SECURITY-INFORMED SAFETY CASE: HELICOPTER OFFSHORE TRANSPORT

José Corrêa de Sá, correa_de_saa@hotmail.com, Portugal

Abstract

Transport of personnel, and cargo, in the Oil and Gas industry is the main civilian (non-military and non-security) application of helicopters. It is a billionaire business. The International Helicopter Safety Team (IHST) set as an objective to reduce the worldwide civil helicopter accident rate, in 80% from 2005 to 2016, that is, from 9,4 to 1,9 accidents per 100k flight hours (which actually as run short since it is expected to be 5,7; even the European rate is expected to be 4,8). Even with lower rates than other helicopter Aviation sectors helicopter offshore transport operations accidents have a higher economic and image impact. The concept of terrorism, developed in Europe, in late XIX century, which evolved with sabotage actions during the WWs, and terrorism outside and inside Europe after the II WW, has reached a new level. Recently, 9/11 and LAX ERAM U2, but also Malaysia Airlines Flight 17, Air France Flight 447 and Germanwings Flight 9525, all raise Critical-System Security, but also Survivability and Safety, issues; in particular, Airworthiness Security issues. As these cases show, several contemporary security factors make the Aviation industry, and, possibly, the helicopter offshore transport operations more complex than ever before. All these factors have implications for the helicopter offshore transport operations safety performance, in several ways, including new threats and hazard scenarios. Kateryna Netkachova, Robin Bloomfield and Robert Stroud, as part of the Security and Safety Modelling (SeSaMo) project presented, in 2013, the Security-Informed Safety Case methodology. It is based on the Claims-Arguments-Evidence formalism, developed by Adelard LLP, which is a simple yet effective notation for structuring arguments to communicate how a system is adequately safe in its environment. The basic idea is that a claim is made, and this claim must be supported by evidence through a valid and structured argument. The approach follows the same rational of the Safety Case methodology. A safety case should consist of a structured argument, supported by a body of evidence that provides a demonstrable and valid argument that a system is adequately safe for a given application in a given operating environment. Safety cases are explicitly required by regulations and standards across a wide range of industries, including the Oil & Gas. Security-Informed Safety Case is the enhancement of the existing Safety Case methodology, in which safety and security properties are considered in an integrated manner, and can / should be used to demonstrate and communicate security requirements in addition to safety. This way one benefits from the mature, effective and time-tested Safety Case, bringing security into focus and highlighting the role of security in the system safety justification. Also, this approach, if properly used, provides a better understanding of the interactions between system safety and security aspects and allows to address the potential issues associated with their interrelations. Security-Informed Safety Cases are more representative and fit for purpose in analysing security- and safety-critical systems. Security is concerned with protecting systems against malicious attacks/intrusions that, exploit weakness, flaws or vulnerabilities of the system, seeking to compromise its confidentiality, integrity and/or availability. Usually, it only considers embedded-system (e.g., avionics), not the (whole) system (e.g., helicopter). In this paper, Airworthiness Security will be seen as: the protection of the airworthiness of an aviation system (e.g., helicopter) from any security threat: an adverse effect on safety due to (direct or indirect) malicious human action(s), throughout its life-cycle. Safety has, by definition, not considered malevolent actions as causes… but that is just a definition! Safety-critical systems may not be as safe as they claim (and are supposed to be), if they are not secure (and survivable). In both safety and security something (the system) is being safeguarded / protected and the issue is how to ensure that the safeguard/protection is adequate. Thus, it is necessary to identify what is being safeguarded/protected (system definition), what it is being protected against (hazard / threat, attack / intrusion), what might cause the safeguard/protection to fail (weakness / vulnerability), what the consequences of failure might be (incident / accident, intrusion), what can be done to reduce those consequences to an possible / acceptable level (mitigation / protection), and how to determine whether this has been achieved (evaluation). The present work aims to evaluate the use of Security-Informed Safety Cases for the improvement of the helicopter offshore transport industry safety performance. To do so, the present paper has shortly resumed Toulmin’s Argument Model, considering its limits, critics, and applications (particularly, in “Argument Case”); the Claims-Arguments-Evidence formalism, considering its evolution, limits, and tools / applications (particularly, in Safety Case); the Security-Informed Safety Case methodology, considering its evolution, limits, critical reviews, and applications (particularly, in Aviation). A preliminary, hypothetical, Security-Informed Safety Case applied to the helicopter offshore transport industry, in Brazil, was carried out. It was compared with a similar Safety Case, where Security is not considered. It concludes that Security has an impact on safety performance, and the use of the Security-Informed Safety Case methodology should be considered. But, to properly do so, one needs to correctly understand

Toulmin’s Argument Model, and argument fallacies. Since this mitigates the major limit to Argument Case / Security-Informed Safety Case: the human, either developer or evaluator.

1. INTRODUCTION

Transport of personnel, and cargo, in the Oil and Gas industry is the main civilian (non-military and non-security) application of helicopters. It is a billionaire business. It is, also, a business which, inherently, involves risk (like any other flight activity).

The International Helicopter Safety Team (IHST) set as an objective to reduce the worldwide civil helicopter accident rate, in 80% from 2005 to 2016, that is, from 9,4 to 1,9 accidents per 100k flight hours (which actually as run short since it is expected to be 5,7; even the European rate is expected to be 4,8). Even with lower rates than other helicopter Aviation sectors helicopter offshore transport operations accidents have a higher economic and image impact.

To deal with the hazards which, eventually, lead to accidents (or incidents) several theories, methodologies, methods, and technologies have been developed (and, are developed all the time) in the field of Safety.

The concept of terrorism, developed in Europe, in late XIX century, which evolved with sabotage actions during the WWs, and terrorism outside and inside Europe after the II WW, has reached a new level. Recently, 9/11 and LAX ERAM U2, but also Malaysia Airlines Flight 17, Air France Flight 447 and Germanwings Flight 9525, all raise Critical-System Security, but also Survivability and Safety, issues; in particular, Airworthiness Security issues. As these cases show, several contemporary security factors make the Aviation industry, and, possibly, the helicopter offshore transport operations more complex than ever before. All these factors have implications for the helicopter offshore transport operations safety performance, in several ways, including new threats and hazard scenarios.

To deal with the threats which, eventually, lead to hazards, which, eventually, lead to accidents (or incidents) several theories, methodologies, methods, and technologies have been developed (and, are developed all the time) in the field of Security.

Security is concerned with protecting systems against malicious attacks / intrusions that, exploit weakness, flaws or vulnerabilities of the system, seeking to compromise its confidentiality, integrity and/or availability. Usually, it only considers embedded-system (e.g., avionics), not the (whole) system (e.g., helicopter). In this paper, Airworthiness Security will be seen as: the protection of the airworthiness of an aviation system (e.g., helicopter) from any security threat: an adverse effect on safety due to (direct or indirect) malicious human action(s), throughout its life-cycle. Safety has, by definition, not considered malevolent actions as causes… but that is just a definition!

