

Safety Demonstration – A Strategy for Assessors

PSAM 14, Los Angeles CA, September 18th 2018

André A. Hauge^a, Vikash Katta^a, Peter Karpati^a and Bjørn Axel Gran^{a,b}

^a Department of Risk Safety and Security, Institute for Energy Technology, Norway

^b NTNU, Trondheim, Norway

Safety Demonstration – A Strategy for Assessors

Outline

Background

The Strategy explained

- The Process
- The Language

The Strategy exemplified

Conclusion and further works

Background

Research within OECD NEA Halden Reactor Project on Safety Demonstration within Digital Instrumentation and Control last 7 years includes

- Interviews with nuclear regulators and support organizations from 6 different countries
- Workshops with industrial experts
- Case studies

Shows

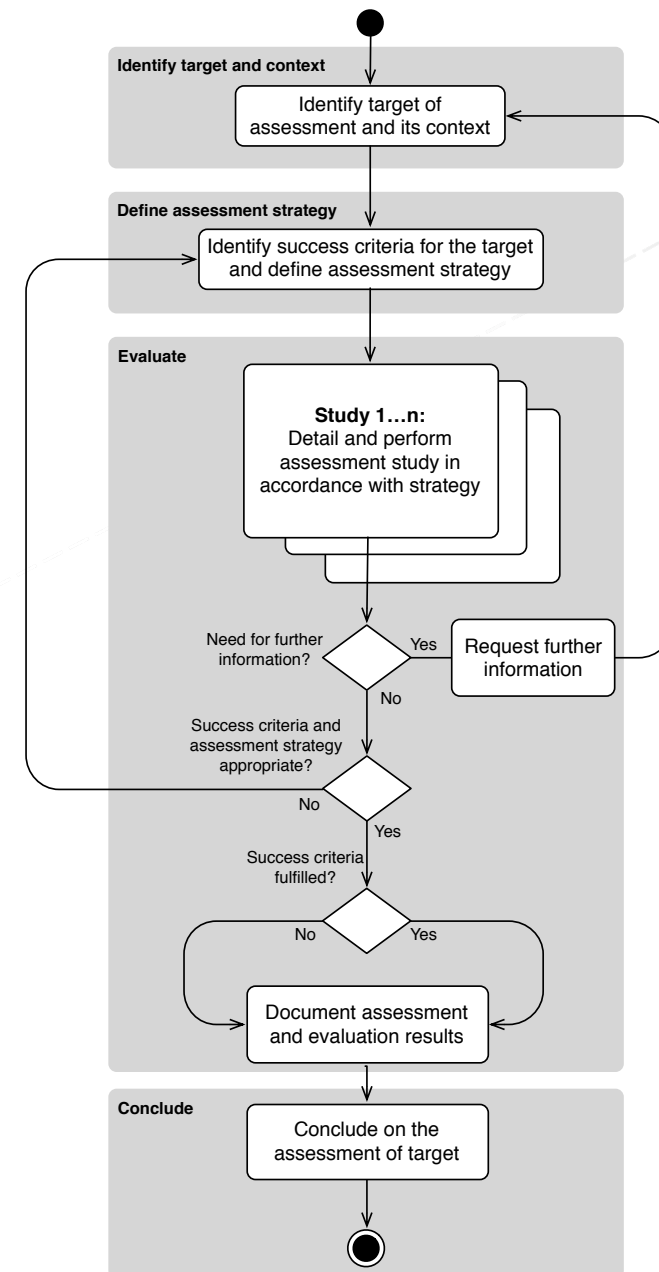
- An assessor needs to evaluate a large quantity of documentation
- Not possible to perform a complete assessment due to resource constraints
- There is no single common approach within the nuclear industry – differences between countries

Assessor needs

- A strategy for limiting the investigation
- To assure sufficient coverage and obtain needed confidence
- A flexible approach, allowing different assessment styles

