POLITECHNIKA GDAŃSKA
WYDZIAŁ ELEKTRONIKI, TELEKOMUNIKACJI I INFORMATYKI

Imię i nazwisko studenta: Patryk Orwat
Nr albumu: 125717
Studia drugiego stopnia
Forma studiów: stacjonarne
Kierunek studiów: Informatyka
Specjalność/profil: Inżynieria systemów i bazy danych

PRACA DYPLOMOWA MAGISTERSKA

Tytuł pracy w języku polskim: Analiza porównawcza dowodów bezpieczeństwa dla europejskich obszarów powietrznych.

Tytuł pracy w języku angielskim: Comparative analysis of European airspace blocks safety cases.

Potwierdzenie przyjęcia pracy	
Opiekun pracy *podpis*	Kierownik Katedry/Zakładu *podpis*
dr inż. Andrzej Wardziński	

Data oddania pracy do dziekanatu:

POLITECHNIKA GDAŃSKA
WYDZIAŁ ELEKTRONIKI, TELEKOMUNIKACJI I INFORMATYKI

OŚWIADCZENIE

Imię i nazwisko: Patryk Orwat
Data i miejsce urodzenia: 27.08.1990, Nowy Dwór Gdański
Nr albumu: 125717
Wydział: Wydział Elektroniki, Telekomunikacji i Informatyki
Kierunek: informatyka
Poziom studiów: II stopnia
Forma studiów: stacjonarne

Ja, niżej podpisany(a), wyrażam zgodę/nie wyrażam zgody* na korzystanie z mojej pracy dyplomowej zatytułowanej: Analiza porównawcza dowodów bezpieczeństwa dla europejskich obszarów powietrznych.
do celów naukowych lub dydaktycznych.[1]

Gdańsk, dnia ....
podpis studenta

Świadomy(a) odpowiedzialności karnej z tytułu naruszenia przepisów ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz. U. z 2006 r., nr 90, poz. 631) i konsekwencji dyscyplinarnych określonych w ustawie Prawo o szkolnictwie wyższym (Dz. U. z 2012 r., poz. 572 z późn. zm.),[2] a także odpowiedzialności cywilno-prawnej oświadczam, że przedkładana praca dyplomowa została opracowana przeze mnie samodzielnie.

Niniejsza(y) praca dyplomowa nie była wcześniej podstawą żadnej innej urzędowej procedury związanej z nadaniem tytułu zawodowego.

Wszystkie informacje umieszczone w ww. pracy dyplomowej, uzyskane ze źródeł pisanych i elektronicznych, zostały udokumentowane w wykazie literatury odpowiednimi odnośnikami zgodnie z art. 34 ustawy o prawie autorskim i prawach pokrewnych.

Potwierdzam zgodność niniejszej wersji pracy dyplomowej z załączoną wersją elektroniczną.

Gdańsk, dnia ....
podpis studenta

Upoważniam Politechnikę Gdańską do umieszczenia ww. pracy dyplomowej w wersji elektronicznej w otwartym, cyfrowym repozytorium instytucjonalnym Politechniki Gdańskiej oraz poddawania jej procesom weryfikacji i ochrony przed przywłaszczaniem jej autorstwa.

Gdańsk, dnia ....
podpis studenta

*) niepotrzebne skreślić

[1] Zarządzenie Rektora Politechniki Gdańskiej nr 34/2009 z 9 listopada 2009 r., załącznik nr 8 do instrukcji archiwalnej PG.
[2] Ustawa z dnia 27 lipca 2005 r. Prawo o szkolnictwie wyższym:
Art. 214 ustęp 4. W razie podejrzenia popełnienia przez studenta czynu podlegającego na przypisaniu sobie autorstwa istotnego fragmentu lub innych elementów cudzego utworu rektor niezwłocznie poleca przeprowadzenie postępowania wyjaśniającego.
Art. 214 ustęp 6. Jeżeli w wyniku postępowania wyjaśniającego zebrany materiał potwierdza popełnienie czynu, o którym mowa w ust. 4, rektor wstrzymuje postępowanie o nadanie tytułu zawodowego do czasu wydania orzeczenia przez komisję dyscyplinarną oraz składa zawiadomienie o popełnieniu przestępstwa.

STRESZCZENIE

Współczesne systemy informatyczne wymagają spełnienia wielu różnorakich kryteriów: bezpieczeństwa, niezawodności, czy wiarygodności, które są krytyczne dla rozwiązań, w których awaria może prowadzić do zagrożenia życia ludzkiego lub olbrzymich strat finansowych. Pomimo olbrzymiego rozwoju informatyzacji wciąż bardzo trudnym jest potwierdzanie ich właściwości w usystematyzowany i przejrzysty sposób.

Z tego powodu w trakcie budowy tego typu systemów wykorzystuje się *assurance case*, którego celem jest wykazanie zgodności z wybranymi aspektami w oparciu o przekonujące dowody. Narzędzie to jest wykorzystywane w wielu dziedzinach przemysłu wykorzystujących wysokie technologie np. transporcie kolejowym, przemyśle nuklearnym, systemach lotniczych oraz branży medycznej.

Pomimo iż każdy system wymaga opracowania osobnego *assurance case* może się zdarzyć, że powstanie kilka *assurance case*, które realizując swoje zadania wzajemnie pokryją się częścią dowodzonych faktów.. Informacja z tych nakładających się części może zostać przeanalizowana i fakty wyciągnięte z tego porównania mogą być wykorzystane do lepszego zrozumienia systemu. Można tutaj wyróżnić dwie następujące sytuacje:

- Systemy, dla których *assurance case* zostały utworzone mogą mieć wspólne części np. pompa insulinowa wyprodukowana przez różnych producentów ma ten sam mechanizm zasilania,
- System lub jakaś część posiada różne wersje i dla nich zostały utworzone *assurance case*.

Nawet, jeżeli te oba systemy lub ich części są zdefiniowane w *assurance case*, mogą być osadzone w innym środowisku (kontekście), które może wpłynąć na dowodzone aspekty. Jednakże w wielu przypadkach kontekst jest ten sam i przez to potencjalny problem z różnym środowiskiem może być złagodzony.

Cel pracy

Celem pracy jest zaproponowanie metody analizy porównawczej *assurance case* opisujących systemy, które posiadają wspólną część. Praca w głównej mierze będzie się skupiać na:

- Identyfikacji odpowiadających sobie elementów w porównywanych *assurance case*,
- Identyfikacji obszarów zgodności i różnic w porównywanych *assurance case*,
- Pomocy w określeniu wpływu różnic na siłę argumentacji.

Przykładem systemu, który spełnia przedstawiony problem są opublikowane dokumenty bezpieczeństwa FAB-ów (opisane w rozdziale 3). Zostały one utworzone aby potwierdzić bezpieczeństwo integracji europejskich obszarów powietrznych (FAB). Dokumenty te spełniają warunki przedstawionego problemu (mają wiele tych samych części) z dwóch powodów:

- Cel dokumentów bezpieczeństwa jest taki sam,
- Umiejscowienie systemów (środowisko) jest bardzo podobne.

Celem opracowania metod było określenie w systematyczny sposób odpowiadających sobie elementów w porównywanych AC, określenie obszarów zgodności i różnic oraz określenie wpływu różnic na siłę argumentacji uwzględniając kontekst różnic pomiędzy systemami. Wyniki te mogą być wykorzystane do:

- Potwierdzenia, że różnice w sprawdzanych systemach są odzwierciedlone w *assurance case*,
- Porównać (siłę) niezależnie utworzonej argumentacji,
- Identyfikacja specyficznych form argumentacji dla poszczególnych systemów,
- Identyfikacja i potwierdzenie zmian dla kolejnych wersji systemów.

Rezultaty pracy

Mając wiele *assurance case-ów*, które dotyczą podobnego zagadnienia można wykonać analizę porównawczą tych dokumentów, jednak kryteriów porównania oraz samych sposobów jest wiele w zależności od zamierzonych celów.

Ta praca omawia dwa zaproponowane typy porównywania *assurance case*:

- Analiza tematyczna, która wyszczególnia poszczególne aspekty lub części systemu. Wynikiem jest zestawienie *assurance case-ów*, które pozwala na stwierdzenie, czy dany aspekt lub część systemu zawiera się albo nie w AC,
- Analiza elementów *assurance case*, przez stworzenie powiązań pomiędzy

analogicznymi strukturami i pokazania mapowania pomiędzy kilkoma AC.

O ile obie metody porównywani dotyczyły sposobu argumentacji, została również przeanalizowana możliwość analizy dowodów.

Dla wszystkich metod oprócz algorytmów zaproponowano model prezentacji informacji. Metody zostały przetestowane oparciu o dokumenty bezpieczeństwa dziewięciu europejskich obszarów powietrznych. Wyniki pierwszej metody są zawarte w Tabeli 2, drugiej metody w Załączniku A.

Uzyskane wyniki wskazują, że uzyskano cel dyplomu tzn. zaproponowane metody zapewniają systematyczne porównanie *assurance case* w stopniu pozwalającym na wykorzystanie ich do przedstawionych problemów.

TABLE OF CONTENTS

FIGURES

TABLES

LISTINGS

ABBREVIATIONS

AC	Assurance Case
A&I	Accidents & Incidents
ALARP	As Low As Reasonably Practicable
ANS	Air Navigation Services
ANSP	Air Navigation Service Provider
ATM	Air Traffic Management
CAE	Claims, Argument, Evidence
CE	Central Europe
DE	Denmark
EC	European Commission
ESARR	EUROCONTROL Safety Regulatory Requirement
EU	European Union
FAB	Functional Airspace Block
FABEC	FAB Europe Central
GSN	Goal Structuring Notation
ICAO	International Civil Aviation Organization
NEFAB	North European FAB
NSA	National Supervisory Authority
SC	Safety Case
SE	Sweden
SES	Single European Sky
SMS	Safety Management System
SW	South West
UK	United Kingdom

SYMBOLS

$\|\boldsymbol{X}\|$	Cardinality of the set **X**
$\emptyset$	Empty set sign
$\rightarrow : \langle A, B \rangle$	Function (mapping) of elements from A to elements from B
$A \backslash B$	Relative complement of A in B
$\{A, B\}$	Set containing elements A and B
$\in$	Set membership
$\langle A, B \rangle$	Tuple containing elements A and B

1. Introduction

Modern systems are required to meet various criteria: safety, security, reliability or dependability which are critical for solutions in which a failure can result in human life or big financial loss. In spite of enormous growth of technology it is still difficult to affirm their properties in a systematic and transparent manner.

For this reason during planning and development process assurance cases are used. Its purpose is to demonstrate a compliance with selected areas combined with supporting evidence.

Despite of the need of a unique assurance case for every system or even its modification, there is a possibility that many assurance cases might cover the same facts. Information from these overlapping parts can be analyzed, and the results of the analysis can be used for better understanding of the system. Two situations can be distinguished here:

- Systems for which assurance cases were created might have common parts (e.g. insulin pumps made by different manufacturers have the same mechanism for power supply),
- A system or its part have different versions and for each of them an assurance case was created (e.g. two versions of an engine for the same aircraft were made).

Even if both of these systems or parts thereof are defined in the assurance case, may be embedded in a different environment (context) which can affect proven aspects. However, in many cases, the context is the same, and thus the potential problem of different environments can be mitigated.

1.1. Thesis objective

The objective of the Thesis is to propose a method for assurance cases comparison for systems which cover the same facts. It focuses on solving the following problems:

- Identification of equivalent elements of assurance cases,
- Identification of compliance areas and differences,
- Assistance in determination of the impact of the difference on trustworthiness of an argumentation.

An example of a system that meets the presented problem are nine Functional

Airspace Block (FAB) safety cases (described in Chapter 3). They were created to confirm the same fact – the safety of the integration process of FABs. These documents satisfy the conditions of the presented problem (they have many of the same parts) for two main reasons:

- The goal of safety cases is the same,
- The environment is very similar.

These documents fall in the first type of situation defines in the beginning of this Chapter.

The proposed methods need to be designed to retrieve the most relevant information from assurance cases. The results can be used to:

- Prove that differences in differences in assurance cases map to assessed systems,
- Compare trustworthiness of independently created argumentation,
- Identify specific argumentation forms for specific systems
- Identify and confirm changes in different system versions.

1.2. Structure of the thesis

This Thesis is divided into six chapters:

- Introduction (Chapter 1) – presents the problem, its context and define the purpose of the work and the structure of the Thesis,
- Introduction to assurance cases (Chapter 2) – the role of the chapter is to provide and clarify definitions and basic aspects of assurance cases
- Definitions of FAB safety cases (Chapter 3) – contains requirements for FAB safety cases, these documents, and definition of FAB.
- Assurance case comparative methods (Chapter 4) – contains a presentation of the expected results of the methods, and then a description of the possibilities of the relationship between the elements of assurance case, the analysis methods based on FAB safety cases and a manual analysis of FAB safety cases,
- Comparison of the two methods (Chapter 5) – consists of a more in-depth comparison of the methods using the FAB safety cases,
- Summary (Chapter 6) – discusses the developed methods and results based on FAB safety cases, analysis of the effectiveness and limitations of the methods. It also includes potential scope of applications and further development.

2. Introduction to Assurance Cases

This chapter contains basic definitions about safety and assurance cases to allow, even people who does not have extensive knowledge about the subject, understand all of the terms used in the Thesis.

There are many documents which are elementary for this Thesis. To give a general overview of possibilities, the most notable are:

- ISO/EIC 15026 [1] and [2],
- EUROCONTROL's Safety Case Development Manual [3],
- GSN Community Standard [4],
- Argumentation Metamodel (ARM) [5] and Structured Assurance Case Metamodel (SACM) [6],
- Reliability and Maintainability (R&M) Case [7].

Definitions used in this Thesis are based mainly on EUROCONTROL's Safety Case Development Manual, although another documents such as ISO/EIC 15026 standard are also used.

2.1. Assurance case definition

Assurance cases (AC) are created to confirm a goal or goals. These statements are called *top-level claims*. An Assurance case delivers a structure composed of many levels of arguments that supports a claim, are backed by evidence and stated assumptions. This elements combined show the truth or achievement of the top-level claim(s) [2].

Typically, an assurance case addresses the reasons to expect and confirm successful production of a system, including concerns of possibilities and risks which need to be dealt with in order to develop and sustain that system. To convince readers of an AC, the possibilities and risks they feel should be addressed whether the authors believe these opinions are important or not.

Assurance case is based on system concepts and requirements stated before the system is built and reflects possibilities and risks. The evidence that support argumentation can come from design and construction or post-construction artifacts e.g. personnel qualification records, reviews, mathematical proof checkers, standards conformance results, analyses, verification and validation activities or trials.

2.2. Assurance case structure

The decomposition of the top-level claim into lower-level elements delivers the vital links between the claim and evidence needed to present the validity of the assurance case's goal. Figure 1 presents all of the available elements of the assurance case defined by EUROCONTROL. Each of these type of element is described in this sub-section.

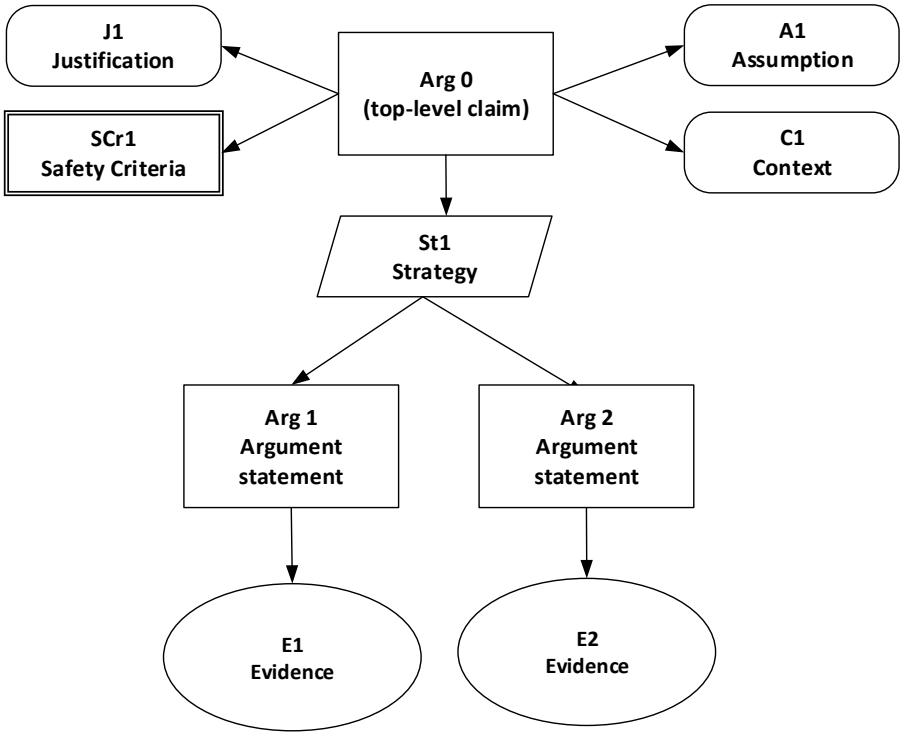

Figure 1 Example of top-level claim and main arguments using EUROCONTROL notation

Each element should fulfill the following requirements :

- Be one of the available type,
- Contain an identifier that recognize the element uniquely; should be numbered hierarchically to reflect logical structure of an AC,
- Contain a textual statement. [4]

Textual statements need to be defined unambiguously that is any word or phrase that can be understood in many ways cannot be used. Words like *normal* or *often* must be precisely defined at the beginning of assurance case or not be used at all. The statements also cannot be to simplified i.e. top-level goal "all hazards have been mitigated" can be recognized as oversimplified because only selected hazards were mitigated

2.2.1. Claim

Claim is a statement that can concern a system with related conditions and boundaries [3]. Each claim should be supported by arguments which ensures the system meets stated problem.

Claims have a form of a predicate (have value either true or false) and can define system behavior.

2.2.2. Argument

Arguments are used to present how AC elements relate to a claim.

It is a reasoned and well-structured statement (or a set of statements) showing how the overall goal is satisfied.

Each premise connecting an argument is strongly connected to all preceding ones, so if any of them contains a defect, all elements which rely on them can be recognized as incorrect.

2.2.3. Evidence

Evidence represents information about the system or its environment. There is a distinction between direct and backing evidence. The first one represents properties of a system while the second concerns trustworthiness of direct evidence by describing its quality and process.

Evidence is used as a premise that an argument is true and to accomplish this, any piece of information must concern specified system.