Traditionally, Safety and Security have been treated as separate disciplines, but this position is increasingly becoming untenable and stakeholders are beginning to argue that if it’s not secure, it’s not safe. [Bloomfield, Netkachova and Stroud 2013]

A research project called SafSec investigated a combined approach to safety and security argumentation. It has shown that there can be practical benefits in performing a combined analysis, and documenting a combined argument, for both safety and security. [Lautieri, Cooper and Jackson 2005]

Kateryna Netkachova, Robin Bloomfield and Robert Stroud, as part of the Security and Safety Modelling (SeSaMo) project presented, in 2013, the Security-Informed Safety Case methodology. [Netkachova, Bloomfield and Stroud 2013] It is based on the Claims-Arguments-Evidence formalism, developed by Adelard LLP, which is a simple yet effective notation for structuring arguments to communicate how a system is adequately safe in its environment. The basic idea is that a claim is made, and this claim must be supported by evidence through a valid and structured argument. [Adelard 2016] The approach follows the same rational of the Safety Case methodology. A safety case should consist of a structured argument, supported by a body of evidence that provides a demonstrable and valid argument that a system is adequately safe for a given application in a given operating environment. Safety cases are explicitly required by regulations and standards across a wide range of industries, including the Oil & Gas. Security-Informed Safety Case is the enhancement of the existing Safety Case methodology, in which safety and security properties are considered in an integrated manner, and can / should be used to demonstrate and communicate security requirements in addition to safety. This way one benefits from the mature, effective and time-tested Safety Case, bringing security into focus and highlighting the role of security in the system safety justification. Also, this approach, if properly used, provides a better understanding of the interactions between system safety and security aspects and allows to address the potential issues associated with their interrelations. Security-Informed Safety Cases are more representative and fit for purpose in analysing security- and safety-critical systems.

Safety-critical systems, like offshore helicopter transport, may not be as safe as they claim (and are supposed to be), if they are not secure (and survivable). In both safety and security something (the system) is being safeguarded / protected and the issue is how to ensure that the safeguard/protection is adequate. Thus, it is necessary to identify what is being safeguarded/protected (system definition), what it is being protected against (hazard / threat, attack / intrusion), what might cause the safeguard/protection to fail (weakness / vulnerability), what the consequences of failure might be (incident / accident, intrusion), what can be done to reduce those consequences to an possible / acceptable level (mitigation / protection), and how to determine whether this has been achieved (evaluation).

For these reasons, the present work aims to evaluate the use of Security-Informed Safety Cases for the improvement of the helicopter offshore transport industry safety performance.

The present work is structured as follows: after a short introduction, in Chapter 1, Toulmin's Argument Model is presented, considering its evolution, limits, critics, and applications (particularly, in "Argument Case"); the Claims-Arguments-Evidence formalism, considering its evolution, limits, and tools / applications (particularly, in Safety Case) is presented, in Chapter 2; in Chapter 3, the Security-Informed Safety Case methodology, considering its evolution, limits, critical reviews, and applications (particularly, in Aviation); a short discussion about what was presented in the first 3 chapters is presented, in Chapter 4; followed, in Chapter 5, by a Case Study, with the application to a preliminary, hypothetical, Security-Informed Safety Case, applied to the helicopter offshore transport industry, in Brazil, and its comparison with a similar Safety Case, where Security is not considered; finally, the conclusions are presented, including future work proposals.

2. TOULMIN ARGUMENT MODEL

The British, Cambridge philosopher, Stephen Edelston Toulmin, in its 1958 book, The Uses of Argument [Toulmin 1958], written while Professor and Head of the Department of Philosophy at the University of Leeds, presented a model for (Logic) argument development and analysis * He further explained and applied the model to different areas in his posterior work (see: [Toulmin 1979]). *.

He developed the model, "ignoring" the dominant, in the previous 400 years, Logic argument view: theoretical, "absolute", formal; because he considered it not to be practical, universal, or completely valid.

Toulmin's Argument Model as the following characteristics:

- Reflects a natural (instinctive) way of thinking;
- Makes use of common (natural) language;
- It has a formal form (structure);
- It is flexible (p.e., allows hierarchy, contra-argumentation, trans-disciplinarity);
- Makes the thinking rational explicit;
- It is simple;
- It is practical; and,
- It is visual;
- etc.

Toulmin's Argument Model can be visualised as a schema (see Figure 1.1, in the end of the paper).

Where, in Toulmin's words [Toulmin 2003], each element can be defined as:

- Backing (B): other assurances, without which the warrants themselves would possess neither authority nor currency.
- Claim (C): conclusion whose merits we are seeking to establish;
- Data (D): facts we appeal to as a foundation for the claim;
- Qualifier (Q): explicit reference to the degree of force which our data confer on our claim in virtue of our warrant;
- Rebuttal (R): circumstances in which the general authority of the warrant would have to be set aside; and,
- Warrant (W): general, hypothetical statements, which can act as bridges, and authorise the sort of step to which our particular argument commits us;

Claim (C) is a (unique) statement or conclusion. It can be a Claim (C) in one argument, but it can also be Data (D) – sub-claim; Rebuttal (R), Backing (B), or contra-argument in other arguments.

Backing (B) is a justification or assurance. It must convince the argument reviewer that the warrant is valid. Its strength implies the strength of the warrant. It can be composed of information, (sub-)claim, and/or opinion.

Data (D) is evidence. It must convince the argument reviewer that the claim is valid. Its strength (jointly with the one of the warrant) implies the strength of the claim. It can be composed of data, information, (sub-)claim, and/or opinion. * In terms of terminology, it is better to use the word Evidence (E) for this element. *

Qualifier (Q) is a judgment (statement). It must show to the argument reviewer how strongly the argument developer fills about the argument. * It is the most subjective element of the argument. The words used should be explained in a Taxonomy. *

Rebuttal (R) is a statement. It must show to the argument reviewer the limits of validity of the Claim (C), either by showing the validity of the Backing (B), Evidence (E), Warrant (W), Backing (B) to Warrant (W), Evidence (E) to Warrant (W), Warrant (W) to Claim (C), and/or Evidence (E) to Claim (C). Its strength implies the strength of the Qualifier (Q) (as so, of the argument). * If it is composed of an argument, it can be used as Contra-Argument. *

Warrant (W) it is a statement. It must convince the argument reviewer that, considering the Data (D), the Claim (C) is valid.

At this point, certain characteristics of Toulmin's argument model must be discussed. All model's elements are necessary and equally important, and should always be made explicit. * Some authors get confuse by Toulmin's element division in primary and secondary, thinking he meant that the secondary could be discarded from the model: he never said that! * The argument is iterative in nature, that is, while developing the argument, in face of the Data (D), Backing (B), or Rebuttal (R), the Warrant (W) and Qualifier (Q) can change. * (This characteristic allows to understand the argument rational evolution, also to consider contra-argumentation, and the evolution of the argument over time. * The argument is meant to be probable, not in the sense used in Probability or Statistic but, in the sense that the claim statement is valid, to a certain degree, most of the time. Toulmin does not believe that arguments need to be (completely) objective, like in Formal Logic; but he also does not believe that they are (completely) subjective, according to Relativism. The model is in himself a demonstration that there is a middle-ground, much more realistic and practical.