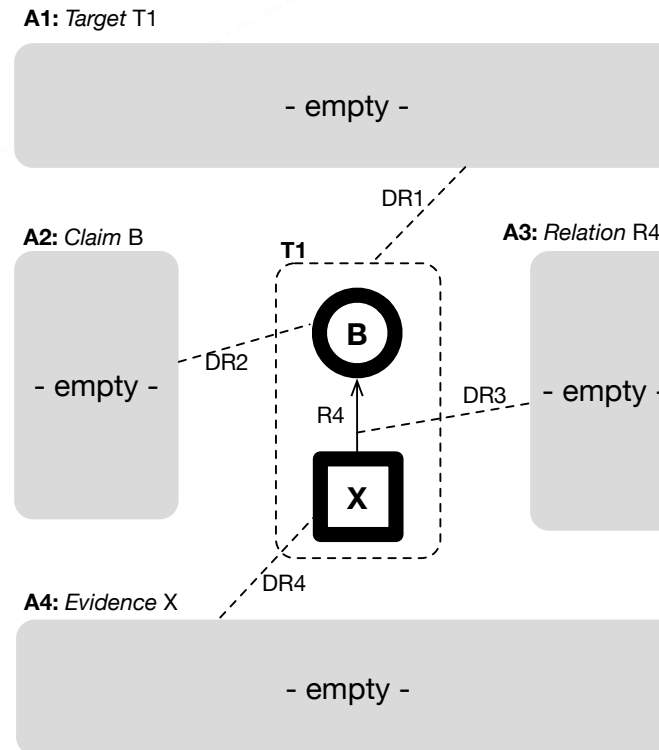
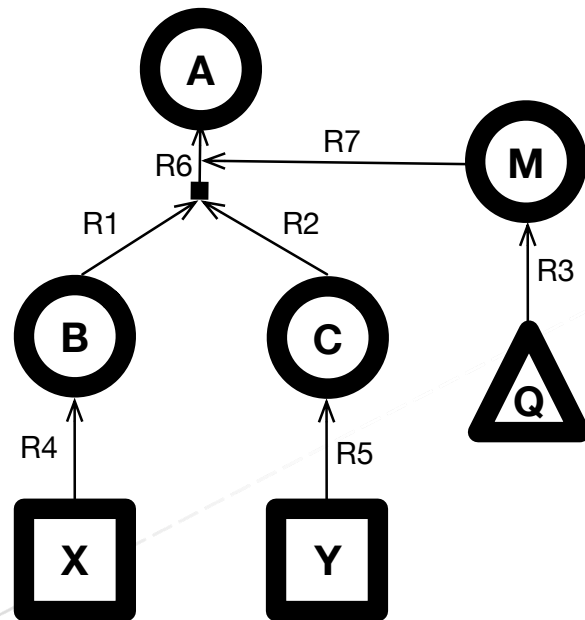
The Strategy Explained The Process

1. **Identify target** of assessment and its context
2. **Define assessment strategy**
3. **Evaluate**
 - Detail and perform assessment study (1..n) in accordance with strategy
 - Document assessment and evaluation results
4. **Conclude** on the assessment of the target