ISO/IEC 15026-1 [1] specifies many sources of evidence (direct and backing), although they are very general, because there is no strict requirement of the source of it. EUROCONTOROL *Safety Case Development* Manual [3] provides a tailored set of three entry points:

- Service experience – all relevant analyses from previous system that is in operation (direct evidence) and assurance that there are no significant differences between previous and current environment (backing evidence),
- Verification and Validation – direct evidence that includes formal proofs using analysis or testing that the process of designing, implementing and deploying was conducted properly and the system itself is working as intended,
- Compliance with standards – direct evidence can be understood as proofs that a

system meets a standard or set of standards whereas backing evidence can be defined as a description of the process of confirming the compliance and confirmations of compliance with standards concerning the development process.

Evidence type elements can be connected only to arguments.

2.2.4. Additional elements

For the purpose of safety case development additional elements are used:

- Strategy – describes how the decomposition of an argumentation is established. It can be connected only to arguments or top-level claim.
- Criteria – defines a reference point of what is meant to be safe and is added to top-level claim. There can be three types of criteria:
  - absolute – relates to a standard or established set of procedures,
  - relative – relates to a level of assurance that provided by previous system,
  - reductive – relates to a level of assurance provided by ALARP principle.
- Context – adds additional information to the top-level claim which helps better understanding of a problem concerning the connected element.
- Justification – explains the reason of a system to be developed or changed. It is added to the top-level claim.
- Assumption – an element which is treated as evidence, no information about validity of this statement is provided. It can be connected to: arguments, strategies and evidence.

2.3. Safety case

Safety case is a special type of assurance case where a top-level claim concerns safety of a system. They are used in process of certification of critical systems which can potentially cause loss of life, injury or environmental damage [8].

As stated at the beginning of the chapter, many definitions regarding safety cases has been created. According to U.K. Defense Standards 00-56 [9] safety case is:

(...) a structured argument, supported by a body of evidence, that provides a compelling, comprehensible and valid case that a system is safe for a given application in a given environment.

In this thesis and in all reviewed FAB safety cases definitions are taken from

EUROCONTOROL *Safety Case Development* Manual [3]. This document was created to provide a manual for creating, approving and reviewing safety cases of new ATM[3] service or changes in existing system.

It distinguishes two types of safety cases: Unit Safety Case which shows safety of a working system and Project Safety Case which shows safety of a change in a working system. FAB safety cases can be classified to Project Safety Case type because of the fact that they show the process of merging two or more existing nation-wide ATM-s.

2.4. Assurance case visualization

Assurance cases can be presented in both free-text and graphical way. However, free-text format can be unclear and difficult [10], and thus the latter forms are more popular.

There are two the most popular graphic notations: Claims-Arguments-Evidence (CAE) and Goal Structuring Notation (GSN). The first was developed by Adelard and the second was developed at the University of York in 1998 and in 2010 it was published as a separate document – GSN Community Standard [4].

Adjusted version of GSN is used in EUROCONTROL's *Safety Case Development Manual* [3] and so all of the reviewed FABs this thesis focus only on this model.

In this notation assurance case is presented in a form of an inverted tree. The top-level claim is represented as a root to which arguments are attached. Each element consists of an identifier, statement and a link to other element. The linkage always directs from general argument (claim) to more specific one.

GSN standard introduces an additional element called *strategy* which helps in understanding the structure and decomposition of a claim. Strategy cannot present any fact about the system.

The EUROCONTORL *Safety Case Development Manual* [3] defines its own modified version of GSN. However, the changes are minor and limits to simplified form of connections between elements and information about continuation of a diagram is represented by an inverted triangle. Figure 1 presents basic elements of an assurance case including mentioned changes.

[3] ATM is, according to ICAO Doc 4444 [12], the management of air traffic and airspace including air traffic services, air traffic flow management and airspace management.

3. Introduction to FAB safety cases

According to Article 1 of the Chicago Convention, each country has complete and exclusive authority over airspace above its territory [11]. It means that each of the country has its own air traffic management (ATM) system that is all of the systems that assist aircrafts during their department, transit and landing [12].

This fragmentation of airspaces is also present over European Union. To unify them, Single European Sky project was proposed whose main objective is to merge them to one, which could improve flight efficiency, safety and capacity [13].

The first phase of this project is introduction of Functional Airspace Blocks (FAB) that are airspace blocks which main purpose is to reduce fragmentation by establishing service provision regardless of country boundaries.

To fulfill the requirements stated by ICAO Annex 11 [14], ATM 2000+ [15] and ESSAR 4 [16] Commission Regulation No 176/2011 [17] places requirement of creating safety case for each FAB with the following information required:

- Provision of common safety policy or plans to establish it,
- Prepared plans for dealing with accident and incident investigation and procedures for reporting safety data collection, analysis and exchange,
- Preventing degradation in safety performance within the FAB,
- Prepared for clearly identifying and allocating the responsibilities and interfaces with respect to the setting of safety targets, safety oversight and the accompanying enforcement measures in regard to the provision of ANS within the FAB,
- Proof that the safety assessment has been conducted before introducing operational changes resulting from the establishment or modification of the FAB.

3.1. FAB safety cases description

European airspace had been divided into nine separate FABs. A safety case for integration process of each FAB has been developed and published on European Commission website[4].

There are several common facts that concerns these safety cases:

[4] All of the safety cases can be found at:
http://ec.europa.eu/transport/modes/air/single_european_sky/fab/index_en.htm

- All of these cases are made to be in compliance with Commission Regulation No 176/2011,
- In all of the FABs there are the same safety requirements defined at the beginning of the Chapter,
- Top-level claims are the same.

This chapter presents a short description of the FABs and their safety cases.

3.1.1. Baltic FAB description

Baltic FAB Safety Case had been created to demonstrate that the Baltic FAB, which consists of Polish and Lithuanian Air Navigation Services, can provide their services in a safe way. This document was published on December 4th 2012 and in this Thesis version 2.0 of this document is analyzed.

3.1.2. BLUE MED FAB description

BLUE MED FAB Safety Case proves that connection of Cyprus, Greece, Italy, Malta, Albania, Egypt and Tunisia ANS can be implemented in a safe way. It consists of two parts:

- *D3.2b – BLUE MED FAB Safety Case (Part A: Regulatory aspects)* includes short description of the FAB, initial assumptions, safety-related assumptions and agreements and statements of initial first and second level arguments. Additionally, there are descriptions of initial and first-level arguments.
- *D3.2b – BLUE MED FAB Safety Case (Part B: Beyond regulatory requirements)* includes safety related arrangements. In Annex 3 decomposition of second-level arguments is shown and in some cases there is decomposition down to evidence.

  In this Thesis version 2.0 which was published on March 27th 2012 is analyzed.

3.1.3. FAB Central Europe description

FAB Central Europe consists of the following countries: Austria, Bosnia and Herzegovina, Croatia, Czech Republic, Hungary, Slovakia and Slovenia. This Safety Case proves that the Functional Airspace Block that consists of these seven countries is implemented in a safe way. In this Thesis version 1.01 which was published on April 6th 2012 is analyzed.

3.1.4. DANUBE FAB description

DANUBE FAB consists of two countries: Bulgaria and Romania. The Safety Case concerns safety of the Air Navigation Services of the DANUBE FAB. In the Thesis version 1.0 which was published on April 25th 2012 is examined.

3.1.5. DK-SE FAB description

DK-SE FAB consists of two countries: Denmark and Sweden. The Safety Case is the smallest one in all of the Safety Cases. It is enclosed in a 11 pages document. The analyzed document had been released on June 21st 2012 and as version 1.00.

3.1.6. FABEC description

FABEC covers the airspace of six countries: Belgium, France, Germany, Luxembourg, the Netherlands and Switzerland. In the Thesis version 1.01 of the Safety Case which was released on June 1st 2012 is analyzed.

3.1.7. NEFAB description

NEFAB consists of four countries: Estonia, Finland, Latvia and Norway. In the Thesis version 3.01 of the Safety Case which was created on December 14th 2011 is analyzed.

3.1.8. SW FAB description

SW FAB Safety Case concerns safety of the combined airspaces over Portugal and Spain. In the Thesis version 1.1 of the Safety Case which was published on June 21st 2012 is analyzed.

3.1.9. UK-Ireland FAB description

UK-Ireland FAB consists of airspaces over two countries: United Kingdom and Ireland. In the Thesis Safety Case which was published on January 17th 2012 is analyzed.

4. Assurance case comparative analysis methods

For many assurance cases that relate to similar problem, a method of comparative analysis can be made. However, the problem is a diversity of comparison possibilities, which can give different results.

Results must reflect the objectives, which include identification of the corresponding elements, areas of compliance and differences in AC and allow determination of the impact of the difference on trustworthiness of an argumentation.

To achieve these results, methods must analyze aspects of the assurance case that show the relationship between them. This can be achieved through the following work:

- Detection of separate parts of a system – Extraction of system components drawn from assurance case and, optionally, their separate analysis,
- Analysis of assurance case elements – Extraction of specific type of elements and their separate analysis.

This chapter presents two comparison methods of assurance case which can provide a comparative analysis of FAB Safety Cases. All of these methods can be used successfully in all types of Assurance Cases e.g. Dependability Cases.

4.1. Expected results

To achieve that the results of a comparison methods comply with the goal, methods should fulfill the requirements defined in Table 1.

Table 1 Requirements for a method

No.	Requirement
1	Analyzed assurance cases must concern the same subject.
2	A method should identify related elements.
3	It is possible to present related elements in a form of a mapping.
4	Each element in the result need to relate to a concrete element/s in AC.
5	There is no technical dependencies e.g. identifiers are not taken into account in a method.

Each of the method described below is tested against these requirements and the result is presented in a form of a table.

Although there are many types of elements present in assurance cases, only arguments will be analyzed, because they provide almost the most information amongst

other types of elements.

4.2. Comparison of the thematic groups

The analysis of assurance cases can be started from analyzing general assets that are presented in them.

To accomplish that, first steps taken to solve the problem of comparison of many assurance cases was thematic comparison.

Each first-level argument's statements needs to be analyzed to find similarities between assurance cases. It allows a brief look into the problem using only a small amount of the data. These statements are analyzed to extract thematic grouping.

It will be proven later that this method, presents similar results in comparison to more complicated method.

4.2.1. Formalization

Consider a scenario presented in Figure 2. There are five first-level arguments connected to the top-level argument. Each of them concerns different aspect of a system. Thus this aspect can be extracted to a thematic group which can be more general and be properly adjusted to let arguments in other assurance cases fall into this group.

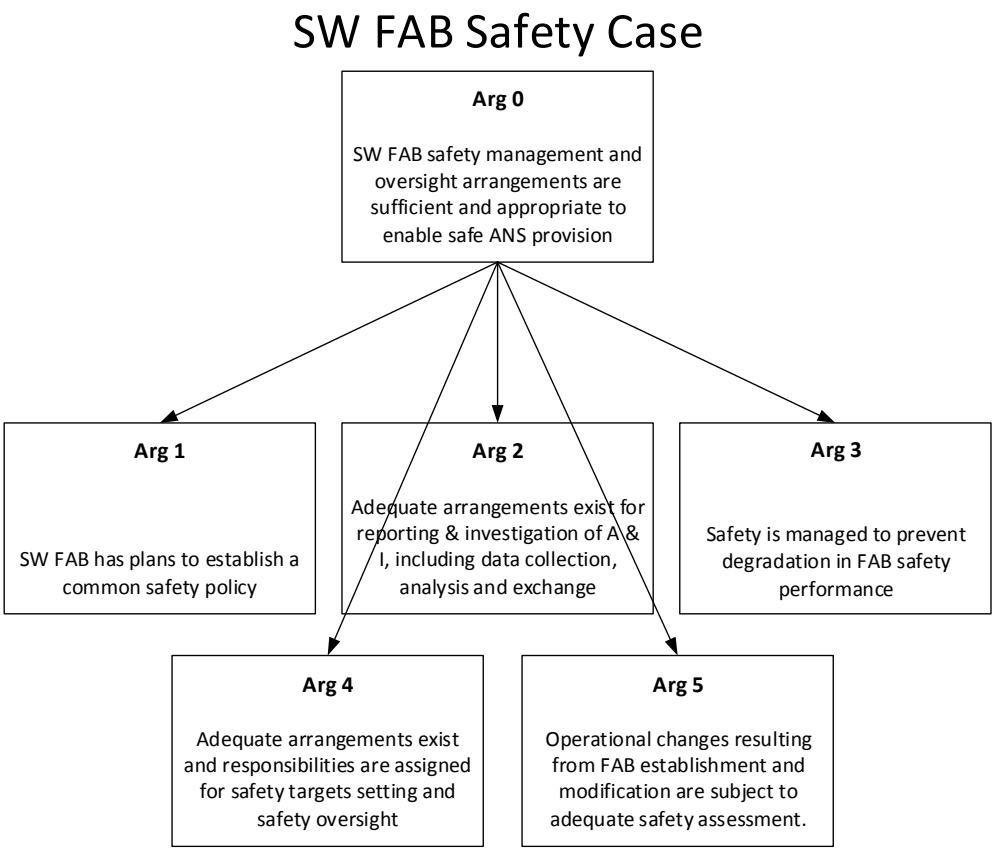

Figure 2 Top-level and first-level arguments for SW FAB Safety Case

Definition 1 (Simplified Assurance Case model).

Define a as a the only node type of an assurance case which is a claim. Each Assurance Case $\mathcal{A}$ is a tuple $\langle A, c, \rightarrow \rangle$, where A means the set of arguments and $c : A \rightarrow S$ which for each argument assigns a statement s. Relation $\rightarrow : \langle A_a, A_d \rangle$ defines links between arguments in the same Assurance Case in which A_a is called ancestor and A_d descendant. Each $\mathcal{A}$ needs to be a directed acyclic graph (DAG) with one root argument. Define it as $root(A)$.

In addition, a number of links from $root(A)$ to a specific a is called a level of a claim l. Each claim at level l can contain a connected set of nodes at level $l + 1$ called *descendants.*

Given nodes a_1 and a_2, if a_2 is placed on the unique path between a_1 and $root(A)$, then a_2 is an ancestor of a_1. Level of a_2 is then smaller than level of a_1.

A node a_p, which level is equal to l_p, is a parent of node a_a if and only if two conditions are met:

- a_p is an ancestor of node a_a and,
- level of $a_a$is equal to $l_p - 1$.

Definition 2 (Thematic comparison).

Define a thematic comparison as a tuple $\langle \mathcal{T}, \rightarrow, \mathbb{A} \rangle$, where $\mathcal{T}$ is a set of t thematic groups, $\rightarrow : \langle \mathcal{T}, A \rangle$ sets a relation between thematic group t and children of $root(A)$ of $\mathcal{A}$ (arguments with the same thematic group), and a set $\mathbb{A}$ containing all considered assurance cases. To be formal $|\mathbb{A}| \geq 2$.

Thematic groups are created by analyzing statements of first-level arguments, e.g. statement *Baltic FAB has a common safety policy* can be assigned to group called *safety policy*. It was achieved by analyzing thematic groups which were mentioned in the first level of argumentation for each Safety Case.

Listing 1 Thematic comparison method

```
Thematic_Comparison(𝔸: set of Assurance Cases , 𝒯: set of thematic groups)
begin
   for each assurance case A in 𝔸
      for each argument a in A
         assign t ← identified thematic groups of a
         if not exists t in 𝒯
            update 𝒯 ← 𝒯 ∪ {t}
         end if
         add_relation( t, a )
      end for
   end for
   shrink( T )
end
```

Listing 2 defines a procedure which is responsible for maintaining reasonable amount of thematic groups.

Listing 2 `Shrink` procedure definition

```
Shrink(𝔸: set of Assurance Cases , 𝒯: set of thematic groups)
begin
   for each thematic group t in 𝒯
      if ∃t_s ∈ 𝒯 such that t_s is similar to t
         assign t_n ← make common thematic group between t and t_s
         update 𝒯 ← 𝒯 ∪ {t}
         for each relation r in t
            move_relation(r, t_n)
         for each relation r in t_s
            move_relation(r, t_n)
         update 𝒯 ← 𝒯\{t, t_n}
      end if
   end for
end
```

The method does not define how two qualify two groups as equivalent. In addition, a thematic group should be:

- Chosen to be present in more than one assurance case,
- Chosen not to be present in all of the assurance cases.

If needed, it can be extended by analysis of lower levels of argumentation or even all of the arguments in assurance case $\mathcal{A}$. So it was done during the comparison of the FAB safety cases.

4.2.2. Results of the method

This study can present overall coverage of each of the Safety Case in the context of each other.

The results of the method were presented in Table 3. It was presented in the form of table but it is also possible to present it in the form of graph.

One row of the table concerns specific thematic group and one column includes information about exact one safety case. Thanks to this each cell presents information about a safety case in the context of specific thematic group.

This method was extended and included all of the arguments in safety cases. So cells can be in one of the three states:

- No presence of a thematic group at all,
- Presence on the first level of argumentation,
- Presence on different level of argumentation.

In total ten different thematic groups were distinguished and all of the nine Safety Cases were analyzed. By looking only at the table several observations can be made:

- Safety cases belonging to Baltic FAB, FAB Central Europe, South West Portugal Spain (SW) FAB and UK-Ireland FAB are very similar in this matter,
- Denmark-Sweden FAB contains only three groups from ten and these groups are also present in first level of argumentation FAB Europe Central,
- DANUBE FAB Safety Case and BLUE MED FAB Safety Case is the only one that covers all of the subjects.

Results of a test against the requirements is presented in Table 2. As it can be seen all of the requirements were provided by this method.

Table 2 Analysis of the first method

No.	**Requirement**	**Result**
1	Analyzed assurance cases must concern the same subject.	Yes, the method is created to work on assurance cases which concern similar subject.
2	A method should identify related elements.	Yes, the method tries to find a general similarities between assurance cases using arguments.
3	It is possible to present related elements in a form of a mapping.	Yes, the method's output is a thematic comparison of assurance cases which can be presented in a form of a mapping.
4	Each element in the result need to relate to a concrete element/s in AC.	Yes, each of the thematic group is related to a concrete argument.
5	There is no technical dependencies e.g. identifiers are not taken into account in a method.	Yes, it relies only on argument's statement and its placement.

4.2.3. Potential problems

The analysis of Safety Cases does need to be performed by a domain expert who has extended knowledge about the subject (in this example aviation-based) though

specific language. The difficulty is based on extraction of the thematic group from the original argument's statement.

The overall amount of thematic groups can vary and it is up to the author of an analysis how many thematic groups will be created. If the author decides that the amount of thematic groups created from the first level of argumentation is insufficient , more level of argumentation can be analyzed.

The more levels is analyzed, the more accurate the results are. It is caused by the fact that assurance cases can have different decomposition.