Following Toulmin's approach certain notations where developed, such as Claims, Arguments and Evidence (CAE) [Bishop and Bloomfield 1998]. * See also ASCAD (Adelard Safety Case Development). [Bloomfield and Froome 1998] and [Bishop, Bloomfield, Emmet, Jones and Froome 2006] * and GSN (Goal Structuring Notation) [Kelly 1998]; and, also, hypertext systems, such as ASCE (Adelard Safety Case Editor) [Adelard 2016], AAA (Author's Argumentation Assistant) [Schuler and Smith 1990] and Aquanet [Marshall, Halasz, Rogers and Jansen 1991]. *

3. CLAIMS-ARGUMENTS-EVIDENCE FORMALISM

Claims, Arguments and Evidence (CAE) formalism * It should be noted that CAE is presented here, instead of another formalism, because it is the basis for the Security-Informed Safety Case. * is a simple and effective notation for presenting and communicating a safety argument. Its schema is presented in Figure 2.1 (in the end of the paper). It was developed by Adelard for structuring safety cases.

Where, in Adelard developers' words [Adelard 2016], each element can be defined as:

- Claim: a statement asserted within the argument that can be assessed to be true or false;
- Argument: a description of the argument approach presented in support of a claim; and,
- Evidence: a reference to the evidence being presented in support of the claim or argument.

The claim is about a property of the system or some subsystem. The claim is to be supported by one or more sub-claims, with respective arguments and evidence. Additionally, the claim node may contain contextual material.

The argument exists to link the evidence to the claim, which explicates how the evidence supports the (parent) claim. If the approach to supporting a claim is straightforward or well understood by the intended audience, it is permissible not to include the node.

Evidence is the basis of the argument. The evidence node will summarise and link out to the relevant report containing the evidence.

The formalism is implemented, as an hypertext argument, in Adelard Safety Case Editor (ASCE). An hypertext argument uses the notation in conjunction with the narrative. That is, at a macro level, the graphical argument is expanded with narrative according to the structure. At a micro level, details about the argument are explained using standard narrative, and situate it in context. In this way, both evidence paths and context can more easily be visualised.

At this point, certain characteristics of Claims, Arguments and Evidence (CAE) formalism in its relation to Toulmin's argument model must be discussed. First, the CAE authors acknowledge that the formalism was created before they got in contact with the model. Second, they always refer the model as the basis of the formalism, and its implementation - ASCE. Third, whenever they present the model, they only present a simplified version of it. Fourth, the ASCE allows to implement the model * Not only by himself, but also as the GSN formalism – this one really based on the model. *

Based on the Claims, Arguments and Evidence formalism certain methodologies were developed, like Safety Case and Security-Informed Safety Case. These can be included in the vast group of "Argument Case" (which include, among other methodologies: Assurance Case, Compliance Case, Confidence Case, Dependability Case, Reliability Case, Risk Case, Safety Case, Security Case, Trust Case, etc.).

4. SECURITY-INFORMED SAFETY CASE METHODOLOGY

The three main approaches used for safety (or security) assessment and justification, that is, to develop / demonstrate that a system is safe; can be characterized in terms of a safety assessment / justification "triangle": [Bishop, Bloomfield and Guerra 2004] and [Netkachova, Bloomfield and Stroud 2013]

- The behaviour of the system:
  - Claims about the systems' safety (and security) behaviour (positive characteristics / behaviour);
  - Analysis of potential vulnerabilities (negative characteristics / behaviour);
- The compliance with / use of accepted standards (regulations) and guidelines (best / standard practice); and,
- The design principles that were used to implement it.

The behaviour of the system refers to the system's behaviour due, directly or indirectly, to emergent properties of the system (i.e., safety and security). It is, here, divided in positive and negative characteristics, that may or may not lead, respectively, to the systems' positive or negative behaviour, in relation with the emergent properties considered. For Security-informed Safety Case, one deals with system's Safety and Security behaviour, safe and secure characteristics, and hazards and threats vulnerabilities.

The compliance with / use of refers to the consideration given to existing practices and regulations. For Security-Informed Safety Case, one deals with Safety and Security standards and practices.

The design principles refers to the (Science / Engineering) Philosophy considered as the foundation for the system's design. As so, it refers to the theory (or theories) considered for the system's design. * Apparently, to be coherent with the Philosophy and Theory used in the development of Security-Informed Safety Case, System Philosophy and System(s) Engineering should be used. * And, more specifically, to the design rational followed for each (significant) decision made during the system design, relatively to a particular system characteristic (or characteristics). For Security-Informed Safety Case, one deals with safety and security decision issues.

The approach is based on the use of safety cases * A Safety Case can be defined as: A documented body of evidence that provides a convincing and valid argument that a system is adequately safe for a given application in a given environment [Bishop, Peter and Bloomfield 1998]. *, on Claims-Arguments-Evidence formalism * It might use other formalism. And, it might be or nor be based on the Toulmin's Argument Model. *, and considers the impact that security might have on existing safety case. [Bloomfield, Netkachova and Stroud 2013]

The Security-Informed Safety Case methodology can be defined as:

> A documented body of evidence that provides a convincing and valid argument that a system is adequately safe and secure, for a given application, in a given environment.

A complete presentation and explanation, of the actual stage of evolution, of a security-informed safety case development is beyond the scope of the present work * The development is similar to the Safety Case: see ASCAD manual [Bloomfield and Froome 1998] or [Bishop, Bloomfield, Emmet, Jones and Froome 2006].*.

A complete presentation and explanation of security-informed safety case is beyond the scope of the present work * See [SeSaMo 2016]. *. Also, its implementation, using ASCE * See [Stroud 2015]. *.

At this point, and before presenting the case study, a discussion about what has been presented before must be done. It is not possible, nor intended, to cover everything that is relevant, or to deepen the discussion. The intention is to give an idea of what needs to be considered * Or, at least, part of what needs to be considered. * to develop or evaluate an “Argument Case”.

5. DISCUSSION

Considering the number of works which reference Toulmin’s book, The Uses of Argument [Toulmin 1958; Toulmin 2003] * Toulmin’s book, The Uses of Argument [Toulmin 1958; Toulmin 2003] has been referenced more than 10,000 times. *, or even those in which a critical review of Toulmin’s Argument Model is made, it is almost impossible to present a summary of them. For that reason, one has decided just to present an incomplete Taxology of the type of reviewers * Note that this Taxology is meant to be anecdotic evidence from the author readings on the subject. *. A list of the, most significant, type of Toulmin’s Argument Model critical reviewers is presented next:

- Formal Logic defenders – these are the reviewers which simply do not accept that there is logic outside Formal Logic;
- “Toulmin’s for dummies” – these are the reviewers which did not completely understand the model, but they tend to “expand” the model * It should be noticed that Toulmin’s book, The Use of Argument, is very much a product of the first-half of the XX century Philosophy, and, as so, the author spends most of the book just discussion about the meaning of words. For that reason, the book it is not easy to read. * ;
- “Indirect Toulmin” – these are the reviewers which have not read Toulmin’s work(s), just someone else’s work bout the model, and they tend to confuse the model with the formalisms based on it; and,
- “Toulmin’s defenders” – these are the reviewers which see the value and depth of the Toulmin’s Argument Model, and, as so, they tend to try to present the model in a simpler and more explicit way, try to expand its areas of application, and/or try to develop formalisms and tools based on it. * The first ones were Brockriede and Ehninger [Brockriede and Ehninger 1960], immediately in 1960, but also Toulmin himself [Toulim 1979], or even the author in this work. *

One last comment about Toulmin’s Argument Model critical reviewers: some “reviewers” try to evolve the model, and/or its formalisms (/tools), to make it more precise (that is, less subjective) and faster to analyse (or, even, develop), making use of Formal language and automation; both ways are contrary to the principles of the model, limit its flexibility, and create more problems than they solve.