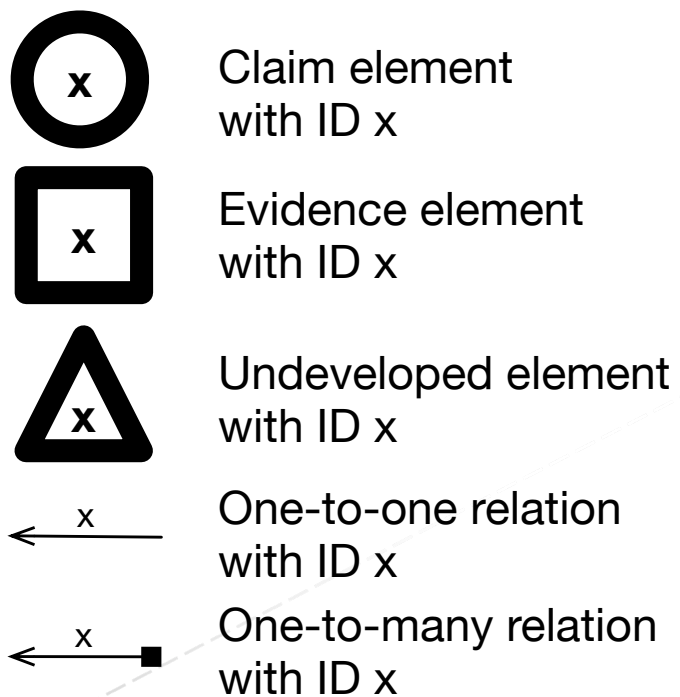
The Strategy Explained - The Language

Consist of an *Argument Model* and an *Assessment Model*

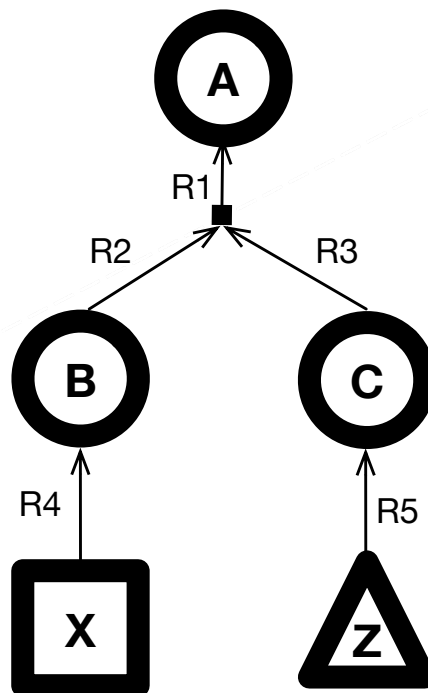


The Language – Argument Model

Legend argument model



Example argument model


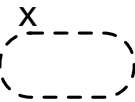
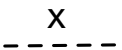


Example representation

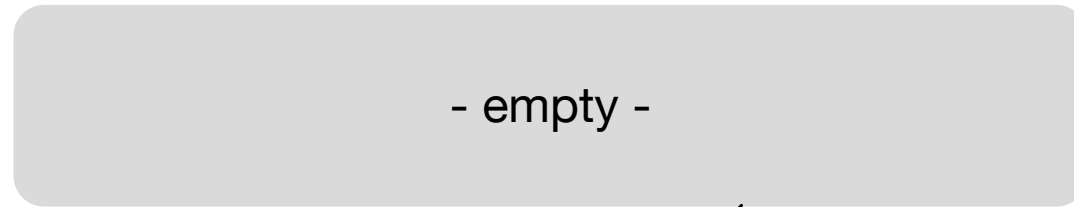
A = <text>
B = <text>
C = <text>
X = <text>
Z = <text, e.g. an assumption>

The Language Assessment Model

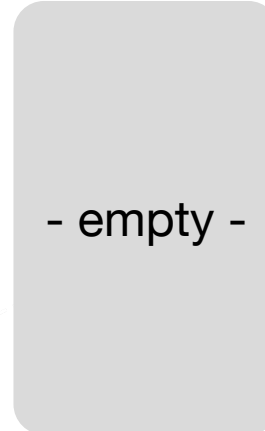
Legend assessment model

-  Assessment container with ID x
-  Target container with ID x
-  Relation with ID x

