td>DO-178C</td>
<td>No</td>
<td>-</td>
</tr>
<tr>
<td>Def Stan 00-56</td>
<td>Yes</td>
<td>• Very high level, very goal based</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Safety Case shall demonstrate safety</td>
</tr>
<tr>
<td>CENELEC 50129</td>
<td>Yes</td>
<td>• Prescriptive processes and prescriptive safety case generation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Safety case shall show that specified requirements are met</td>
</tr>
<tr>
<td>ISO 26262</td>
<td>Yes</td>
<td>• Quite prescriptive processes, lots of freedom for safety case generation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Safety case shall show that safety goals are complete and met</td>
</tr>
</tbody>
</table>
Content of a Safety Case

- Generally, a Safety Case is a document containing a top level claim saying:

  "The system is safe BECAUSE..."

  ... compelling and convincing arguments and evidence follow

- What "safe" means in the context has to be defined
- Often other documents and analyses are referenced
→ General Form of a Safety Case

Form:
- Can be simply textual
- But: Difficult to structure, difficult to read

Safety Requirements & Objectives

Safety Evidence

The claims, goals, etc. that we want to prove

The valid arguments

The pieces of evidence (documents, test results, …) supporting the arguments

[Kel&04]
Is a Safety Case a Proof?

- In an ideal world: Yes.
- In the real world: No.

- But it depends on your understanding of the word "proof"…
- A safety case is rarely as strong as a mathematical proof
- But it should be as strong as a proof in law

<table>
<thead>
<tr>
<th>Law</th>
<th>Safety</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defendant is innocent until proven guilty</td>
<td>System is dangerous until proven safe</td>
</tr>
<tr>
<td>In case of the slightest doubts, the defendant is not guilty</td>
<td>In case of the slightest doubts, the system is not safe</td>
</tr>
</tbody>
</table>

- And of course, as all proofs: it can contain flaws…
Arguments vs. Rhetorics

A Safety Case must be "convincing" (not merely "persuasive")

It must contain good (valid, compelling, comprehensible) arguments!!!

Good rhetorics is not necessary (but can help)

If you don't understand a safety case, there is a high chance that it is crap!
Guidelines for a persuasive (not convincing) Safety Case Report (1) ;-) 

- Write a lot of text, e.g. copy the complete system description and safety plan into the safety case document
- Don't be too clear – this allows you to always interpret the statements in your preferred way
- Use many different terms for the same concept
- Use the same term for different concepts (the context helps to understand the right meaning anyway)
- Use lots of technical jargon that has no relevance to the overall safety, but that sounds professional
- Make the assessor look incompetent when questions are asked
- Include some easy to find typos and other irrelevant errors so that reviewers can comment without understanding the contents
- Use a lot of marketing phrases from your products
- Write that your company is successful with the product
- Play bullshit bingo with your safety case
- Mention how hard everybody has worked
Guidelines for a persuasive (not convincing) Safety Case Report (2) ;-) 

→ Use **lots of references**, so that readers are intimidated to check them 

→ **References ad infinitum**: always put lots of further references in your referenced documents, so that readers have to hop many times before finding the information they are looking for 

→ **Circular references**: You can design it that way that after some hops you land at the originating document again 

→ Preferably **reference books and papers that are out of print/not available** any more 

→ Always make **conclusions from one to all** 

→ Always **extrapolate** from some event in the past into the future 

→ **Repeat invalid conclusions** many times, then they will eventually be believed 

→ Remember: "Tell a man that there is wet paint on a bench and he will have to touch it to make sure. Tell a man there are 100 billion stars in the universe and he will believe you."
Disclaimer and Warning

→ Use the above guidelines at your own risk! We strongly advise not to use a single one!

→ If you work with people with only the slightest bit of experience with safety cases, these guidelines will not work at all!
The Safety Case is not a document!