About Toulmin’s Argument Model, besides what has been said before about its type of critics, something more need to be said, now about (logic) arguments in general. (Logic) arguments are developed and/or evaluated by persons, as so, they are subjected to person’s limitations. Particularly relevant for our discussion are logical fallacies, which people use when defending (or attacking) a claim, during an argument. Following the work of Greenwell, Knight, Holloway and Pease [Greenwell, Knight, Holloway and Pease 2006], and to facilitate the detection of these fallacies, a taxonomy of argument fallacies * The work of Greenwell, Knight, Holloway and Pease considered safety (case) argument fallacies. Further work needs to be done to upgrade the taxonomy for argument (case) fallacies. *, based upon existing taxonomies described in the philosophical literature adapted according to experience, is presented next. The taxonomy should consider, at least: emotional appeals (that is, in which a claim is asserted to be true on the basis of a personal desire or vested interest in it being true); malicious (that is, which convey acts of wilful deception); formal; syllogistic; and, causal fallacies * Their taxonomy did not included all these fallacies, but they assumed that some of the fallacies excluded from the taxonomy might appear with sufficient frequency to warrant inclusion, and there might exist fallacies that were not considered. *. The taxonomy’s topology groups fallacies into categories, with respect to the types of arguments they address: a) Circular reasoning - occurs when an argument is structured so that it reasserts its claim as a premise or defines a key term in a way that makes its claim trivially true: Circular Argument; and, Circular Definition; b) Diversionary arguments – occurs when an argument contains excessive amounts of irrelevant material that could distract a reader from a weakly supported claim: Irrelevant Premise; and, Verbose Argument; c) Fallacious appeals – occurs when an argument invokes irrelevant authorities, concepts, or comparisons as evidence: Appeal to Common Practice; Appeal to Improper/Anonymous Authority; Appeal to Money; Appeal to Novelty; Association Fallacy; and, Genetic Fallacy; d) Mathematical Fallacies – occur when an argument contains common pitfalls in probabilistic and statistical inferences: Faith in Probability; Gambler’s Fallacy; Insufficient Sample Size; Pseudo-Precision; and, Unrepresentative Sample; e) Unsupported assertions – occur when an argument includes claims stated without evidence: Arguing from Ignorance; Unjustified Comparison; and, Unjustified Distinction; f) Anecdotal Arguments – occur when arguments show that their claims hold in some circumstances but fail to generalize their validity: Correlation Implies Causation; Damning the Alternatives; Destroying the Exception; Destroying the Rule; and, False Dichotomy; g) Omission of key evidence - occurs when an argument otherwise complete omits evidence that is necessary to establish its validity: Omission of Key Evidence; Fallacious Composition; Fallacious Division; Ignoring Available Counter-Evidence; and, Oversimplification ; and, h) Linguistic fallacies – occur when an argument makes use of misleading language that might lead the reader to an unwarranted conclusion: Ambiguity; Equivocation; Suppressed Quantification; Vacuous Explanation; and, Vagueness; h) Emotional fallacies – occur when an argument accepts or wilful attempts at deception in favour of a claim: Emotional Bias; and, Emotional Fallacy; i) Formal fallacies – occur when an argument is one which involves an error in its form, arrangement or technical structure; j) Syllogistic fallacies – occur when an argument is one which involves an error in its deductive reasoning used to arrive at a conclusion; k) Casual fallacies - occur when an argument attempts to establish linear, false, or unsupported causal relationships between events: Linear Casualty; False Casualty; and, Unsupported Casualty. It is important that whoever develops or evaluates an "Argument Case" knows which argument fallacies exist, so he/she does not fall in or does not detect one.

About the "Argument Case" development, and evaluation, some considerations need to be made, to focus attention into some particulars which ensure a proper argument, respectively.

The Burden of Proof always falls with the developer (and not with the evaluator). [Weinstock, Charles and Lipson 2013]

Confidence derived from the use of a (Safety or Security) standard is generally transferred via conformance or compliance mechanisms. An artifact conforms to a standard if it voluntarily meets the requirements of that standard. Transferring confidence in self-assessed conformance requires that the stakeholder trust the developers' claims of conformance. In contrast, an artifact complies if a regulator forces it to meet the requirements; this typically results in a certificate attesting to compliance. Transferring confidence through this mechanism requires that the stakeholder trust that the regulator's assessment established all the required properties. Neither conformance nor compliance mechanisms are wholly sufficient. [Graydon, Habli, Hawkins, Kelly and Knight 2012] Is the author belief that, argue conformance explicitly is the best possible way.

Also, confidence in an argument can only be obtained using an "Argument Case", developed and, eventually, previously, evaluated by a credible developer and/or evaluator (for more detail, see discussion below).

For Safety- and/or Security-critical systems, "Argument Case" should be developed in parallel and complementarily to the Design process. In the sense that, "Argument Case" should be used to support decision making during Design. [Alder and Perkins 2003]

Also, for (Safety and/or Security) critical-systems, "Argument Case" should be considered the "best" and only way to perform Certification.

"Argument Case" should be developed, and cyclically evaluated, during the system (entire) life-cycle. But, it should also be used to predict the impact of possible change in the system in itself, its context / environment, and its mission(s) / service, and to evaluate the "real" impact of a change made in the respective system.

Also, it should be used to predict the impact of possible system's context change in the respective system, and to evaluate the "real" impact in the system of a system's context change.

It should, also, be used to predict the impact of possible system's mission / service change in the respective system, and to evaluate the "real" impact in the system of a system's mission and/or service change.

Some authors have been researching the use of automation to develop or evaluate "Argument Case". [] It is the author belief that automation is contrary to the principles of Toulmin's Argument Model, and, as so, to the "Argument Case" methodology, since it limits its flexibility, and creates more problems than it solves. []

Also, and finally, some authors have been researching the use of Formal Language to develop or evaluate "Argument Case". It is the author belief that Formal Language is contrary to the principles of Toulmin's Argument Model, and, as so, to the "Argument Case" methodology, since it limits its flexibility, and intelligibility, and creates more problems than it solves.

About the "Argument Case" some of its advantages, but also some of its disadvantages, should be pointed out.

"Argument Case" make (or should make) developer's rational explicit, which, among other things, during the process, facilitates error detection, and decision making, and, in the future, facilitates rational understanding, and knowledge development by others.

"Argument Case" facilitates and should be used to support (system) design, decision making, communication, property / behaviour assessment, and certification.

"Argument Case" facilitates and should be used for knowledge development, maintenance and preservation.

The "Argument Case" is flexible enough, in its formality, to allow dealing with any system's

particularities and specificities, facilitating innovation and precision.
Attention should be made to the fact that "Argument Case" development and evaluation is culture dependent. * Leveson's critical review [Leveson 2011], implicitly, shows that "Argument Case" use and efficacy depends on culture: some cultures (like the American) do not seem to accept the flexibility / "subjectivity" of argumentation in Certification, they seem to prefer standard processes. * Cultural differences lead to "Argument Case" differences, in both development and evaluation, which imply that any approach to "Argument Cases" must consider culture issues.

