Assurance Case Templates: Principles for Their Development and Criteria for Their Evaluation (Appendices)

By

Thomas Chowdhury, M.Sc.

A Thesis

Submitted to the School of Graduate Studies
in Partial Fulfillment of the Requirements for the Degree

Doctor of Philosophy

McMaster University

Appendices

Appendix A

Assurance Case Template complying with *ISO 26262* and *SAE J3061*

In this appendix we show the partial ACT for safety complying with *ISO 26262*. We also present partial ACT for safety and security complying with both *ISO 26262* and *SAE J3061*.

A.1 Partial Assurance Case Template complying with *ISO 26262*

In this section, we illustrate partial ACT complying with *ISO 26262*. Figures A.1, A.2, A.3, A.4, A.5, A.6, A.7 and A.8 show the template complying with *ISO 26262*.

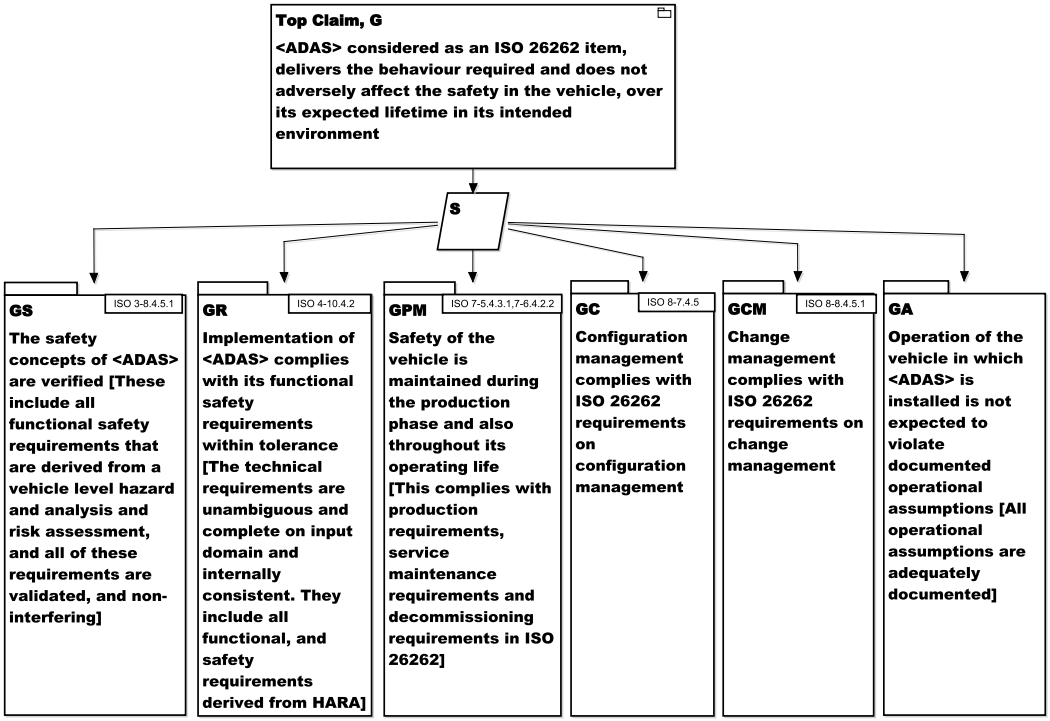

Figure A.1: Top Level Claim for <ADAS> with Argument

Figure A.1 shows a top-level claim supported by sub-claims. The top-level claim shows "<ADAS> considered as an ISO 26262 item, delivers the behaviour required and does not adversely affect the safety in the vehicle, over its expected lifetime in its intended environment". The top claim is supported by 6 sub-claims. Five sub-claims are compliant with *ISO 26262*. Similarly figures A.2, A.3, A.4, A.5, A.6, A.7, A.8 show different arguments of that template.