The *Safety Case* is "a structured argument, supported by a body of evidence that provides a compelling, comprehensible and valid case that a system is safe for a given application in a given operating environment." [DS00-56]

The *Safety Case Report* is the corresponding document, i.e. "a key deliverable that summarises the Safety Case at a particular instant in time" [DS00-56]

A document-centric approach is not desirable

- "We need the safety case" is often misunderstood to mean "This annoying document has to be written up by someone now"

"It is possible to possess a document called the Safety Case and for there to be no safety case" [Kel&04]
Safety Argument

"An argument is a connected series of statements intended to establish a proposition" [Spr12, p.2]

"You use an argument to persuade others of the validity of some claim" [Spr12, p.2]
– My opinion: "persuade" should be replaced by "convince"

Properties of a good safety argument presentation
– It has to be understandable
– It has to be easy to read
– Its logic correctness has to be verifiable
– Logical faults shall be easy to spot
– The notation shall be well defined and uniquely interpretable
– It has to be clearly visible if there are unfinished parts
– It shall be reusable
→ Textual Arguments

...can be good...

The Defence in Depth principle (P65) has been addressed in this system through the provision of the following:

- Multiple physical barriers between hazard source and the environment (see Section X)
- A protection system to prevent breach of these barriers and to mitigate the effects of a barrier being breached (see Section Y)

For hazards associated with warnings, the assumptions of [7] Section 3.4 associated with the requirement to present a warning when no equipment failure has occurred are carried forward. In particular, with respect to hazard 17 in section 5.7 [4] that for test operation, operating limits will need to be introduced to protect against the hazard, whilst further data is gathered to determine the extent of the problem.

...but are more often horrible!
**Tabular Structure**

- (+) Clear differentiation between elements of an argumentation:
  - Claims
  - Arguments
  - Evidences

- (-) Not practicable for large safety cases

- (-) Hierarchical Levels not straightforward to represent

<table>
<thead>
<tr>
<th>Claim</th>
<th>Argument</th>
<th>Evidence / Assumptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>There is no fault in the software implementation</td>
<td>Formal proof of specified safety properties</td>
<td>The design is simple enough to be amenable to proof</td>
</tr>
<tr>
<td></td>
<td>Formal proof that code implements its specification</td>
<td>Proof tool is correct (or unlikely to make a compensating error)</td>
</tr>
<tr>
<td>Software reliability exceeds system requirement</td>
<td>Reliability can be assessed under simulated operational conditions</td>
<td>Compiler generates correct code (sub-argument might use formal proof, past experience, or compiler certification)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>High quality V&amp;V process</td>
</tr>
</tbody>
</table>

Test results

Statistical test results

[Kel98]
GSN- GOAL STRUCTURING NOTATION
GSN – Goal Structuring Notation

- Developed by Tim Kelly et al., University of York
- "Forces" author to develop clear arguments
- Graphical Notation
- Safety cases in GSN easier to read than text
- Reduces fault probability in safety cases
- Tool support available
- Currently being standardized

Clearly shows
- Goals (aka "Claims")
- Arguments (aka "Strategies")
- Evidence (aka "Solutions")
¬ GSN Symbols Overview (Subset)

- **Goal Name**: Claim to be established as true
- **Context Name**: Context of a claim or a relevant reference for it
- **Solution Name**: Evidence supporting a claim
- **Justification Name**: Explanation why a solution satisfies a goal
- **Strategy Name**: Decomposing argument into additional claims
- **Assumption Name**: Statement assumed (but not demonstrated) to be true

- **SupportedBy**
- **InContextOf**
GSN GOAL

- A Goal is a proposition to be established.
  - Is a statement that can be “TRUE” or “FALSE”
- Represents a claim, the truth of which is to be demonstrated by argument
- The Goal text should be of the form subject-verb(-object)
→ Top Goal – your top level claim

→ For a safety case, it is typically something like "The System is acceptably safety for a given application in a given environment"

→ The top goal is typically divided into several sub-goals, sub-sub-goals, etc. which are easier to prove

→ GSN development typically is a top-down approach – you start with the top level proposition you want to show to be true

"A claim can be purely subjective, for example I could make a claim about wine grape varieties, “Syrah is better than Merlot”. I may believe it to be true and make an argument on that basis, but you may believe the opposite and refute my argument. At this point bottles of wine could be opened, and we may lose track of the arguments..." [Spr12]
Excercise: Which of the following claims could be used as a Top Goal?