Something must be discussed about the "Argument Case" developers / evaluators, namely, the competence they must have to properly develop / evaluate an "Argument Case".
Assurance is ultimately based upon the competence of the people involved in the safety process, and individual competence is a vital requirement for assessing the validity of any safety or security claims, made by those providing assurance based upon expert opinion and judgement. [Sandom and Cooney 2016]
Competence can be considered to have three components, which are: a) Knowledge. Which is acquired through training, both formal and on-the-job, and is required to enable people to formulate an accurate plan of action to undertake an activity; b) Skills, both physical and mental. Mental skills can be thought of as the abilities, that experienced people often use subconsciously, brought to bear on the formulation of a plan. Physical skills can be thought of as the execution part of a plan of action; and, c) Attributes, associated with personal qualities. [Sandom and Cooney 2016]
Competence involves much more than technical training and expertise. It includes a person's attitude and behaviour, as well as experience and knowledge of the application domain [UK Health & Safety Executive 2007]. Competence might be transferable from one work situation to another, but the extent to which this is possible depends very much on the context in which apparently similar competence is required. [Sandom and Cooney 2016]

Security-Informed Safety Case is the enhancement of the existing Safety Case methodology, in which safety and security properties are considered in an integrated manner, and can / should be used to demonstrate and communicate security requirements in addition to safety. This way one benefits from the mature, effective and time-tested Safety Case, bringing security into focus and highlighting the role of security in the system safety justification. Also, this approach, if properly used, provides a better understanding of the interactions between system safety and security aspects and allows to address the potential issues associated with their interrelations. Security-Informed Safety Cases are more representative and fit for purpose in analysing security- and safety-critical systems. [Netkachova, Bloomfield and Stroud 2013]
Even so, certain things need to be made explicit and coherent, namely: the Science Philosophy used to develop it; align its, the formalism used (CAE), and tool (ASCE) development with the (correct) Toulmin's Argument Model; and, the training of its users.

Since the "terrorist" might be, most likely, anyone involved in the transport operation life-cycle, or helicopter life-cycle, "all" possible "terrorist" (i.e., crew, passenger, and/or maintenance personnel, etc.) should be considered. "External terrorists" should be considered as well.
To determine "terrorists" and "external terrorists" one must consider that, it must be someone with certain particular psychological characteristics – for radicalization and extreme action -, academic background, profession, and social expectations, which expectations have been foiled by the actual political and economic situation.
Considering the (actual) Brazilian Culture, and actual Brazilians, the most likely candidates, one believes, to become "terrorists" in the near future, at least in relation to Petrobras, and in particular to its offshore transport operations; are Engineers, in particular, the ones which have graduated from the top Brazilian Engineering schools * Since pilots, are in their vast majority ex-military and, with their training and experience, they can easily obtain, better paid, work abroad, one believes they constitute a less likely threat. *. Accordingly, "external terrorist" might be graduates from the top Brazilian schools.

A, possible, attack might consist in use of any means, and taking advantage of any system vulnerability, including, but not limited to, Data and Cyber ones.
A complete presentation and explanation of a possible, specific, attack, which might occur against / in the Brazilian offshore transport, in particular / or against an helicopter; which could be considered in a Security-Informed Safety Case, is beyond the scope of the present work. More, since it involves Security, information – even if hypothetical one – sensibility issues are always present, for obvious ethical reasons, since vulnerabilities' information might be used to perform "terrorist" attacks.

Last, but not the least - on the contrary-, something must be said about the Human (Sub-)System, present in the Security-Informed Safety Case.

There are, generally, two relevant groups of Human (Sub-)System, present in the Security-Informed Safety Case: the “terrorist” (or “external terrorist”); and, the “Argument Case” developer / evaluator.

First, as has been said before, the “terrorist” might be, most likely, anyone involved in the system, or any sub-system, life-cycle; and, “external terrorist” might be anyone not involved in the transport operation. Also, it must be someone with certain particular psychological characteristics – for radicalization and extreme action -, academic background, profession, and social expectations, which expectations have been foiled by the social, political, and/or economic situation. So, “all” possible “terrorist” and “external terrorist” should be considered.

To do so, the “Argument Case” developer / evaluator must have, significant, knowledge of the culture(s) and history (or histories) of the system, sub-systems, and respective environment. * It is the author’s belief that the fact the someone is competent in Argument does not mean that it is capable to develop / evaluate any “Argument Case”. *

The “Argument Case” developer / evaluator must, also, have, as has been discussed before, certain specific Argument competence.

A, preliminary and hypothetic, case study will be presented to demonstrate the impact that security might have on a safety case. * This part of the work is mainly based in [Corrêa de Sá 2011] and [Corrêa de Sá 2012]. *

6. CASE STUDY

Offshore personnel and cargo transportation, in the petroleum exploration industry, is the biggest civil (non-military and non-security) application of helicopters - it is a billionaire business. It is a (extremely) complex helicopter operation, due to, among other, logistics, resources, Safety, Security, economic and weather characteristics. And the entire offshore business depends on it to guaranty that the right person is on the right place at the right time, so the continuous production can continue.

Brazil was in 2007 the country with the third bigger petroleum exploration operation at high-sea of the world. However, after the public declaration on the part of Petrobrás of the discovery of deposits of oil in the depth of Pré-Sal at the Bacia de Santos, in 8 November 2007, the possibility is to not only become the country with the greater, but - it is well probable - also the most complex operation of this sort. Petrobrás was, in 2012, the biggest Brazilian company, and the fifteen’s greater of the world.

5.1 Company

Petrobras was created in 3 of October 1953, by President Vargas, as a public company holding the monopoly of the petroleum industry in Brazil, by the nationalization of the existing national and foreign private companies. It still holds the monopoly, but at Pré-Sal it can work in partnership with foreign companies.

Petrobras is a private company, own (mainly) by the Brazilian Government, which holds the monopoly of the industry which has the most influential economic impact in the country economy. Its administration and politic is (completely) controlled by the Brazilian Government. Its budget, together with the one from Vale do Rio Doce company, is (probably) higher than all other Brazilian companies put together; (probably) only being, in the country, overtaken by the Brazilian Government.

Petrobras is seen as “public service”, and has a “public service” culture and organization. When someone enters the company (after a standard exam), he/she gets a “work for life”. That is, he/she does not expect to get fired, ever!

It is also seen as an organization (as other “public service” ones) where “compadrio” * “Compadrio” is a certain type of collusion, typical in the Brazilian culture, which implies the use of power to influence decisions in favour of someone, group of people, or organization * and corruption * Corruption (in Brazil) is by (legal) definition the inefficacious and/or inefficient use, improper use, per example in benefit of someone, group of people, or organization, of public money.* are standard practice.

5.2 Operation

Petrabras started exploring offshore, in 1961, in the coast from Espírito Santo to Maranhão, up to 200m depth. In 1974, oil was found in Bacia de Campos (RJ), at 100m depth. The extraction started in 1977. In the Campo de Albacora, in the Bacia de Campos (RJ), in 1984, were found the first big petroleum reserves, in depth water. In 1986, petroleum was found, for the first time, in Amazonas, at the Campo de Urucu (AM). The extraction started in 1988. Finally, in 2007, petroleum was found, in ultra-depth water, at the pre-salt layer, in Campo de Tupi, at Bacia de Santos (SP). The extraction started in 1 of May 2009.

For these activities of exploration and extraction, Petrobras (and its partners * It should be noted that, Petrobras controls offshore transport in Brazil, since it is part of the partnership agreement to be so. *) need to transport their personnel to and from offshore positions * It is common practice to use helicopters instead of boats, due to efficacy, efficiency, and comfort reasons. But, technological developments and actual distance that paradigm should be challenged. *.