Table 3 Thematic comparison of the FAB Safety Cases

Thematic group	Baltic FAB	FAB CE	SW FAB	UK-Ireland FAB	DANUBE FAB	DK-SE FAB	FABEC	BLUE MED FAB	NEFAB
Safety policy	A 1	A 1	A 1	A 1	A 1-7	-	A 3-2-3-1	A 1	A 1-1
Appropriate FAB regulatory framework	A 0 [2]	A 0 [2]	A 0 [2]	A 0 [2]	A 1	A 1	A 1	A 0 [2]	A 1
Safety culture	-	-	-[1]	-[1]	A 3-2	-	-	A 1	-
Safety Management System	A 3-1	A 3-1	A 3-1	A 3	A 3	-	A 3-2-3	A 1	A 1-3-1, A 3
Reporting and Investigation of Accidents and Serious Incidents	A 2	A 2	A 2	A 2	A 1-4-1, A 2-2-5, A 3-1-2	-	A 1-2-1-3, A 2-3-2-2, A 3-2-1, A 3-2-2-2	A 2-1	A 1-2
Safety oversight	A 4-4	A 4-4	A 4-4	A 4	A 2	A 2	A 2	A 2	A 1-4
Safety degradation avoidance (Safety performance)	A 3	A 3	A 3	A 3	A 1-5, A 1-7, A 3	-	A 2-2	A 2-2	A 1-3
Safe service provision	-	-	-	-	A 3	A 3	A 3	A 3	A 3
Responsibilities and interfaces	A 4	A 4	A 4	A 4	A 2	-	A 3-2-1, A 3-2-3-3	A 2-3, A 3	A 1-4
Operational changes	A 5	A 5	A 5	A 5	A 2-2-3, A 3-1-3	-	A 2-3-2-2, A 3-2-2-2	A 2-4	A 2

Notes

1. Although information about Just Culture was mentioned.
2. A 0 means top level argument

\+ Thematic group is present in the first level of argumentation

\- Thematic group is present below the first level of argumentation

\- Thematic group is not present in a safety case

4.3. Arguments comparison

Although the first method gives an overall view about compared assurance cases, a more in-depth method is presented in this subsection.

There were cases in which a pair of Safety Cases each one of them had an argument's statement that the meaning or even the sentence itself was the same. Figure 3 presents this case.

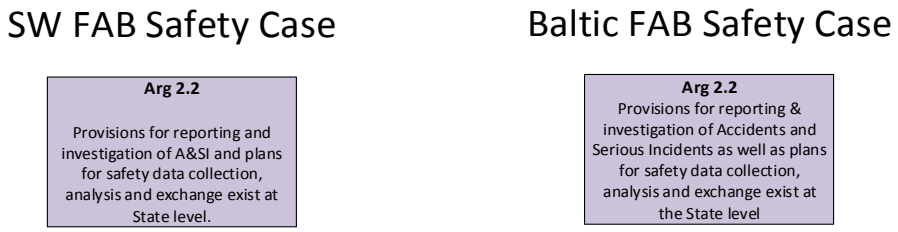

Figure 3 The same arguments

During the process of the review similar arguments had similar or almost the same decomposition. An example of the same decomposition is presented in Figure 4.

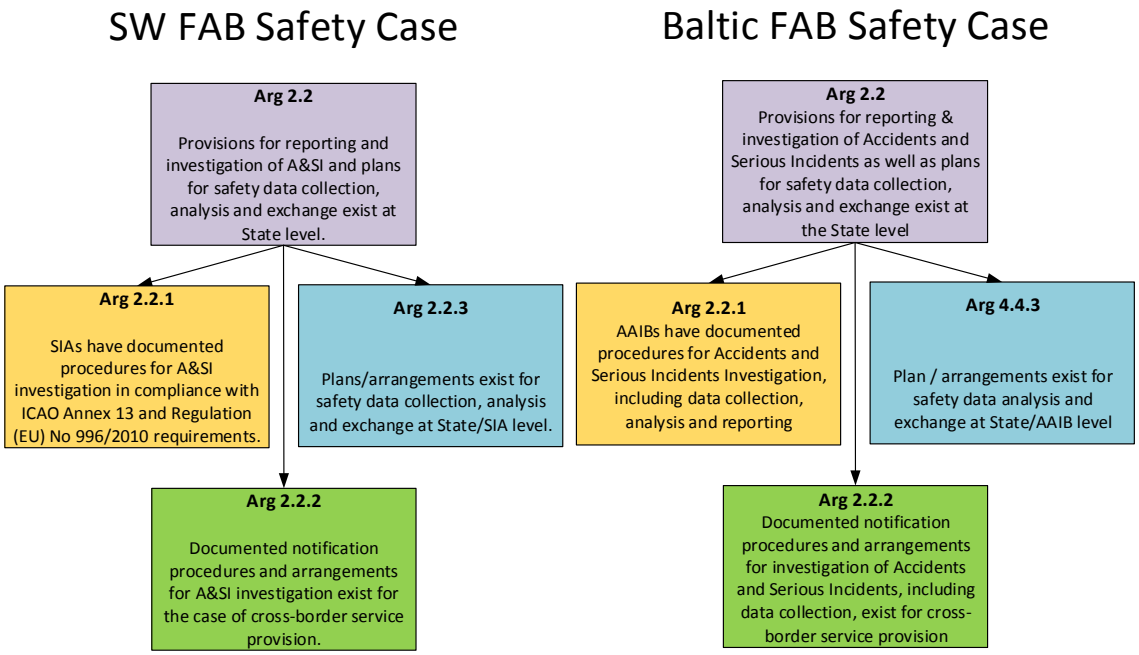

Figure 4 Equivalent arguments and its decomposition

There were also cases where argument statements were equivalent but their decomposition was different. This example is presented in Figure 5. In this example arguments 4.4 from SW FAB SC and FAC Central Europe SC have similar decomposition except for Arg. 44.2 in SW FAB SC.

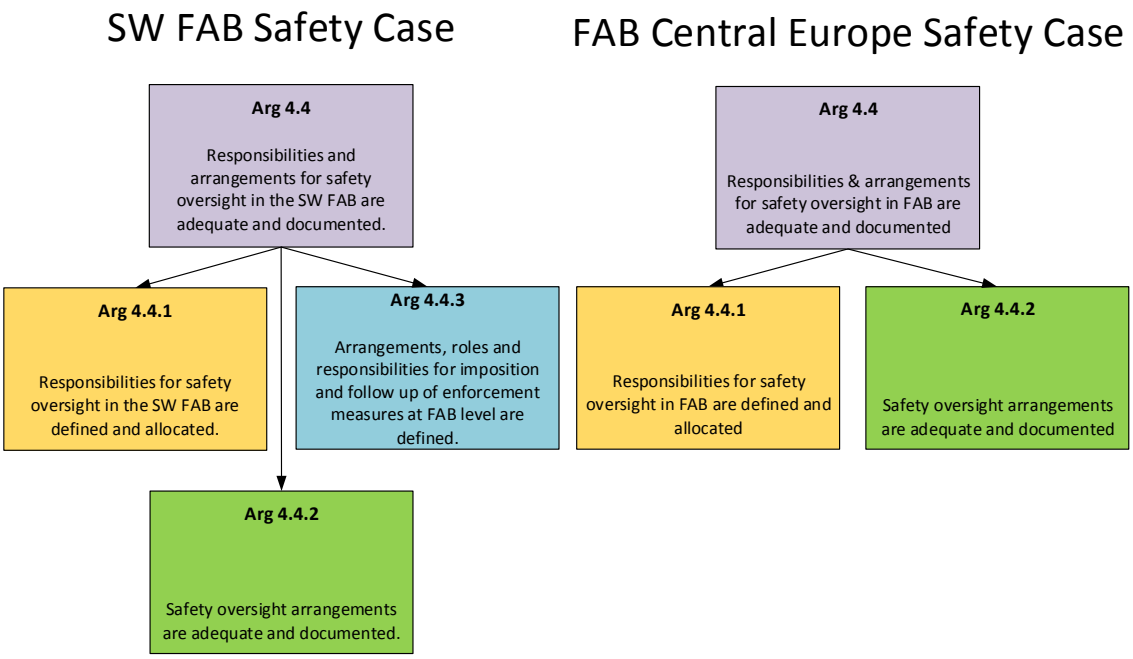

Figure 5 The same argument with different decomposition

More complicated cases are presented in Figure 6. This comparison exposes a possible case where an Argument 5 from SW FAB Safety Case and Argument 3.1.3.2 from Danube FAB Safety Case are similar, and:

- Argument 5.1 from SW FAB Safety Case are similar to Argument 3.1.3 from Danube FAB Safety Case. This case shows a contradiction in which more general argument in one Safety Case is presented as a detailed one.
- Argument 5.4 from SW FAB Safety Case is similar to Argument 3.1.3.2.5.3 from Danube FAB Safety Case. This one presents situation in which both arguments are not on the same level of decomposition.
- There is a similarity between Argument 5.3 from SW FAB Safety Case and Argument 3.1.3.2.1 and Argument 3.1.3.2.2 from Danube FAB Safety Case. The argument in SW FAB SC is represented as two arguments in Danube FAB SC.

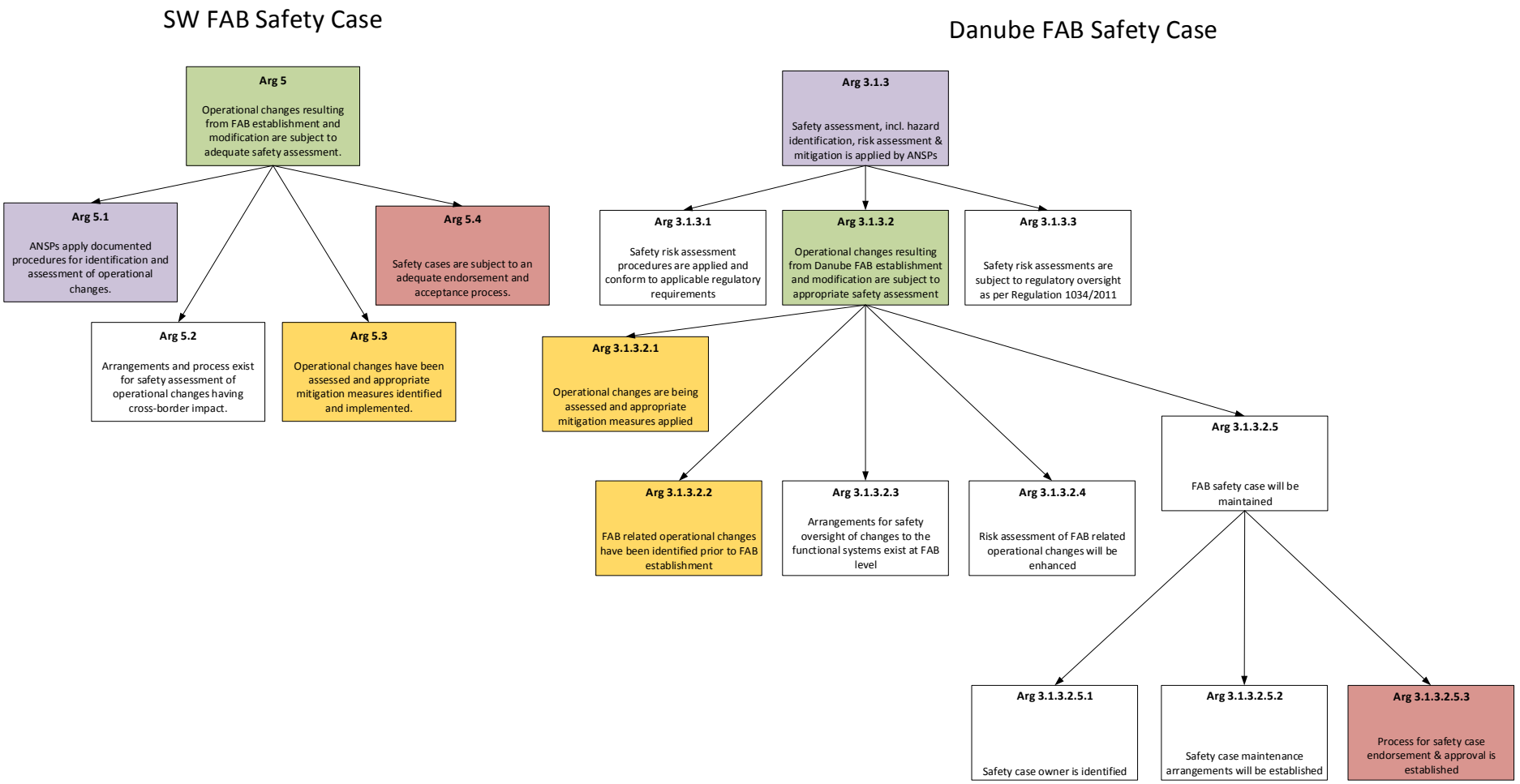

Figure 6 Comparison of simmilar arguments of two Safety Cases

To simplify the diagrams and present only relevant information additional symbol was introduced. It represents a part of the argumentation tree that its content is irrelevant when presenting specific arguments. The symbol is presented in Figure 7.

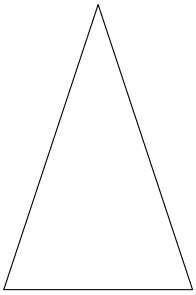

Figure 7 Additional symbol representing a part of a tree

To emphasize the fact that a team that is preparing similar Safety Cases can adopt different method of decomposition, Figure 8 presents a case in which two arguments (Arg. 2.2 and Arg. 2.4) from SW FAB SC can be connected a pair of the same arguments in Danube FAB Safety Case but they are in different parts of the Safety Case.

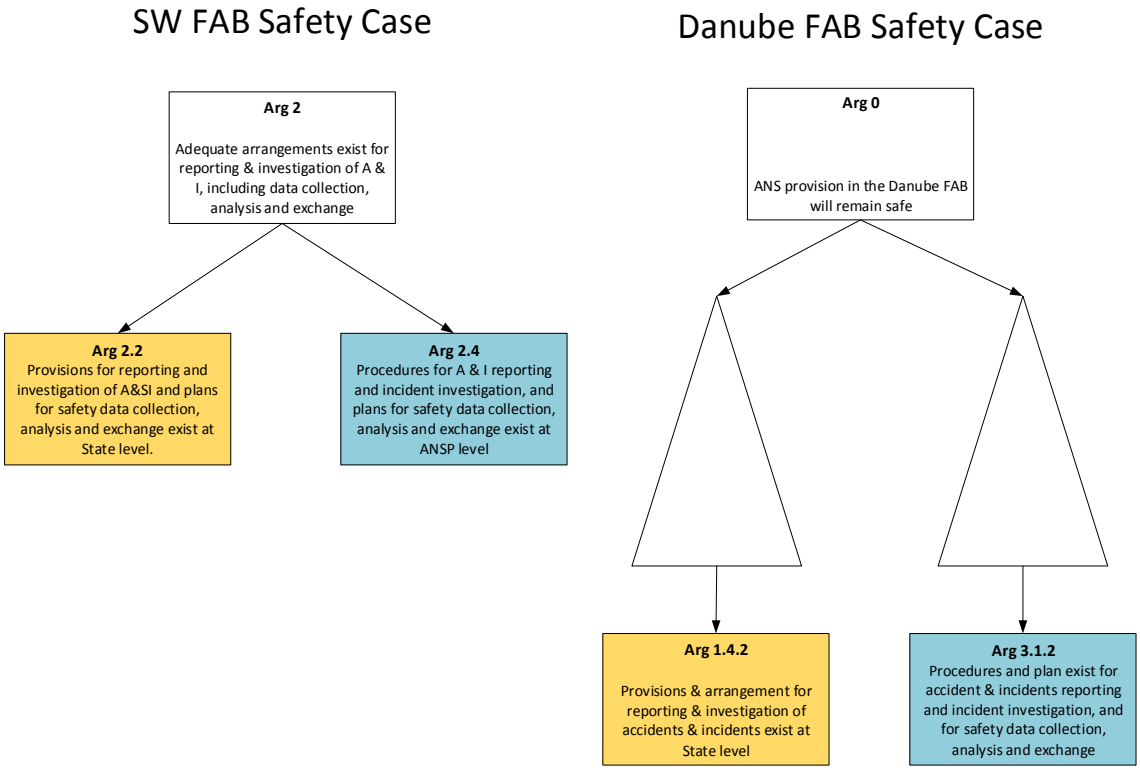

Figure 8 The same arguments located in different parts of Safety Cases

4.3.1. Assumptions

The examples presented in the previous subsection compared various possibilities of connections between arguments. To enable more accurate comparison between Safety Cases even arguments that their statements are not equivalent should be taken into account.

To provide better consistency of the diagrams lets introduce classification of relations between two arguments:

- Identical – if there is the same argument or arguments in another assurance case (colored in green),
- Equivalent – if there is similar but not the same argument or arguments in another assurance case (colored in yellow). In this Thesis words equivalent and similar are used alternatively,
- Different – if there is neither equivalent nor same argument or arguments in another assurance case (colored in grey)

Each similarity between arguments will be marked by a dashed line between those arguments.

The first and most basic connection is connection between two identical arguments. It is presented in Figure 9. Although the statement is not the same, that is, in SW FAB Safety Case in contrast to FAB CE Safety Case the FAB is defined precisely as SW FAB, the overall meaning is the same.

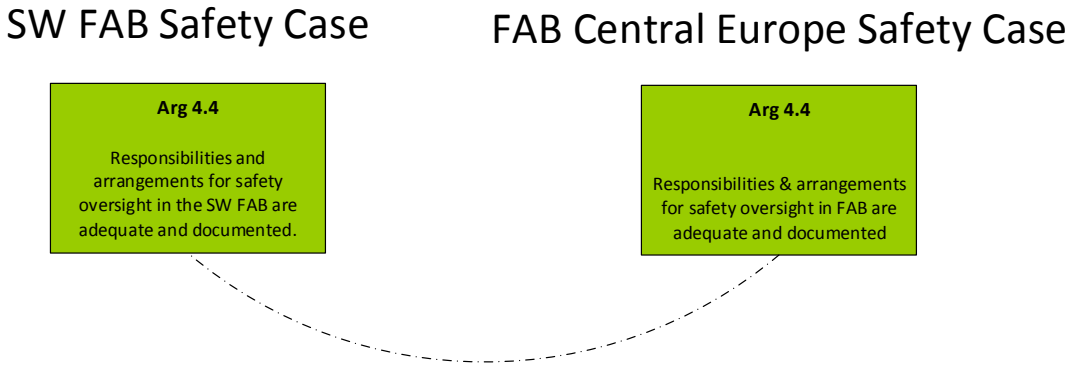

Figure 9 Two identical arguments

The same arguments can have the same sub arguments (Figure 10). Here, as same as in earlier example, arguments' statements are not equal, but the meaning of the sentences is the same.