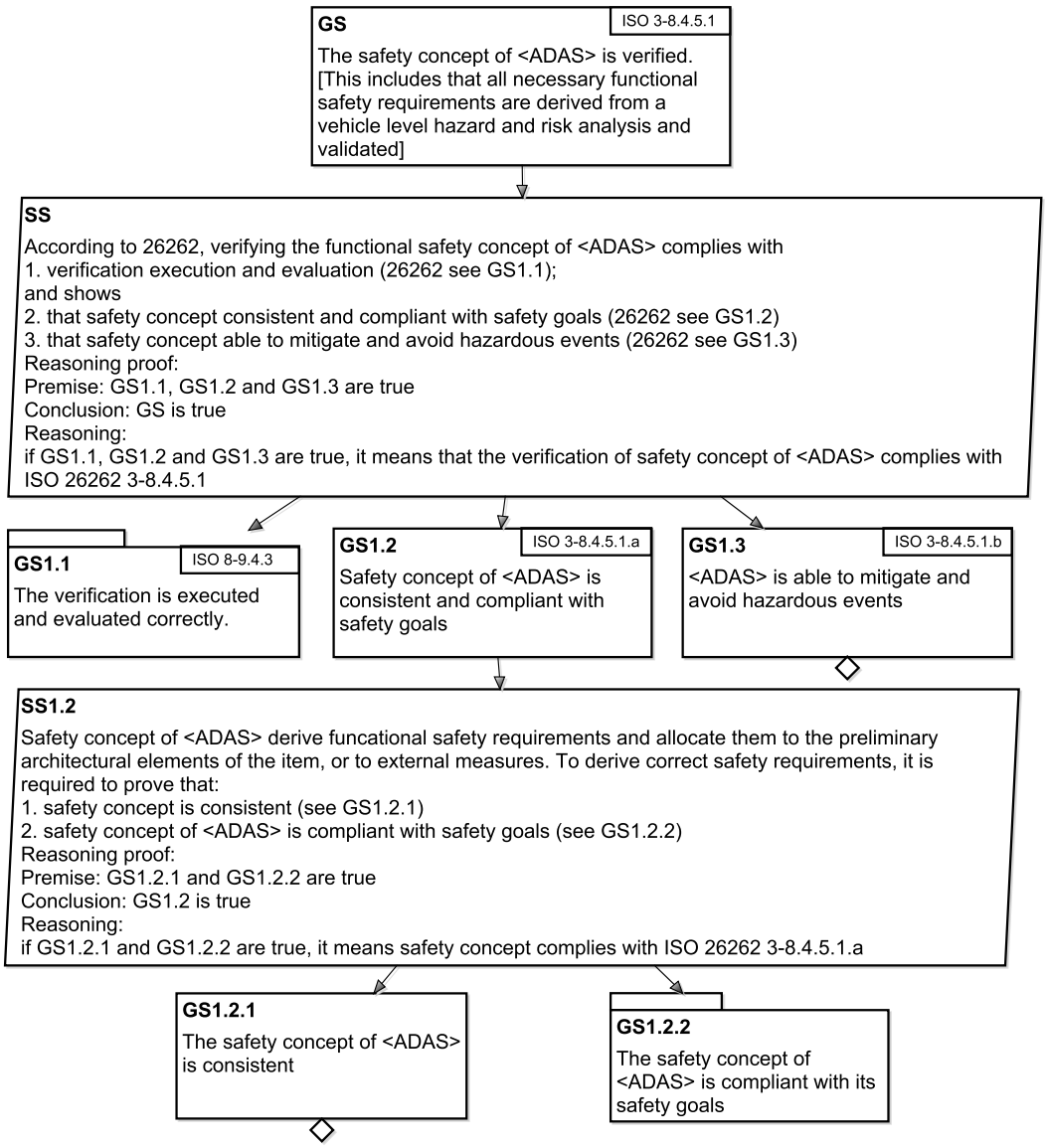

Figure A.2: Claim GS with Arguments

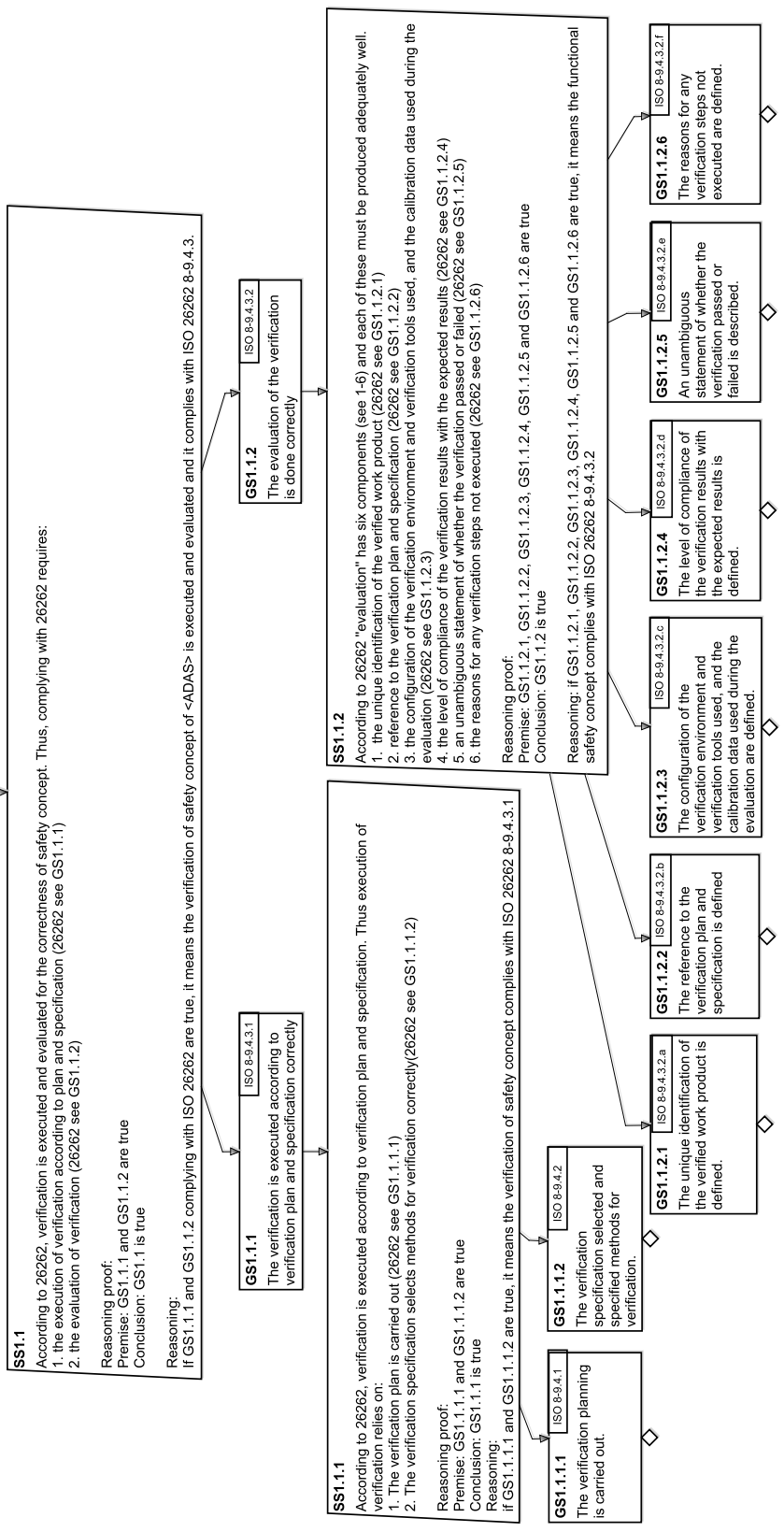

Figure A.3: Claim GS1.1 with Arguments

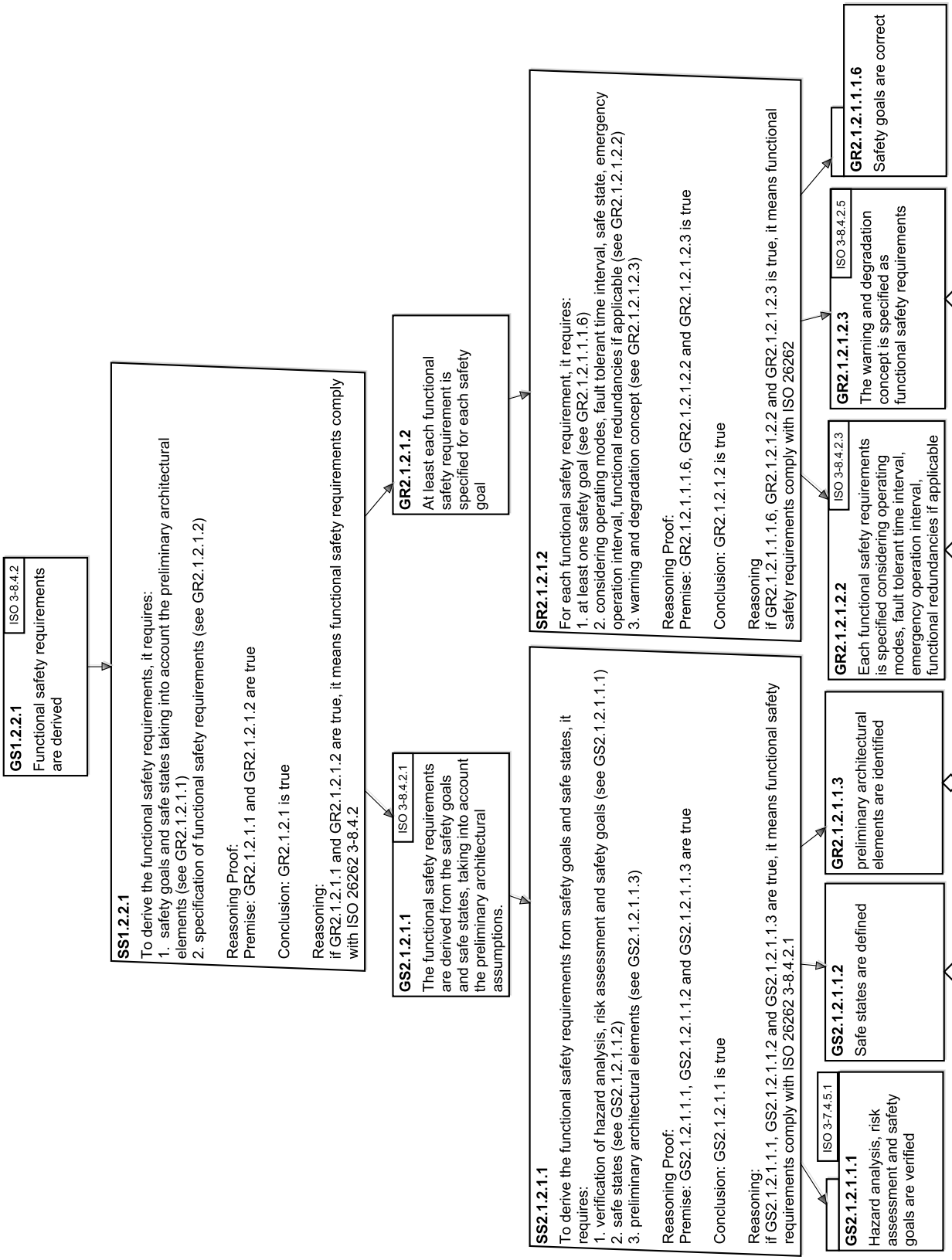

Figure A.4: Claim GS1.2.2.1 with Arguments

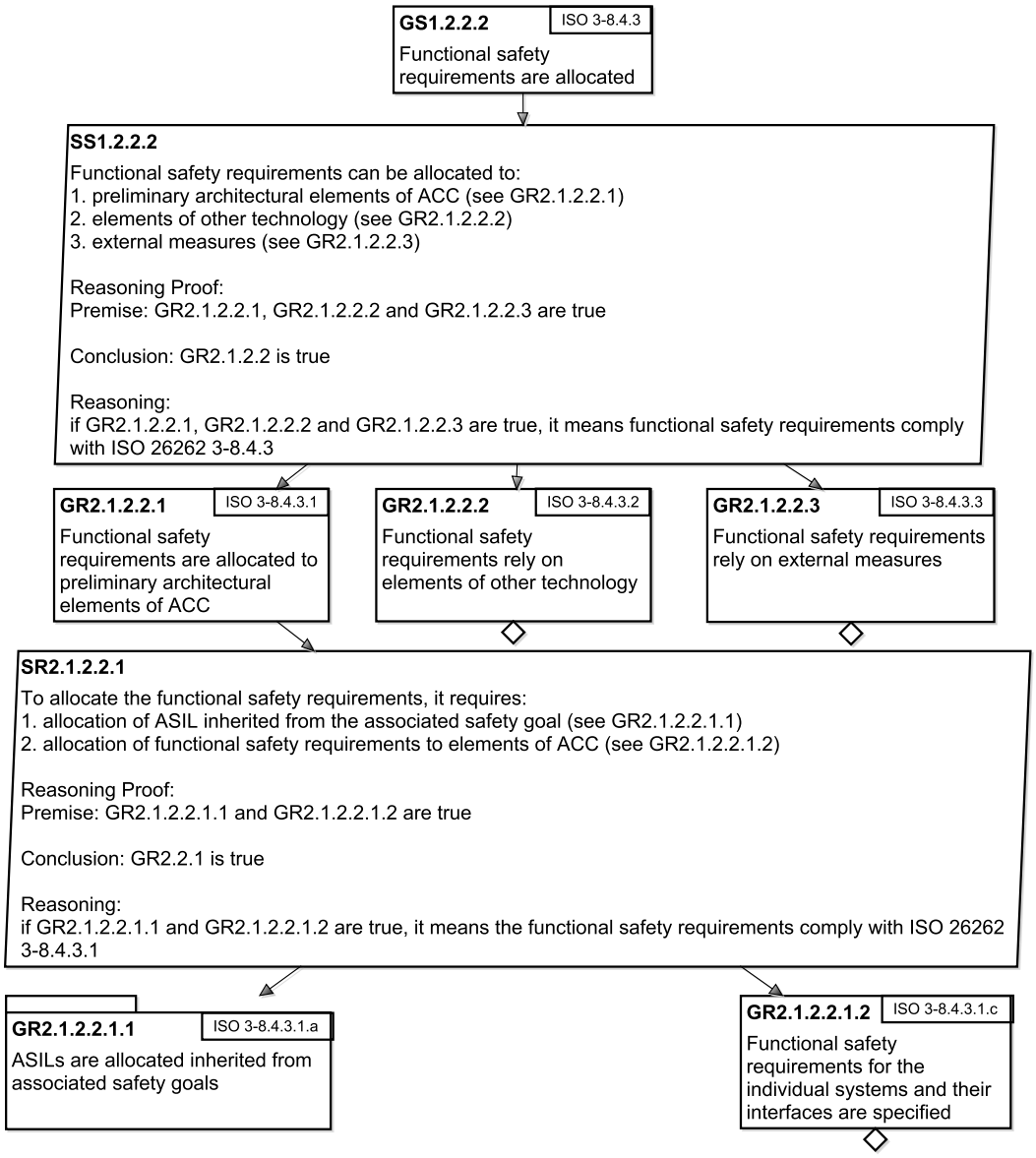

Figure A.5: Claim GS1.2.2.2 with Arguments

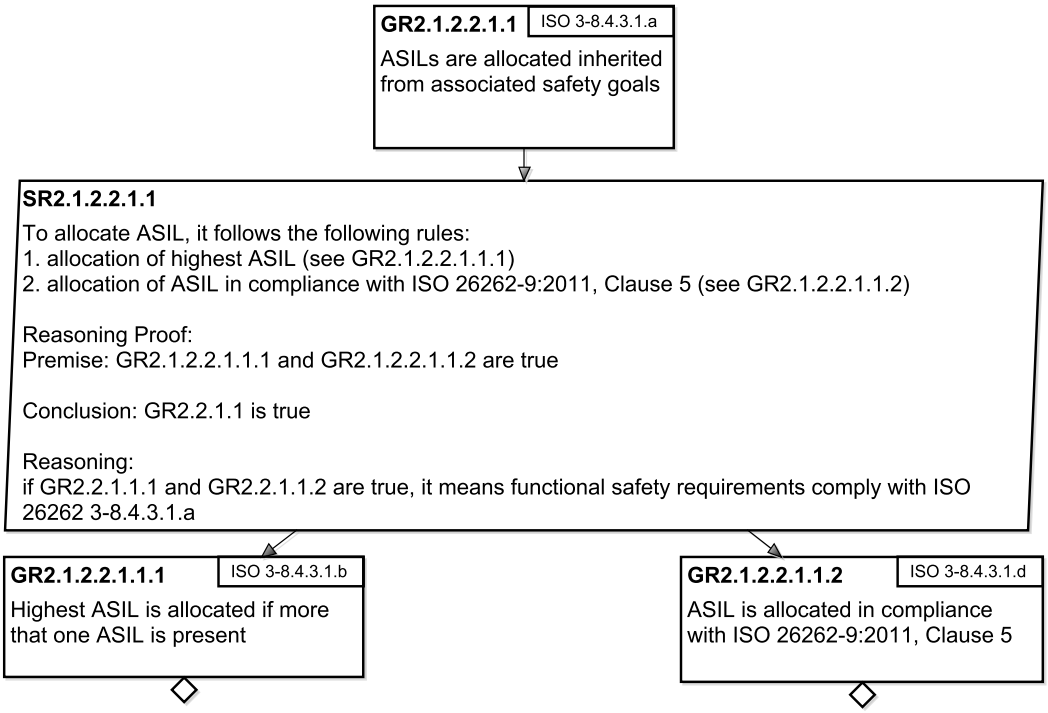

Figure A.6: Claim GoalGR2.1.2.2.1.1 with Arguments

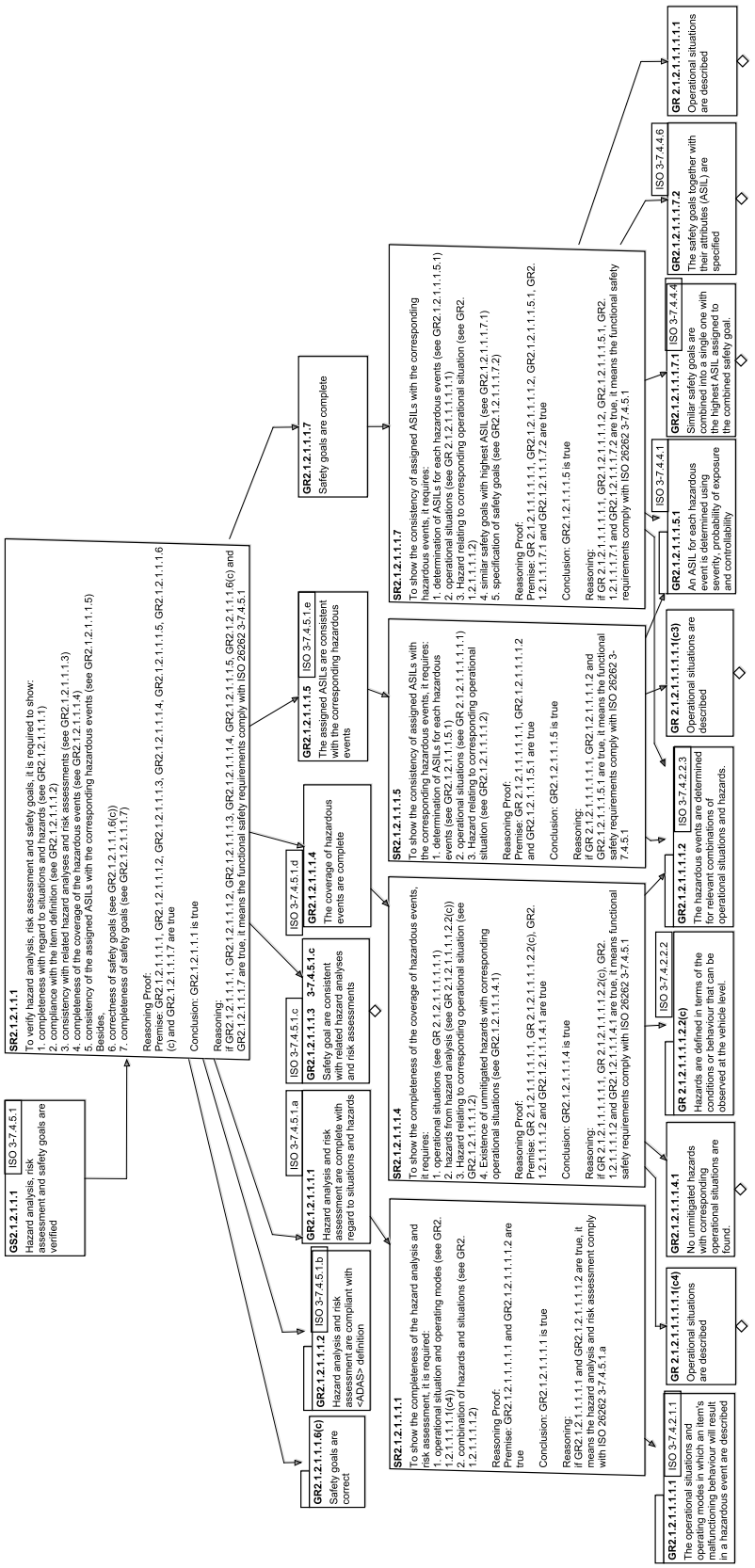

Figure A.7: Claim GS2.1.2.1.1.1 with Arguments

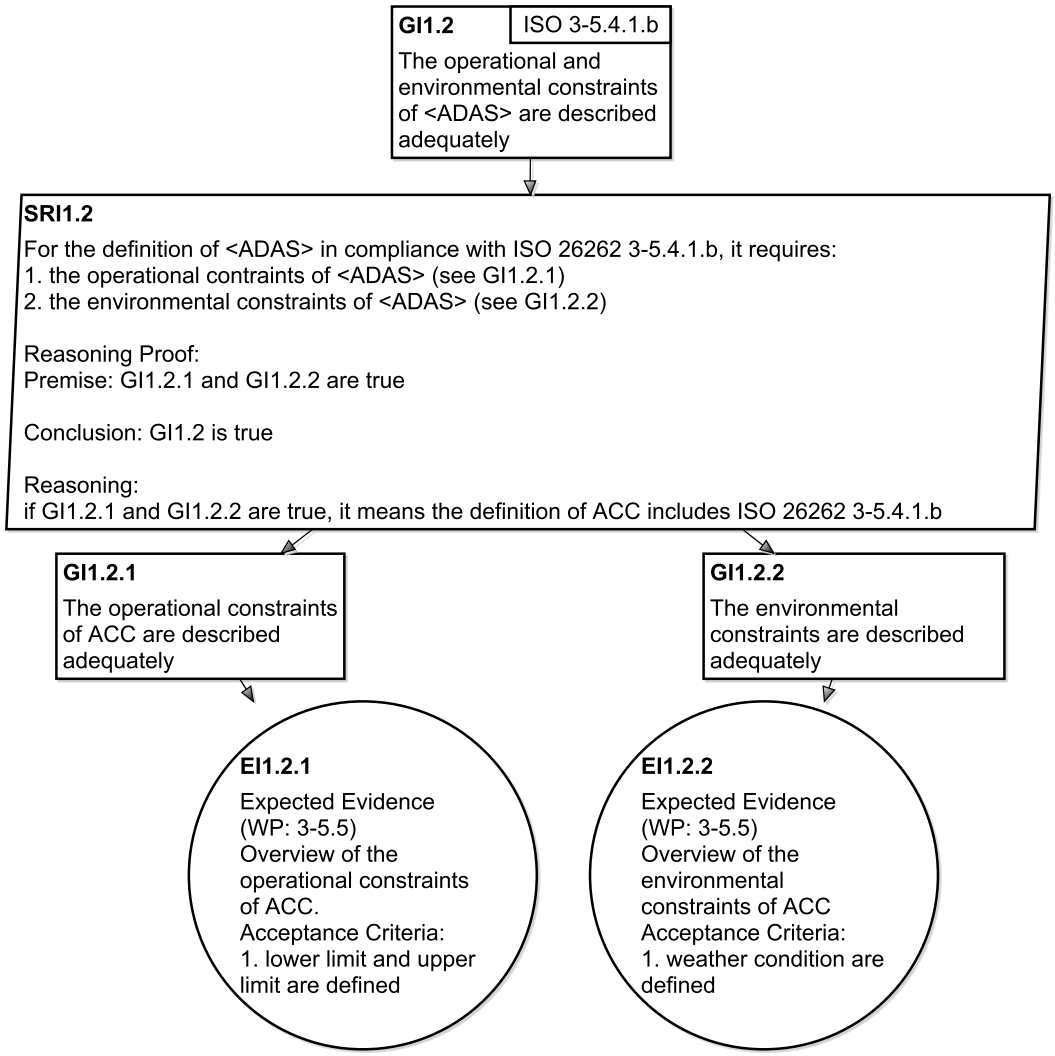

Figure A.8: Claim GI1.2 with Arguments

A.2 Partial Assurance Case Template complying with both *ISO 26262* and *SAE J3061*

In this section, we illustrate partial ACT complying with both *ISO 26262* and *SAE J3061*. Figures A.9, A.10 and A.17 show the template complying with both *ISO 26262* and *SAE J3061*. Figures A.11, A.12, A.13, A.14, A.15, and A.16 show the template complying with *SAE J3061*.

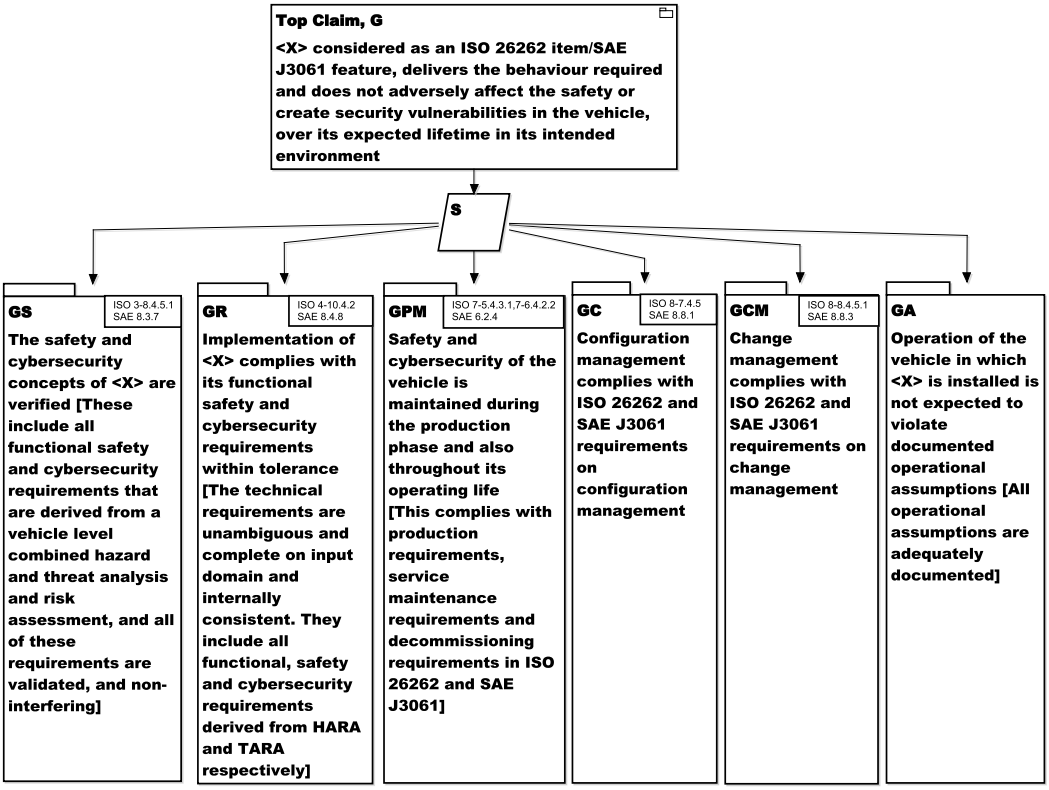

Figure A.9: <X> Top Level Claim with Argument

A.3 Partial Assurance Case Template for OTA updates complying with both *ISO 26262* and *SAE J3061*

In this section, we illustrate partial ACT for OTA updates complying with both *ISO 26262* and *SAE J3061*. Figures A.18 and A.19 show safety and security arguments of the template complying with both *ISO 26262* and *SAE J3061*.