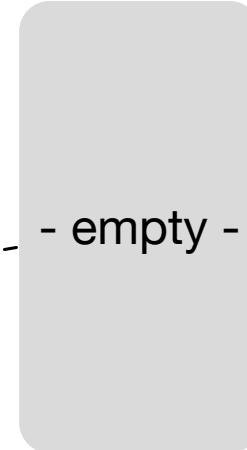
A1: Target T1



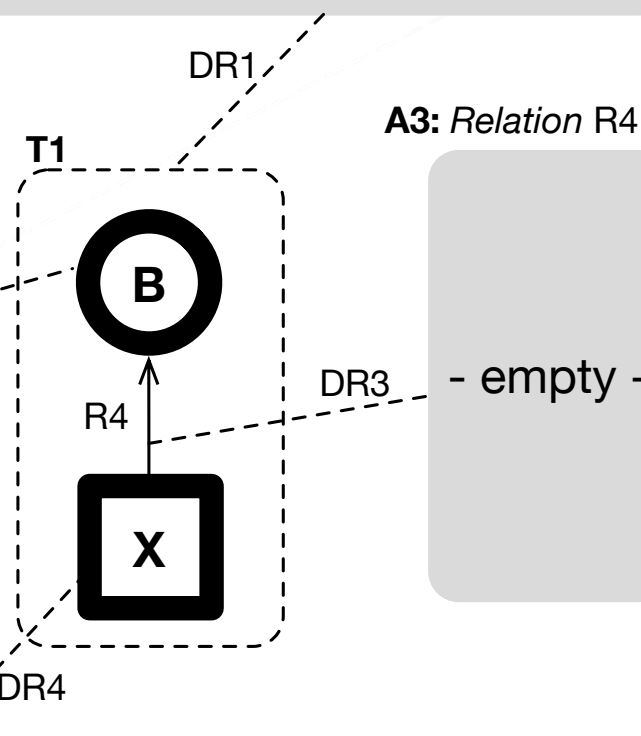
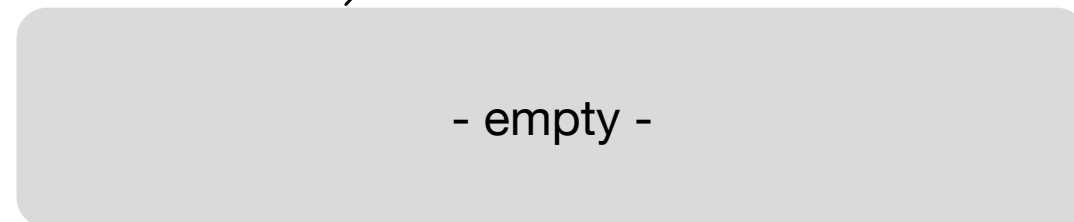
A2: Claim B



A3: Relation R4



A4: Evidence X



The Strategy Exemplified

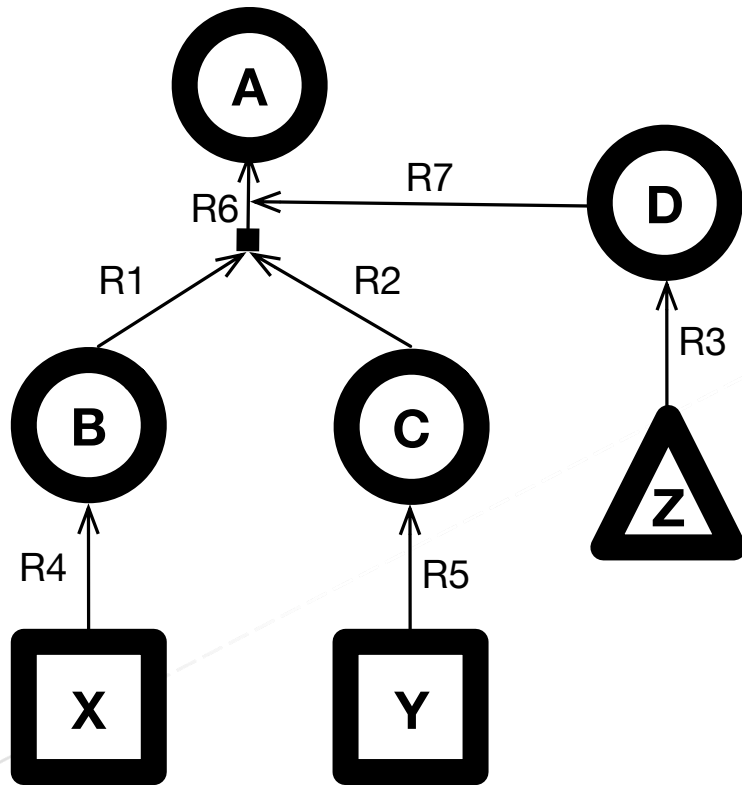
Step 1: Identify target; Step 2: Define strategy; Step 3: Evaluate; Step 4: Conclude

Example below is an extract, somewhat abstract, from Safety Analysis Report (SAR) on design of DI&C system submitted to a nuclear regulator

*...[**Claim A1 unfolded**]...because Claim B1 and Claim C1 [R1 & R2]. Claim B1 and Claim C1 together are equivalent with Claim A1 [**Claim D1 unfolded**] because we know [R3]...[**Undeveloped element Z1 unfolded**]... .. Text with no safety argument relevance [**Claim B1 unfolded**]... because of [R4] Evidence X1. ...[**Claim C1 unfolded**]... because of [R5] Evidence Y1.*

The Strategy Exemplified

Step 1: Identify target; Step 2: Define strategy; Step 3: Evaluate; Step 4: Conclude