Some information about the offshore transport operations in Brazil are presented next, to give an idea of the complexity of the operations, and the numbers envolved, namely. In Brazil the three main offshore areas are: Southwest Coast (which includes Espírito Santo, São Paulo, Rio de Janeiro, and Paraná coasts), North Coast (which includes ? coasts), and Amazonas.

For the offshore personnel transportation operation, at Pré-Sal, per example: the exploration takes place offshore along 800 Km of coast; on a strip with 200 Km; consisting in an area of 160 km2; and, it is (mainly) located 300 Km from the coast.

The climate characteristics are not as bad as, per example, the North Sea (per example, visibility conditions), or the Golf of Mexico (per example, hurricane season), but still constitute a problem, even if flights are (mainly) limited to day-time.

Several air taxi companies work for Petrobras. * But, since Petrobras has not a transparent information politic, the information about who, were, and when is contracted, how the selection is done, and how much the service costs, is not clear. * They, usually, operate from a single airport or helipad, but they each operate different types and models of helicopters.

In terms of equipment, the 2011 numbers, for Pré-Sal operation, were: 50 helicopters, distributed: 33 at Macaé (SBME), 7 at São Tomé (SBFS), 5 at Jacarepaguá, and 5 at Vitória; with, 65, 30, 15 and 15 flights/day respectively.

Basically helicopters with limited capacity - 12 to 18 passenger per trip - are used to transport their staff to the offshore platforms. [Hermeto and Müller 2014] But, per example, for Pré-Sal operation the numbers are much lower * Actually, due to the distance that need to be covered, only a couple of passengers are being transported in each flight. *.

Petrobras, does not own helicopters, but it supports supplier to purchase theirs; it contracts each helicopter for a certain period (usually, 5 years).

The main mission is standard personnel transportation, but it also includes special personnel transportation, MedEvac, and SAR missions. Several problems exist, per example: there is no helicopter on the market which is "ideal" for the Pré-Sal operation; there is a lack of helicopters needed in the market; there is a lack of total maintenance capability in Brazil; and, there are no more operational pilots available;

The characteristics of the medical evacuations (MedEvac) depend on the situations. And, the transport equipment needs to have specific characteristics and capacities, so, usually, it is a specific one, that serves only that function. And, usually, has a small impact in the transport operation normal functioning. At Pré-Sal, in 2011, there were 3 MedEvac helicopters: 2 for Bacia de Campos (RJ), stationed at Jacarépaguá and Macaé (SBME); and, 1 for Bacia de Santos (SP), situated at Itanhaém airports. They are allowed to flight 24 hours per day, VFR or IFR, if there are conditions for it.

Several heliport types, both in airports and helipads, are being used, with different characteristics and capacities.

Per example, Baia de Campos's operation, in 2014, the passengers were transported through: Cabo Frio (SBCB), Campos dos Goytacazes (SBCP), and Macaé (SBME) Airports, and São Tomé (SBFS) helipad.

In 2012, Pré-Sal operation made used of 4 airports: Macaé (SBME), São Tomé (SBFS), Jacarepaguá, and Vitória.

The operations, also, involve several different helipoint types, which imply helicopters with specific characteristics (per example, size, and weight).

Per example, 30 rigs, with more 50 expected (16 in the year of 2011) for the Pré-Sal operation.

And, 86 fixed rigs and 46 floating rigs, in the other exploration areas.

In terms of passengers (offshore personnel) transported, the numbers in 2011 were: 25,000 offshore workers to be transported with a cycle of 2 weeks offshore, 3 weeks onshore; and, 45,000 passengers per month;

According to Infraero [Infraero 2016], Macaé (SBME) Airport had, in 2013, a work volume of: 443,000 passengers; and, 66,000 (flight) movements.

5.3 Context

Brazil has lived, up to the last couple of years, one period of economic and social "prosperity" and "development".

It was the consequence of several facts, namely: the monetary / financial / economic stabilization, initiated with Plano Real, in 1994; the "economic growth", due to the 2008 international financial crash; China "economic growth"; and, the "discover" of "huge" petroleum deposits in Pré-Sal.

The economic and social bloom is, also, due to: raw material exportation, Government investment in infrastructure * Including Football 2014 World Cup, and 2016 Summer Olimpic Games. *, and populist financial aid.

But, in the last couple of years, reality has settled in, and Brazil is living (another, maybe its worse ever) economic fall. It is due to: petroleum low market price; and, China economic stagnation.

And the first major (visible) "consequence" has been the Lava-Jato corruption scandal * It should be noticed that similar and connected scandals had already occurred in previous years, but not with same impact. *, which involves a significant portion of the most influential political, economic, and industrial Brazilians, and Brazilian organizations and institutions * Including Petrobras. *. This scandal has united political instability with the existing economic instability.

The consequences for Brazil, in all areas, are still to be seen.

*** news of Petrobras downsize or stop ***

*** news of Lava-Jato [http://lavajato.mpf.mp.br/lavajato/index.html (in Portuguese)] and Dilma impeachment ***

5.4 “Terrorist”

Following the logic presented in Gambetta and Hertog work [Gambetta and Hertog 2009] and [Gambetta and Hertog 2016], the “terrorist” * “Terrorist” is defined here as a person which makes use of excessive violence with the intension of having (local, national, regional, and/or international) social (political or media) impact in name of a person (himself/herself or other), group, or organization, to promote / defend a ideology, religion, or culture. * might be, most likely, anyone involved in the transport operation life-cycle, or helicopter life-cycle. But, most likely will be a member of the company, of a service provider, or a partner company. One that has seen is expectations foiled by the actual political and economic situation. Of course, it must be someone with certain particular psychological characteristics – for radicalization and extreme action -, academic background, profession, and social expectations * In the Brazilian culture, social status is, completely, determined by economic status. *.

5.5 Threat(s)

To give an idea of how Security can have an impact in Safety Case development, one will consider in particular the helicopter, used in the Brazilian Oil & Gas transport operation, possible vulnerabilities, through its life-cycle.

In general terms, an helicopter life-cycle can be divided in the following phases: 1) development; 2) deployment; 3) operation; 4) change; and, 5) disposal. And, further sub-divided in, at least (just considering the development and operation phases): 1.1) design; 1.2) certification; and, 1.3) manufacture; 3.1) schedule; 3.2) transport; and 3.3) maintenance.

Using the same logic, considering the (conventional) helicopter as a system, while flying, it can be divided, at least, in the following (functional) sub-systems: a) engine(s); b) transmission; c) main rotor; d) tail rotor; e) fuselage; f) controls; g) instruments; h) communication; and i) crew.

So, on one hand, in the development of a Safety Case one should consider “all” safety vulnerabilities that might lead to hazards (and, eventually, to incident or accident). Per example, a failure in the engine can be, at least, consequence of an error in design, certification, manufacture, maintenance, operation (i.e., flight procedures), crew (i.e., flight action), and/or environment (i.e., weather or bird strike).

Since the “terrorist” might be, most likely, anyone involved in the transport operation life-cycle, or helicopter life-cycle, “all” possible “terrorist” (i.e., crew, passenger, and/or maintenance personnel, etc.) should be considered.