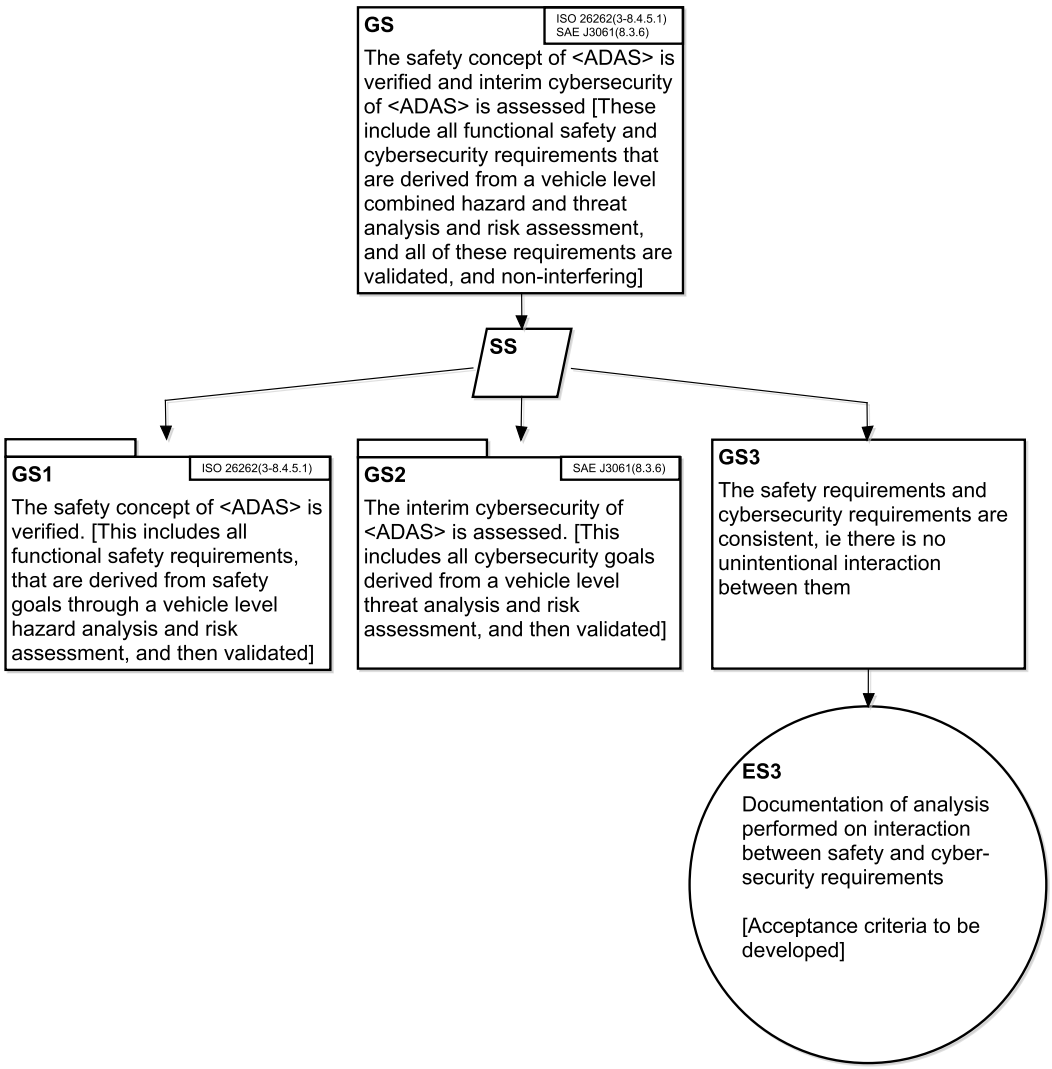

Figure A.10: Claim 'GS' with Arguments

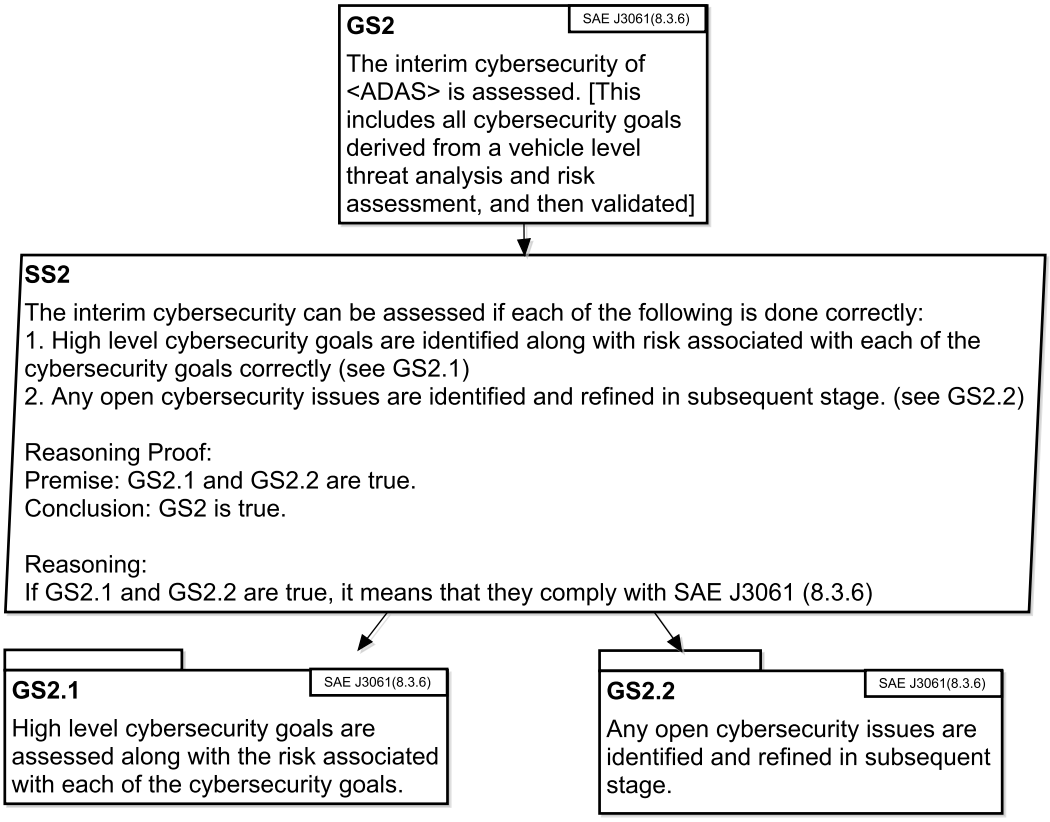

Figure A.11: Claim 'GS2' with Arguments

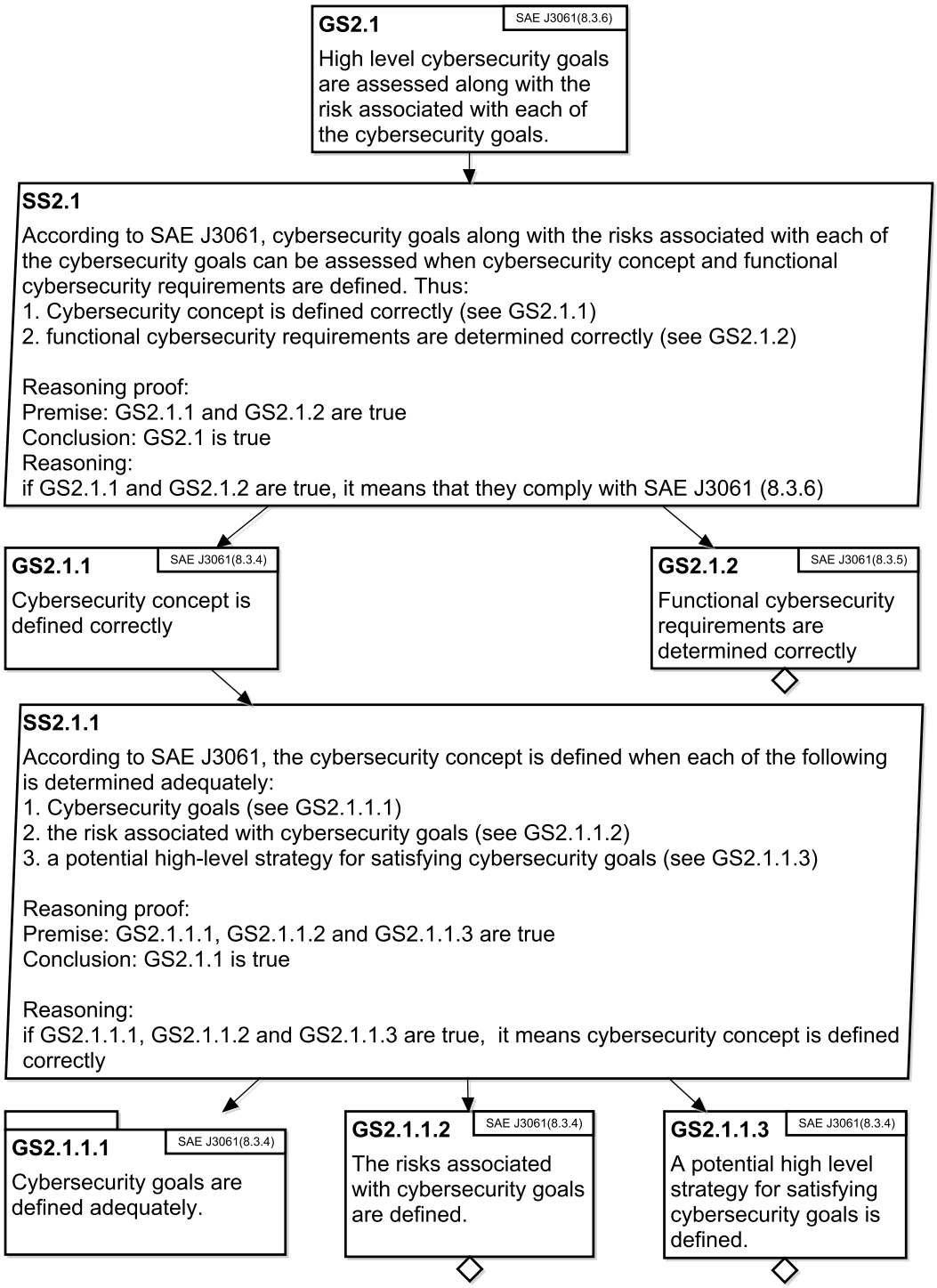

Figure A.12: Claim 'GS2.1' with Arguments

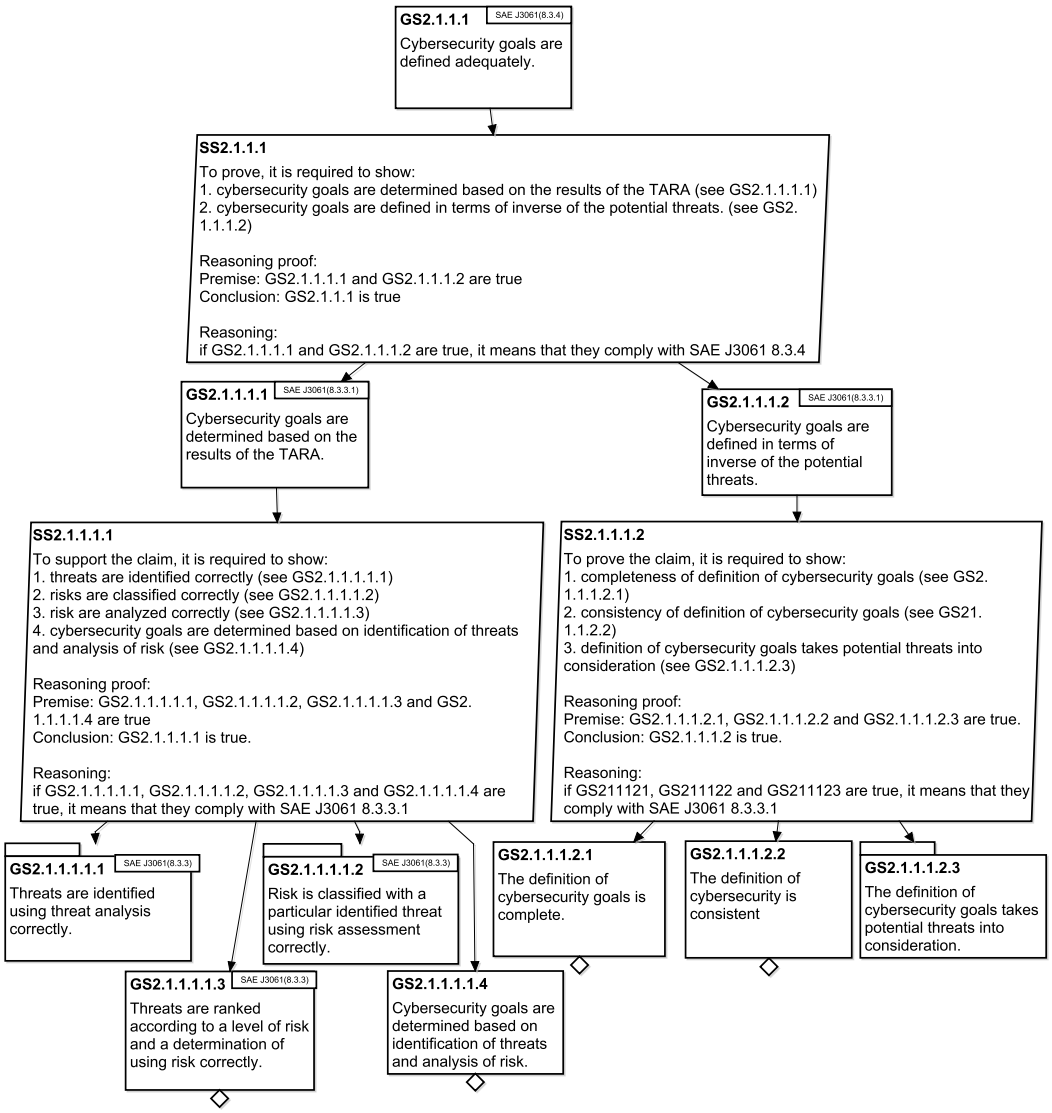

Figure A.13: Claim 'GS2.1.1.1' with Arguments

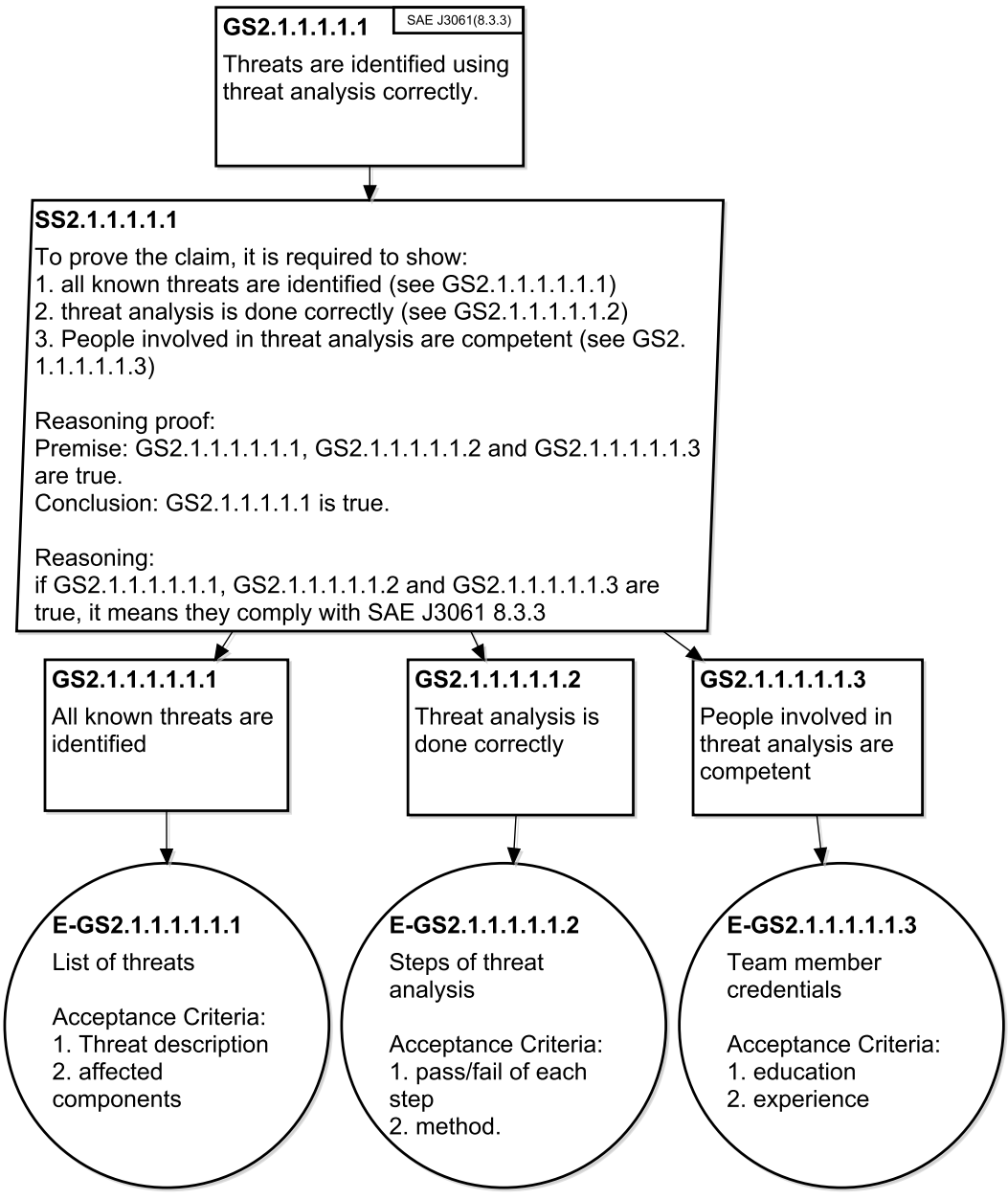

Figure A.14: Claim 'GS2.1.1.1.1.1' with Arguments

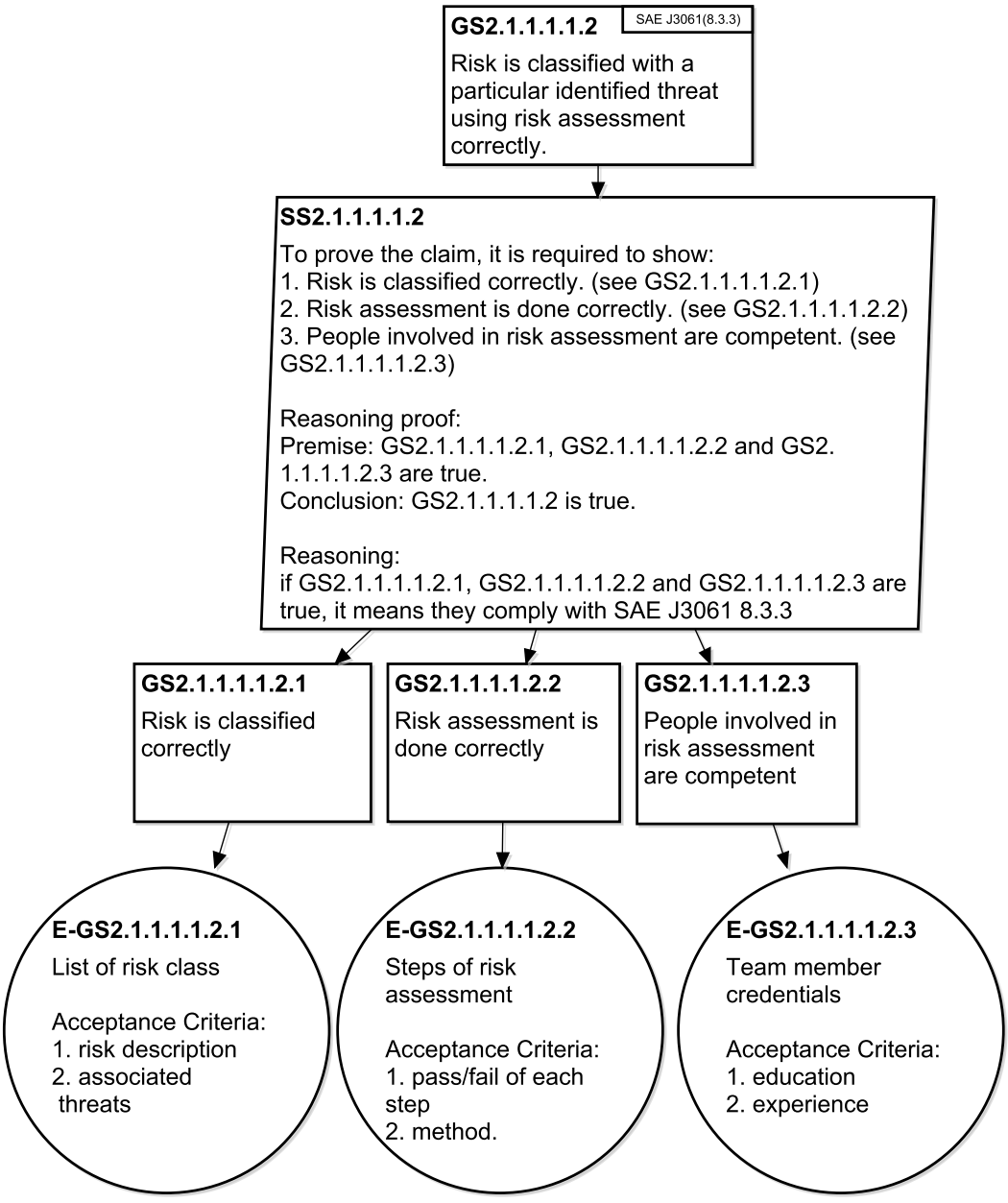

Figure A.15: Claim 'GS2.1.1.1.1.2' with Arguments

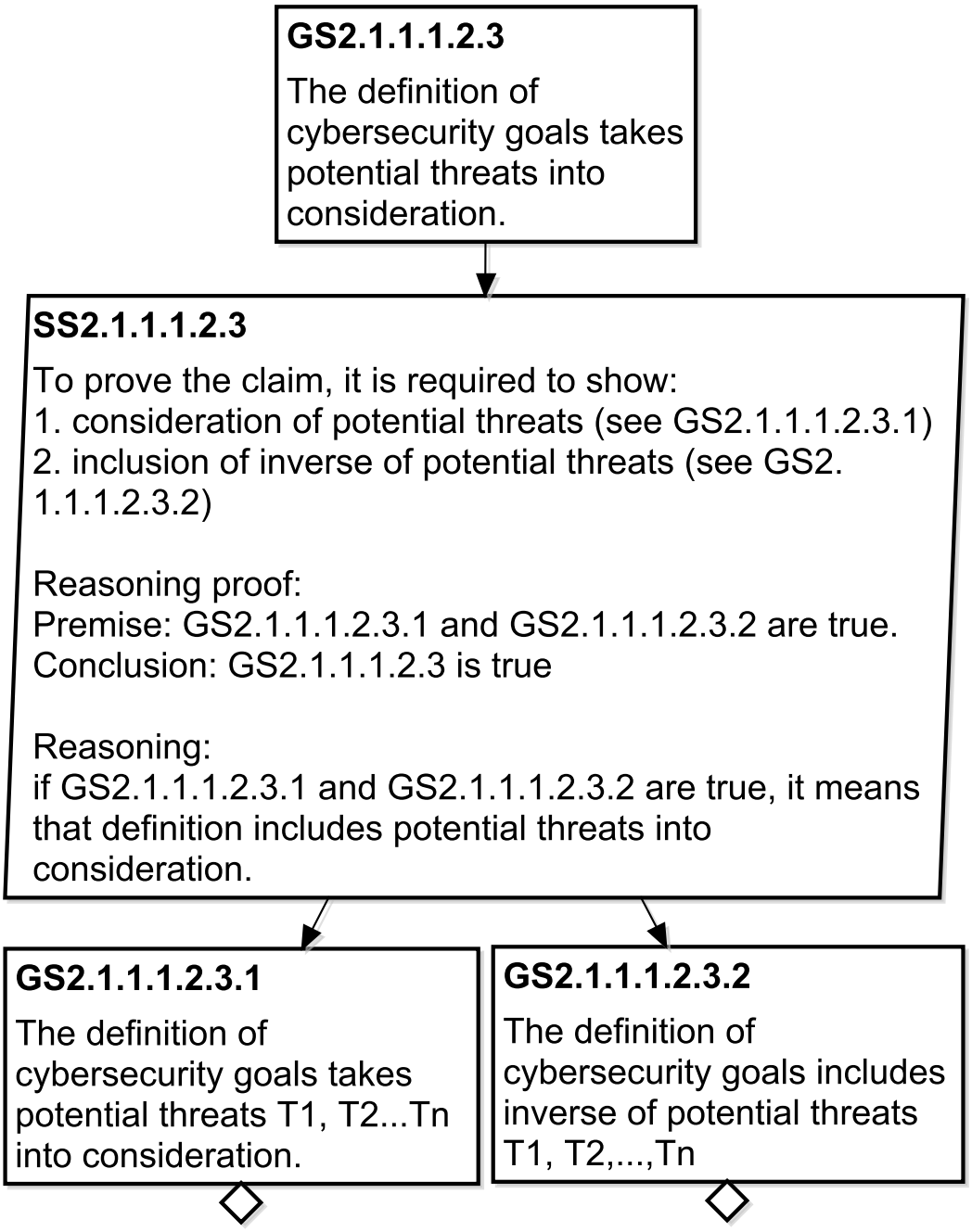

Figure A.16: Claim 'GS2.1.1.1.2.3' with Arguments

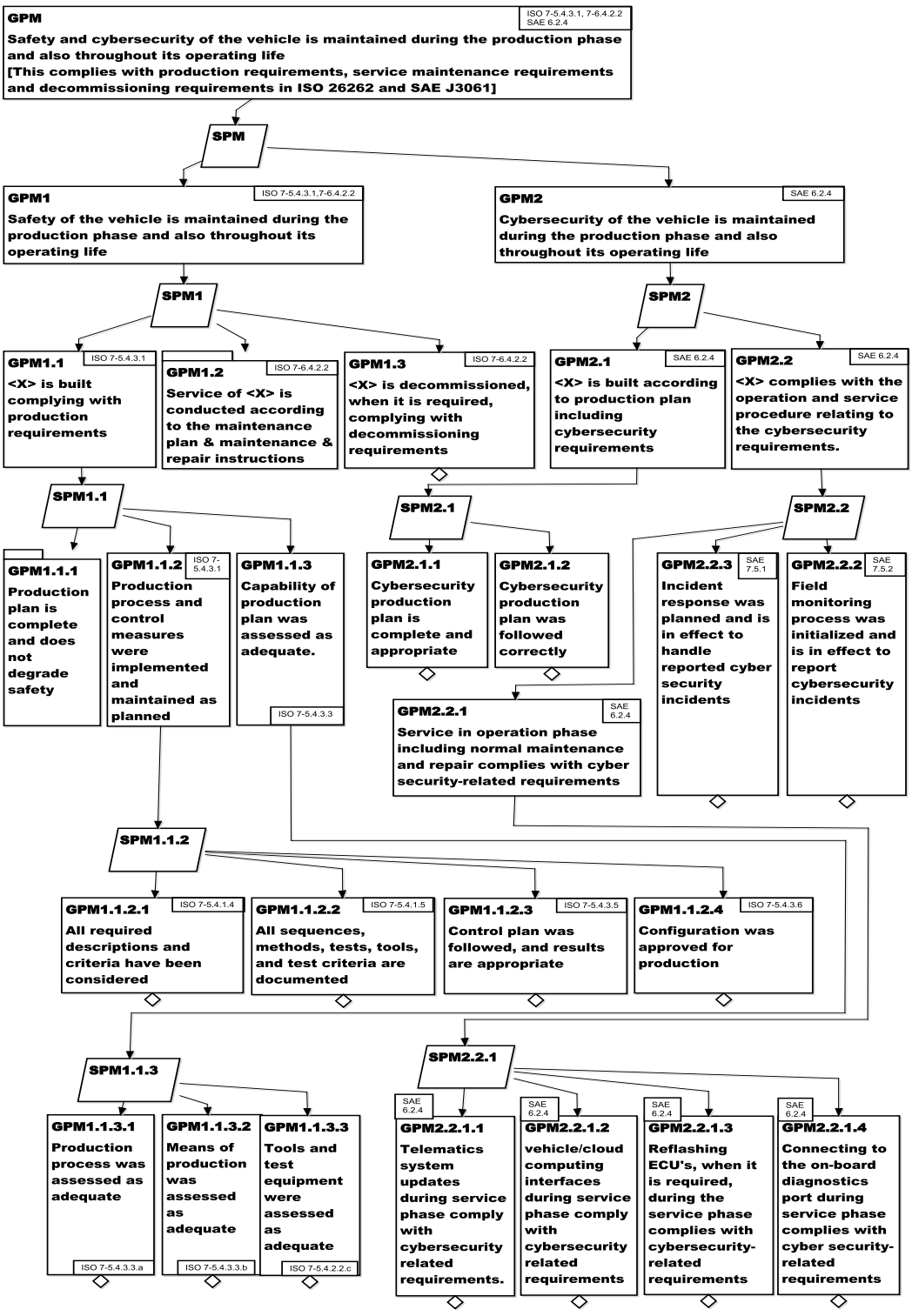

Figure A.17: Claim GPM with Arguments

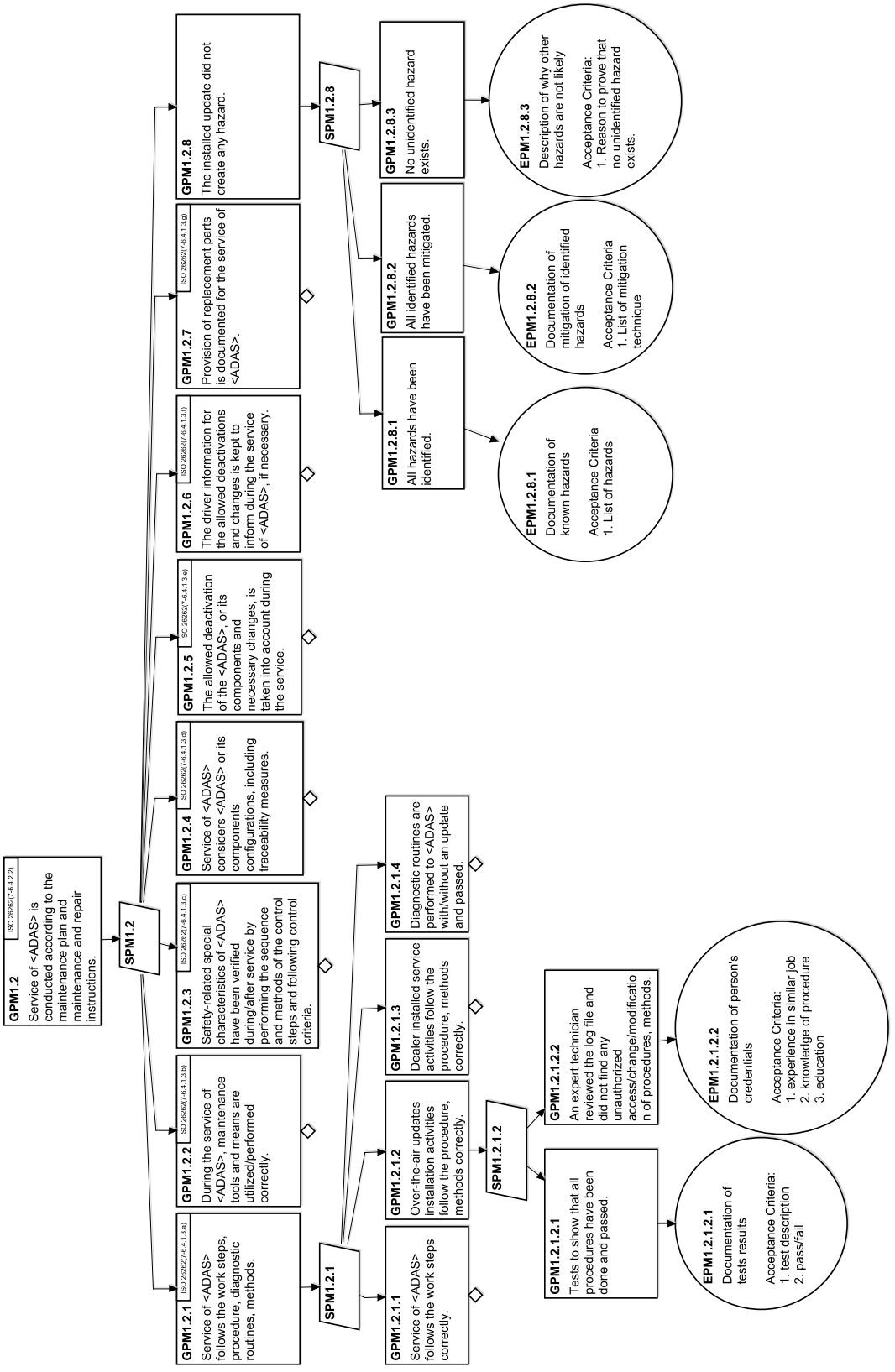

Figure A.18: OTA updates Safety Arguments

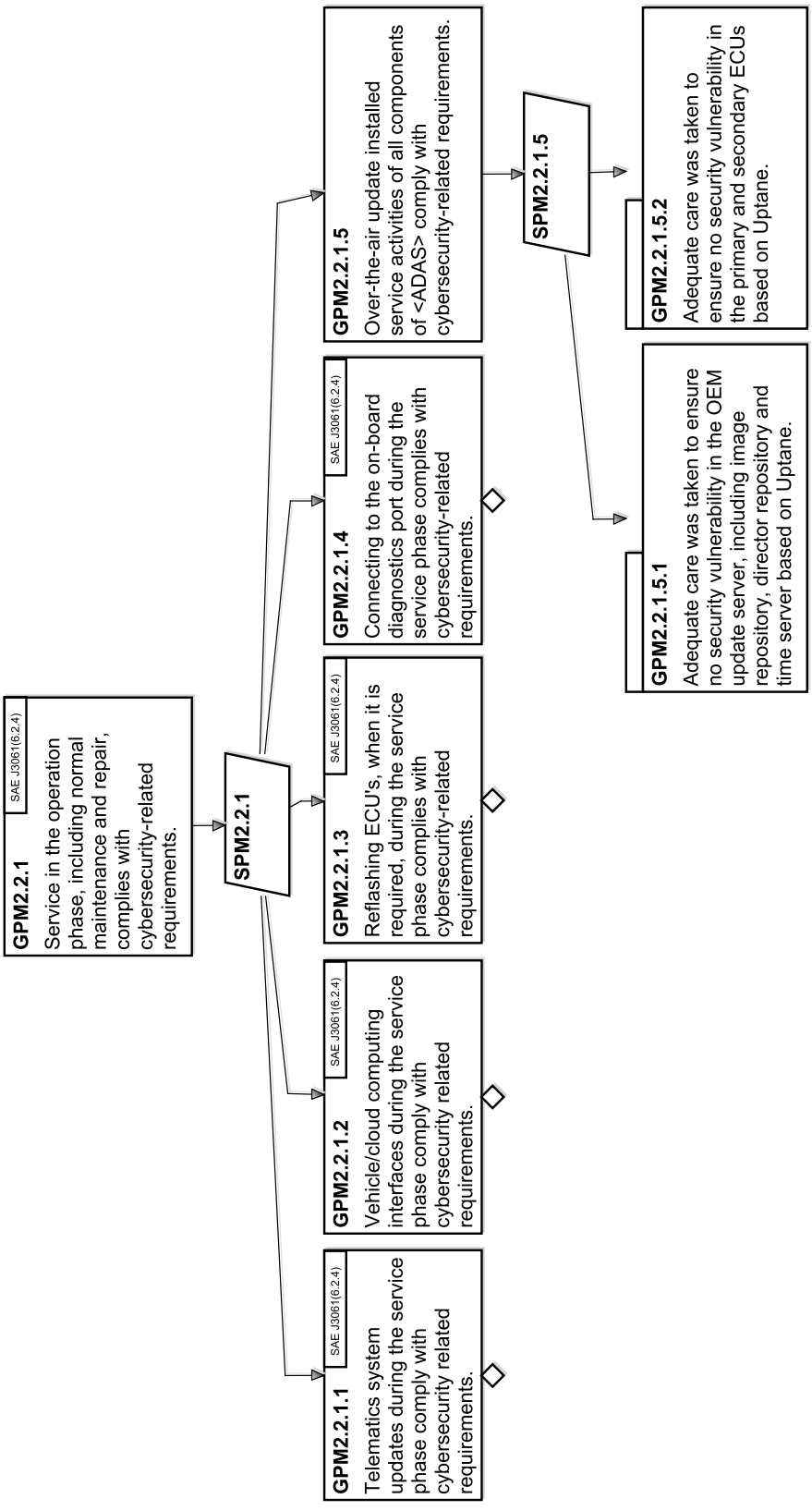

Figure A.19: OTA updates Security Arguments

Appendix B

Preliminary Evaluation of Assurance Cases

In this appendix we illustrate evaluation results of two external assurance cases to validate our proposed evaluation process. Section B.1 shows preliminary evaluation result of assurance case of the ADS-B-APT system. Furthermore, section B.2 shows a partial evaluation of AFI RVSM Pre-Implementation Safety Case using two structure criteria.

B.1 Preliminary Evaluation Result of ADS-B-APT Assurance Case

Reference [100] is a preliminary (and partial) safety case (PSC) for the ADS-B-APT system (ADS-B Airport Surface Surveillance application) published by the European Organisation for the Safety of Air Navigation (EuroControl). The ADS-B system uses aircraft to broadcast information to improve aerodrome control service. The top-level claim of the PSC is *"Use of ADS-B surveillance information to support provision of aerodrome control service (ADS-B-APT) will be acceptably safe"* which is supported by five subclaims. In this PSC, only the first two subclaims are described and the remainder are left for local airport authorities to build local safety cases. The organization uses "Argx.x" to represent "claimx.x". Brief evaluation results using the proposed criteria are given below. Given the historical nature of the safety case,

we have no developer information, so only evaluation from the perspective of an external reviewer is provided.

B.1.1 Evaluating structure/notation of an assurance case

We used all the criteria to evaluate structure of the PSC.

B.1.1.1 Syntax

The PSC uses GSN. All notations were correctly used. Three new elements were introduced and defined in the report. There were no significant syntactic errors in the PSC.

B.1.1.2 Traceability

In lieu of an explicit traceability matrix/table, EuroControl listed the section of the report with each associated claim. EuroControl also noted that the ADS-B-APT system follows the standard "EUROCAE/RTCA ED-163/DO-321" [101], but did not include any traceability to specific items in the standard. No evidence was provided since this is a preliminary safety case. So traceability between system artefacts and evidence could not be checked. The PSC is accompanied by a report consisting of all known hazards and safety requirements along with associated assumptions. This provides a trace between hazards, mitigations and safety requirements. Arg2.2.4 provides assurance that all risks have been mitigated sufficiently and this claim is supported by five subclaims. Each subclaim listed appropriate cross-references. Each subsection listed hazards, assumptions, safety requirements and safety objectives. To show traceability between the impact of differences and the PSC, Arg2.2.1.2 provided assurance of the reconciliation of the impact of differences between the reference system and the ADS-B-APT system. We conclude that the organization provided substantial traceability information.

B.1.1.3 Robustness

The decomposition of Arg0 is related to five contiguous phases of the engineering lifecycle; the outcome of each branch is intended to demonstrate acceptable

levels of safety. Only Arg2.2.1.2 dealt with an assurance of the impact of differences. No other claims refer to changes or invalid claims which are at a lower level (5^{th} level) in the diagram; any change that may affect the PSC will be in this level or below. The PSC may be considered robust.

B.1.1.4 Understandability

The layout of the PSC is easy to understand because of its structure (i.e. easy to navigate, readable font colors and sizes, subclaims of a parent claim are on the same decomposition in the PSC etc). Furthermore, it fits in one page, there are no external cross-links, or ambiguous terminology used.

B.1.1.5 Efficiency

The organization created the PSC so that it faciliates review by basing the decomposition on five contiguous stages of the engineering lifecycle. In doing so, the organization made them independent and used this to help argue that the ADS-B-APT system was acceptably safe. For example, in Arg2.2.4, the claim said *"All risks from internal ADS-B-APT Logical Design failure have been mitigated sufficiently and satisfy ST002"*.

B.1.2 Evaluating the content of an assurance case

We used all criteria to evaluate the content of the PSC.

B.1.2.1 Convincing Basis

In the PSC, to ascertain whether there is a convincing basis, the following are considered:

- *Top-level claim:* The top-level claim is comprehensible and unambiguous. The description of the top-level claim is complete because it mentions environmental constraints and intended operation explicitly in the description. The top-level argument specifies: the context where the purported benefits of the ADS-B surveillance in aerodrome control service arise; typical operational environment; reference system with no surveil-

lance; and issues related to all mobiles in the maneuvering area; and finally criteria to describe "acceptably safe" behaviour.