2. My Business Plan is complete and ready for review by the Board
3. This burial site is probably that of Rædwald, King of the East Angles
4. This painting should be attributed to Albrecht Dürer
5. This equipment fulfils the essential requirements of the RTTE Directive
6. Beryllia is a carcinogen
7. Hazard Identification and Risk Assessment
8. Assurance is provided that safety requirements raised on the software are valid
9. The GSN Symbol for a Goal is a rectangle
10. The colour of the sky
GSN "CONTEXT"
The truth of a claim depends on the context!

What does a typical top level claim "The system is acceptably safe" actually mean?

- What does safe mean here?
- How much/little safety is acceptable?
- In which environment?
- For which use or application?
→ It all depends on context…

The causes and consequences of operational errors are not linear in their magnitude.
GSN CONTEXT

- Context provides, or references out to, definitions and other supporting material

- Always on the end of an open-headed arrow
  - Important: DO NOT hang other contextual information from them

- Environmental Context

- External References
GSN CONTEXT

Another example

Beryllia is an oxide of beryllium, BeO. This argument considers the dust produced when machining the material.

Beryllia is a carcinogen

A carcinogen is a substance that is a direct cause of cancer.

Too much context probably means your goal uses too many vague terms.

Makes GSN less readable.
Context Exercise

My factory manager wants to persuade me that one of her preventative maintenance procedures, known as PMP5, is adequate to keep the factory power supply running. She claims, “PMP5 is fit for purpose”. We want to document the argument so that in future, if someone wants to change the procedure, they will be able to ensure that they do not “break” it. Using GSN, how could the claim, “PMP5 is fit for purpose”, and its Contexts be presented?
GSN "GOALS AND SUBGOALS"
GSN Goals and Sub-Goals

- Goals are typically decomposed into sub-goals
- Truth of Sub-Goals is *sufficient* to establish truth of Goal
- GSN is meant to be read in the deductive form
  - "D is true because A, B and C are true"
- Not in the inductive form
  - "Because A, B and C are true, we can conclude that D is true"
GSN Goals and Sub-Goals

- Similar to a mathematical proof, which is usually in the form: Theorem – Proof

- Sub-Claims which are accepted by the reader without detailed proof can be skipped by the reader

![Diagram](https://via.placeholder.com/150)
→ **GSN does not preclude fallacies**

→ The reader must judge if the argument is logically flawed!

→ Of course again, all depends on context (which is missing here)! Who is meant by "Socrates" here?
A more realistic example

Important to add enough information into goals to make argument understandable
Adelle is the daughter of Bertrand and Celine. Celine’s parents are Didier and Estelle. Construct a simple argument in GSN claiming that Adelle is Estelle’s granddaughter.
Excercise

Adelle is the daughter of Bertrand and Celine. Celine’s parents are Didier and Estelle. Estelle’s brother Frederic is married to Gabrielle; they have a son, Henri. Construct an argument in GSN that Gabrielle is the great aunt of Adelle by decomposing this Top Goal into two appropriate Sub-Goals, and then decompose your Sub-Goals one level, as necessary.
GSN "ARGUMENT STRATEGY"
GSN STRATEGY

- Part of the argumentation
  - Contain a brief description of the argument approach

- Always links to Goals with a solid-headed arrow
  - Only one incoming arrow from above
  - Many outgoing arrows below

- Contextual information referenced with open-headed arrow

- Note that the symbol is optional, sub-goals can be linked directly to goals
  - Describes the rationale why goals are divided into the specific chosen sub-goals
  - Massively improves readability and comprehensibility
Note: Numbering GSN elements

- It is convenient to give unique IDs to all elements in a GSN
- Makes references and reusing elements possible
- GSN does not specify how elements shall be numbered

- There are several methods, e.g.
  - Unique Names
  - Numerical sequential IDs
  - Hierarchical numbering (preferred way, used here)
Security Example with Strategy

- The base-station site has adequate physical security

  - The Security Management Manual defines the level of security required for an outstation, also the signage requirements

  - Argument over the set of security provisions designed to deter or detect intrusion

- Fencing meets BS EN 1722-10: Anti-intruder fences

- The site has a tall fence

- Buildings on the site are locked and remain secure if the perimeter is breached

- Suitable warning signs are displayed

- Vehicle and pedestrian entry points have access controls to admit only authorized persons