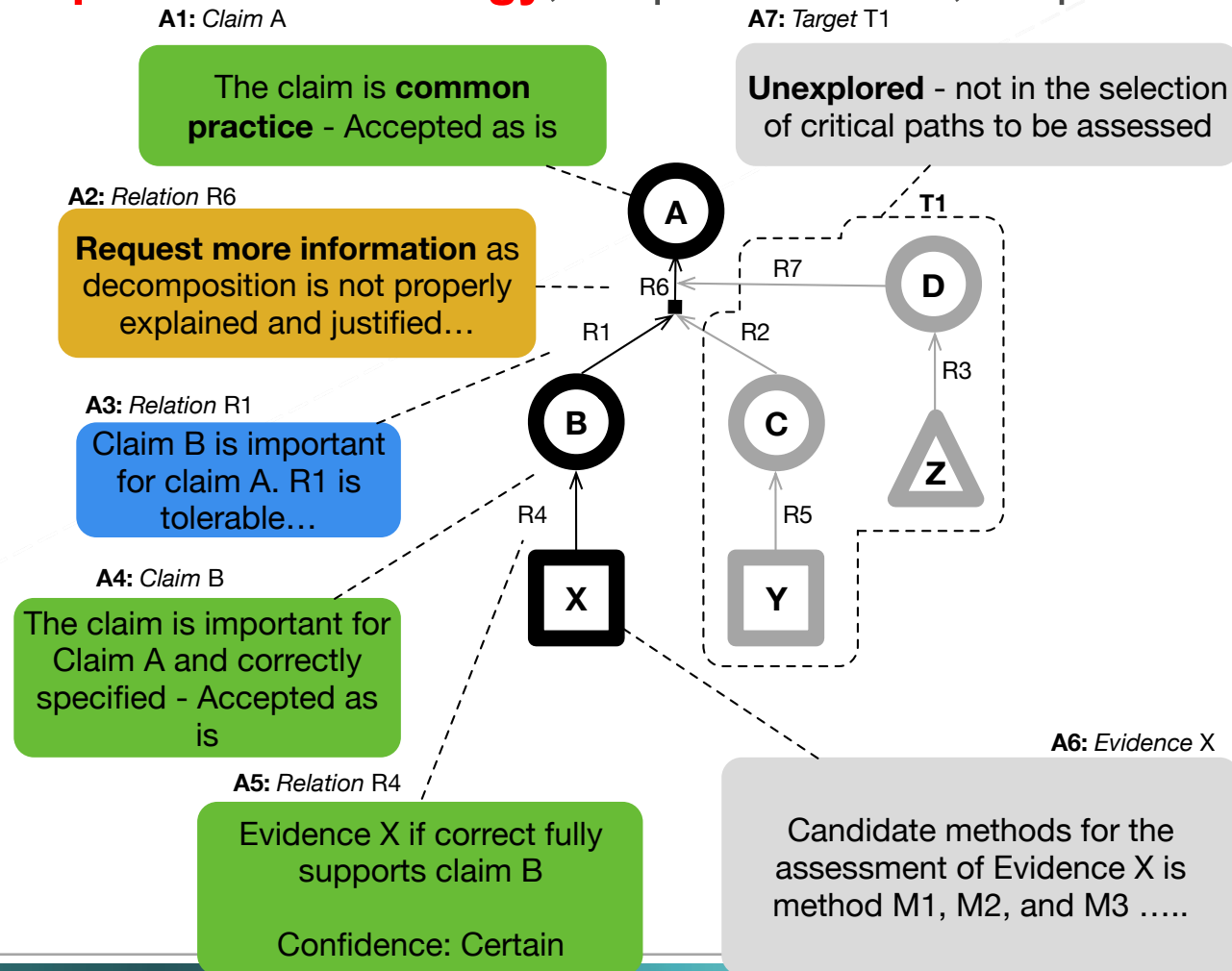
ID	Description
A	...[Claim A unfolded] ... because Claim B and Claim C [R1 & R2]
B	...[Claim B unfolded] ... because of [R4]
C	...[Claim C unfolded] ... because of [R5]
D	...[Claim D unfolded] ... because we know [R3]
X	Evidence X
Y	Evidence Y
Z	[Undeveloped element Z unfolded]... Text with no safety argument relevance ...
R1	... because Claim B and Claim C [R1 & R2]
R2	... because Claim B and Claim C [R1 & R2]
R3	...we know [R3] ...
R4	...because of [R4] Evidcence X
R5	...because of [R5] Evidcence Y
R6	R6 express combination ... [R1 & R2]
R7	R7 express justification of R6