- *Explicit reasoning for the argument:* All arguments (except the reasoning that shows Arg2.2.1.n n=1,...,4, supports Arg2.2.1) are implicit. In all cases, the authors described how the upper-level claims decomposed into subclaims in the report. They did not provide any justification for use of those strategies. As such, application of our criterion implies that the PSC can be improved by providing explicit reasoning.

- *Avoiding "confirmation bias":* In the PSC, Arg2.4 said *"The Evidence for the ADS-B-APT Logical Design is trustworthy"*. To support that, the organization mentioned in the report that the claim can be supported by the following:

  – "approach and methods applied during the design of the ADS-B-APT system are well recognized, and specific adaptations of the methods for surveillance have been done and documented when necessary;

  – these approaches and methods were applied by competent personnel

  – concerning safety aspects, these methods and approached are compliant with regulatory requirements"

  To support the first subclaim, the organization stated that the process followed is defined in EUROCAE ED-78A, and methods followed are defined in the SAM. To support the second subclaim, the organization stated that RFG participants (from EUROCONTROL, Egis Avia, LFV, MITRE, Sensis Corporation, John Hopkins University, FAA, FAA WJH Tech Centre, QinetiQ) were involved in the design process. They describe credentials of people involved in the design process, including their experience and education/training, as acceptance criteria for competent people. To support the third subclaim, the organization stated that the PSC passed a safety regulatory review process conducted by representatives of National Supervisory Authorities/States within the SRC Coordination Group acting on behalf of the Safety Regulation Commission. They also briefly mentioned a verification process and a validation

process as acceptance criteria to further demonstrate compliance with relevant standards. The recommendations help to avoid "confirmation bias" by pre-selecting relevant evidence based on acceptance criteria.

B.1.2.2 Rigour of the arguments

In the PSC, all arguments showed only how upper-level claims are decomposed into lower level subclaims. The organization did not provide explicit reasoning in any form that showed how sublaims supported parent claims. We concluded that there was little to no rigour in the argument in the PSC.

B.1.2.3 Quality of the hazard analysis

Arg2.2.4 claims that all risks have been mitigated sufficiently and satisfies ST002 (safety target). This is supported by five subclaims Arg2.2.4.1 through Arg2.2.4.5. Arg2.2.4.1 states "All reasonable foreseeable hazards have been identified". To support this claim, the PSC provides a list of operational hazards and the information that these hazards were identified during brainstorming sessions with operational and safety experts. The PSC should have provided valid rationale for why a best practice hazard analysis was not used, as well as the credentials of those experts. The PSC does refer to a section of the standard [101] for further details about the types of hazards identified. To support the claim that severity of effects of hazards was correctly established, the ED-78A [102] classification scheme was referenced. The calculation of safety objectives from the standard [101] was used to support that safety objectives were determined correctly (Arg2.2.4.3). Fault tree analysis was used to support identification of reasonably foreseeable causes of each hazard (Arg2.2.4.4), and the list and description of safety requirements was used to support the claim that safety objectives were satisfied (Arg2.2.4.5).

B.1.2.4 Arguing completeness

In the report, the organization linked hazards with corresponding safety requirements but did not provide explicit rationale as to why unidentified hazards are unlikely. The arguments presented (both implicit and explicit (in GSN)) did not specify rebuttals which could be used to argue completeness. Based

on the analysis, it is recommended to add rationales for unidentified hazards and rebuttals in the final safety case. As it is a PSC, the organization did not provide any verification test results including mathematical and simulation.

B.1.2.5 Repeated arguments

We did not find any repeated arguments in the PSC.

B.1.2.6 'ALARP'

Based on one of the criteria, it is found that all known hazards have been identified and safety requirements with assumptions are defined to mitigate or reconcile those hazards. Moreover, there are two arguments (first argument among Arg0, Arg1, Arg2, Arg3, Arg4 and Arg5 and second argument among Arg2, Arg2.1, Arg2.2, Arg2.3 and Arg2.4) which provided reasonings as to why the system is acceptably safe. Based on the analysis, the organization applied "ALARP" in forming an argument in a reasoned and methodical way.

B.1.2.7 Confidence

The organization did not provide any quantitative confidence assessment results. As an external reviewer, confidence assessment may be performed to measure the confidence of the PSC provided by the organization. As an initial attempt, a confidence assessment was initiated based on one of the confidence assessment methods by Duan et al. [81]. According to this method, safety experts initially express their opinion about evidence nodes in terms of degree (b), disbelief (d) and uncertainty (u). Belief, disbelief and uncertainty in claims supported by evidence are calculated using beta distribution. In case of two pieces of evidence supporting a claim, the authors of this method relate Jϕsang's *consensus operator* for opinions $\pi_A = b_A, d_A, u_A$ and $\pi_B = b_B, d_B, u_B$. Then *logical OR* operation is performed to measure the opinion of an intermediate claim supported by two subclaims. Then the opinion is converted to a beta distribution. The PSC does not have an explicit description of evidence, so we cannot include evidence in evaluation of confidence. However, it could be factored in when the PSC is ultimately completed.