This case (the same arguments have the same sub arguments) is common when

comparing the following Safety Cases: SW FAB Safety Case, FAB CE Safety Case, NEFAB Safety Case and Baltic FAB Safety Case.

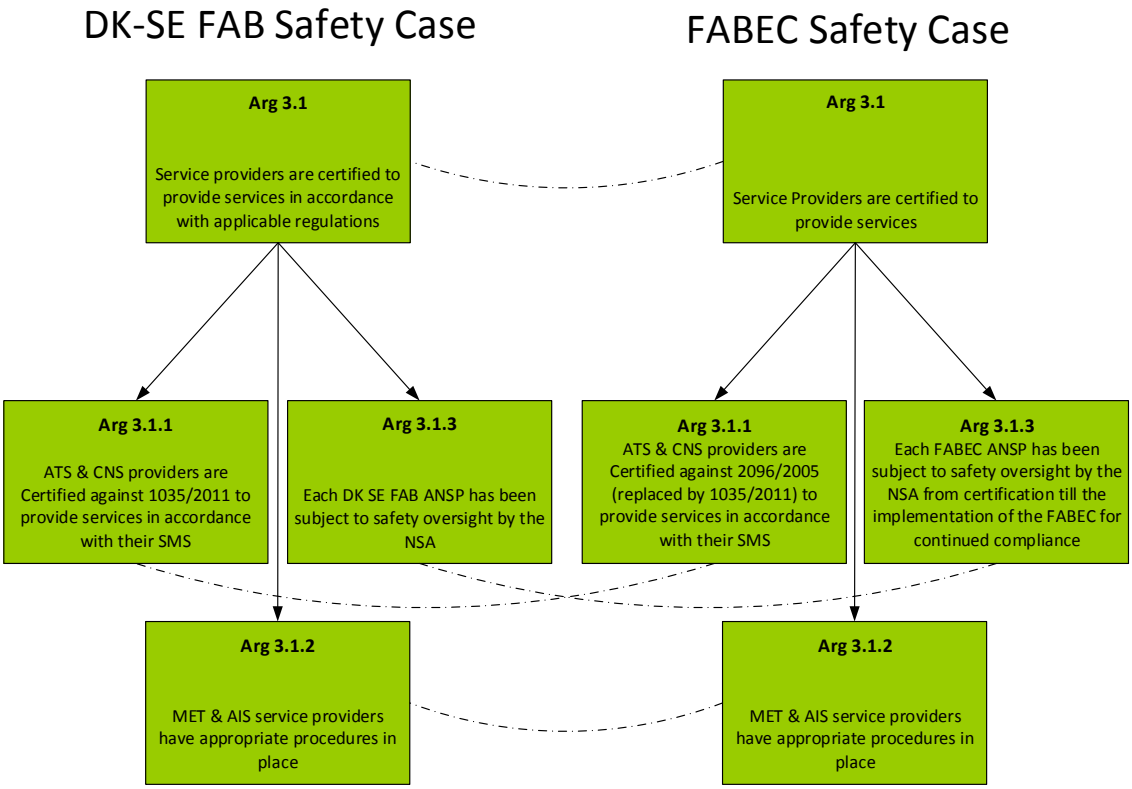

Figure 10 The same arguments with the same sub arguments

There might be cases in which the same arguments had different sub-arguments. Apart from different decomposition there can be many fallacies an author of an assurance case can introduce. Several fallacies according to [18] can have impact to the method:

- Association fallacy – statement contains statement that a system contains properties of an another system just because of the fact that two systems are related somehow,
- Genetic fallacy – justification of an argument merely by the subject's origins,
- Oversimplification – relevant information in argument is omitted,
- Ambiguity – argument has more than one meaning,
- Equivocation – the meaning of a term is shifted between arguments,
- Vagueness – an argument uses a term that is poorly defined.

Although an argument with no sub-arguments should not be colored in green, this method does not consider relations of argumentation hierarchy. An example of this case is presented in Figure 11.

It is worth mentioning that the same arguments can be used in different context of a assurance case but their meaning is always the same.

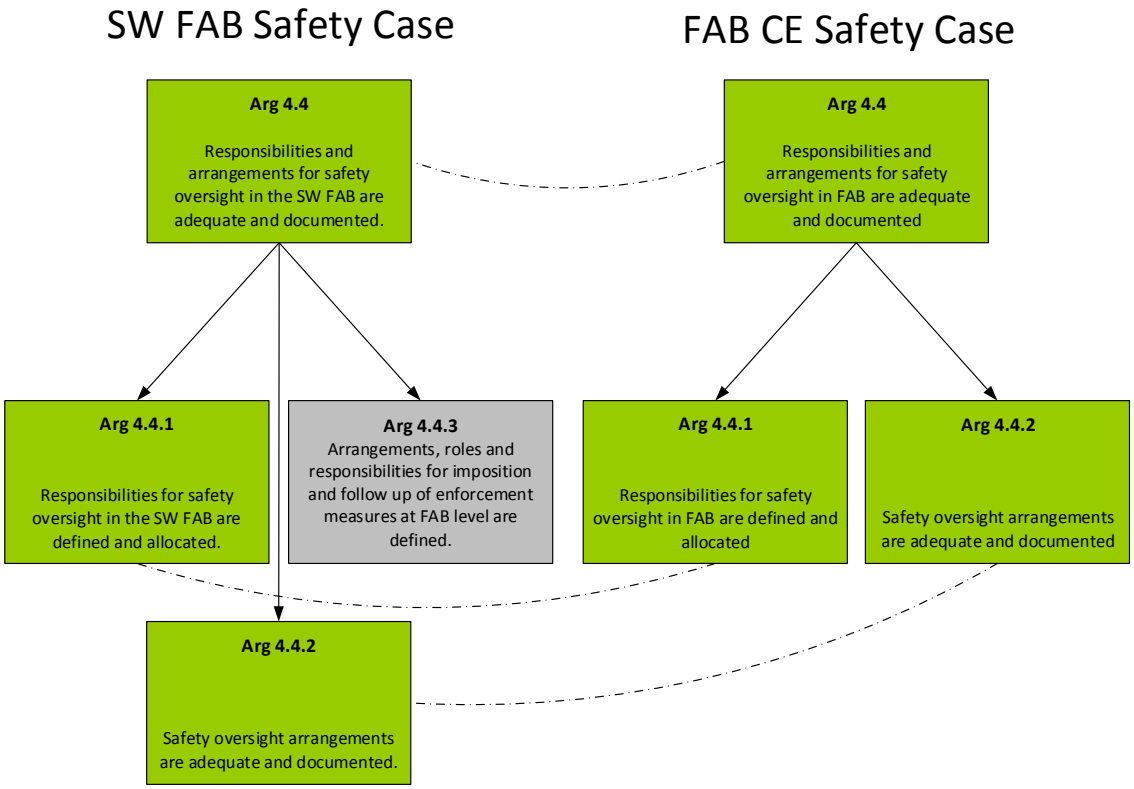

Figure 11 The same arguments with different sub-arguments

In many cases some arguments can have similar meaning. By similar it means that both arguments are related but there is too big difference to mark them as the same. It can be caused in insufficient coverage of the problem – one of the statements does not cover all the facts from the other one.

An example of two similar arguments is presented in Figure 12.

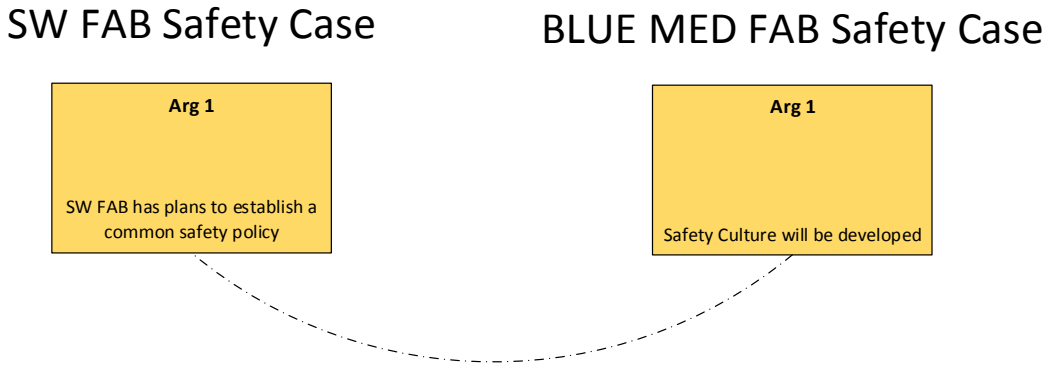

Figure 12 Two similar arguments

Sometimes a statement from a single argument in one Safety Case can be mapped by more than one argument in other Safety Case. To emphasize this case one argument is marked as identical and the rest is marked as equivalent as presented in Figure 13. This example can be often found when comparing Safety Cases.

The most notable examples can be found in between UK-Ireland FAB Safety Case and SW FAB Safety Case.

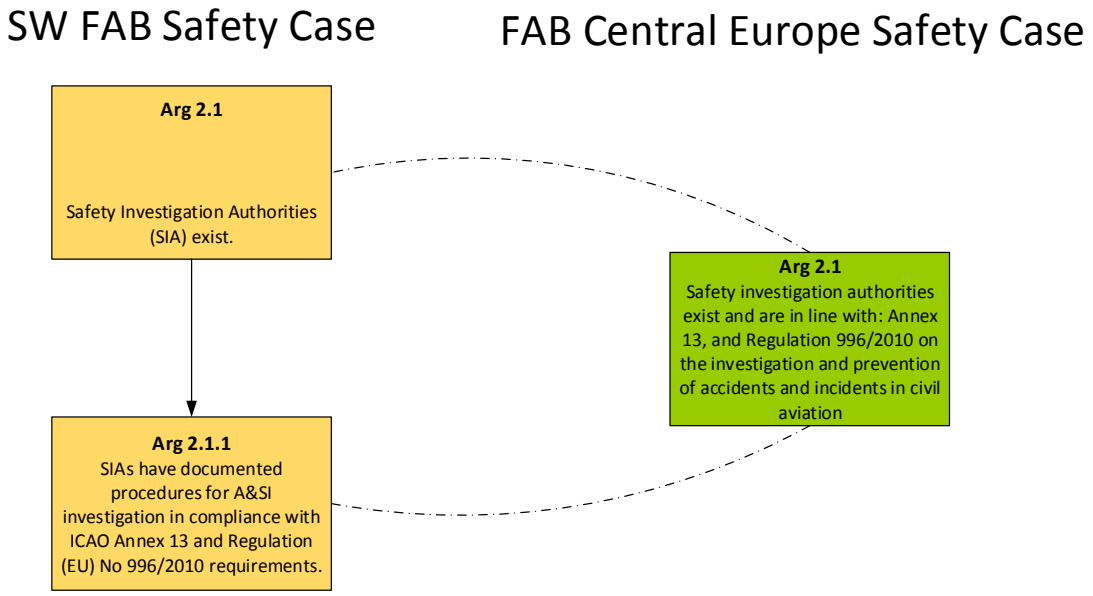

Figure 13 Two arguments connected with one argument

Let's consider more complex case in which there are two equivalent or the same arguments, the first one has direct descendants and analogous or the same elements to them in another AC are placed on different level of argumentation and are not connected to parent's analogous argument. Figure 14 presents an example of this problem in which equivalent elements are on different level of argumentation.

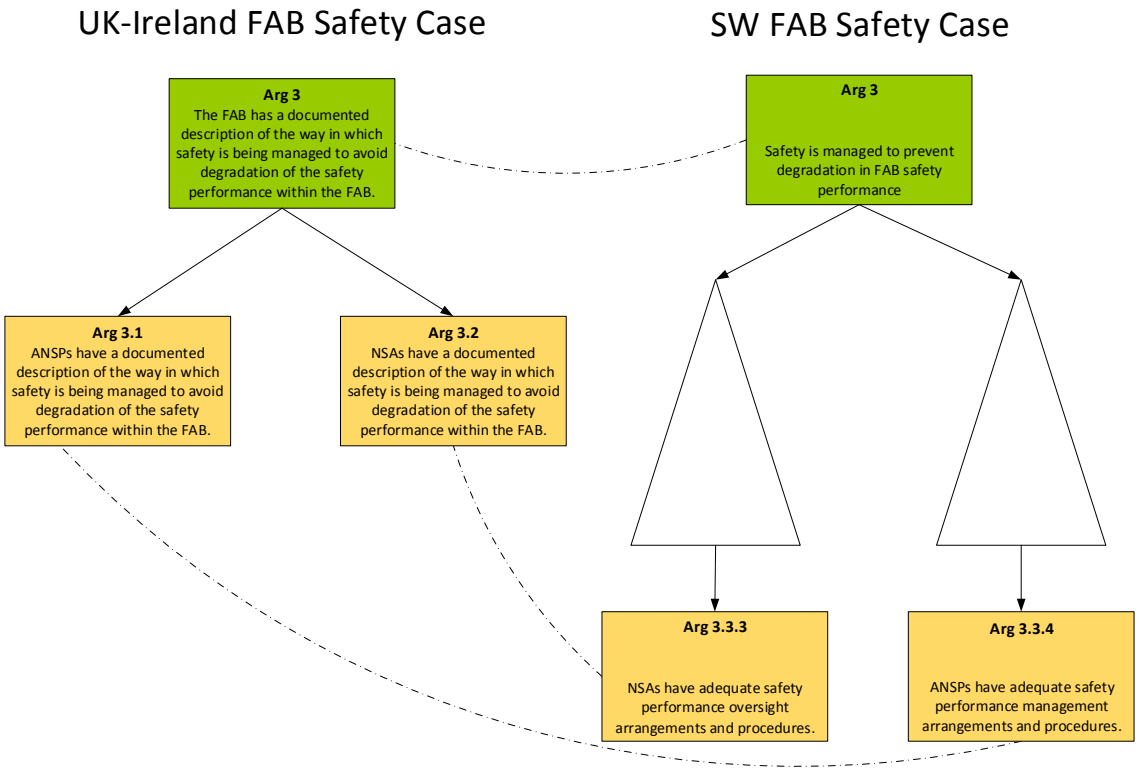

Figure 14 Similar arguments in different parts of a tree

It is also possible that even two arguments that have not a common argument, have common descendants. In Figure 15 two unrelated arguments have similar descendants.

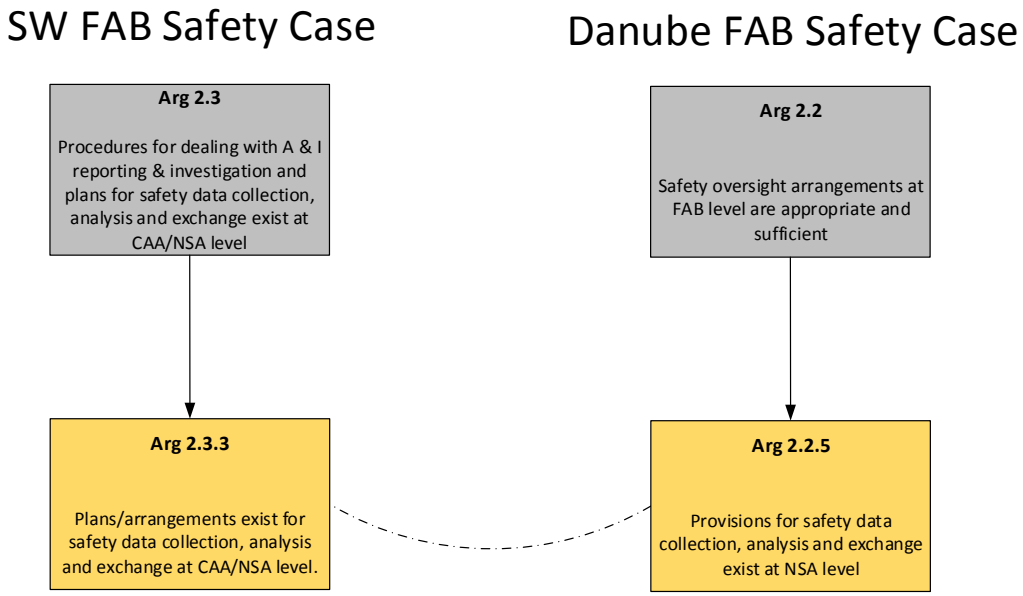

Figure 15 The same arguments originating from unrelated arguments

As it can be seen in Figure 16, one argument can have connection to more than

one argument in which all of them create a path on an argumentation tree. In this case, all elements on the path should be marked as similar.

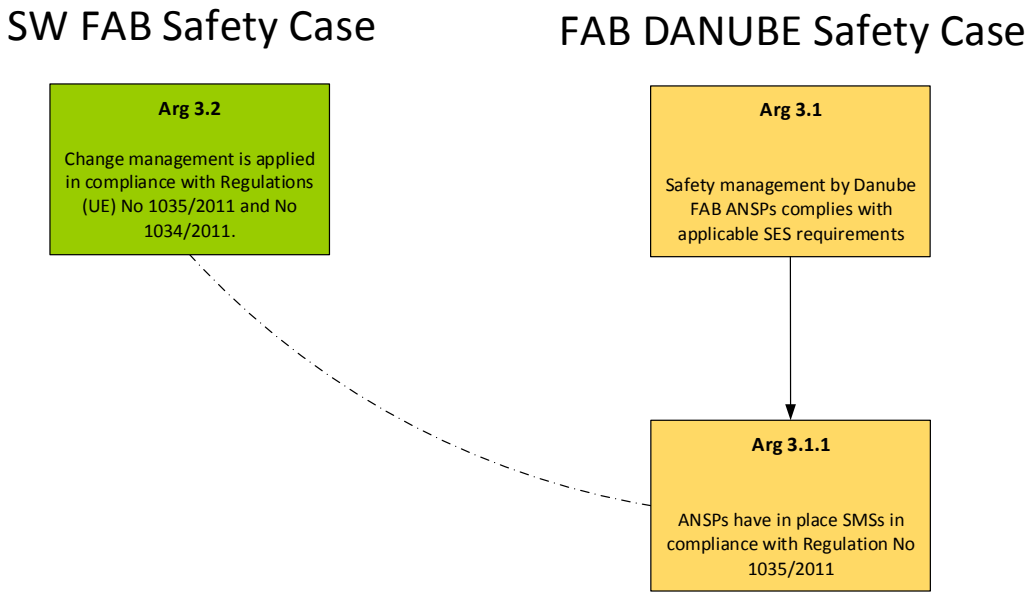

Figure 16 Similar ancestor and descendant

There are also cases in which an argument has multiple connections to the same or equivalent arguments. In this case the argument could be marked as the same or equivalent but to ease the process, only the equivalent kind of argument's similarity should be presented. Figure 17 visualizes this problem.