The Strategy Exemplified

Step 1: Identify target; **Step 2: Define strategy**; Step 3: Evaluate; Step 4: Conclude

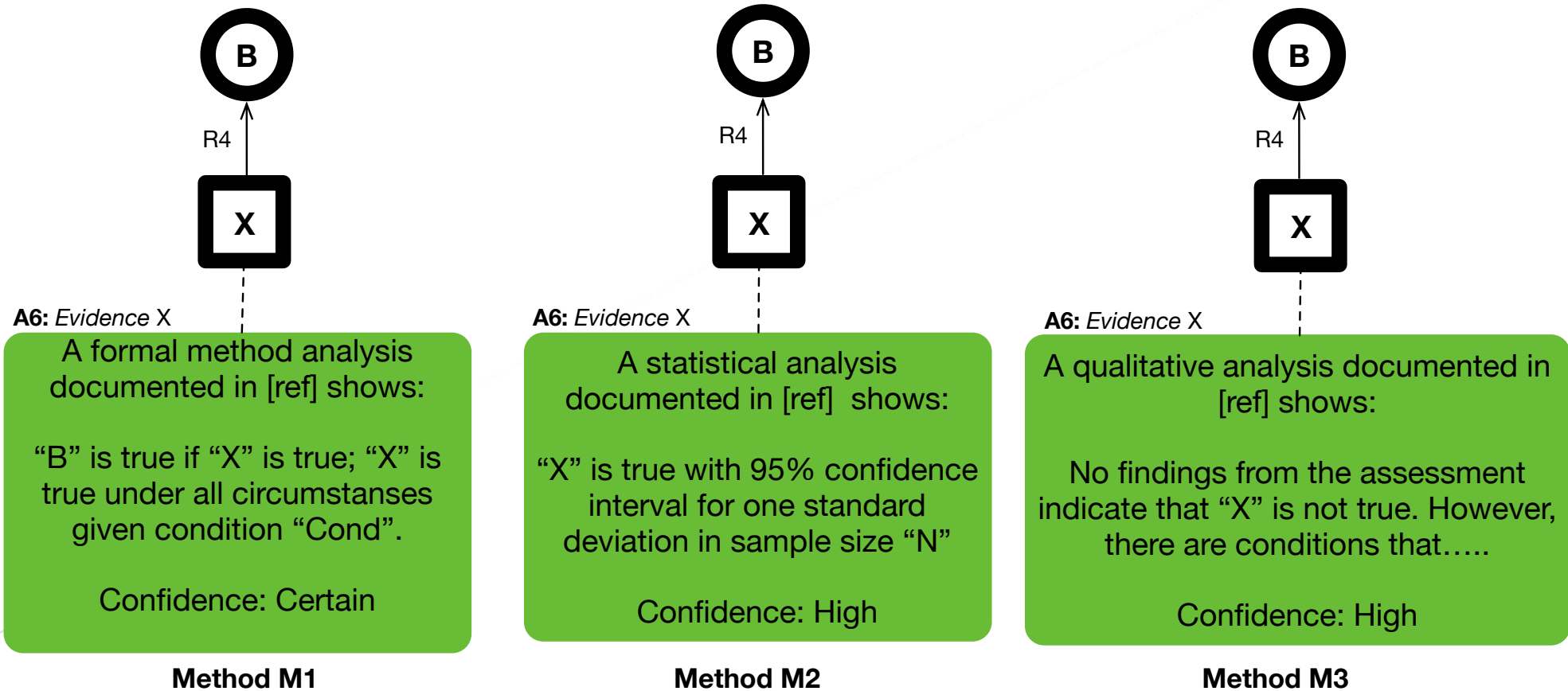
Legend (colouring)

- Not Evaluated
- Evaluated - Acceptable
- Evaluated - Tolerable
- Evaluated - Opposable
- Evaluated - Rejectable