B.1.3 Outcome of the evaluation

The evaluation of the PSC is subjective, but the proposed criteria facilitate discussion on why an evaluation has resulted in a specific outcome. Our focus in using these criteria is to discover unacceptable issues in an AC so that they can be fixed. In this PSC, inconsistencies have been discovered which motivate improvement. The criteria provide neither a quantitative measure of unacceptable issues nor a quantitative measure of an overall evaluation of an AC. Based on our analysis using these criteria, we conclude that the PSC is "good" with respect to syntax, understandability, efficiency, convincing basis, quality of the hazard analysis, repeated arguments and ALARP. The PSC needs to be improved with respect to traceability, completeness, robustness and rigour of the argument. Confidence cannot be evaluated adequately since evidence does not exist yet.

B.2 Partial Evaluation of AFI RVSM Safety Case

We evaluated AFI RVSM Pre-Implementation Safety Case using two criteria (e.g. syntax check and traceability) of structure.

B.2.1 Validation of "Syntax check" (A Structure Criterion)

To illustrate our syntax check process, we use AFI RVSM Pre-Implementation Safety Case [103] as an example. It uses GSN for documentation. The safety case shows safety arguments of RVSM (Reduced Vertical Separation Minimum) implementation and maintenance to reduce the vertical separation between Flight Levels 290 and 410 (inclusive) from 600m to 300m in AFI airspace. The rules for syntax check show what to check for identifying errors in syntax. Notation attribute in a class "AssuranceCase" denotes 'GSN' and rules for 'CheckGraphSyntax' will apply. Concerning rule (1), we consider the GSN community Standard 2.0 [12] as a reference. Concerning rule (2), by review we note that shapes of goal and strategy comply with the standard. However, the

example refers to a solution as *evidence*, and they used a rounded rectangle for evidence instead of a circle. They used one context and did not use any assumption or justification in their safety case, though mentioned those terms in their example safety case, and they otherwise comply with the standard. However, the shape of the context used in the safety case does not comply with the standard. Concerning rule (3) and (4), there is one and only one valid association ('SupportedBy') that exists between any two nodes. For rule (5), the terminal nodes (in some pages, terminal nodes are goals, and in some pages, terminal nodes are evidence)have no outgoing association with other goals. With rule (6), the label of goals, strategies and evidence follows a hierarchy. Thus, with rule (2), one shape (context) does not comply with the standard. 'GenerateRecommend' should produce recommendations with criticality ("highly recommended") to fix the shape to comply with the standard, or to explicitly document how and why they deviate from the standard.

B.2.2 Validation of "Traceability" (A Structure Criterion)

For traceability, we use the same example used for syntax check. We first check traceability between evidence to system artifacts using rules defined in 'CheckEvidenceToSystemTrace.' The authors of the safety case categorized evidence into two groups: direct evidence and backing evidence to support direct evidence. Direct evidence supports a logical argument of a product, and backing evidence supports a valid argument of a process/competency in support of direct evidence. It contains 7 rules. We found that all evidence refers to sections number of the document. Concerning rule (1), we find that backing evidence mention section number of the document. For instance, evidence 'E1.2.1' refers to section '3.3.1' of the 'PISC' (Pre-Implementation Safety Case), and evidence 'E1.2.2' refers to section '3.3.2' of the 'PISC.' We find that evidence 'E3.1.1.4' refers to section '5.3.4' of the 'PISC,' and the section describes the compliance. Furthermore, evidence 'E3.1.2.2' refers to section '5.3.6' of the 'PISC,' which shows implementation requirements based on recognized standards. Direct evidence relates to product-related evidence. Concerning rule (2), we find that direct evidence mentions section number of

the document. For instance, evidence 'E1.1.1' refers to section '3.3.1' of the 'PISC'; evidence 'E1.1.3' refers to section '3.3.3' of the 'PISC'. Concerning rule (3), we find that backing evidence deals with validation and refer to specific sections of the 'PISC.' Here we identify that instead of product validation, they validate processes for the right product. For instance, evidence 'E1.2.4' refers to section '3.3.4' of the 'PISC,' where it describes how 'FHA' and 'CRA' techniques are validated. Concerning rule (4), we find that evidence supporting claims related to the competency of people refers to specific sections of the 'PISC' describing the competency of people. For instance, evidence 'E2.1.7.2.1' refers to section '4.3.8.6' of the 'PISC' that describes the related experience of people involved in 'MASPS' development. Concerning rule (5), we do not find any acceptance criteria to show compliance with evidence. Concerning rule (6), we do not find any counter-evidence in the 'PISC.' Concerning rule (7), we find that evidence supporting claim related to change management refers to a specific section of the PISC. For instance, evidence 'E3.2.1.2' refers to a specific section '5.4.2' of the PISC that describes the implementation of necessary changes. To check traceability between the previous version and the current version, we use rules defined in'CheckRecentToPastVersionTrace'. We find that they provided a list of different versions released at a different time. Concerning rules (1) and (2) there is no explicit link or reference between the previous version of claims/arguments/evidence/supporting terms and the current version of claims/arguments/evidence/supporting terms. To identify traceability between argument pattern and instantiated argument, we use rules defined in 'CheckArgumentPatternTrace.' We find that in the 'PISC,' the authors make a clear distinguish using strategies: a direct (product-based) argument with supporting evidence and a backing (mainly process-based) argument with supporting evidence. Concerning rule (1), we find that direct evidence support product-related claims and backing evidence support mainly process-related claims. Based on evaluation guided by three checks, 'GenerateRecommend' can provide the following recommendations: a) it is highly recommended to provide acceptance criteria for evidence which help to avoid "confirmation bias." b) it is recommended to provide an argument relating to counter-evidence. If no counter-evidence exists, it is recommended to mention explicitly. c) It is recommended to provide explicit links between previous

claims/arguments/evidence and current claims/arguments/evidence to show the difference.

Appendix C

Assurance Case for a Coffee Cup

In this appendix we present an assurance case for a coffee cup <KCoffeeCup> to validate our proposed evaluation approach (presented in Chapter 7).

C.1 Assurance Case for a Coffee Cup

In this section, an assurance case for a coffee cup <KCoffeeCup> is illustrated. Figure C.1 shows the top-level claim, that mentions "The coffee cup <KCoffeeCup> is safe in its intended environment and in its intended uses". The top-level claim is supported by four sub-claims, 'CR', 'CI', 'CPM' and 'CA'. These sub-claims assure validation of requirements, implementation and resolve two rebuttals. Figure C.2 shows the argument supporting a claim 'CR' that assures validation of requirements. Figures C.3, C.4, C.5, C.6, C.7, and C.8 show argument branches that support upper level claim 'CR'. Figure C.9, and C.10 show argument branches that support upper level claim 'CA'. Figure C.11 shows an argument branch that supports upper level claim 'CPM'. Figures C.12, C.13, C.14, C.15, C.16, C.17 show argument branches that support upper claim 'CI'.