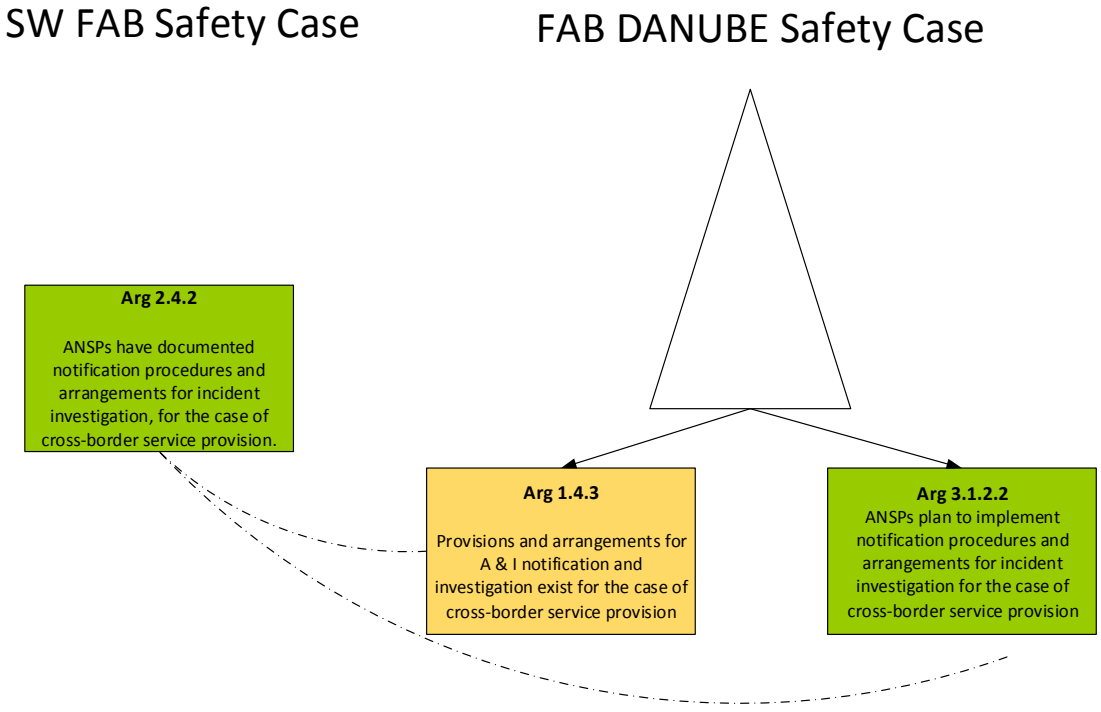

Figure 17 Many kinds of common arguments

4.3.2. Formalization

For the need of comparing many similar Safety Cases an algorithm which connects analogous arguments was created. It links the most similar arguments in one of two levels of relationship: the same or equivalent.

Definitions from thematic comparison method are valid and used also here in this method definitions. Formalized definition of the first algorithm is presented in Listing 2. It starts with top-level argument and ends when all of elements in assurance case are processed.

Definition 3 (Types of equivalence)

Assurance cases statements are not always equal and a classification mechanism for distinguishing their type of equivalence is proposed here. In this Thesis three relation classifications are distinguished:

- 1 – identical arguments,
- ½ – equivalent arguments,
- 0 – no equivalence at all.

The meaning of words *equal* and *equivalent* is not precisely defined. Each implementation of the algorithm should have it defined.

Having defined kinds of similarity let define a function $\sigma: (A, A) \rightarrow \mathbb{S}$, for each pair of arguments it assigns a label from scale $\mathbb{S}$. As stated before, for the purpose of the Thesis $\mathbb{S} = \{0, ½, 1\}$.

Although the meaning of the words used in the definition is not strictly defined, function σ should have either precise definition or it should be processed manually.

Definition 4 (Comparison of arguments).

Having defined Assurance Case, define a similarity of arguments $\mathcal{S}_{\mathcal{A}}$ which is a tuple $\langle \mathbb{A}, \rightarrow, l, m \rangle$, where $\mathbb{A} = \{\mathcal{A}_1, \mathcal{A}_2\}$, $A_1 \in \mathcal{A}_1$ and $A_2 \in \mathcal{A}_2$, whereas function $\rightarrow : \langle A_1, A_2 \rangle$ connects arguments between sets A_1 and A_2 that belongs to two different $\mathcal{A}$.

$l : (\rightarrow) \rightarrow \mathbb{S}$ is a labeling function that for each edge assigns a specific kind of similarity (weight) v.

$m : A \rightarrow \mathbb{S}$ gives for each argument kind of similarity based on connections in $\mathcal{S}_{\mathcal{A}}$. It returns the biggest value assigned from function l on the argument.

$\mathcal{S}_{\mathcal{A}}$ is a directed hypergraph, that is, a graph where edges (in this case

arguments) have multiple vertices.

Definition 5 (Finding similar arguments).

Giving the basic definitions, the algorithm for finding similar arguments in assurance cases is as follows:

Listing 3 Finding similar arguments

```
Find_arguments(𝔸: {𝒜1, 𝒜2}, 𝒮𝒜: digraph with equivalent arguments)
begin
  assign at ← root(𝒜1)
  Analyze_argument (at, 𝒜2, 𝒮𝒜,)
end

Analyze_argument(at, 𝒜2, 𝒮𝒜)
begin
  for each argument a in 𝒜2
    assign v ← σ(at, a)
    if v ≠ 0
      update 𝒮𝒜 ← 𝒮𝒜 ∪ ⟨{at, a}, v⟩
    end if
  end for
  for each children argument ac in at
    Analyze_argument (ac, 𝒜2, 𝒮𝒜,)
  end for
end
```

The algorithm from Definition 3 adds connections between assurance cases. It defines two functions:

- `Find_arguments` - The main function responsible for analyzing all of the arguments,
- `Analyze_argument` - Recurrent function which traverse over $\mathcal{A}_1$ to find equivalent arguments.

After the whole process is done, the result stored in $\mathcal{S}_{\mathcal{A}}$ can be visualized. Figure 18 presents a miniature of the results of the algorithm between SW FAB Safety Case and UK-Ireland Safety Case.

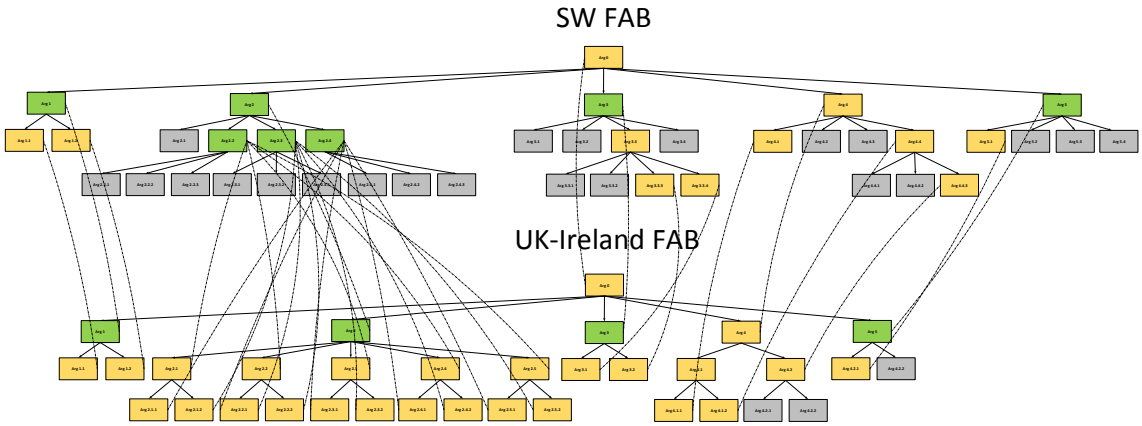

Figure 18 Miniature of the result of the algorithm

4.3.3. Analysis of the method

Table 4 presents the results of an analysis of the requirements stated at the beginning of the Thesis. All of the requirements are satisfied, and thus a test using FAB safety cases can be conducted.

Table 4 The anlysis of the second method

No.	Requirement	Result
1	Analyzed assurance cases must concern the same subject.	Yes, the method tries to find a general similarities between assurance cases using arguments.
2	A method should identify related elements.	Yes, the method tries to find similarities in argumentation between assurance cases.
3	It is possible to present related elements in a form of a mapping.	Yes, the output of the method is a mapping of related arguments.
4	Each element in the result need to relate to a concrete element/s in AC.	Yes, the resulting mapping connects concrete elements in assurance cases.
5	There is no technical dependencies e.g. identifiers are not taken into account in a method.	Yes, the method is based only on argument's statement and connections.

4.4. Arguments comparison method application

The method defined in Section 4.3 was used to conduct a comparison of nine of

the FAB Safety Cases. All of them are presented in Appendix A. Each comparison is presented on two diagrams: first with arguments, their connections and marked equivalent arguments, and the second with marked connections indicating equivalence between safety cases. They are presented as dash-dotted line.

4.4.1. Analysis of the results

Each of the comparison was conducted by the author of the Thesis. The amount of time and effort was different for each of the comparison and it was related to the size of compared assurance cases.

It varied from about 15 minutes on DK-SE FAB Safety Case vs. FABEC Safety Case comparison to about 4 hours for comparison of SW FAB Safety Case vs. Danube FAB Safety Case.

The method gives two important information:

- Coverage of arguments between two assurance cases,
- Placement of arguments from one assurance case to another.

For the check of the method seven comparisons between FAB safety cases were made. Each sub-section below describes the results of the test including a table with a summary containing amount of elements of specific type.

Level of similarities between each of the argument was determined by the author of the Thesis.

4.4.1.1. SW FAB Safety Case vs. FAB Central Europe Safety Case

As it can be seen in the diagram, there is strong similarity between arguments in those safety cases. 88% of those arguments were marked as *the same*. In addition the placement of the arguments is almost the same. The summary of elements grouped by type of similarity is presented in Table 5.

The only differences are very minor and it is easy to see that SW FAB Safety Case contains more arguments (6:1) (and possibly more information) marked as *not similar* than FAB Central Europe Safety Case.

Table 5 SW FAB Safety Case vs. FAB Central Europe Safety Case summary

Safety Case FAB	Identical	Equal	Different	Total
SW FAB	32	2	6	40
FAB CENTRAL EUROPE	33	0	1	34

4.4.1.2. SW FAB Safety Case vs. NEFAB Safety Case

In the case of comparison of the SW FAB Safety Case and NEFAB Safety Case it is easy to see that the second SC contains the first Safety Case starting from Argument 1. The only exception is Arg. 5 from SW FAB Safety Case which was not found to have common arguments in another safety case.

Additionally, Arg. 2 and Arg. 3 and their descendants from NEFAB Safety Case does not have any common arguments. Because of that 21 elements of this safety case is marked as *different* as present in Table 6.

Table 6 SW FAB Safety Case vs. NEFAB Safety Case summary

Safety Case FAB	Identical	Equal	Different	Total
SW FAB	31	0	9	40
NEFAB	31	1	21	34

4.4.1.3. SW FAB Safety Case vs. Baltic FAB Safety Case

According to the algorithm SW FAB Safety Case and Baltic FAB Safety Case have almost the same arguments. The only exception is Arg. 4.4.4 from Baltic FAB Safety Case – it is not connected to any other argument. This case is present in Table 7.

Table 7 SW FAB Safety Case vs. Baltic FAB Safety Case summary

Safety Case FAB	Identical	Equal	Different	Total
SW FAB	40	0	0	40
BALTIC FAB	40	0	1	41

4.4.1.4. DK-SE FAB Safety Case vs. FABEC Safety Case

Looking at comparison between DK-SE FAB Safety Case and FABEC Safety Case it looks like arguments from DK-SE FAB Safety Case are an excerpt of the other one. About 21% of arguments in the first SC are included in the second safety case as presented in Table 8.

Table 8 DK-SE FAB Safety Case vs. FABEC Safety Case summary

Safety Case FAB	Identical	Equal	Different	Total
DK-SE FAB	8	0	0	8

FABEC	8	0	31	39

4.4.1.5. SW FAB Safety Case vs. Danube FAB Safety Case

The comparison of these safety cases is more complicated than the previous ones. It can be stated that there are no common bigger hierarchies of arguments that are shared between those two safety cases.

Only about 23% of the arguments were stated to be the same. In addition, many of the arguments are not common and are distributed very uniformly. The summary of the comparison is presented in Table 9.

Table 9 SW FAB Safety Case vs. Danube FAB Safety Case summary

Safety Case FAB	Identical	Equal	Different	Total
SW FAB	12	16	12	40
DANUBE FAB	13	21	30	34

4.4.1.6. SW FAB Safety Case vs. BLUE MED FAB Safety Case

Applying the comparison algorithm on SW FAB Safety Case and BLUE MED FAB Safety Case found none of arguments to be the same and only about 16% of them to be similar. The rest of them is not common. This anomaly is present in Table 10.

Table 10 SW FAB Safety Case vs. BLUE MED FAB Safety Case summary

Safety Case FAB	Identical	Equal	Different	Total
SW FAB	0	6	34	40
BLUE MED FAB	0	8	39	47

4.4.1.7. SW FAB Safety Case vs. UK-Ireland FAB Safety Case

The last comparison presents a case in which almost all of the arguments in UK-Ireland Safety Case is similar to arguments in SW FAB Safety Case but only 45% of the arguments in SW FAB Safety Case have common arguments in UK-Ireland Safety Case (Table 11).

This inequality is caused by the fact that Arg. 2.2, 2.3 and 2.4 from SW FAB Safety Case have from five to six connections to the other safety case. It means that about half of the arguments can be mapped to almost all of the arguments from UK-

Ireland Safety Case.

Table 11 SW FAB Safety Case vs. UK-Ireland FAB Safety Case summary

Safety Case FAB	Identical	Equal	Different	Total
SW FAB	7	11	22	39
UK-Ireland FAB	4	26	3	33

4.4.2. Potential problems

The method allows creating many comparisons. Their amount given n assurance cases can be expressed mathematically as the triangular number:

$$N = \frac{n(n-1)}{2}.$$

For a comparison of a bigger amount of assurance cases, it might be hard for a single person to conduct full comparison using this method e.g. for full FAB safety cases comparison it is needed to perform 36 comparisons.

To ease this problem it is encouraged to use the results from the first method as described in the next section.

5. Comparison of the two methods

These methods, although showing different level of detail, are based on arguments and thus a correlation between them can be found. The first method is able to group assurance cases by their existence or absence of thematic groups. As it can be seen in Table 2, two groups of safety cases can be distinguished. The first group consists of four safety cases:

- Baltic FAB Safety Case,
- FAB Central Europe Safety Case,
- SW FAB Safety Case,
- UK-Ireland Safety Case.

The second group is smaller, contains three safety cases:

- DANUBE FAB Safety Case,
- DK-SE Safety Case,
- FABEC Safety Case.

It was observed that when safety cases in the same group were compared using the second method contained more the same arguments than elements from different groups.

As stated in previous paragraph, because of the fact that the number of diagrams is proportional to the square of the number of assurance cases for the purpose of the FAB safety cases comparison only selected number of comparisons was made.

The comparisons stated below were selected from the first method:

- SW FAB Safety Case – FAB Central Europe Safety Case,
- SW FAB Safety Case – Baltic FAB Safety Case,
- SW FAB Safety Case – UK-Ireland Safety Case,
- DK-SE Safety Case – FABEC Safety Case.

The rest of the comparisons were made after analysis of safety cases to check if there are some similarities.

An interesting fact is SW FAB Safety Case – NEFAB Safety Case comparison which shows serious similarity but the first method did not presented it. It is caused because of the fact that four of the first level arguments from SW FAB Safety Case are located a level lower in NEFAB Safety Case.

The rest of the comparisons (SW FAB Safety Case – DANUBE FAB Safety Case and SW FAB Safety Case – BLUE MED FAB Safety Case) present a level of

similarity but it is not as systematic as the rest of the comparisons.

5.1. Top-level claim comparison

As shown in Table 12, for all of the FABs have top-level goal defined differently, although some of them are similar. Baltic FAB Safety Case, FAB CE Safety Case and SW FAB Safety Case states that established *safety management* and *safety oversight* will provide safe services provision.

Because of lack of description of these terms, a short description is provided here. The term *safety management,* according to ICAO Doc 9859 [19], means that an organization recognized all safety risks and they were acceptably reduced or eliminated. To introduce this approach, Safety Management System (SMS) is created. EUROCONTROL provides guidance on creating and maintaining SMS in ESARR 3 SMS Framework. This document has been also used in EU Commission Regulation No 2096/2005 [20] which mandates Safety Management System in every ATM in all member states of the EU.

To explain the term *safety oversight* a citation from EU Commission Regulation No 1315/2007 [21] is presented:

National supervisory authorities shall exercise safety oversight as part of their supervision of requirements applicable to air navigation services as well as to ATFM and ASM, in order to monitor the safe provision of these activities and to verify that the applicable safety regulatory requirements and their implementing arrangements are met.

This regulation places requirement on every ATM belonging to EU Member States to implement service monitoring and ensure consistency between the European and state law and reality.

Top level claim in SW FAB Safety Case, FAB Central Europe Safety Case and Baltic FAB Safety Case defines *safety management* and *safety oversight*.

UK-Ireland FAB Safety Case top-level goal looks very similar to the goals described above, but it refers only to *safety management*.

The rest of reviewed FABs (Danube FAB, DK-SE FAB FABEC, BLUE MED FAB and NEFAB safety cases) as a top-level claim provide general statement that service provision within FAB is and/or will be safe.

Presented in this section grouping is shown in Table 12 in *Similarity group no* column and is equal to grouping observed in the resulting Table 2.

Table 12 FABs top-level goals

FAB	Top-level claim (identifier and statement)	Similarity group no
Baltic FAB	**G0** Baltic FAB safety management and oversight arrangements are sufficient and appropriate to enable safe ANS provision.	1
FAB CE	**G0** FAB CE safety management and oversight arrangements are sufficient and appropriate to meet IR requirements.	1
SW FAB	**G0** SW FAB safety management and oversight arrangements are sufficient and appropriate to enable safe ANS provision.	1
UK-Ireland FAB	**Goal 0** FAB Safety Management arrangements are sufficient and adequate.	2
Danube FAB	**Arg 0** ANS provision in the Danube FAB will remain safe.	3
DK-SE FAB	**G0** DK-SE FAB is operational and safe and will remain safe.	3
FABEC	**G0** FABEC is safely implemented and will remain safe.	3
BLUE MED FAB	**Arg 0** The FAB will be implemented in a manner which is acceptably safe.	3
NEFAB	**Arg 0** NEFAB is and will be maintained acceptably safe.	3

5.2. First-level arguments

This section describes the first level of decomposition of safety case. As stated in previous sub-section the mandatory of FAB safety case is stated by Regulation (EC) No 550/2004 [13] and Regulation (EC) No 176/2011 [17]. The latter Regulation defines

five elements that must be provided in safety case.