“External terrorists”, that is, “terrorists” which are not involved in the transport operation * It should be noted that, historically and statistically, “terrorists” will, most likely, be Brazilian. So, external here should not be interpreted as alien / foreign. *, should be considered as well.

And, the attack might consist in any means, and use any system’s vulnerability * At this point, it would be useful to make use of an example to argument in favour of this claim. But, since Security is a sensitive issue, and any information might be used to perform an attack. One will exempt himself from do it – has (ethically) he should. Even so, several examples of attacks, perpetrated against / in the Aviation industry, are not Data or Cyber attacks, which “prove” the claim made. *.

So, on the other hand, in the development of a Security-Informed Safety Case one should also consider “all” security vulnerabilities that might lead to threats (which lead to hazards, and, eventually, to incident or accident). Per example, a failure in the engine can be, at least, also consequence of an intended, malicious, action (or actions) of a “terrorist” (or “terrorists”) * Actions, that make use of security vulnerabilities, of people without malicious intentions should also be considered. *.

A complete presentation and explanation, of a preliminary security-informed safety case is beyond the scope of the present work. * More, since it involves Security, information – even if hypothetical one – sensibility issues are always present. For obvious ethical reasons, vulnerabilities’ information might be used to perform “terrorist” attacks. *

7. CONCLUSION

Toulmin’s Argument Model, can be concluded, is the “ideal” foundation for practical Argumentation, as so, it is the “ideal” foundation for any “Argument Case”.

Even so, anyone using it, or even more if researching it, should be careful when selecting which bibliography to consider, since, as has been shown, some is defective.

Also, Argument fallacies need to be known and avoided.

Formalisms and tool, developed based on Toulmin's Argument Model, should be evaluated, and, if necessary, evolved, or even changed, to become coherent with the model.
Also, the tools need to be flexible enough so the user can adapt them to the particular system is Arguing about.

Security-Informed Safety Cases fit the purpose, better than any other methodology or process, of analysing Security- and Safety-critical systems, in a proactive manner.
How to develop and evaluate a Security-Informed Safety Case still needs to be further elaborated.
Also, how to use it to evaluate the impact of change need to be researched.

Any Case Study, used for Security-Informed Safety Case, in Aviation, will always be complex, and huge, since Aviation systems are complex, and ?; and contain huge amounts of variables, and information.
Further, since it is information-sensitive, it is not simple to obtain the necessary information, or to disclose some information, and conclusions.

The present work main goal was to evaluate the use of Security-Informed Safety Case for the improvement of the helicopter offshore transport industry safety performance.
To attain the main goal, several sub-goals were considered, namely:
to show that Security-Informed Safety Case methodology is valid; and "ideal" for Safety- and Security-critical systems; like the ones in Aviation;
to show that Security threats are relevant for Safety; and in (helicopter) offshore transport operations; and,
to show that Safety performance depends on how hazards are eliminated or mitigated.

The implicit goal of the present work is to "spark", in all persons involved with helicopters (rotorcrafts) – in particular Engineers –, the interest in Safety and Security, the development of the conscience that both are complex and complementary, and embedded in a context, need to be talked with honesty and rationality, making use of explicit argumentation.
And, also, to initiate an open discussion – hopefully, with everyone making use of Toulmin's Argument Model – about the influence of (certain) system properties (per example, Security and Survivability) in its Safety, in particular for helicopters (rotorcrafts), and offshore transport.

The size and intent of the present work did not allow to deepen the presentation and discussion of the covered subjects, that will have to be done in a future work. Also, several other related subjects will need to be worked in the future. Among other, to expand the methodology to include Survivability, that is Security-Survivability-Informed Safety Case * This will be presented by the author in a future work. *; to demonstrate that the basic principles of argumentation necessary in different methodologies (i.e., Assurance Case, Compliance Case, Confidence Case, Dependability Case, Reliability Case, Risk Case, Safety Case, Security Case, Trust Case, etc.) are the same, and can be used to develop a general case: the "Argument Case" * This work is mainly one of compilation and comparison. *; to present an Engineer(ing) Perspective of the Toulmin's Argument Model, to make it more understandable for Engineers, and diminish the existing less correct interpretations of it * This work, already being done by the author, is mainly one of bibliographic review, and synthesis. *; to expand Argument Case Developers / Evaluators Competence / Characteristics work to include Ethical Reasoning / Behaviour * There is work done in this subject (see [Habli, Kelly, Macnish, Megone, Nicholson and Rae 2015], [IET 2007], [Sandom 2015], [Sandom 2016] and [Sandom and Cooney 2016]), but (as far as one knows) not in this specific important point. *; which leads to the necessity of work in the subject of their Accountability.

REFERENCES

Adelard LLP; Adelard Safety Case Editor (ASCE); homepage; http://www.adelard.com/asce/choosing-asce/index.html (accessed on July 2016)
Alder, W. and Perkins, J.; The Use of a Safety Case approach to support Decision Making in Design; Symposium Series 149:807-813; Institution of Chemical Engineers (IChemE); Rugby, England, UK; 2003.
Bishop, Peter and Bloomfield, Robin and Emmet, Luke and Jones, Claire and Froome, Peter; Adelard Safety Case Development Manual (ASCAD); Adelard LLP; London, England, UK; 2006. (actual version)
Bishop, Peter and Bloomfield, Robin and Guerra, Sofia; The future of goal-based assurance cases; 2004 International Conference on Dependable Systems and Networks (DSN-2004); 28 June - 1 July, 2004; Florence; Toscana, Italia; Institute of Electrical and Electronics Engineers (IEEE); 2004.
Bishop, Peter and Bloomfield, Robin; A Methodology for Safety Case Development; 6th Safety-Critical Systems Symposium (SSS'98); February, 1998; Birmingham, England, UK; Safety-Critical Systems Club (SCSC); 1998.
Bloomfield, Robin and Froome, Peter; Adelard Safety Case Development Manual (ASCAD); Adelard LLP; London, England, UK; 1998. (original version)

Bloomfield, Robin and Netkachova, Kateryna and Stroud, Robert; Security-Informed Safety: If It’s Not Secure, It’s Not Safe; Software Engineering for Resilient Systems (Lecture Notes in Computer Science); 8166():17-32; 2013.

Brockriede, Wayne and Ehninger, Douglas; Toulmin on Argumentation: An Interpretation and Application; Quarterly Journal of Speech 46(1):44-53; 1960.

Corrêa de Sá, José; A System Engineering Framework for Offshore Personnel Transport: Aviation Safety and Airworthiness at Pré-Sal; Science Doctorate, Aeronautic and Mechanic Engineering; Instituto Tecnológico de Aeronáutica (ITA); São José dos Campos, SP, Brazil; 2012. (unedited)

Corrêa de Sá, José; Offshore Personnel and Cargo Transport Service: Aviation Safety and Airworthiness Modelling; Science Doctorate, Aeronautic and Mechanic Engineering; Instituto Tecnológico de Aeronáutica (ITA); São José dos Campos, SP, Brazil; 2012. (unpublished)

Gambetta, Diego and Hertog, Steffen; Engineers of Jihad: The Curious Connection between Violent Extremism and Education; Princeton University Press; Princeton, NJ, USA; 2016.

Gambetta, Diego and Hertog, Steffen; Why are there so many Engineers among Islamic Radicals?; European Journal of Sociology 50(2):201–230; 2009.