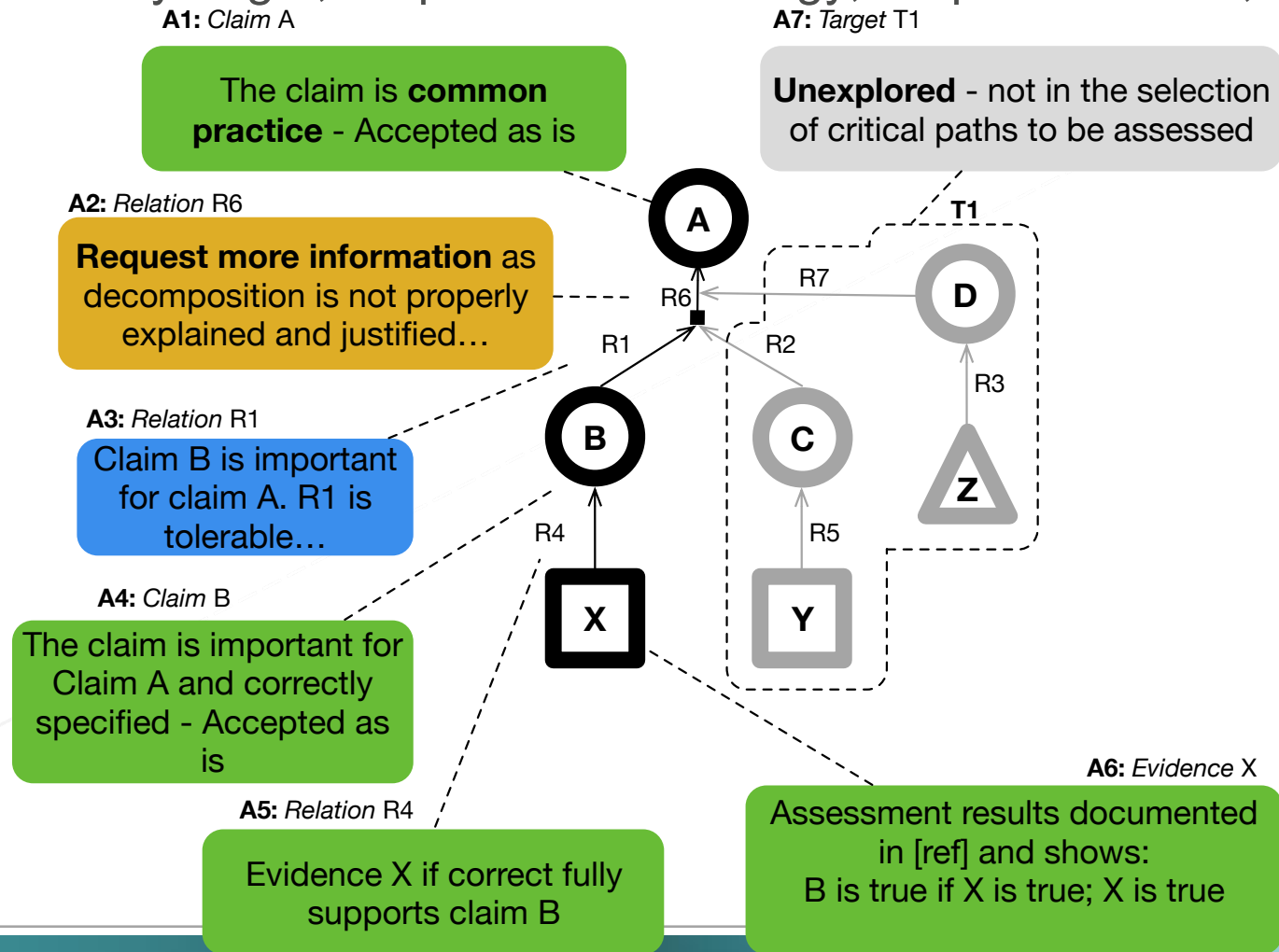
The Strategy Exemplified

Step 1: Identify target; Step 2: Define strategy; **Step 3: Evaluate**; Step 4: Conclude