Four of the FAB safety cases (group 1 in Table 13) (Baltic FAB, FAB CE, SW FAB and UK-Ireland FAB) put these elements into first-level arguments.

The next three safety cases belonging to Danube FAB, DK-SE FAB and FABEC divide top-level goal into *regulatory framework*, *safety oversight* and *safety management*.

BLUE MED FAB takes different approach. It defines that the safe implementation consists of three main parts: *safety culture*, *safety* in general and *safety oversight*.

On the opposite, Arg. 1 in NEFAB safety case is equivalent to the top-level argument of Baltic FAB, SW FAB and FAB CE. The next argument could satisfy fifth requirement of the Regulation (EC) No 176/2011 [17]. The last one provides information that on-going operations are acceptably safe.

Table 13 FAB first-level arguments

FAB	**First-level arguments (identifier and statement)**	**Similarity group no**
Baltic FAB	**G1** Baltic FAB has a common safety policy **G2** Arrangements for reporting and investigation of Accidents and Serious Incidents, including data collection, analysis and exchange are adequate **G3** Safety performance is managed for continuous improvement **G4** Adequate arrangements exist and responsibilities are assigned for safety targets setting and safety oversight **G5** Operational changes resulting from FAB establishment and modification are subject to adequate safety assessment	1
FAB CE	**G1** FABCE has a common safety policy or plans to establish a common safety policy **G2** Adequate arrangements exist for reporting & investigation of A & I, including data collection, analysis	1

	and exchange **G3** Safety performance is managed to prevent degradation in FAB safety performance **G4** Adequate arrangements exist and responsibilities are assigned for safety targets setting and safety oversight **G5** Changes in ATM functional systems resulting from FAB establishment and modification are subject to adequate safety assessment	
SW FAB	**G1** SW FAB has plans to establish a common safety policy **G2** Adequate arrangements exist for reporting & investigation of A & I, including data collection, analysis and exchange **G3** Safety is managed to prevent degradation in FAB safety performance **G4** Adequate arrangements exist and responsibilities are assigned for safety targets setting and safety oversight **G5** Operational changes resulting from FAB establishment and modification are subject to adequate safety assessment	1
UK-Ireland FAB	**Goal 1** The FAB has a documented common safety policy or plans to establish a common safety policy **Goal 2** The FAB has a documented description of the arrangements dealing with accident and incident investigation and plans on how to address safety data collection, analysis and exchange **Goal 3** The FAB has a documented description of the way in which safety is being managed to avoid degradation of the safety performance within the FAB **Goal 4** The FAB has a documented description of the arrangements clearly identifying and allocating the responsibilities and interfaces with relation of the setting	1

	of safety targets, safety oversight and the accompanying enforcement measures in regard to the provision of air navigation services within the FAB **Goal 5** The FAB has documentation and/or statements that the safety assessment including hazard identification and mitigation has been conducted before introducing operational changes resulting from the establishment of modification of the FAB	
Danube FAB	**Arg 1** Regulatory framework applicable to Danube FAB is sufficient and appropriate to enable safe ANS provision **Arg 2** Safety oversight in Danube FAB is sufficient and appropriate to enable safe ANS provision **Arg 3** Safety management in Danube FAB is sufficient and appropriate to enable safe ANS provision	2
DK-SE FAB	**G1** DK-SE FAB regulatory framework is appropriate **G2** The safety oversight of the DK-SE FAB is coordinated and appropriate **G3** Service provision within DK-SE is and will remain safe	2
FABEC	**G1** FABEC Regulatory Framework is appropriate for the safety rulemaking of FABEC **G2** There is appropriate safety oversight of ANSPs and coordinated oversight of the FABEC **G3** Service Provision within FABEC is safe and will remain safe[5]	2
BLUE MED FAB	**Arg. 1** Safety Culture will be developed **Arg. 2** Safety will be managed **Arg. 3** Safety oversight on ATM/ ANS will be provided	3

[5] FABEC placed a strategy between each first-level argument and top-level goal. This table does not take these strategies into account.

	in a coordinated manner	
NEFAB	**Arg 1** NEFAB safety management and oversight arrangements are sufficient and appropriate to enable safe NEFAB declaration **Arg 2** All changes are managed in safe and systematic way **Arg 3** NEFAB on-going operations are acceptably safe	4

5.3. Arguments decomposition

This section presents a manual way arguments can be connected to each other. Tables 14-18 present grouped FAB safety cases' arguments in terms of equality. In order to create these tables every assurance case needs to be analyzed.

The process is analogous to the second method and is as follows:

- Analyze each of the assurance case,
- During the process of analysis, try to find out common parts from all of the previous analyzed assurance cases,
- For each of the common part of the assurance case create separate table in which the same parts of the assurance cases will be stored.

Comparing these tables with the result of the second method gives the same results – arguments in the table are marked as either the same or there is no similar element.

Table 14 Baltic FAB, FAB CE, SW FAB and UK-Ireland FAB Arg. 1 decomposition

FAB	**Arguments (identifier and statement)**
Baltic FAB	**G1-1** The Baltic FAB Safety Policy is published **G1-2** A process exist to modify Baltic FAB Safety Policy
FAB CE	**G 1-1** The FABCE safety policy is approved at the ANSP level **G 1-2** NSA/States have plan to establish common safety policy **G 1-3** A process exist to modify FABCE safety policy

SW FAB	**G 1-1** Both Spain and Portugal have published safety policies and a process exists to modify their safety policies. **G 1-2** A process exists to establish and modify the SW FAB safety policy.
UK-Ireland FAB	**Goal 1-1** FAB Safety Policy is documented and published in the FAB SMM for ANSPs and the XXX for the NSA. **Goal 1-2** There is a defined and documented process for amending the FAB Safety Policy in the FAB SMM for ANSPs and the XXX for the NSA.
DANUBE FAB	**Arg 1-7-1** Provisions exist for the establishment of a FAB common safety policy **Arg 1-7-2** A plan exists to establish a FAB common safety policy

Table 15 Baltic FAB, FAB CE, SW FAB, UK-Ireland FAB Arg. 2 and NEFAB Arg. 1-2 decomposition

FAB	**Arguments (identifier and statement)**
Baltic FAB	**G2-1** Safety investigation authorities exist **G2-2** Provisions for reporting & investigation of Accidents and Serious Incidents as well as plans for safety data collection, analysis and exchange exist at the State level **G2-3** Procedures for dealing with A&I reporting & investigation and plans for safety data collection, analysis and exchange exist at CAA/NSA level **G2-4** Procedures for accident and incident reporting and incident investigation, and plans for safety data collection, analysis and exchange exist at ANSP Level
FAB CE	**G 2-1** Safety investigation authorities exist and are in line with: Annex 13, and Regulation 996/2010 on the investigation and prevention of accidents and incidents in civil aviation **G 2-2** Provisions for reporting & investigation of A & SI and plans for safety data collection, analysis and exchange exist at State level

	G 2-3 Procedures for dealing with A & I reporting & investigation and plans for safety data collection, analysis and exchange exist at NSA level **G 2-4** Procedures for occurrence reporting and investigation and plans for safety data collection, analysis and exchange exist at ANSP level
SW FAB	**G 2-1** Safety Investigation Authorities (SIA) exist. **G 2-2** Provisions for reporting and investigation of A&SI and plans for safety data collection, analysis and exchange exist at State level. **G 2-3** Procedures for dealing with A & I reporting & investigation and plans for safety data collection, analysis and exchange exist at CAA/NSA level **G 2-4** Procedures for A & I reporting and incident investigation, and plans for safety data collection, analysis and exchange exist at ANSP level
UK-Ireland FAB	**Goal 2-1** The FAB has a documented description for dealing with accident investigations. **Goal 2-2** The FAB has a documented description for dealing with incident investigations. **Goal 2-3** The FAB has documented plans on how to address safety data collection. **Goal 2-4** The FAB has documented plans on how to address safety data analysis. **Goal 2-5** The FAB has documented plans on how to address safety data exchange.
NEFAB	**Arg. 1-2-1** Safety Investigation Authorities (SIA) exist **Arg. 1-2-2** Provisions for reporting & investigation of A & SI [Accidents and Serious Incidents] and plans for safety data collection, analysis and exchange exist at State level **Arg. 1-2-3** Procedures for dealing with A & I reporting & investigation and plans for safety data collection, analysis and

	exchange exist at CAA/NSA level **Arg. 1-2-4** Procedures for A & I reporting and incident investigation, and plans for safety data collection, analysis and exchange exist at ANSP Level

Table 16 Baltic FAB, FAB CE, SW FAB Arg. 2-2 and NEFAB Arg. 1-2-2 decomposition

FAB	**Arguments (identifier and statement)**
Baltic FAB	**G2-2-1** AAIBs have documented procedures for Accidents and Serious Incidents Investigation, including data collection, analysis and reporting **G2-2-2** Documented notification procedures and arrangements for investigation of Accidents and Serious Incidents, including data collection, exist for cross-border service provision **G2-2-3** Plan / arrangements exist for safety data analysis and exchange at State/AAIB level
FAB CE	No decomposition
SW FAB	**G 2-2-1** SIAs have documented procedures for A&SI investigation in compliance with ICAO Annex 13 and Regulation (EU) No 996/2010 requirements. **G 2-2-2** Documented notification procedures and arrangements for A&SI investigation exist for the case of cross-border service provision. **G 2-2-3** Plans/arrangements exist for safety data collection, analysis and exchange at State/SIA level.
NEFAB	**Arg. 1-2-2-1** SIAs have documented procedures for A & SI investigation in compliance with Annex 13 and Regulation (EU) No 996/2010 requirements **Arg. 1-2-2-2** Plans / arrangements exist for safety data collection, analysis and exchange at State/SIA level

Table 17 Baltic FAB, FAB CE, SW FAB Arg. 2-3 and NEFAB Arg. 1-2-3 decomposition

FAB	**Arguments (identifier and statement)**
Baltic FAB	**G2-3-1** NSA have documented procedures for dealing with A & I reporting and investigation, including data collection **G2-3-2** Documented NSA notification procedures and arrangements exist for dealing with reporting and investigation of A & I, for the case of cross-border service provision and **G2-3-3** Plans / arrangements exist for safety data analysis and exchange at NSA level
FAB CE	No decomposition
SW FAB	**G 2-3-1** CAAs/NSAs have documented procedures for dealing with A&I reporting and investigation. **G 2-3-2** Documented CAA/NSA notification procedures and arrangements exist for dealing with reporting and investigation of A&I, for the case of cross-border service provision. **G 2-3-3** Plans/arrangements exist for safety data collection, analysis and exchange at CAA/NSA level.
NEFAB	**Arg. 1-2-3-1** CAAs/NSAs have documented procedures for dealing with A&I reporting and investigation **Arg. 1-2-3-2** Plans / arrangements exist for safety data collection, analysis and exchange at CAA/NSA level

Table 18 Baltic FAB, FAB CE, SW FAB Arg. 4-4 and NEFAB Arg. 1-4-4 decomposition

FAB	**Arguments (identifier and statement)**
Baltic FAB	**G4-4-1** Responsibilities for Safety oversight in Baltic FAB are defined and allocated **G4-4-2** Safety oversight arrangements are adequate and documented **G4-4-3** Arrangements roles and responsibilities for imposition and follow up of enforcement measures at FAB level are defined

	G4-4-4 ANSPs have documented procedures to support proper oversight and implementation of enforcement measures
FAB CE	**G 4-4-1** Responsibilities for safety oversight in FAB are defined and allocated **G 4-4-2** Safety oversight arrangements are adequate and documented
SW FAB	**G 4-4-1** Responsibilities for safety oversight in the SW FAB are defined and allocated. **G 4-4-2** Safety oversight arrangements are adequate and documented. **G 4-4-3** Arrangements, roles and responsibilities for imposition and follow up of enforcement measures at FAB level are defined.
NEFAB	**Arg. 1-4-4-1** Responsibilities for safety oversight in NEFAB are defined and allocated **Arg. 1-4-4-2** Safety oversight arrangements are adequate and documented **Arg. 1-4-4-3** Arrangements, roles and responsibilities for imposition and follow up of enforcement measures at NEFAB level are defined **Arg. 1-4-4-4** ANSPs have documented procedures to support proper oversight and implementation

5.4. Methods extension - evidence analysis

Methods described in Sections 4.2 and 4.3 concern argumentation analysis, but assurance case also consists of other kinds of elements including evidence. Evidence analysis is beyond the scope of the Thesis, this chapter discusses the possible extension of the argumentation analysis method.

5.4.1. Examples of the evidence

As it can be seen in the Appendix A, many of the leafs of the argumentation tree has similarities. This fact can be very helpful. As it can be seen in Figure 20 evidence

between the same arguments has similarities.

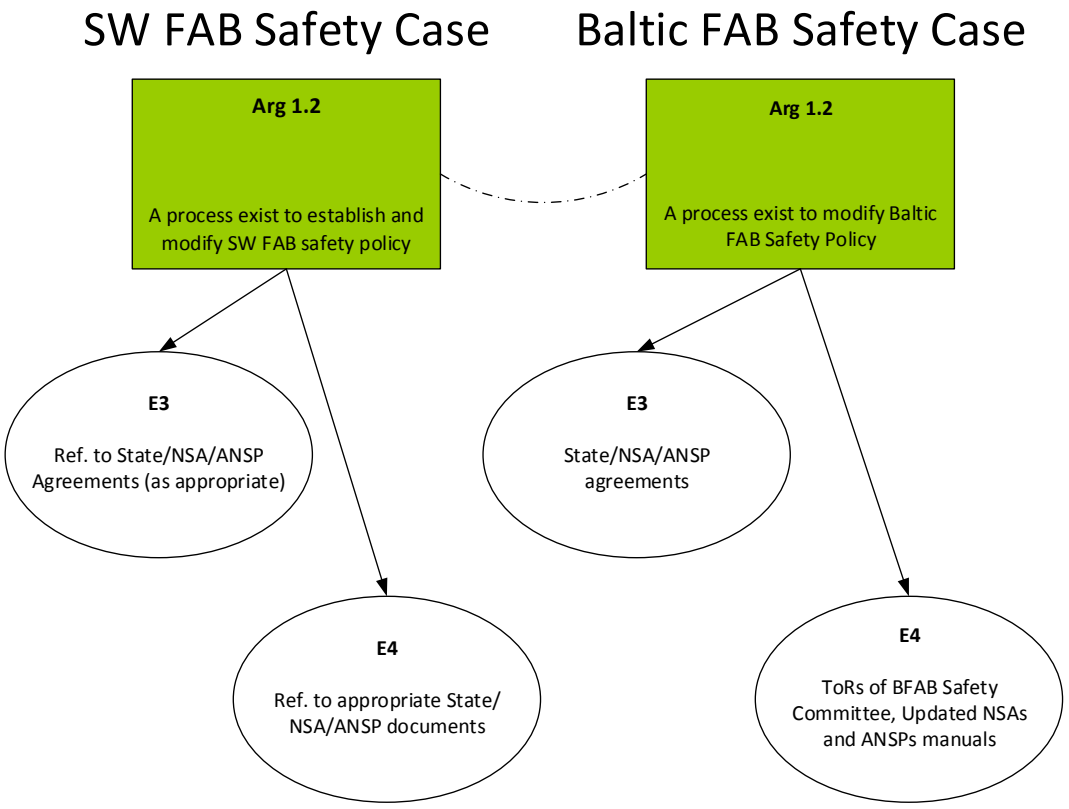

Figure 19 Evidence for the same arguments

In this example arguments are very general and this causes the similarity. In many cases general statements are described but in some of them it is not obvious.

Evidence 3 and 4 BALTIC FAB Safety Case is not defined in the document. SW FAB Safety Case defines it very precisely (19, parargaph 9.1.3.1) but from unknown reasons Evidence 3 and 4 from this safety case is duplicated.

Another example is presented in Figure 21. Definition of evidence 30 and 31 in SW FAB Safety Case is described in one section (19, sub-section 9.3.3) and states that the agreement betwee the Civil National Supervisory Authorities of the Republic of Portugal and the Kingdom of Spain, signed On May 17th 2012 by INAC, I.P. and AESA established a framework for cooperation which includes continouus compilance and safety oversight.