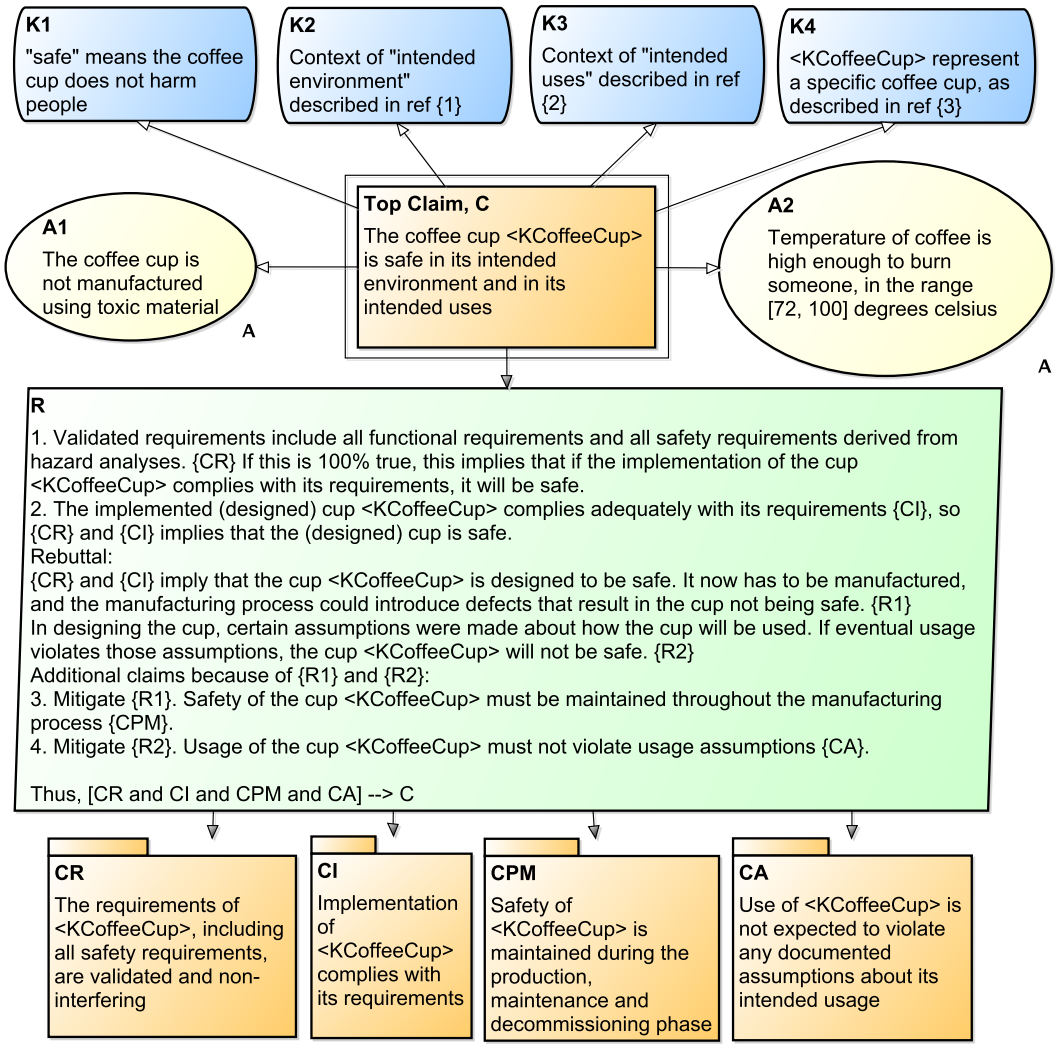

Figure C.1: Coffee Cup Top Level, 'C' with Arguments

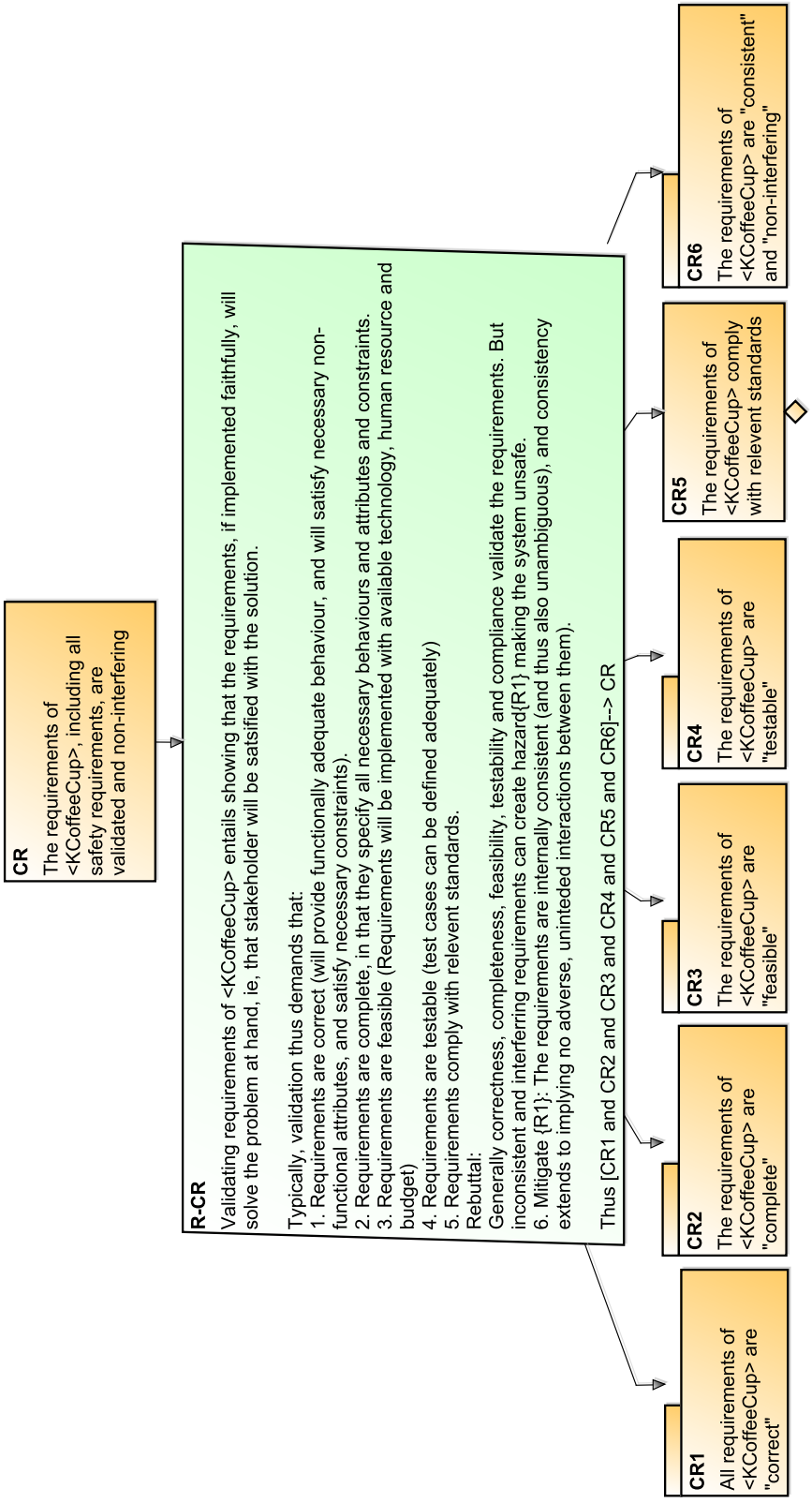

Figure C.2: Claim 'CR' with Arguments

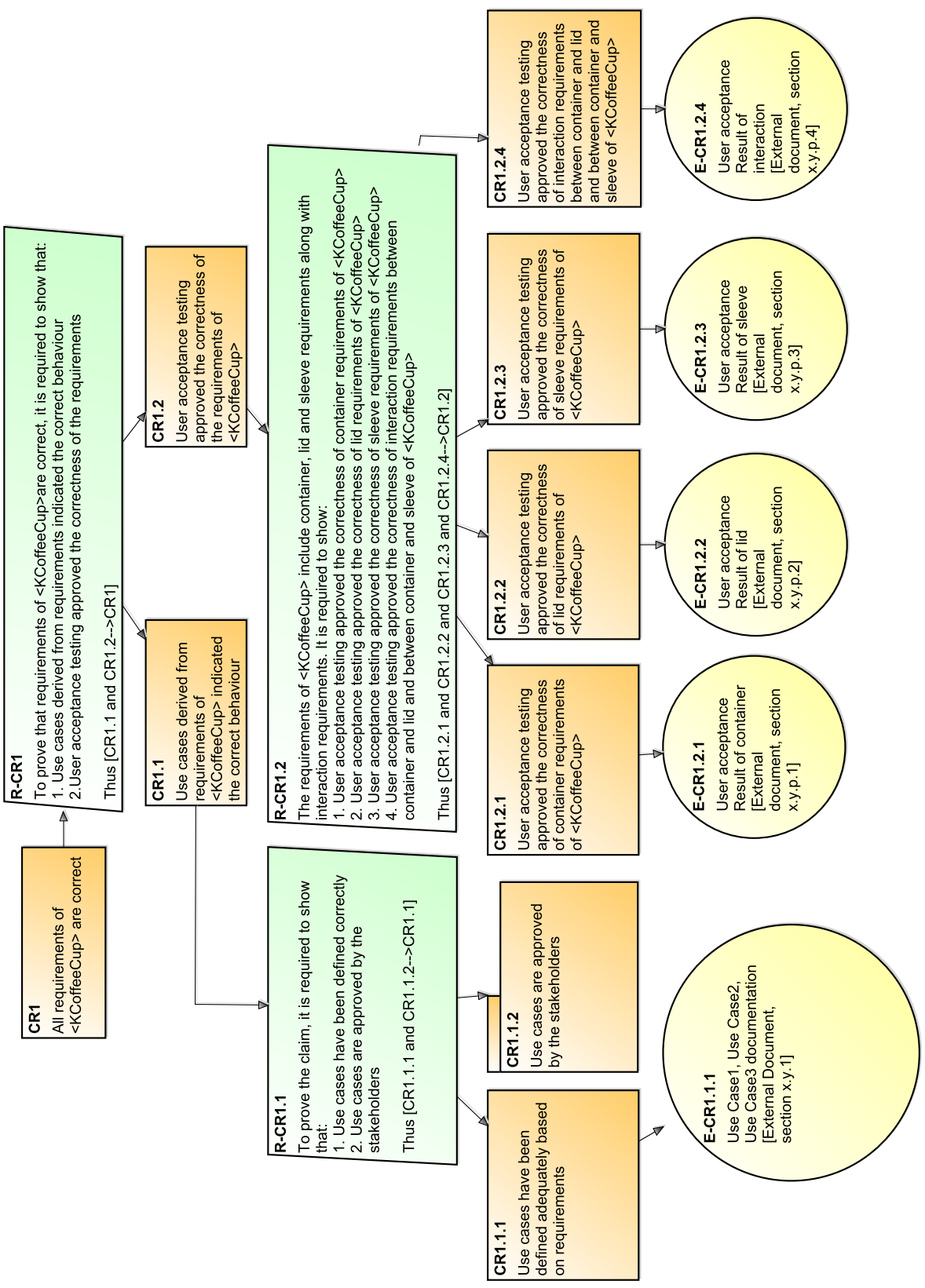

Figure C.3: Claim 'CR1' with Arguments

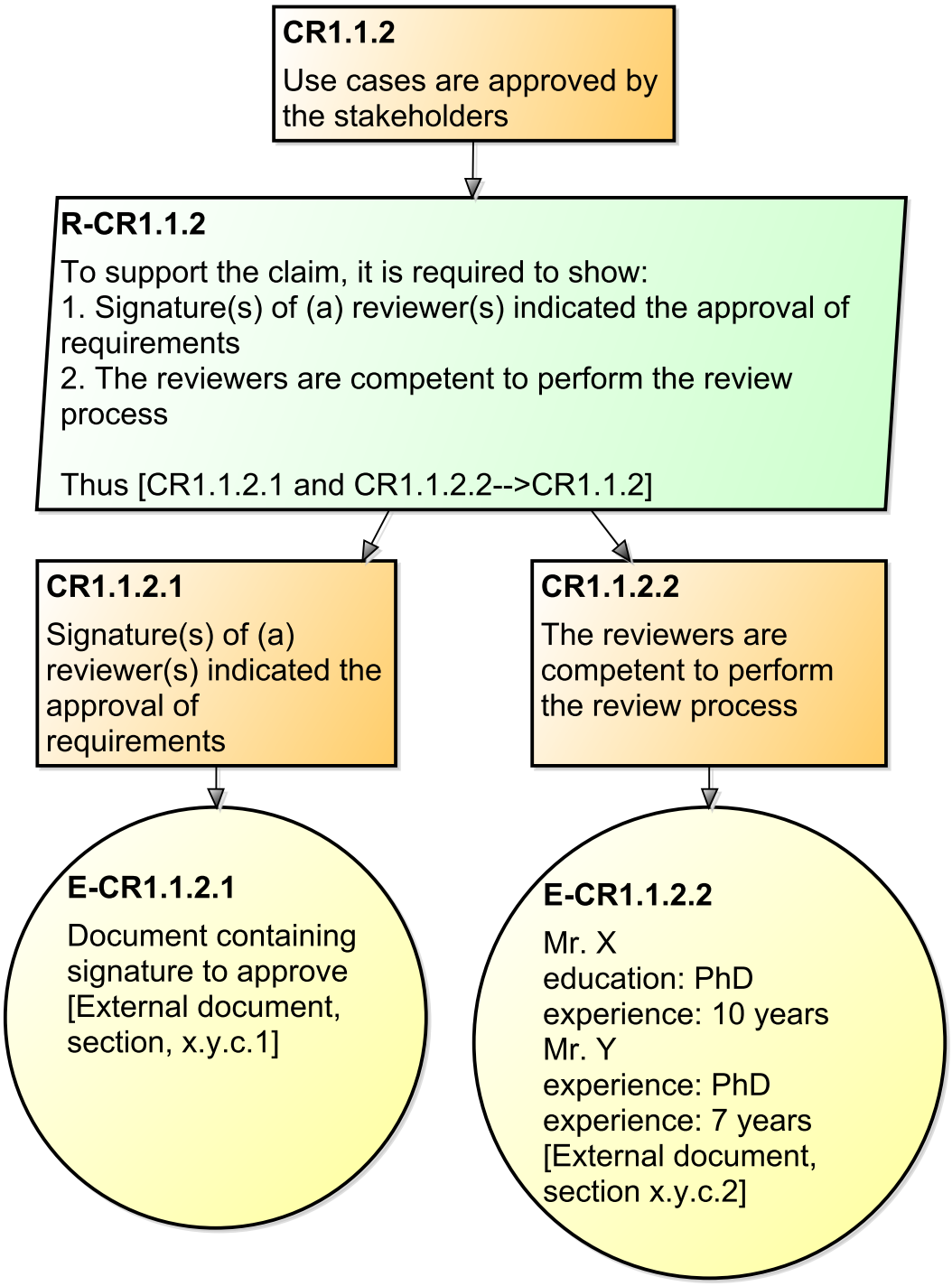

Figure C.4: Claim 'CR1.1.2' with Arguments

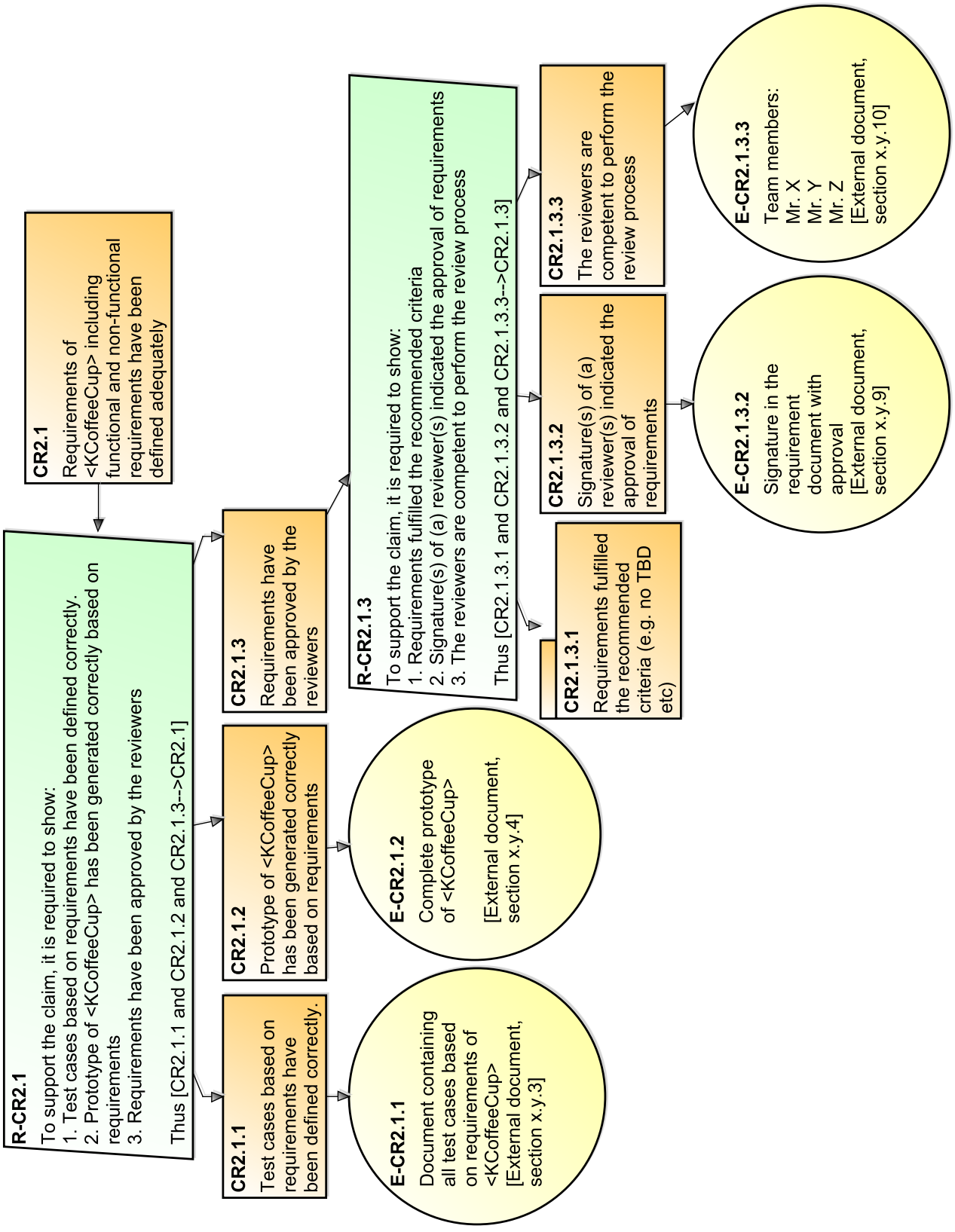

Figure C.5: Claim 'CR2.1' with Arguments

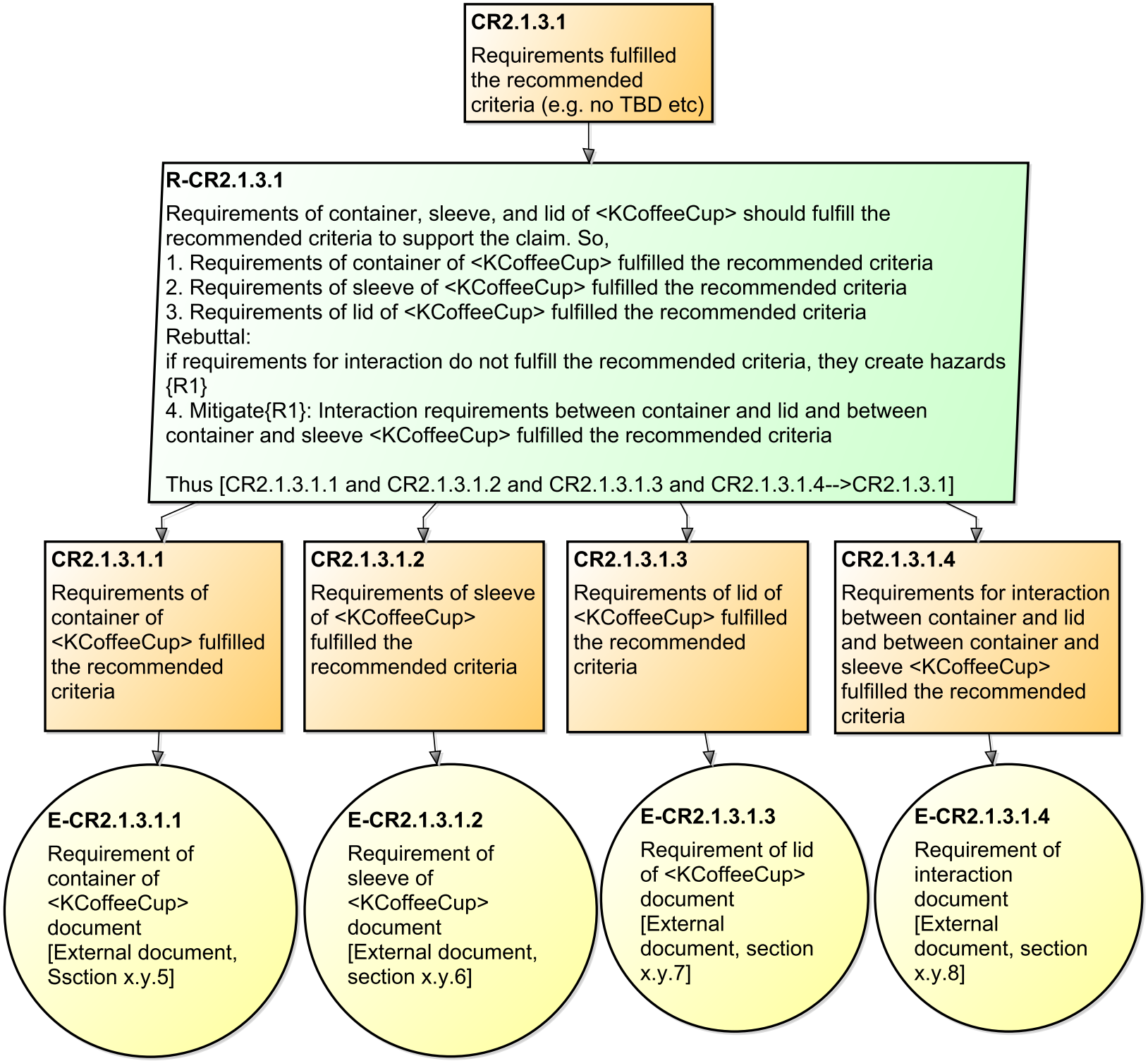

Figure C.6: Claim 'CR2.1.3.1' with Arguments

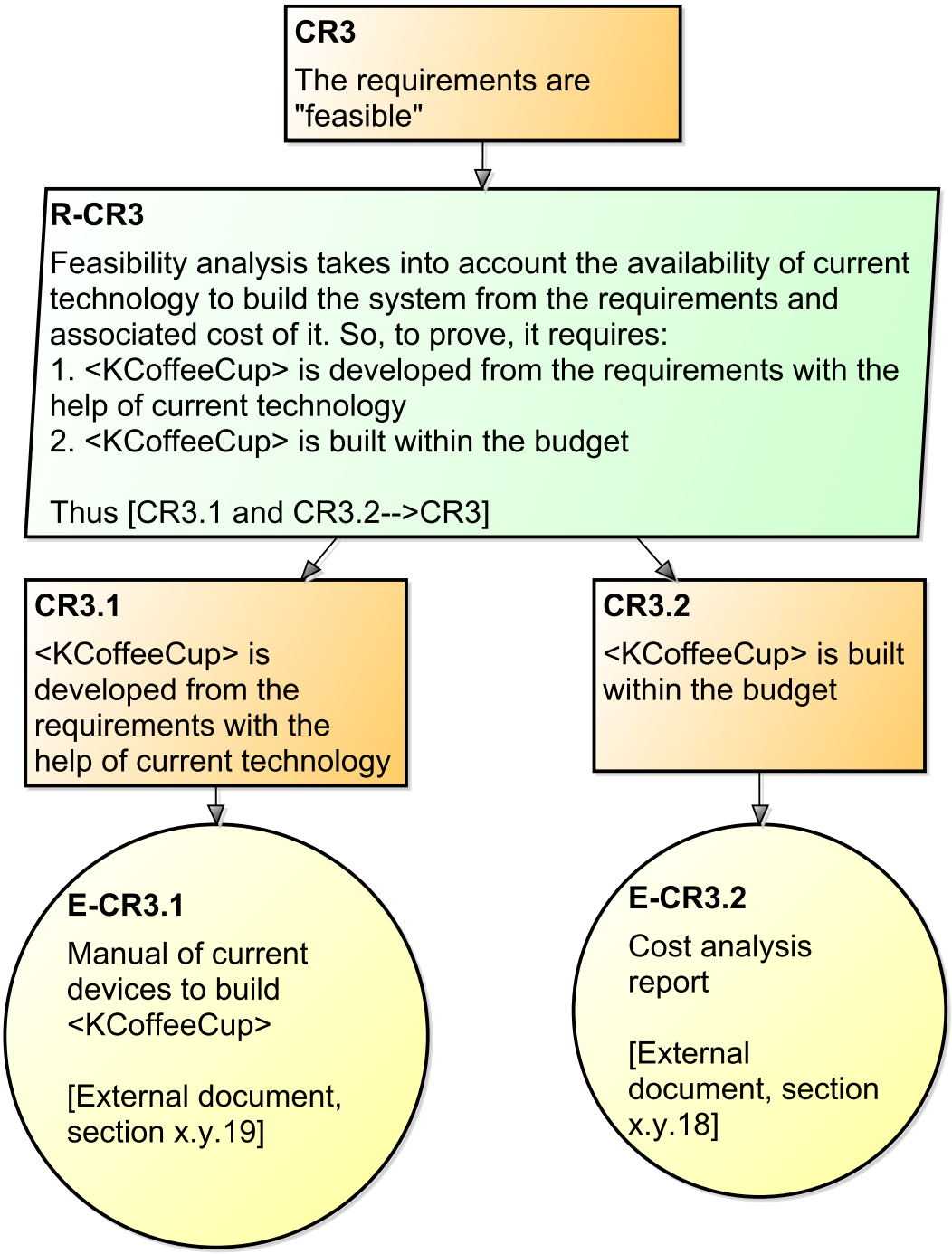

Figure C.7: Claim 'CR3' with Arguments

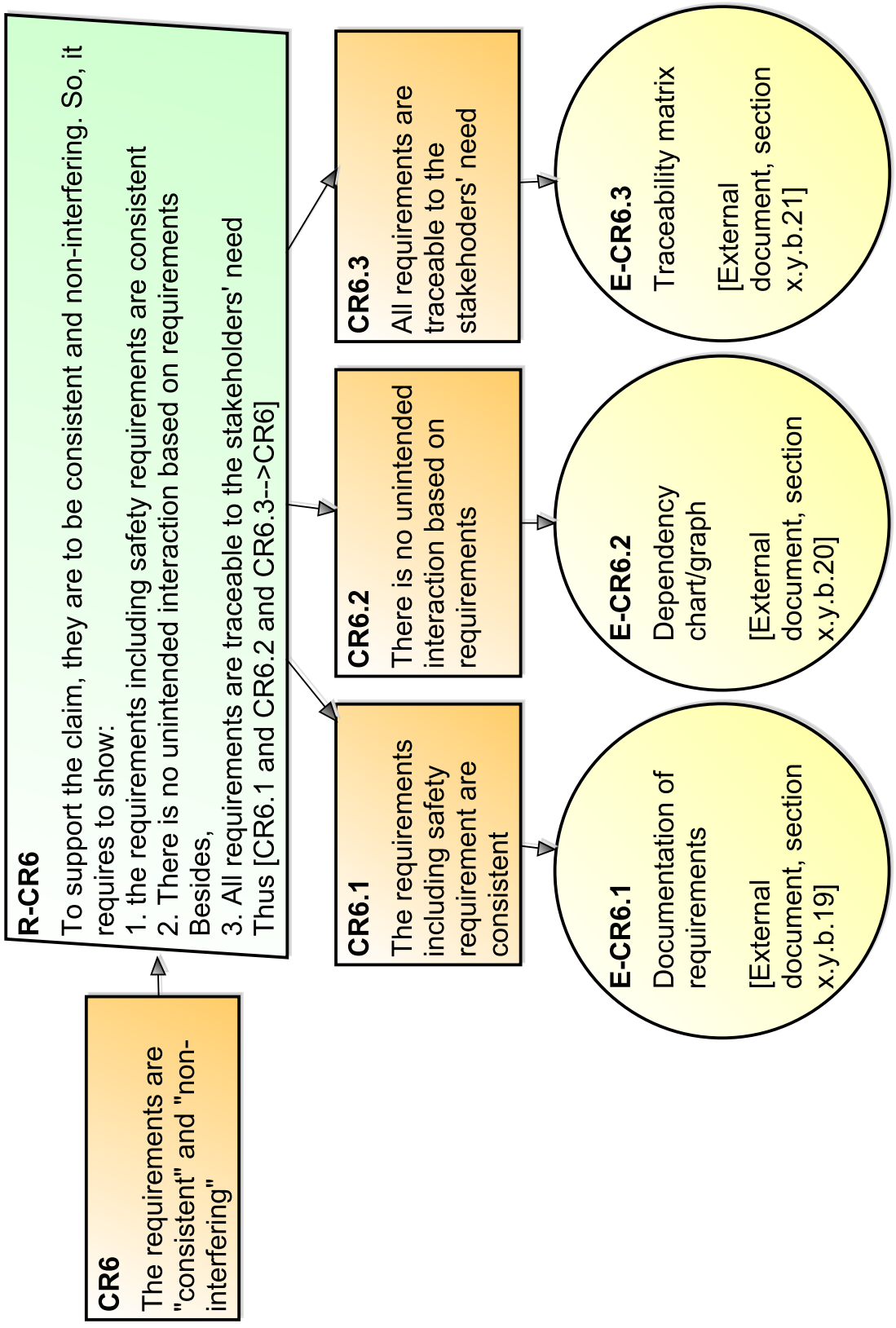

Figure C.8: Claim 'CR6' with Arguments