- CCTV & other Intruder Detection Systems enable fast response to any intrusion attempt

- CCTV is Closed-Circuit Television
→ **Excercise**

→ Is there anything missing from the top level of this Goal Structure?
→ How would you express this example using Sub-Goals, rather than multiple Strategies?
GSN "JUSTIFICATION"
→ GSN JUSTIFICATION

→ Provides extra explanation or rationale
  – A reason for what you have done

→ Is a contextual information
  – Always associated with the element being justified

→ We use it to say…
  – Why the sub-goals have been chosen when others may have been more obvious
  – Alternatively, a Justification may contain a simple “If A then B” argument
Refer out to an existing argument

- **C3a** BP-02, "Procedure for preparing business plans"
- **G3** Correctly following Procedure BP-02 produces a complete Business Plan
- **J3a** This is argued in an Annex to procedure BP-02
→ **GSN JUSTIFICATION**

→ **Split-up**

- **G0**
  - The system is adequately safe to operate

- **S0.1**
  - Argue that the system is safe to operate in normal operation

- **S0.2**
  - Argue that the system remains safe under failure conditions

{ Volume 1 }

- **J0**
  - That the system remains safe under failure conditions is argued in Volume 2

{ Volume 2 }

- **J0**
  - That the system is safe under in normal operation is argued in Volume 1

- **G0**
  - The system is adequately safe to operate
If A than B

- **G0**: Option C is the best of the candidates

- **S0**: Argument over the set of candidates

- **J0**: If option C is better than each candidate, then it is best overall

- **G1**: Option C is better than Option A
- **G2**: Option C is better than Option B
- **G3**: Option C is better than Option D
- **G4**: Option C is better than Option E
GSN "ASSUMPTION"
GSN ASSUMPTION

→ An assumption is something taken to be true for the purpose of the argument

→ Simplify a situation
  - Argument may be invalid in general, but perfectly adequate in the conditions you assume.
  - Argument is valid for specified conditions.

→ It is very important to state your assumptions explicitly

→ The symbol itself says “I assume that …”, so there is no need to repeat it in the text.

→ An assumption helps you to say that a statement in a Goal is TRUE
Fragment of an argument about traffic lights at a road junction with pedestrian crossings

Exercise: Are the three assumptions appropriate?

C6.3
"All signal lights" includes those for pedestrians

A6.3a
It is assumed that vehicle traffic is in the junction

G6.3
On detection of any of the specified failure conditions, all signal lights are extinguished

A6.3b
The failure conditions are specified in the concept of operations

S6.3
Argue over each failure condition & any combination thereof

A6.3c
The system fulfils its electromagnetic interference susceptibility requirements
GSN ASSUMPTION

Revised fragment of an argument about traffic lights at a road junction with pedestrian crossings

C6.3a
"All signal lights" includes those for pedestrians

G6.3
On detection of any of the specified failure conditions, all signal lights are extinguished

S6.3
Argue over each failure condition & any combination thereof

C6.3b
The failure conditions are specified in the concept of operations

A6.3
The system fulfils its electromagnetic interference susceptibility requirements
GSN "SOLUTION"
→ Where is the final proof?

→ Well, the argument is correct

→ But who says that the premises are true?
  – Are all men mortal?
  – Is Socrates a man?

→ Solutions provide the evidence that the lowest sub-goals are actually true

→ Without this evidence, the argument is not complete!
Solutions (aka Evidence)

- **G1**: All men are mortal
- **Sn1**: The Methusaleh Report

The Methusaleh Report concludes, from epidemiological studies, that all men are mortal.

- **J1**: Xanthippe is "Mrs. Socrates" – she should know...

Socrates is a man

- **Sn1**: Witness statement from Xanthippe

The Methusaleh Report concludes, from epidemiological studies, that all men are mortal.
A single Goal can have one or more evidences
- Do not bundle them
- Use separate Evidence symbol for each

If an evidence supports more than one Goal
- Label each evidence item uniquely
- Use the same Evidence and not update the index

Solutions or Evidences make no claim
- Simply references to evidence artefact that provide support for a particular claim
"Both argument and evidence are crucial elements of the safety case that must go hand-in-hand. Argument without supporting evidence is unfounded, and therefore unconvincing. Evidence without argument is unexplained – it can be unclear that (or how) safety objectives have been satisfied." [Kel&04]
Where does Evidence come from?