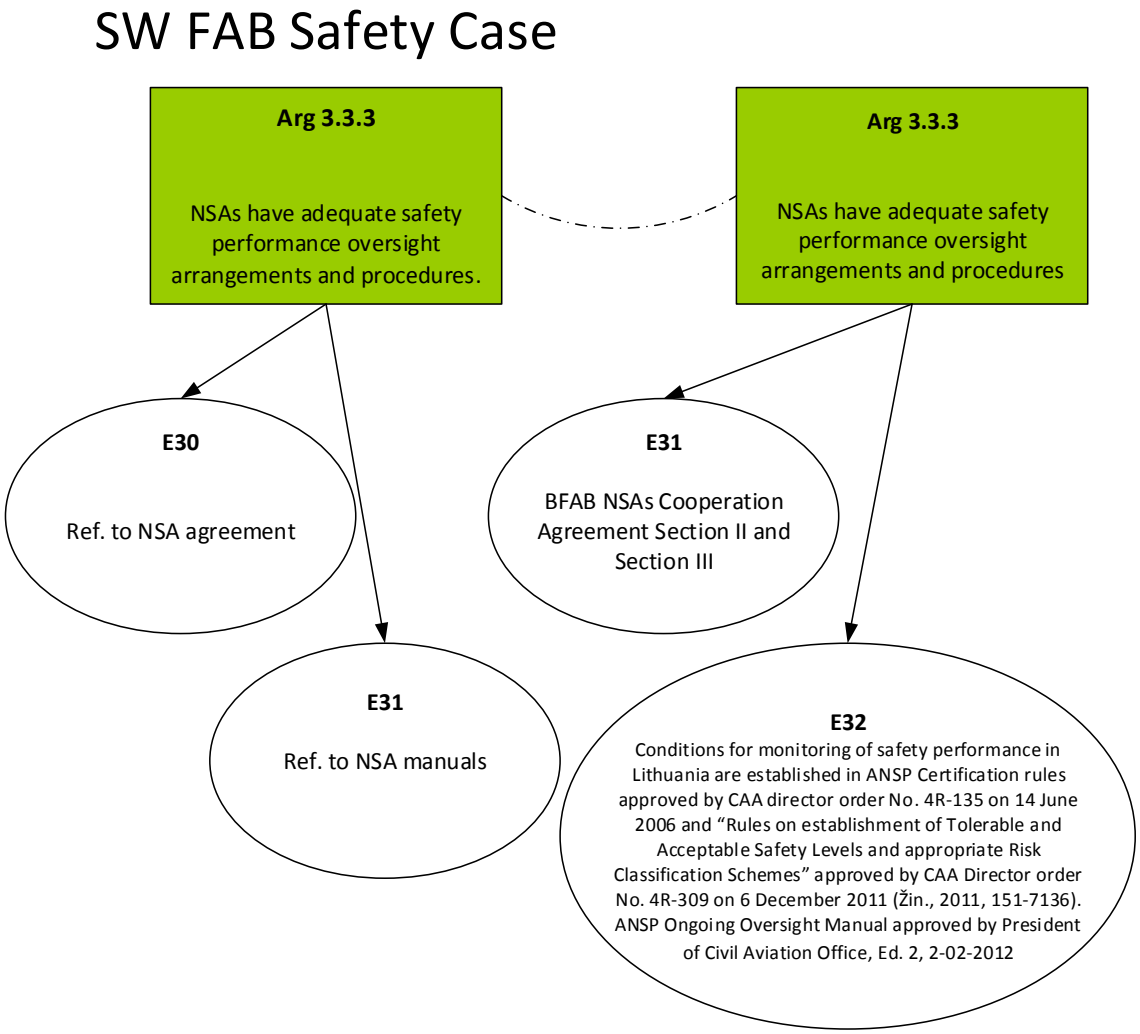

Figure 20 Evidence of the same arguments

By looking at these examples it it easy to notice that the argument's evidence can be very different. All the documents, agreements and acts are different in each FAB, so it require much effort to conduct a comparison which will result in useful results.

On the other hand the general statements which briefly describe evidence can be useful. Table 19 presents comparison of two similar arguments *Safety Policy is published* and *A process exists to modify Safety Policy*.

These two arguments were compared together because of the fact that in many cases they are presented in a form of one argument.

All of the nine safety cases were analyzed. Safety cases belonging to two of the FABs did not contain any evidence supporting Safety Policy argument:

- BLUE MED FAB Safety Case,
- DK-SE FAB Safety Case.

Table 19 Comparsion of the safety cases for safety policies

FAB	**Argument and Evidence**	
Baltic FAB	**Arg 1.1** The Baltic FAB Safety Policy is published	**Arg 1.2** A process exist to modify Baltic FAB Safety Policy
	- Multilevel (State/NSA/ ANSP) Safety Policy - Updated NSAs and ANSPs manuals	- State/NSA/ANSP agreements - ToRs of BFAB Safety Committee
NEFAB	**Arg 1.1.1** NEFAB common safety policy is published	**Arg 1.1.2** A process exist to modify NEFAB safety policy
	- Safety policy will be developed and published with close cooperation of all involved states.	- Safety policy is integral part of NEFAB SMS - NEFAB safety policy is document that is published by States. Refer to State/NSA/ANSP agreement for arrangements dealing with safety policy
BLUE MED FAB	Strategy 1.1 introduces Safety Policy, but it is not extended	
FAB CE	**Arg 1.1** The FABCE safety policy is approved at the ANSP level	
	- ANSPs Safety Policy - Safety Policies of 7 ANSPs NSA Cooperation agreement	

DANUBE FAB	**Arg 1.7.1** Provisions exist for the establishment of a FAB common safety policy	A plan exists to establish a FAB common safety policy
	- FAB State agreement	- SMS roadmap
FABEC	Evidence 32 describes that there is a Safety Policy, but yet is not officially signed and there is also a plan to modify this document.	
SW FAB	**Arg 1.2** A process exist to establish and modify SW FAB safety policy	
	- Listed State/NSA/ANSP Agreements - Listed State/NSA/ANSP documents	
UK-Ireland FAB	**Arg 1.1** FAB Safety Policy is documented and published in the FAB SMM for ANSPs and the XXX for the NSA.	**Arg 1.2** There is a defined and documented process for amending the FAB Safety Policy in the FAB SMM for ANSPs and the XXX for the NSA.
	- Common Safety Policy has been developed but not yet signed - The FAB SMM has been developed but not yet signed	- The process of changing Safety Policy is defined in the FAB SMM -
DK-SE FAB	No information	

6. Summary

The goal of this Thesis was to create comparative analysis methods for assurance cases which concern similar matter. To solve problem of assurance case comparison, two methods were developed:

- Thematic comparison, which gives an overview how assurance cases relate to each other,
- Arguments comparison, which gives in-depth information how one assurance case's arguments are similar to arguments in another assurance case.

For the tests FAB safety cases were used. It is a set of nine safety cases which concern safety of the process of establishing Functional Airspace Blocks over the European Union territories.

The safety cases were used to test two of the methods to assert their compliance with the goal and requirements. The results are as follows:

- Thematic comparison gives an overview about a scope of an assurance case in comparison to other assurance cases. Table 1 presents results of the method for FAB safety cases. In total ten thematic groups were discovered in different safety cases.
- Arguments comparison gives more in-depth information about assurance cases. Appendix A includes seven visualizations of the comparisons between arguments. For each of the comparison two safety cases were tested.

In the Thesis an analysis of the evidence based on FAB safety cases was conducted. The results showed that it is difficult and more complex than comparison of arguments and it requires further research to find out how effective this method is.

For the methods general algorithms are provided and it is possible to use this method by auditors who need to analyze similar assurance cases or be implemented in an expert system.

The results of the algorithm is a mapping which might be hard to understand and interpret by a reader. To ease this, a visualization models are developed together with the methods. The model of data representation for the thematic comparison is a table in which the columns represent tested assurance cases and each of the row defines a extracted thematic group.

All of these methods can be implemented in a software to automate the process of analysis although for each of the method there is a manual work to be conducted in

order to create a comparison:

- For thematic comparison method an extraction of thematic group from arguments statements need to be done by an expert who has an extensive knowledge about the subject of a safety case,
- For arguments comparison method also an expert is needed to be present to perform a classification of a pair of arguments from different assurance cases to one of a type of similarity.

7. Bibliography

1. **ISO/IEC.** 15026-1:2010 Systems and Software Assurance — Part 1: Concepts and Vocabulary. 2010.

2. **ISO/EIC.** 15026-2:2010 Systems and Software Assurance — Part 2: Assurance Case. 2010.

3. **European Organisation for the Safety of Air Navigation (EUROCONTROL).** Safety Case Development Manual. 2006.

4. **Origin Consulting (York) Limited.** GSN Community Standard Version 1. 2011.

5. **Object Management Group.** *Argumentation Metamodel (ARM).* 2010.

6. —. *Structured Assurance Case Metamodel (SACM).* 2013.

7. **United Kingdom Ministry of Defence.** 00-42 Reliability and Maintainability (R&M) Assurance Guidance Part 3. 2003.

8. *Integrated Analysis of Complex Safety Critical Systems.* **Wilson, Stephen and McDermid, John.** 1995, The Computer Journal.

9. **United Kingdom Ministry of Defence.** 00-56 Safety Management Requirements for Defence Systems. 2004.

10. **Kelly, Timothy Patrick.** *Arguing Safety – A Systematic Approach to Managing Safety Cases.* 1998.

11. **Convention on International Civil Aviation. Chicago : s.n., 1944.**

12. International Civil Aviation Organization (ICAO). ***Doc. 4444 Air Traffic Management Fifteenth Edition.*** **2007.**

13. European Parliament. ***Regulation (EC) No 550/2004 of the European Parliament and of the Council of 10 March 2004on the provision of air navigation services in the single European sky (the service provision Regulation).*** **2004.**

14. International Civil Aviation Organization (ICAO). ***Annex 11 to the Convention on International Civil Aviation, Air Traffic Services – Air Traffic Control Service, Flight Information Service and Alerting Service.*** **2001.**

15. European Organisation for the Safety of Air Navigation (EUROCONTROL). ***Air Traffic Management Strategy for the Years 2000+.*** **203.**

16. —. Risk Assessment and Mitigation in ATM. 2001.

17. European Commission. ***Commission Regulation (EU) No 176/2011 of 24 February 2011 on the information to be provided before the establishment and***

modification of a functional airspace block. **2011.**

18. Greenwell, William S. ***A Taxonomy of Fallacies in System Safety Arguments*** **. 2006.**

19. International Civil Aviation Organization (ICAO). ***Doc. 9859 Safety Management Manual (SMM) Second Edition.*** **2009.**

20. European Commission. ***Commission Regulation (EC) No 2096/2005 of 20 December 2005 laying down common requirements for the provision of air navigation services.*** **2005.**

21. —. ***Commission Regulation (EU) No 1315/2007 of 8 November 2007 on safety oversight in air traffic management and amending Regulation (EC) No 2096/2005.*** **2007.**

22. FAB CE Safety Subcommittee. FAB CE Safety Case. 2012.

23. Department of Civil Aviation of Cyprus. BLUE MED D3.2a – BLUE MED FAB SAFETY CASE – Part A: Regulatory aspects. 2012.

24. Safety Group within SQSE WG. DANUBE FAB Safety Case. 2012.

25. Sundell, Morgan. DK-SE FAB Safety Case. 2012.

26. Chairman Standing Committee Safety. FABEC Safety Case. 2012.

27. North European Functional Airspace Block. SAFETY CASE REPORT. 2011.

28. Safety Management Division, AENA. SW FAB Safety Case. 2012.

29. FAB, UK-Ireland. Documentation to confirm compliance with: COMMISSION REGULATION (EU) No 176/2011. 2012. Appendix E, F.

30. Emmet, Luke and Cleland, George. Graphical Notations, Narratives and Persuasion: a Pliant Systems Approach to Hypertext Tool Design. ***in Proceedings of ACM Hypertext 2002.*** **2002.**

31. (Poland), Civil Aviation Office and (Lithuania), Civil Aviation Administration. ***Baltic FAB Safety Case.*** **2012.**

32. The Railways and Other Guided Transport Systems (Safety) Regulations 2006, SI 2006/599.

33. Weinstock, Charles B., Goodenough, John B. and Hudak, John J. ***Dependability Cases.*** **s.l. : Carnegie Mellon University, 2004.**

34. Executive, Health and Safety. ALARP "at a glance". [Online] [Cited: 2013 08 05.] http://www.hse.gov.uk/risk/theory/alarpglance.htm.

35. ***No More Spineless safety Cases: A Structured Method and Comprehensive***

Tool Support for the Production of Safety Cases. **Wilson, S., et al. 1995.**

36. European Commission. ***European Commission Guidance Material for the Establishment and Modification of Functional Airspace Blocks (FAB), edition 2.0 of 08 December 2011, following the positive opinion (about Version 1.0) of the Single Sky Committee in its 38th session on 3 Dece.*** **2011.**

37. —. ***Commission Regulation (EC) No 2096/2005 of 20 December 2005 laying down common requirements for the provision of air navigation services.*** **2005.**

38. —. ***Commission Regulation (EC) No 1315/2007 of 8 November 2007 on safety oversight in air traffic management and amending Regulation (EC) No 2096/2005.*** **2007.**

39. National Aeronautics and Space Administration. ***NASA System Safety Handbook, Volume 1.*** **2011. Vols. Volume 1, System Safety Framework and Concepts for Implementation.**

7.1. Contents of the CD

`\Master thesis`

`Patryk Orwat - Master thesis.doc` – master thesis in MS Word format

`Patryk Orwat - Master thesis.pdf` – master thesis in PDF format

Appendix A: Comparisons of arguments

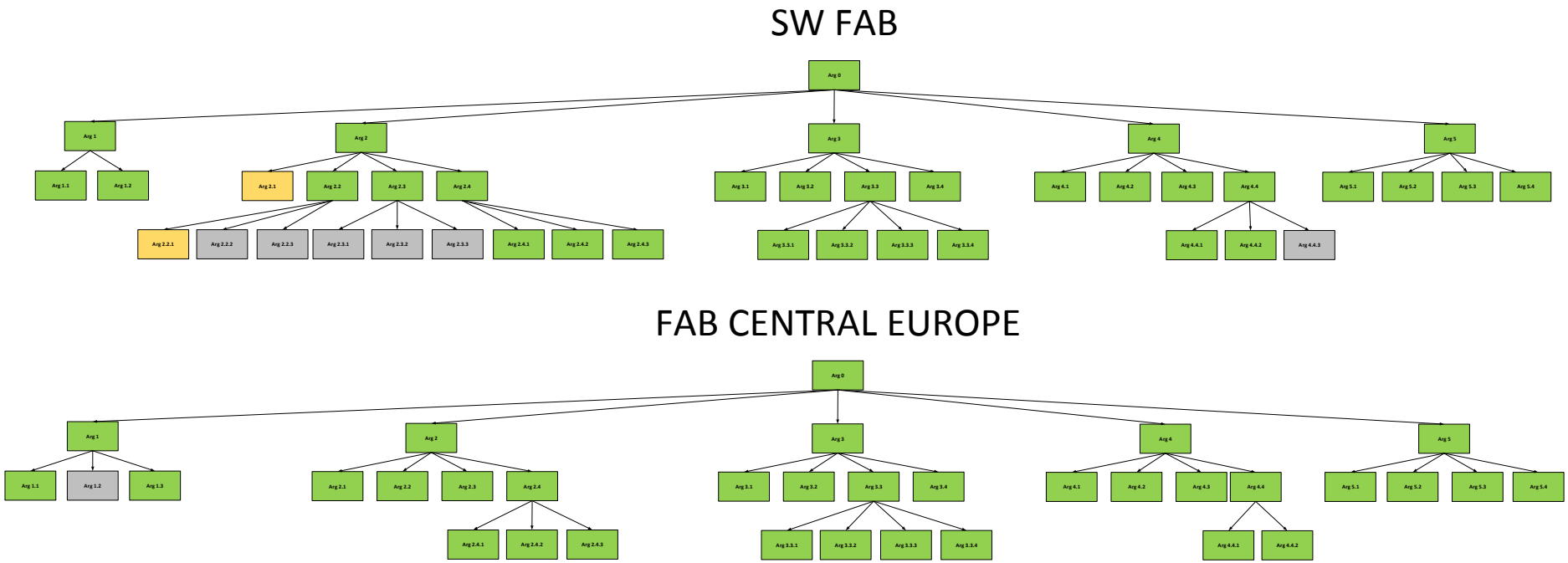

Figure 21 SW FAB Safety Case vs. FAB Central Europe Safety Case without connections between analogous elements

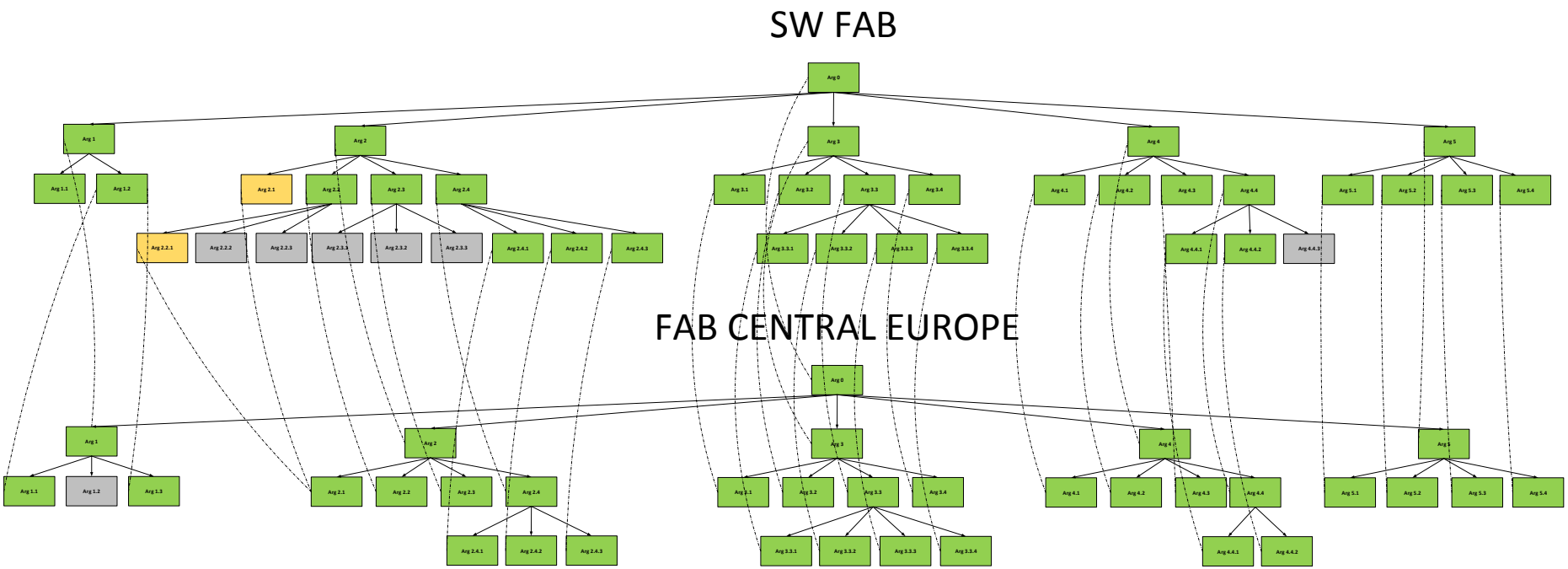

Figure 22 SW FAB Safety Case vs. FAB Central Europe Safety Case with connections between analogous elements