Graydon, Patrick and Habli, Ibrahim and Hawkins, Richard and Kelly, Tim and Knight, John; Arguing Conformance; IEEE Software 29(3):50-57; 2012.

Greenwell, William and Knight, John and Holloway, Michael and Pease, Jacob; A Taxonomy of Fallacies in System Safety Arguments; 24th International System Safety Conference (ISSC 2006); 31 July - 4 August, 2006; Albuquerque, NM, USA; International System Safety Society (ISSS); 2006.

Habli, Ibrahim and Kelly, Tim and Macnish, Kevin and Megone, Christopher and Nicholson, Mark and Rae, Andrew; The Ethics of Acceptable Safety; 1 October, 2015; London, England, UK; Safety-Critical Systems Club; 2015.

Hermeto, Thyago and Müller, Carlos; Analysis of Offshore Helicopter Air Traffic Operations at the Campos Basin; 18th ATRS World Conference; 17-20 July, 201; Bordeaux, France; Air Transport Research Society (ATRS); 2014.

HSE (Health & Safety Executive); Managing Competence for Safety-related Systems, Part 1: Key Guidance; Health & Safety Executive; UK; 2007.

IEC (International Electrotechnical Commission); Functional Safety of Electrical/ Electronic/ Programmable Electronic Safety Related Systems (IEC 61508), version 2; Annex B; ; 2010.

IET (Institute of Engineering and Technology Code of Practice); Competence Criteria for Safety-related System Practitioners; IET Publications; Stevenage, England, UK; 2007.

IET (Institute of Engineering and Technology Code of Practice); Institute of Engineering and Technology Code of Practice: Competence for Safety-Related Systems Practitioners; IET Publications; Stevenage, England, UK; 2016.

Infraero (Empresa Brasileira de Infraestrutura Aeroportuária); Statistics; homepage; http://www.infraero.gov.br/portal/index.php/us/statistics.html (accessed on July 2016)

Kelly, Timothy; Arguing Safety: A Systematic Approach to Managing Safety Cases; PhD Thesis; University of York; York, England, UK; 1998.

Lautieri, Samantha and Cooper, David and Jackson, David; SafSec: Commonalities Between Safety and Security Assurance; 13th Safety Critical Systems Symposium (SSS’05); February, 2005; Southampton, England, UK; Safety-Critical Systems Club (SCSC); 2005.

Leveson, Nancy; The Use of Safety Cases in Certification and Regulation; Journal of System Safety 47(6):1-5; 2011.

Marshall, Catherine and Halasz, Frank and Rogers, Russell and Jansen Jr., William; Aquanet: a hypertext tool to hold your knowledge in place; HyperText 91; 15-18 December, 1991; San Antonio, TX, USA; Association for Computing Machinery (ACM); 1991.

Netkachova, Kateryna and Bloomfield, Robin and Stroud, Robert; Security-Informed Safety Cases; Security and Safety Modelling - D3.1 – Specification of Safety and Security Analysis and Assessment Techniques - Version 01; chapter 3; pp. 19-24; Security and Safety Modelling (SeSaMo) Project; 2013.

Norddal, Ida; Optimization of Helicopter Hub Locations and Fleet Composition in the Brazilian Pre-Salt Fields; Master of Science (Industrial Economics and Technology Management); Norwegian University of Science and Technology; Trondheim, Norway; 2013.

Sandom, Carl and Cooney, Andrew; Competence for Safety-Related Systems Practitioners; SCSC Newsletter 25(2):-; 2016.

Sandom, Carl; Competence Considerations for Systems Safety; 24th Safety-critical Systems Symposium 2016 (SSS16); 2-4 February, 2016; Brighton, England, UK; Safety-Critical Systems Club; 2016.

Sandom, Carl; Unconscious Competence and Safety Assurance; 33rd International Systems Safety Conference (ISSC2015); 24-28 August, 2015; San Diego, CA, USA; International System Safety Society; 2015.

Schuler, Wolfgang and Smith, John; Author's Argumentation Assistant (AAA): A Hypertext Based Authoring Tool for Argumentative Texts; 1st European Conference on Hypertext (ECHT'90); 27-30 November, 1990; Versailles, France; Association for Computing Machinery (ACM); 1990.

Security and Safety Modelling (SeSaMo) project; homepage; http://sesamo-project.eu/ (accessed on July 2016)

Stroud, Robert; Security-Informed Safety Cases using ASCE; 18th ASCE User Group Forum; 10 December, 2015; Royal Academy of Engineering, London, England, UK; Adelard LLP; 2015.

Toulmin, Stephen Edelston and Rieke, Richard and Janik, Allan; An Introduction to Reasoning; Macmillan; London, England, UK; 1979.

Toulmin, Stephen Edelston; The Uses of Argument (Updated Edition); Cambridge University Press; New York, NY, USA; 2003.

Toulmin, Stephen Edelston; The Uses of Argument; Cambridge University Press; Cambridge, England, UK; 1958.

Walters, Steve; Accident Data and the Helicopter Offshore Safety Case; 2008 Regional Seminar; 30 May - 1 June, 2008; Adelaide, Australia; Australian Society of Air Safety Investigators (ASASI); 2008.

Weinstock, Charles and Lipson, Howard; Evidence of Assurance: Laying the Foundation for a Credible Security Case; ?; Software Engineering Institute, Carnegie Mellon University; Pittsburgh, PA, USA; 2013.

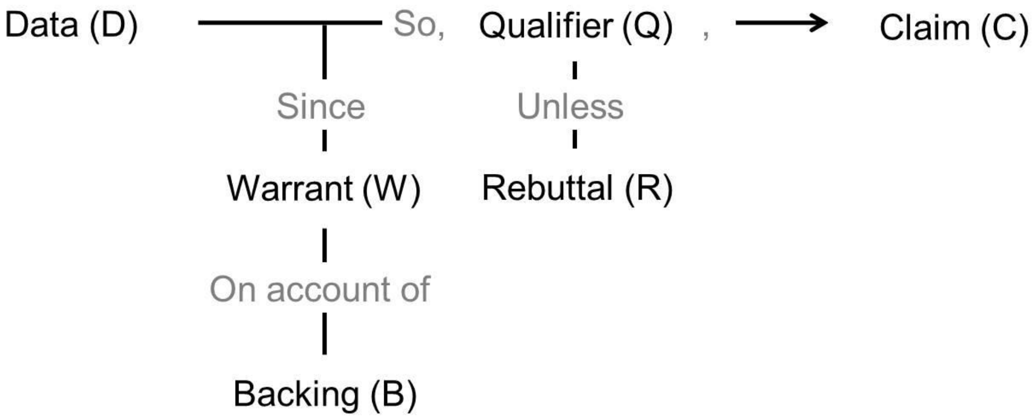

Figure 1.1: Toulmin’s Argument Model Schema (based on [Toulmin 2003]).

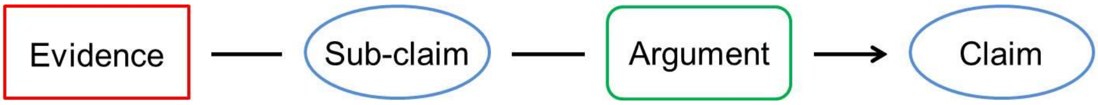

Figure 2.1: Claims, Arguments and Evidence Schema (based on [Adelard 2016]).