Direct Evidence
- tells something about the **product**
- e.g. product features, test results, static analysis results, formal proofs,...

Backing (indirect) Evidence
- tells something about the **process**
- e.g. well established process according to ISO9000, reviews were conducted properly,...

Due to the difficulty of providing sufficient direct evidence for software, backing evidence plays a crucial role
GSN elements are intended to be combined to represent logical structure. GSN provides two types of linkage between elements:

1. SupportedBy
   - Inferential relationships declare that there is an inference between goals in the argument
   - Evidential relationships declare the link between a goal and the evidence used to substantiate it
   - Goal-to-goal, goal-to-strategy, goal-to-solution, strategy to goal

2. InContextOf
   - Declares a contextual relationship
   - Goal-to-context, goal-to-assumption, goal-to-justification, strategy-to-context, strategy-to-assumption and strategy-to-justification
COMMON ERRORS
Confirmation Bias

- You look for what you want to find

- Searching for counter-evidence is crucial

- Somebody needs to challenge the safety case
Avoidance of Common Errors in GSN

The statements made in GSN goal, context and solution elements should be stated atomically
- A single node should contain exactly one claim or reference
- Goals should only contain claims
- Solutions should only refer to evidence
- Strategies should only summarise the argument approach

The statements made in GSN goal elements capture the claims made in the argument
- The statements should be expressed in the form <noun-phrase><verb-phrase>

Similarly, assumptions should be stated atomically in GSN
Avoidance of Common Errors in GSN

GSN **strategy** elements record the approach used in structuring the argument
- It should be possible to remove all of the strategy elements without affecting the logical flow of the claims being made
- Like "comments" in programming languages, they enhance readability

**Strategy** elements are intended as a description of the argument approach which has been carried out to relate claims stated at different levels of detail
- For example, the strategy “Interlocks used” should be phrased “Argument by appeal to the use of interlocks”, to focus the reader’s attention on the argument process, rather than on the design of the system.
Avoidance of Common Errors in GSN

- **Context** elements should not be used to refer to information which is intended to support the validity of a claim.

- **Context** elements are sometimes used where a GSN assumption or justification may be more appropriate.

- **Context** and **Solution** elements in GSN should provide references to artefacts stored elsewhere
  - A single noun-phrase should be sufficient to identify these artefacts
  - It is not necessary to summarize the content of the artefact in the GSN node
Fallacies in Safety Cases [Gre&06]

A critical review of three publicly available safety cases showed that fallacies are quite common.
Safety Argument Fallacy Taxonomy [Gre&06]

→ Circular Reasoning
  – Circular Argument, Circular Definition

→ Diversionary Arguments
  – Irrelevant Premise, Verbose Argument

→ Fallacious Appeals
  – Appeal to Common Practice, Appeal to Improper/Anonymous Authority, Appeal to Money, Appeal to Novelty, Association Fallacy, Genetic Fallacy

→ Mathematical Fallacies
  – Faith in Probability, Gambler’s Fallacy, Insufficient Sample Size, Pseudo-Precision, Unrepresentative Sample

→ Unsupported Assertions
  – Arguing from Ignorance, Unjustified Comparison, Unjustified Distinction

→ Anecdotal Arguments
  – Correlation Implies Causation, Damning the Alternatives, Destroying the Exception, Destroying the Rule, False Dichotomy

→ Omission of Key Evidence
  – Omission of Key Evidence, Fallacious Composition, Fallacious Division, Ignoring Counter-Evidence, Oversimplification

→ Linguistic Fallacies
  – Ambiguity, Equivocation, Suppressed Quantification, Vacuous Explanation, Vagueness
→ Any fallacies here?

**C0.1**  
"Sufficiently secure" means that it is guaranteed that no unauthorised access will ever take place

**G0**  
The computer system is sufficiently secure

**C0.2**  
CIA computer system storing all strategic plans for future CIA activities

**G1**  
The developer had security know-how

**G2**  
No security leaks were found during analysis

**G3**  
A paid hacker could not break into the system

**Sn1.1**  
Training Certificate

**Sn2.1**  
Analysis Report

**Sn3.1**  
Hacker Report

---

*Sufficiently secure* means that it is guaranteed that no unauthorised access will ever take place.
Any fallacies?