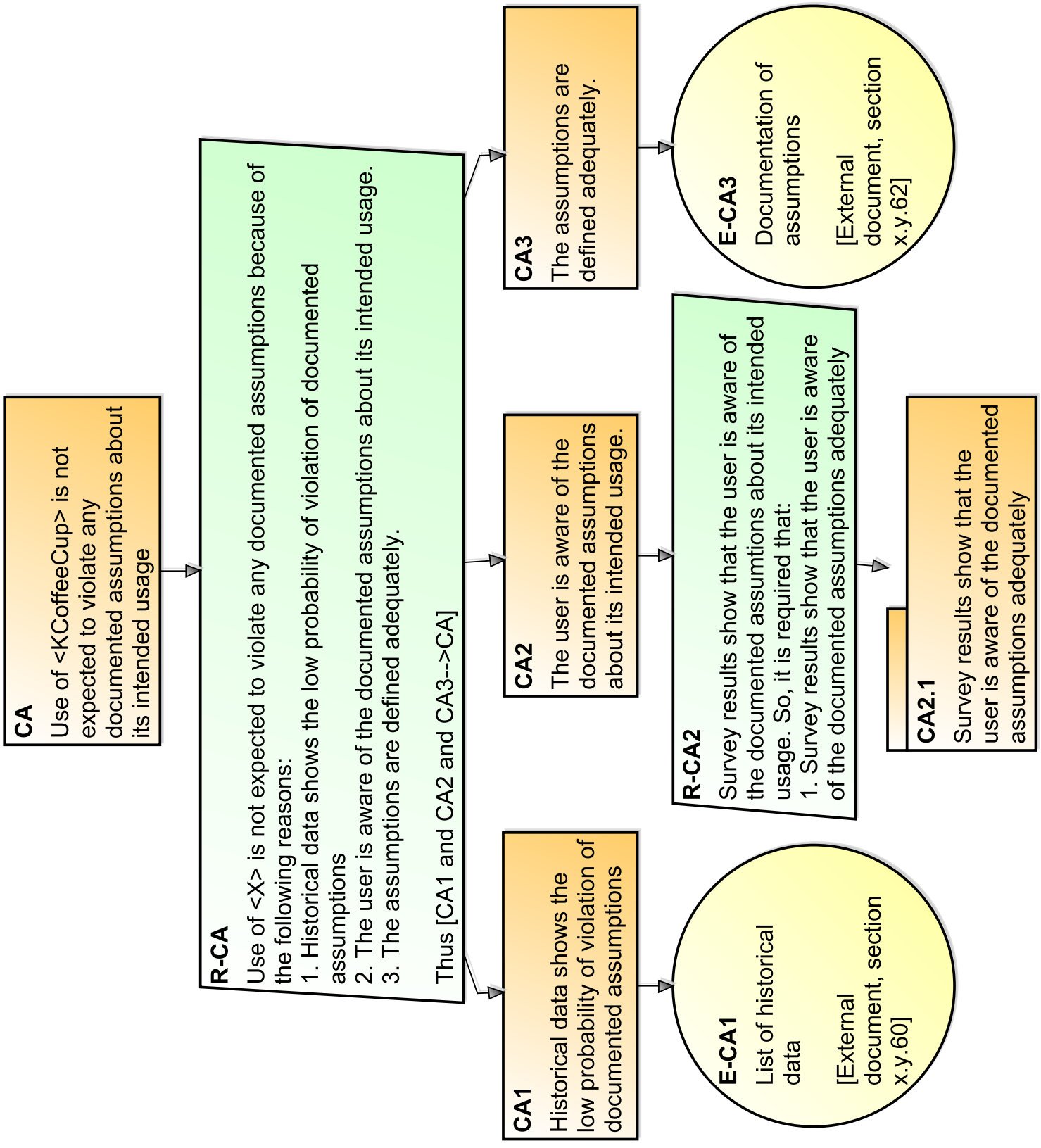

Figure C.9: Claim 'CA' with Arguments

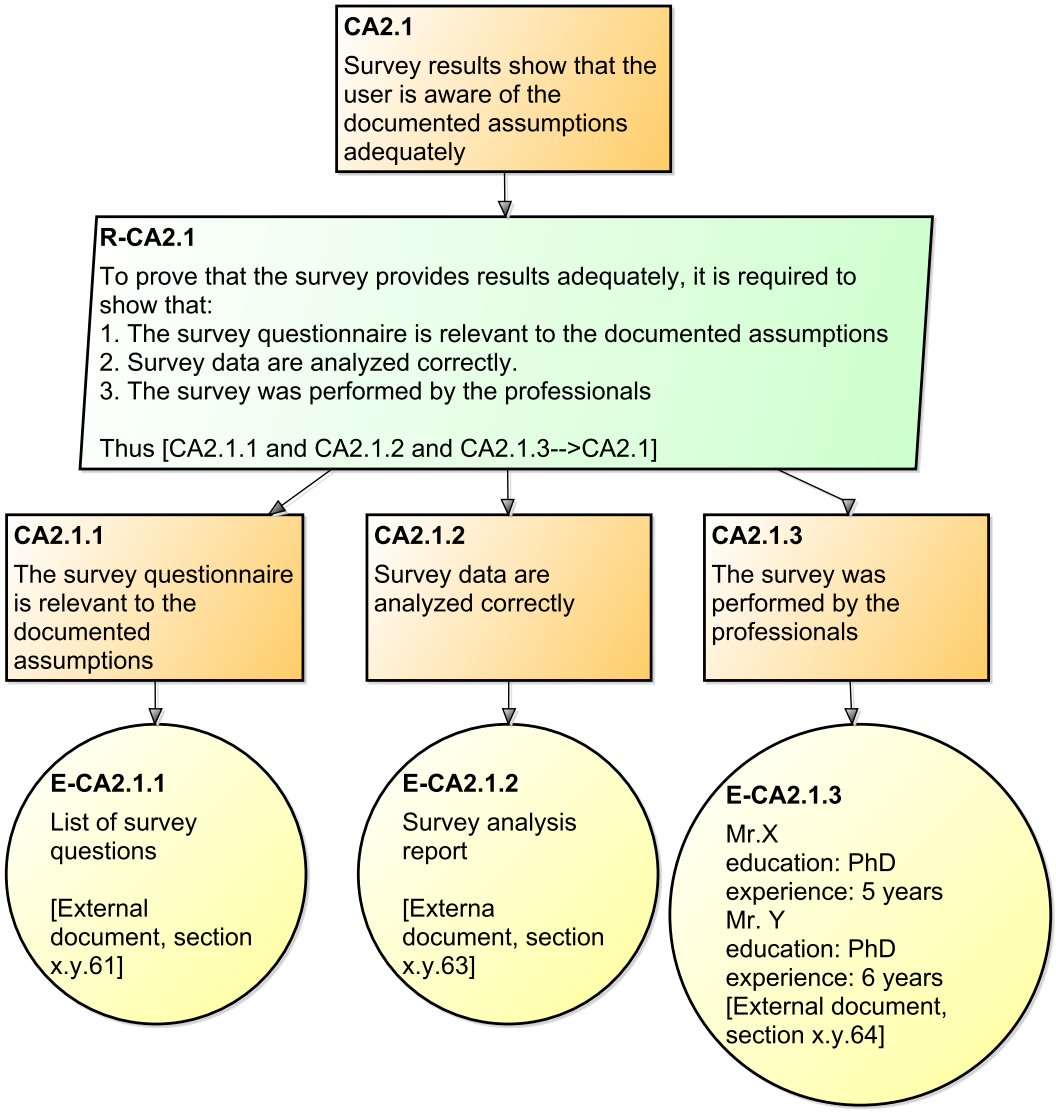

Figure C.10: Claim 'CA2.1' with Arguments

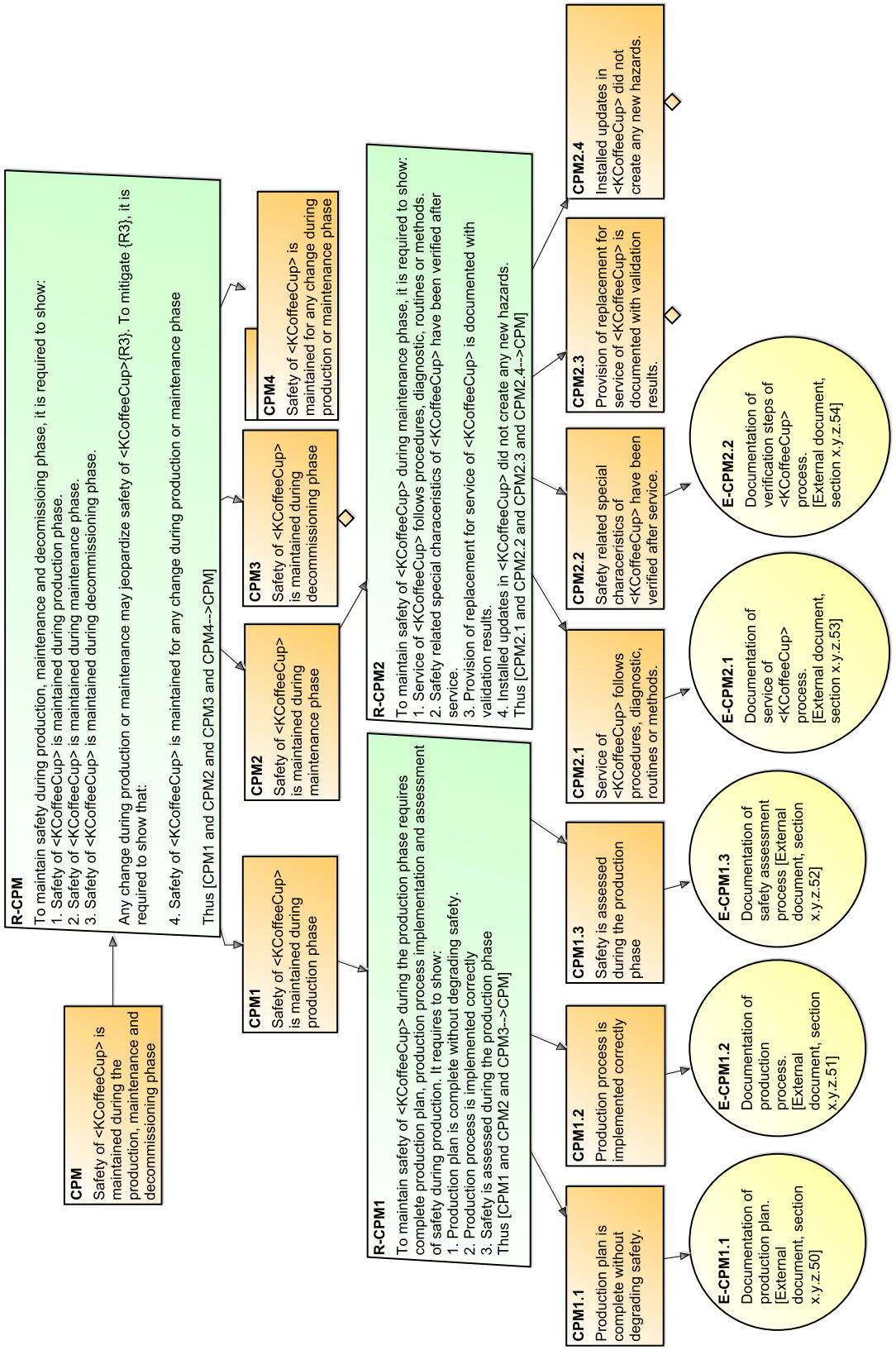

Figure C.11: Claim 'CPM' with Arguments

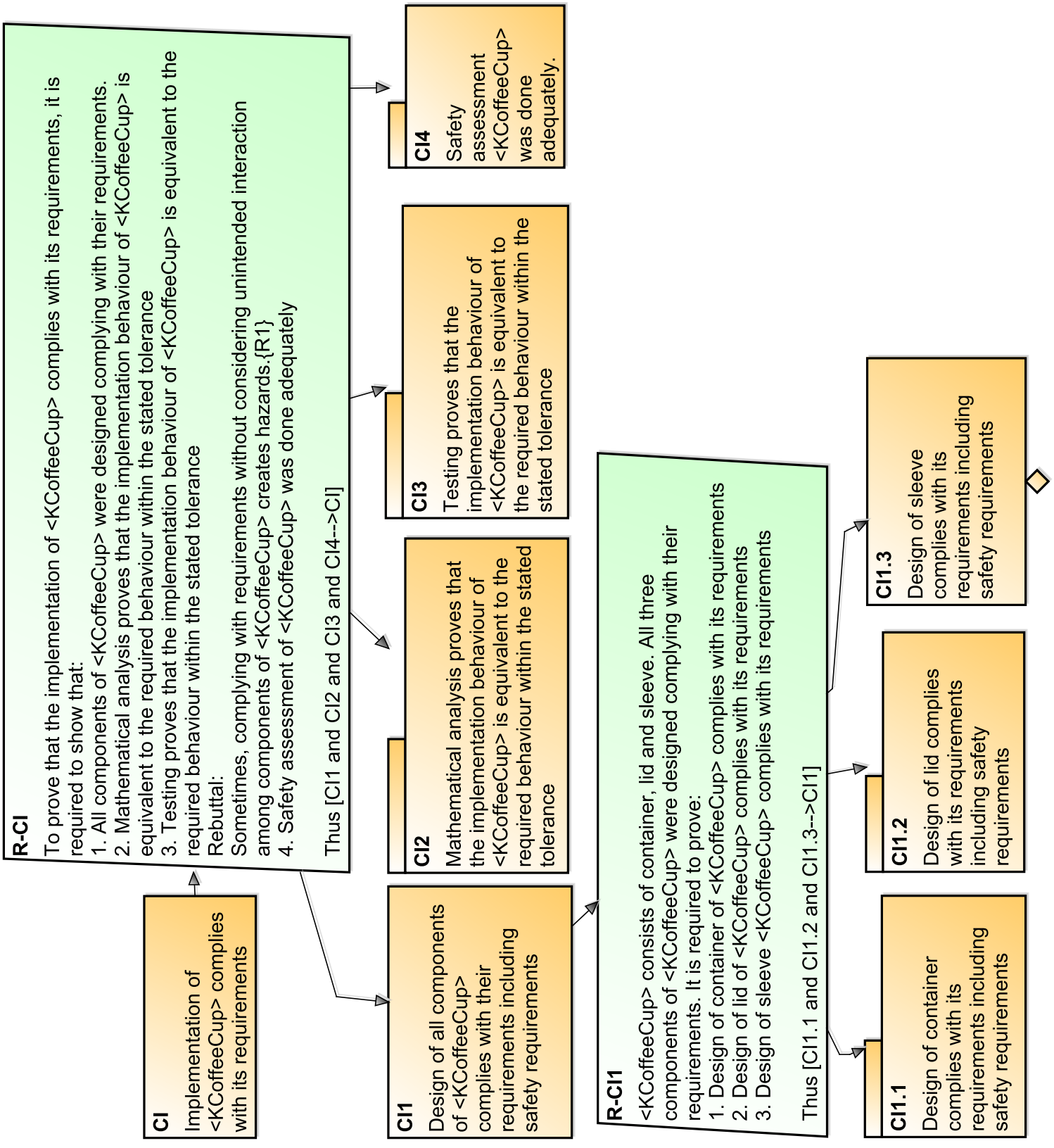

Figure C.12: Claim 'CI' with Arguments

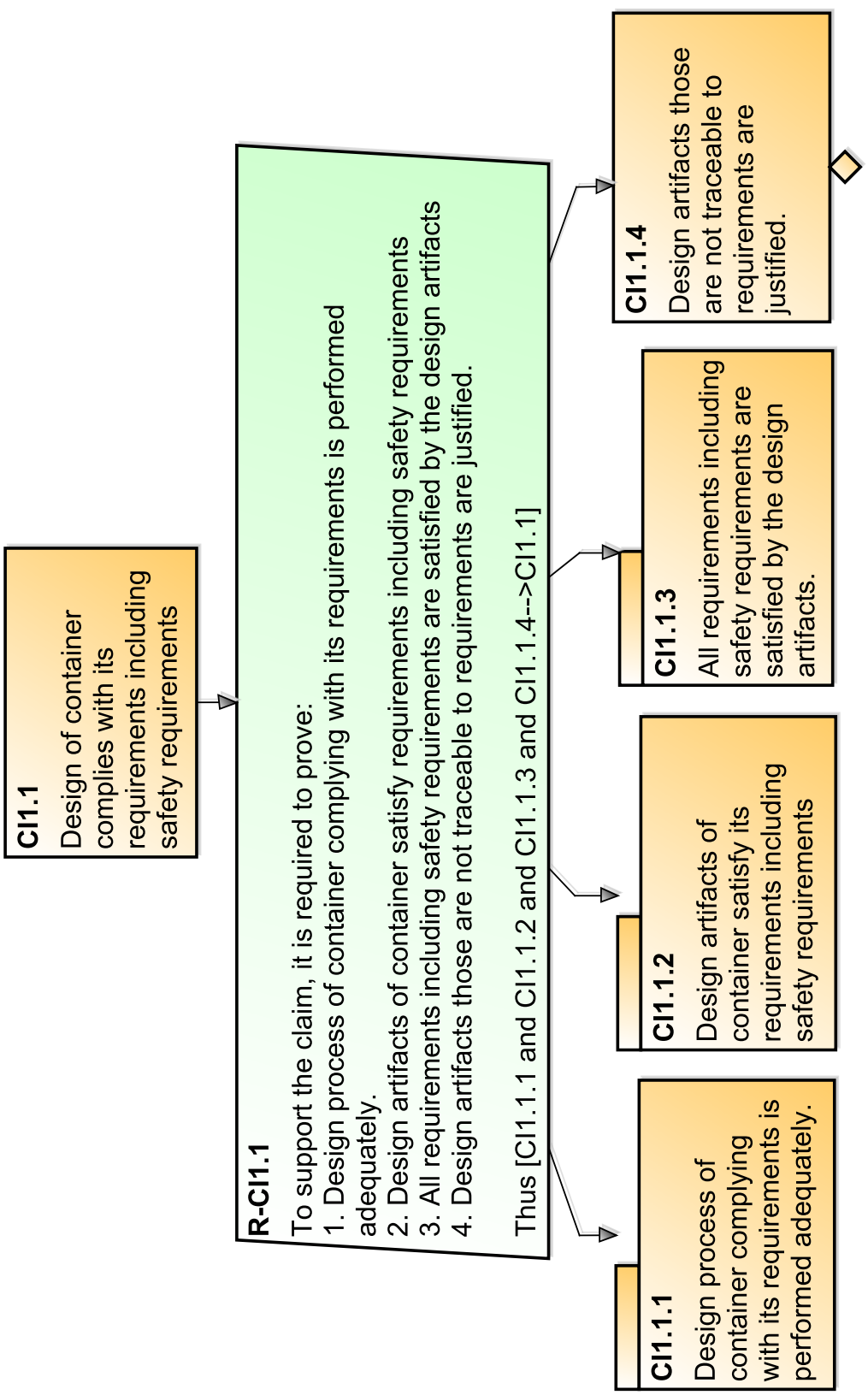

Figure C.13: Claim 'CI1.1' with Arguments

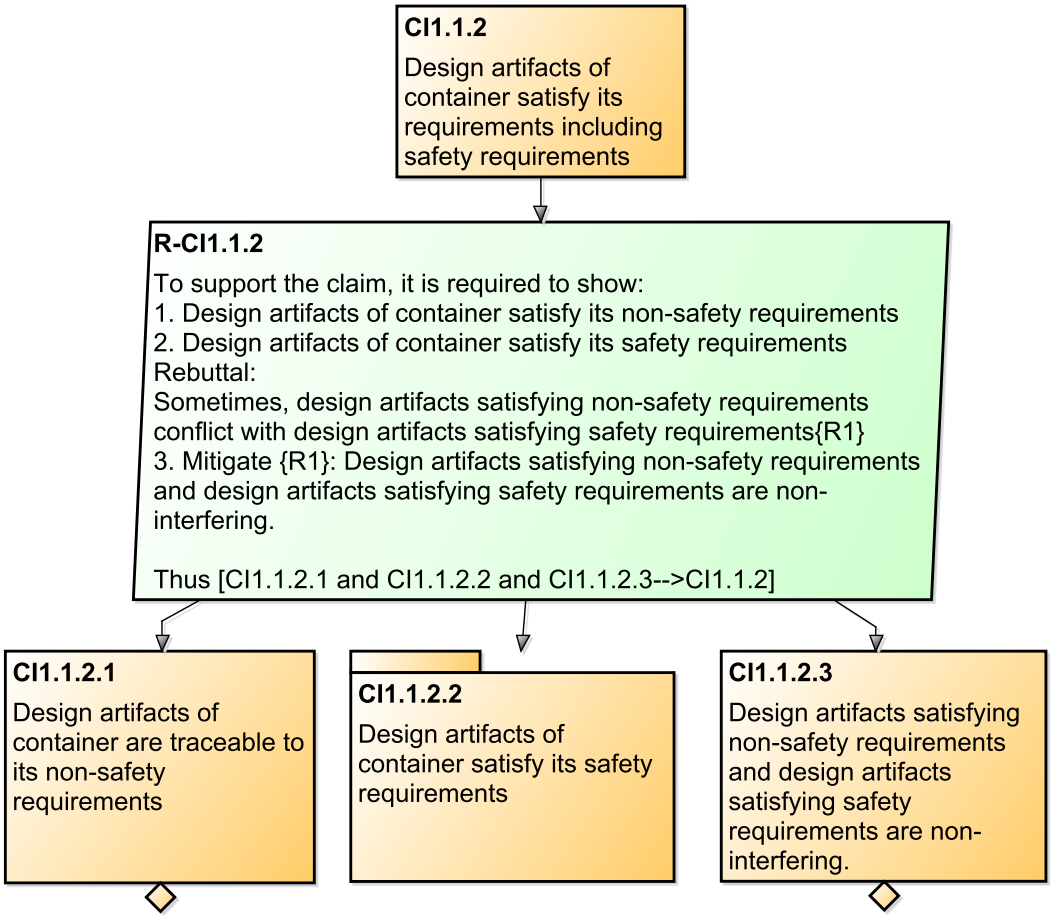

Figure C.14: Claim 'CI1.1.2' with Arguments

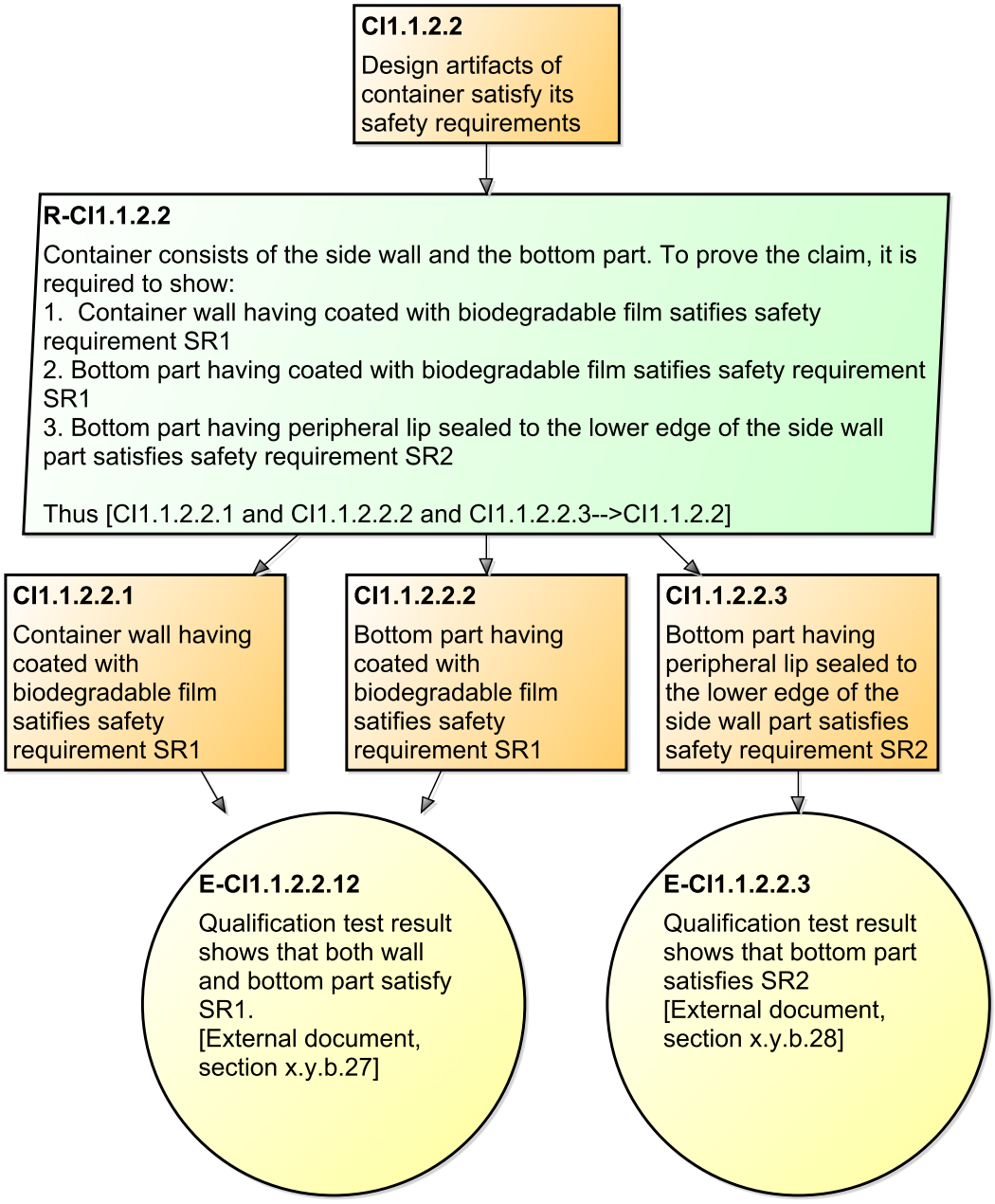

Figure C.15: Claim 'CI1.1.2.2' with Arguments

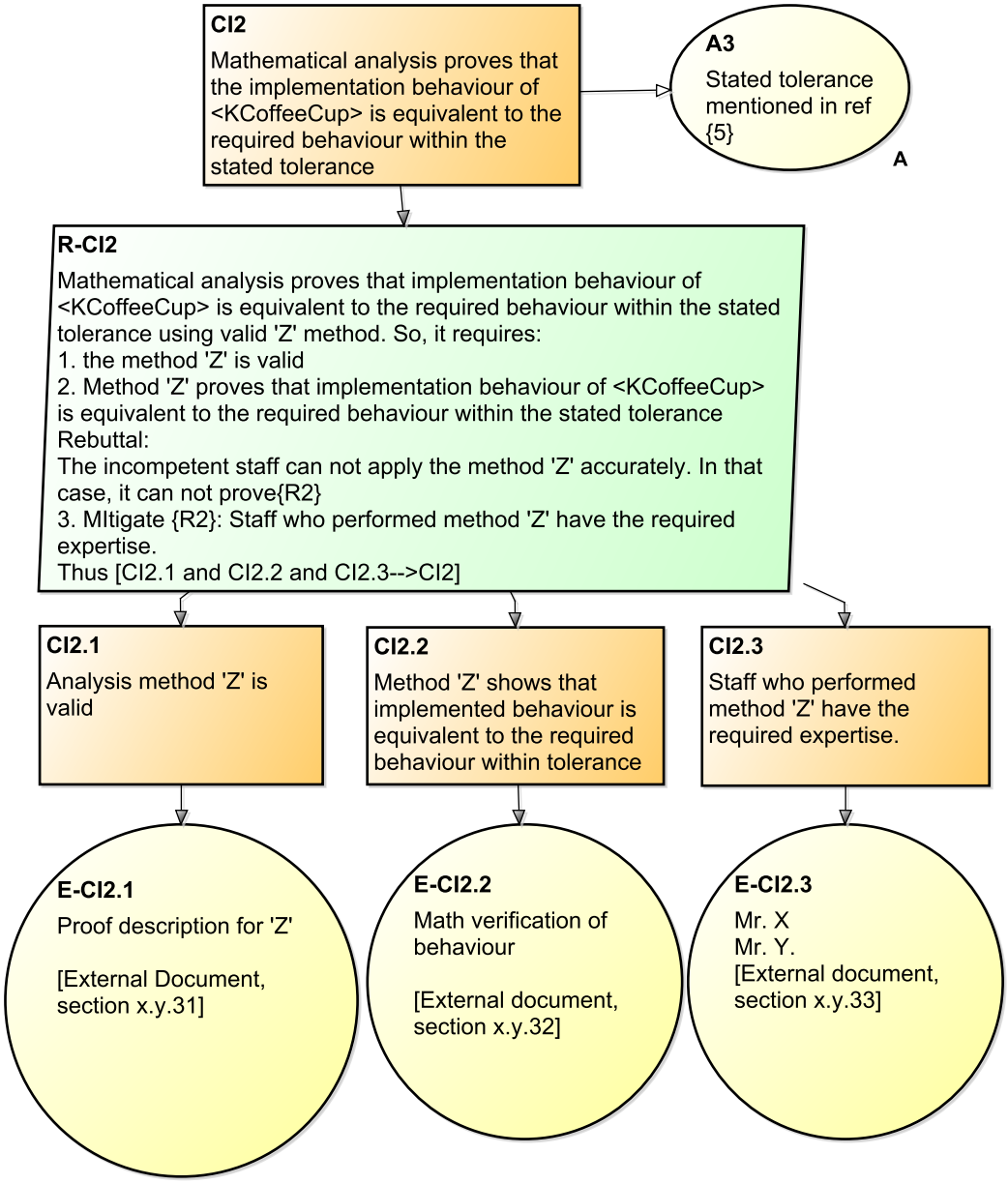

Figure C.16: Mathematical Analysis Argument

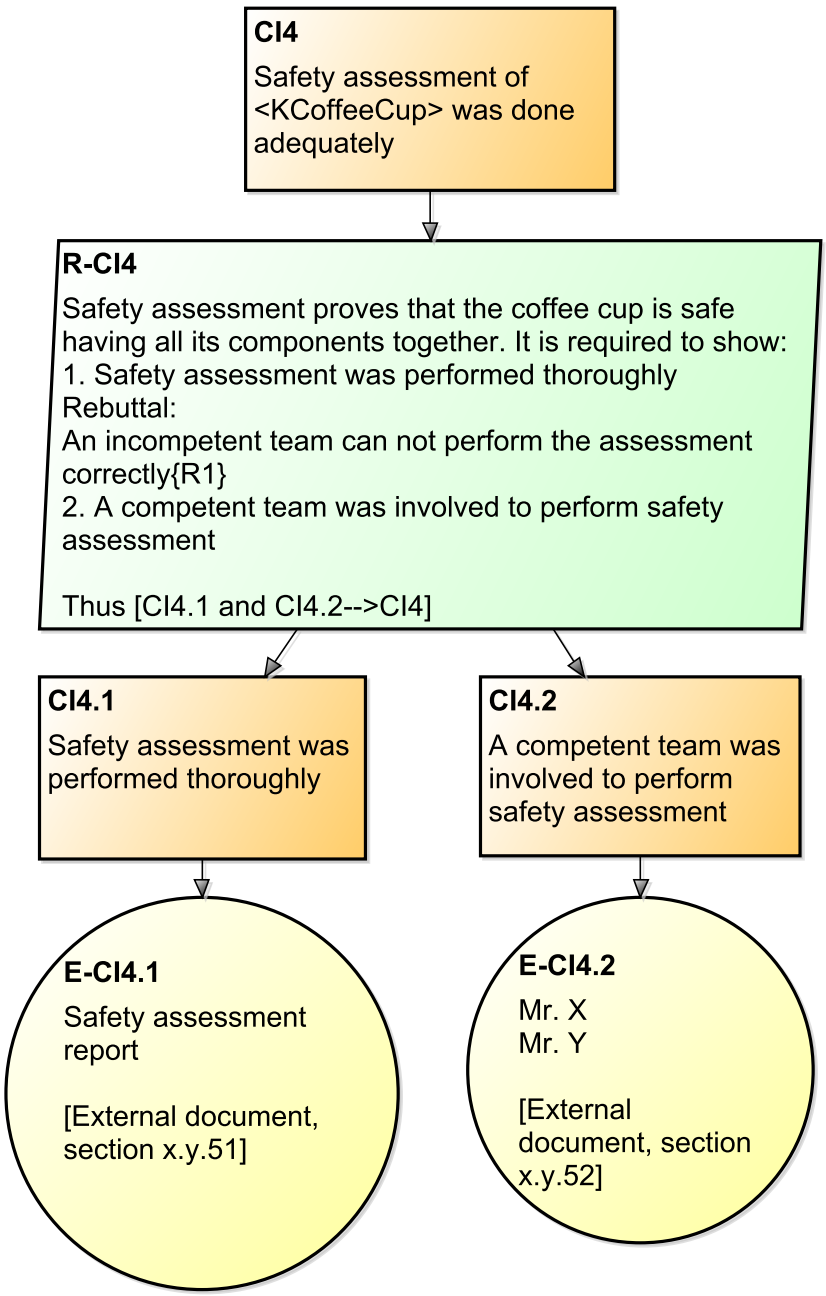