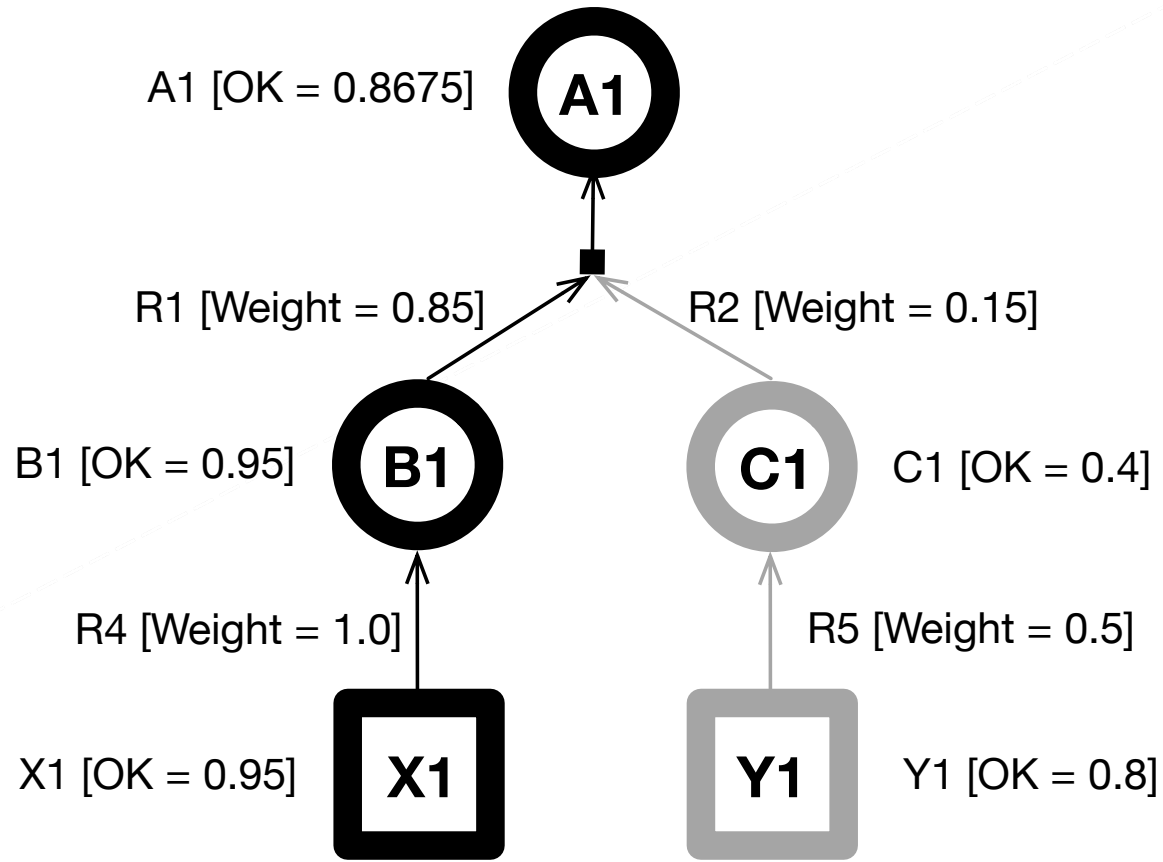
The Strategy Exemplified

Step 1: Identify target; Step 2: Define strategy; Step 3: Evaluate; **Step 4: Conclude**



The Strategy Exemplified

Step 1: Identify target; Step 2: Define strategy; Step 3: Evaluate; **Step 4: Conclude**



Conclusion and Further Work

Conclusions

- An assessor is likely to: adapt its investigative process as new knowledge is acquired; use different assessment approaches depending on kind of evidence; combine different evidences on the basis of experience; use judgement.
- We propose a process and a language supporting assessors in developing their assessment strategy and documenting it. The goal is to offer a systematic approach to capturing the mental process of the assessor – how claims and evidences are developed, combined and evaluated
- A prototype tool named Instruct is developed at the Halden Reactor Project that supports supervised identification and extraction of claims and evidence into an argument structure from documentation (e.g. pdf files)

Further work:

- Provide a clear definition of the syntax and semantics of the language
- Offer guidance on how an assessor may aggregate individual assessment results
- Empirical evaluation with assessors

Thank you

André A. Hauge
Senior Research Scientist, PhD
Institute for Energy Technology (IFE)
andre.hauge@ife.no
(+47) 996 16 690