A0.1  COMPANY shares are in the Dow Jones

G0  Prices of COMPANY shares will rise within the next year

G1  Experts say COMPANY has a bright future

G2  The Dow Jones Index will rise within the next year

G3  Interest rates are low

Sn1.1  Newspaper

Sn2.1.1  Historical Records

Sn3.1  Bank Commercials

C0.1  "Rise" means that the price at the end of the last trading day is higher than at the beginning of the first trading day in a year.
Any fallacies?

G0
MEDICATION X helps to alleviate a common cold

G1
Dr. X confirms that MEDICATION X works

Sn1
Dr. X's testimonial

G2
There are several success stories available

Sn2
Detailed doc of three success stories

G3
Last time when I had a cold, I took MEDICATION X and my cold was gone within three days

Sn3
My own testimonial

G4
MEDICATION X does not have any unwanted side effects

Sn4
Rigorous randomized double blind evidence-based study about absence of side effects of MEDICATION X
Excerpt of EUR RVSM Safety Case – can you find fallacies?

**S2.3.1**
Argue that there is sufficient direct evidence of flight crew training design validity.

**G2.3.1.1**
FC RVSM & Transition Training specified.

**G2.3.1.2**
FC Aircraft Contingency training specified.

**G2.3.1.3**
Flight planning training specified.

**G2.3.1.4**
Hazards and risks controlled and mitigated.

**S2.3.1.1**
PISC 5.4.3 & 5.4.4

**S2.3.1.4**
PISC 5.4.6

**G2.3**
Flight crew training design complies with safety requirements.
CASE STUDY
Case Study

- Read the handout
- Create a GSN for a claim like
  "The system is acceptably safe…"
- Please form groups of <=5 people
- Time: 40min for elaboration, 20min for discussion
SOME FINAL NOTES
Problems with Traditional Safety Case Development: "Retrospective Safety Case"

- Large amounts of re-design necessary because safety case cannot be constructed
- Less robust safety case – safety engineers have to live with the current design instead of influence the design
- Lost safety rationales – rationales for certain design features might not be recorded and therefore lost

Design Lifecycle

Safety Lifecycle

[Kei98], p. 67
Better: Evolutionary Safety Case Development

- (Intermediate) Safety Cases are produced at each major milestone in a project
- GSN supports the evolutionary development of safety cases
Three publicly available Safety Cases

Unfortunately, most safety cases are not publicly available

Should safety cases affecting the public be publicly available? (cf. sessions and decisions in a criminal court)

1. [EUR01] The EUR RVSM Pre-Implementation Safety Case
   Reduced vertical separation safety case
   GSN and text

2. [Kin01] Eurocontrol Whole Airspace ATM System Safety Case
   Common airspace for all Eurocontrol member states
   GSN and text

3. [NAG02] Project Opalinus Clay: Safety Report
   Long-term radioactive waste storage facility
   Text, heavy use of bullet points
Potential problems with Safety Cases

- Confirmation bias: People who have a vital interest that the top level claim is true provide the evidence.
- People who build the system also build the safety case, they only see the positive evidence.
- Re-inventing the wheel many times instead of using successful processes which are successful over many years.
- "The problem is that it is always possible to find or produce evidence that something is safe." [Lev11]
- "Care should be taken when utilizing techniques such as Goal Structured Notation [...] to avoid falling into the trap of assuming the conclusion [...], or looking for supporting evidence for the conclusion instead of carrying out a proper analysis of risk." [Lev11]


Active searching for counter-evidence is important! (and not finding counter-evidence is no guarantee that it does not exist)
Some conclusions with my personal view

- Good processes, techniques and measures are *necessary* but not *sufficient* to assure safety
- A Safety Case must be easy to follow and understandable
- The Safety Case is the most important document for assuring safety
- There shall be freedom in the design of the safety case
- ISO 26262 combines necessary prescriptions with the goal-based approach of a Safety Case in the best way
- GSN improves readability of Safety Cases massively
- GSN is an excellent way to document or to support the documentation of Safety Cases
Thank You!