Figure C.17: Safety Assessment Argument

C.2 Acceptance Criteria from an ACT for a Coffee Cup

This section shows a few examples of acceptance criteria from an ACT for a coffee cup to show that evidence comply with acceptance criteria. Figure C.18 shows acceptance criteria for evidence 'E-CI2.1', 'E-CI2.2' and 'E-CI2.3'. Figure C.16 shows evidence that comply with acceptance criteria mentioned in figure C.18.

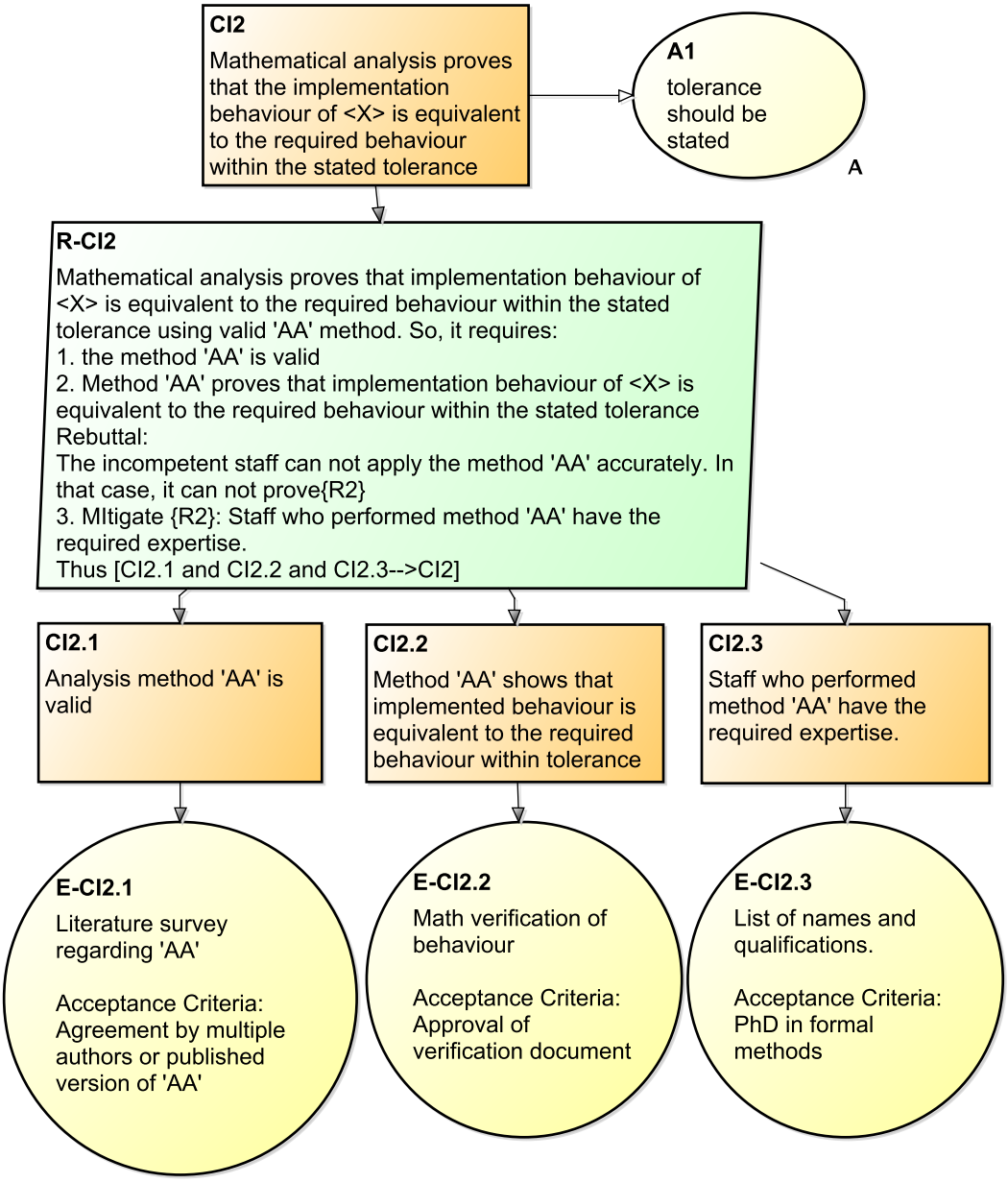

Figure C.18: Mathematical Analysis Argument

Similarly, figure C.17 shows evidence that comply with acceptance criteria mentioned in figure C.19.

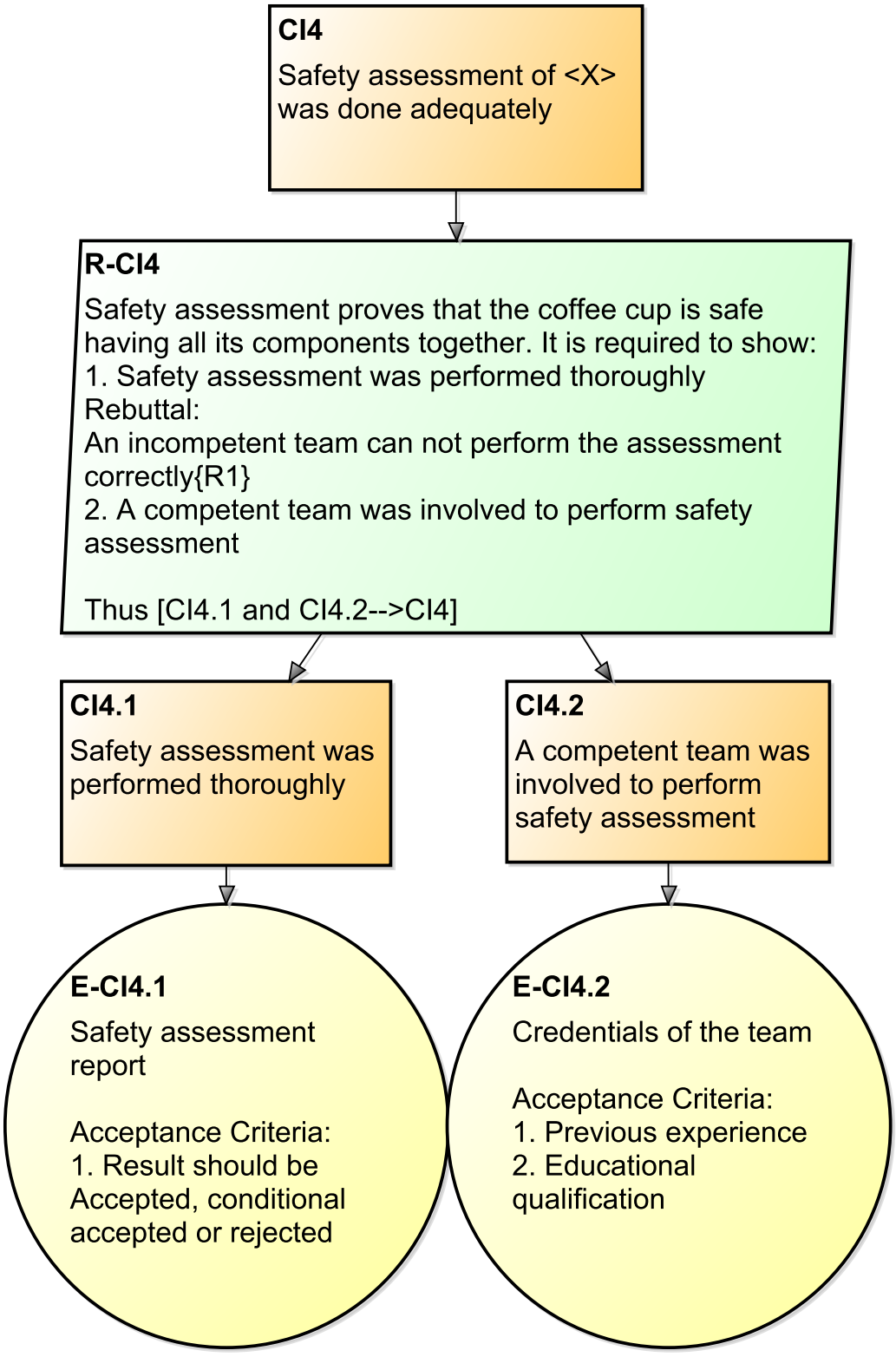

Figure C.19: Safety Assessment Argument