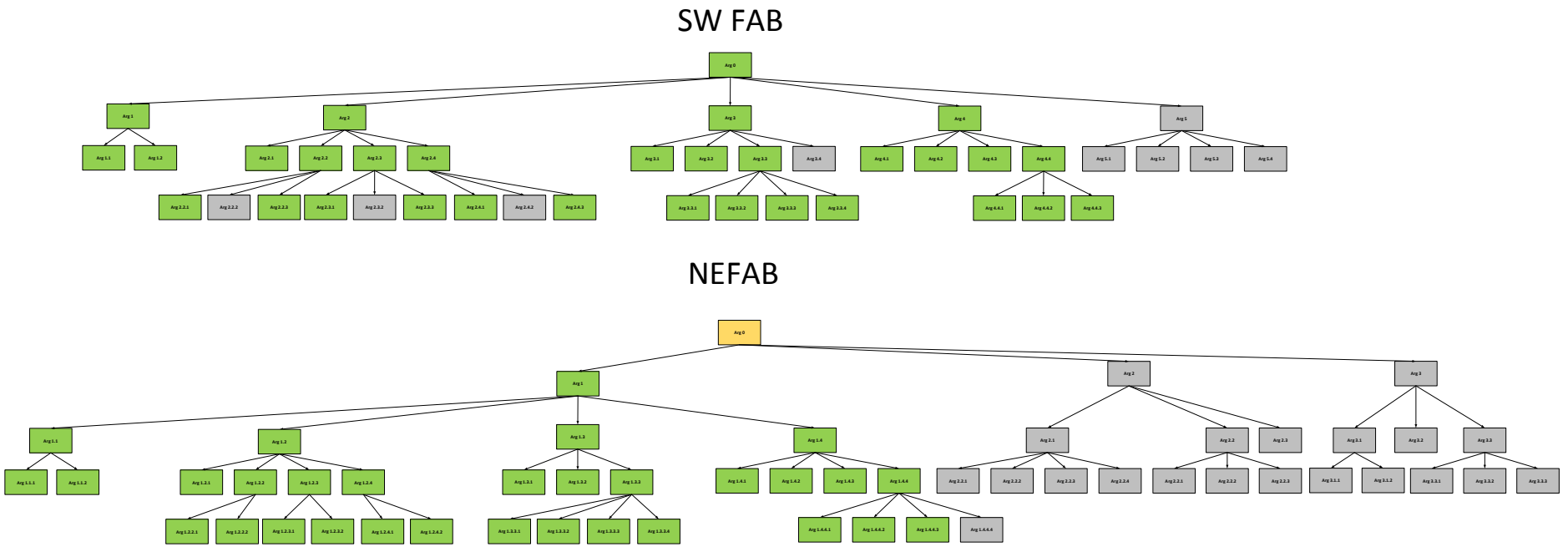

Figure 23 SW FAB Safety Case vs. NEFAB Safety Case without connections between analogous elements

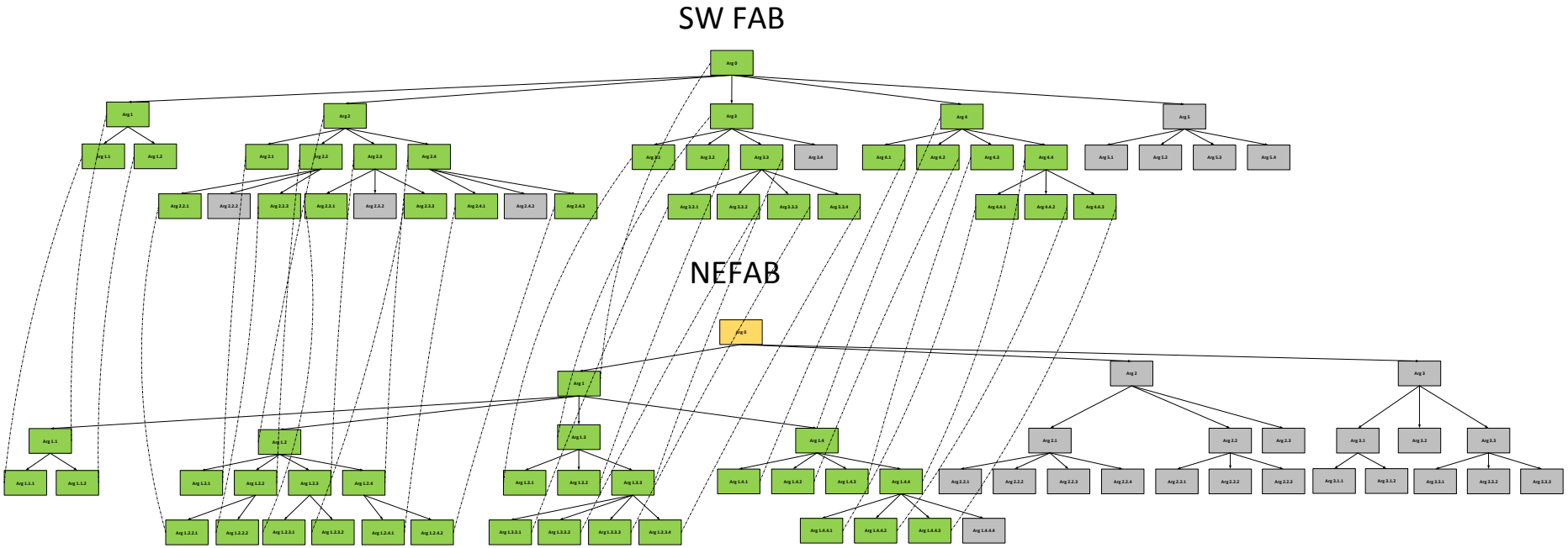

Figure 24 SW FAB Safety Case vs. NEFAB Safety Case with connections between analogous elements

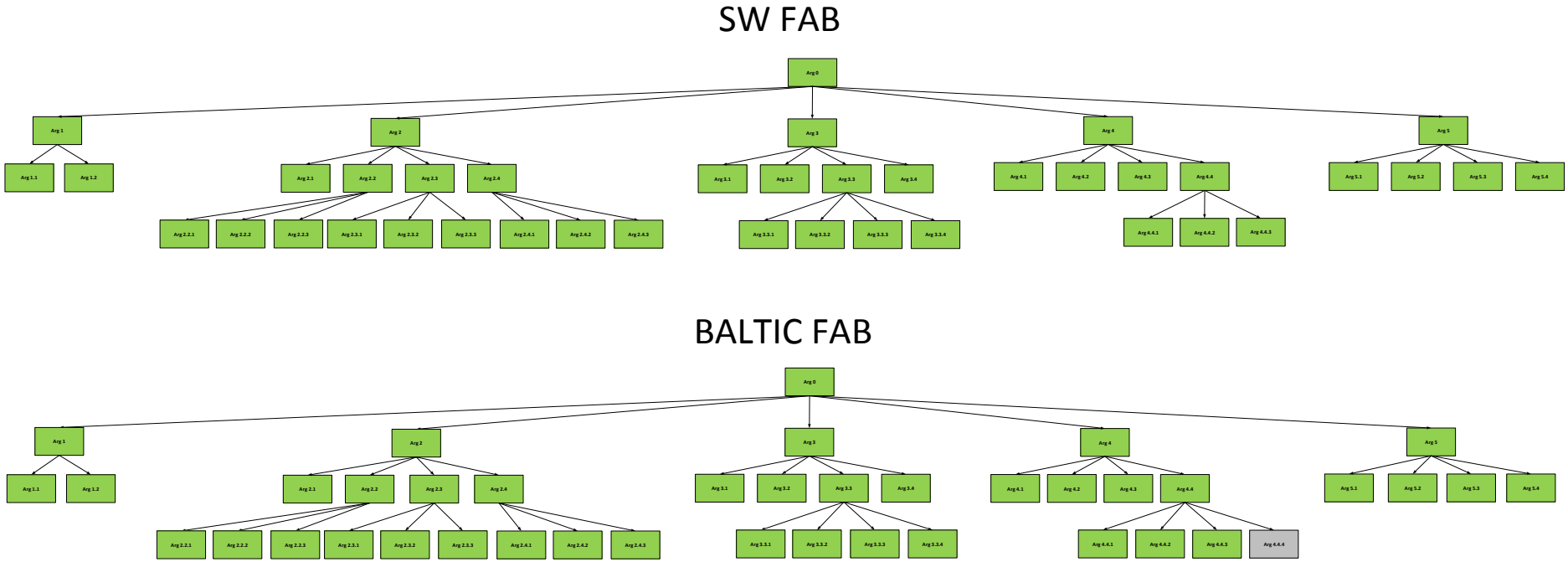

Figure 25 SW FAB Safety Case vs. Baltic FAB Safety Case without connections between analogous elements

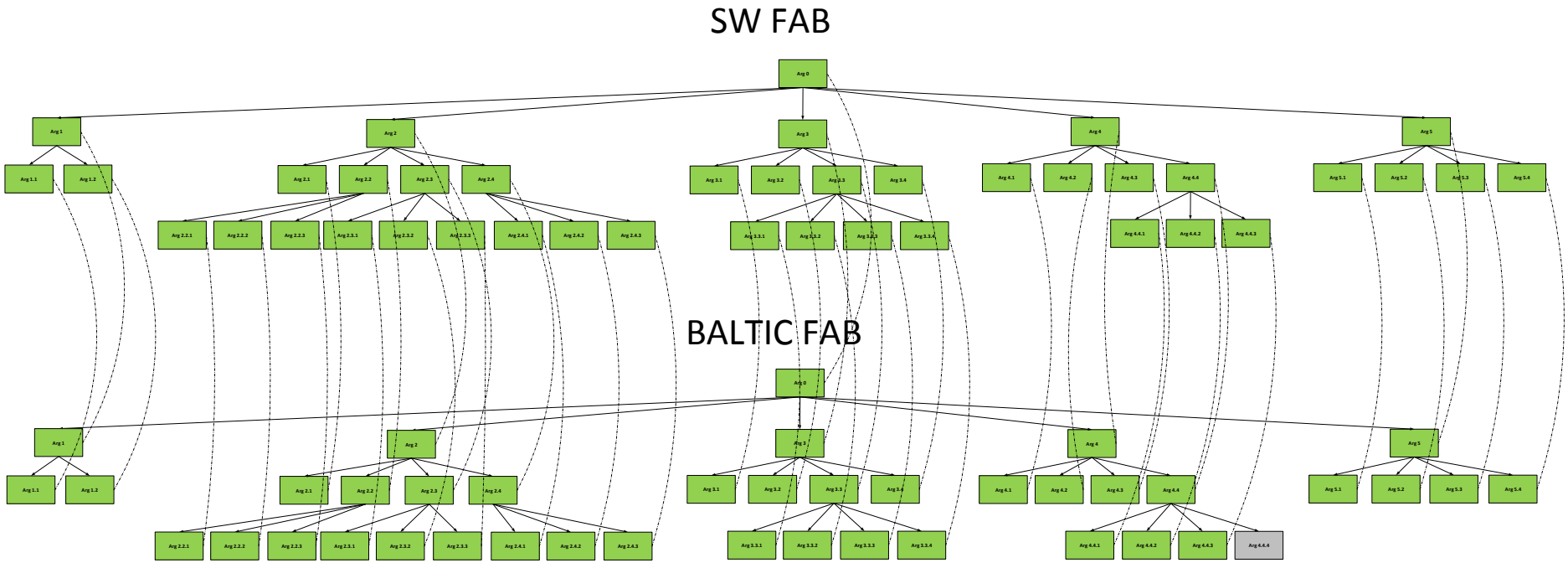

Figure 26 SW FAB Safety Case vs. Baltic FAB Safety Case with connections between analogous elements

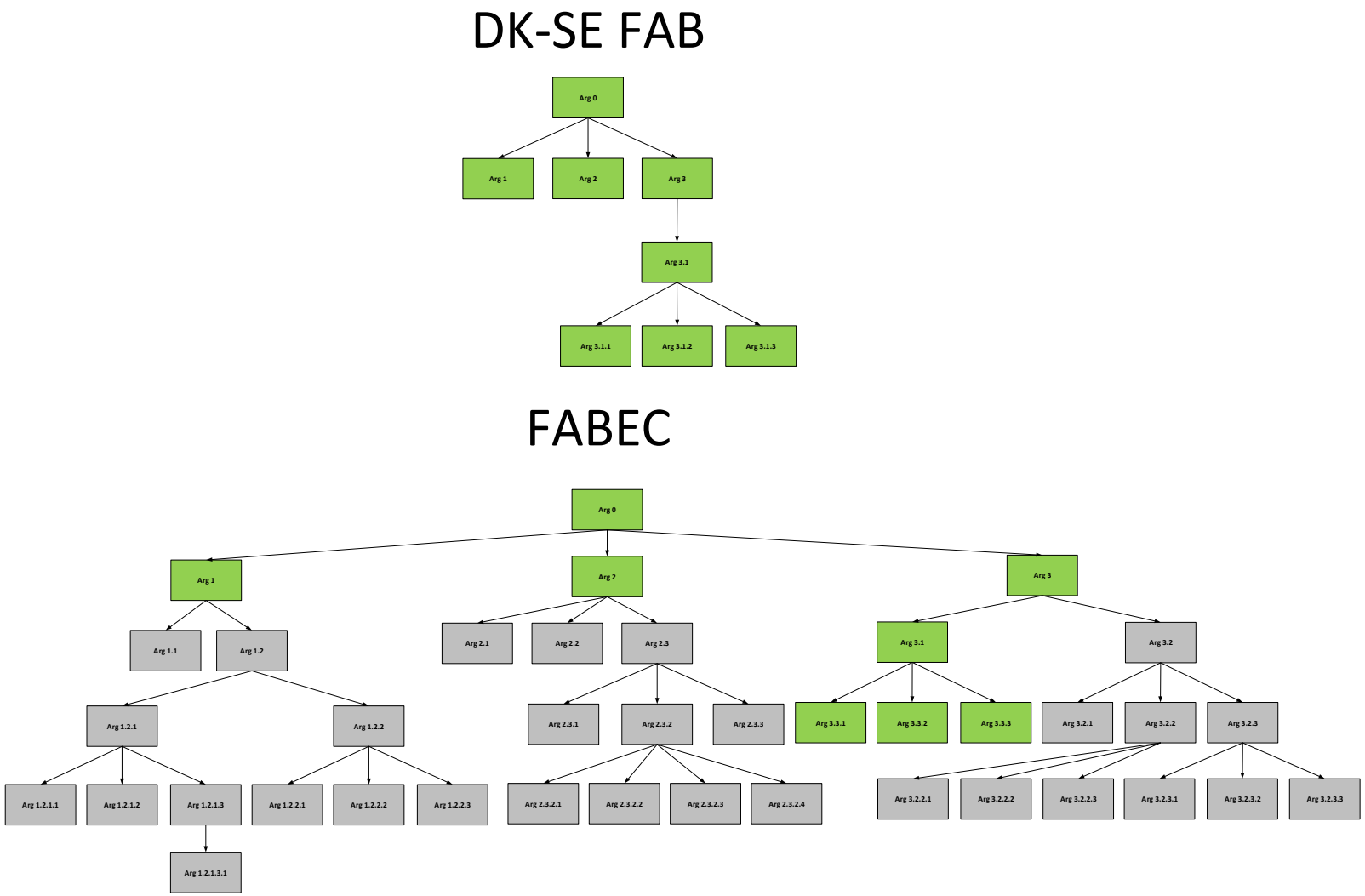

Figure 27 DK-SE FAB Safety Case vs. FABEC Safety Case without connections between analogous elements

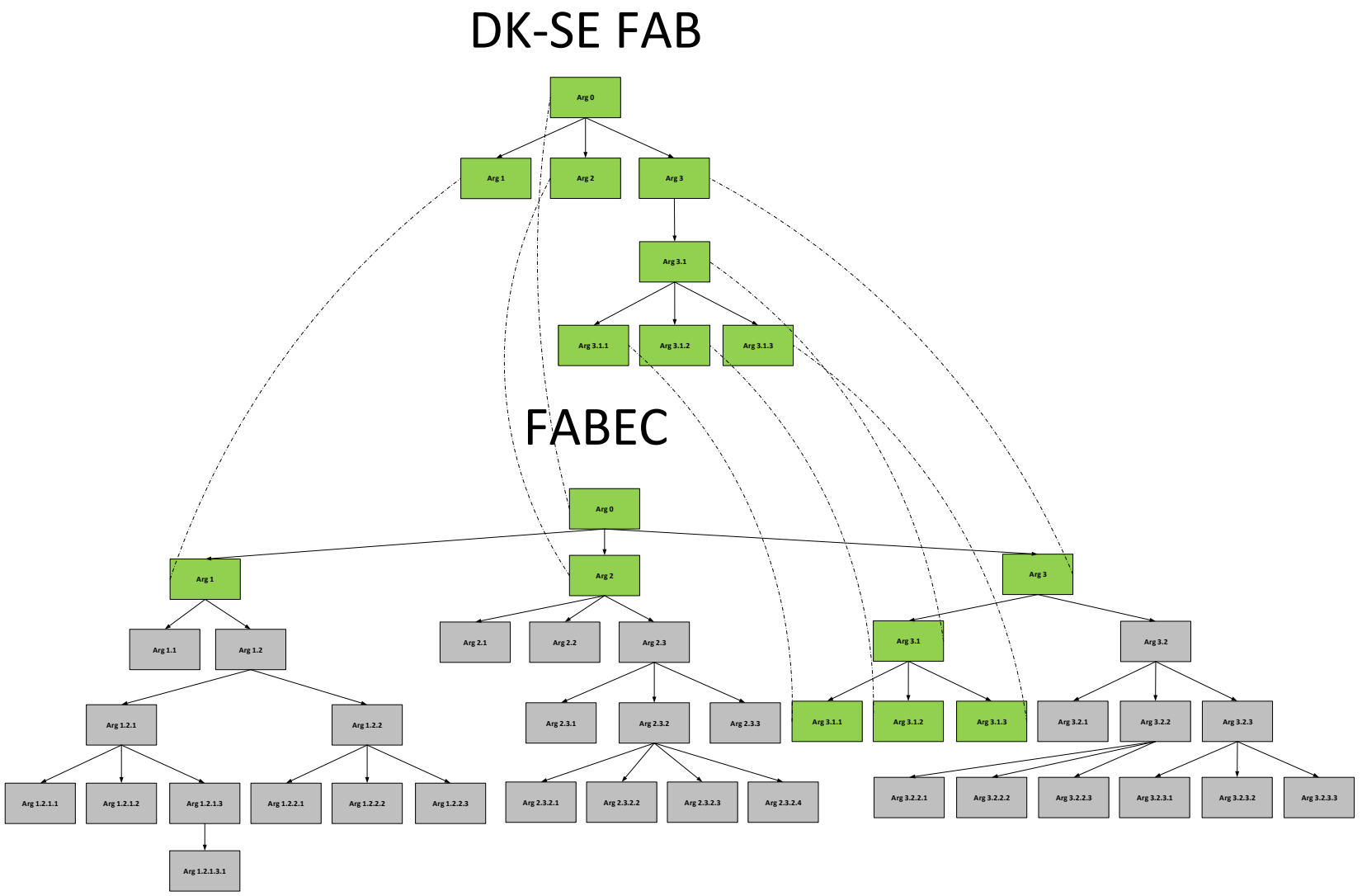

Figure 28 DK-SE FAB Safety Case vs. FABEC Safety Case with connections between analogous elements

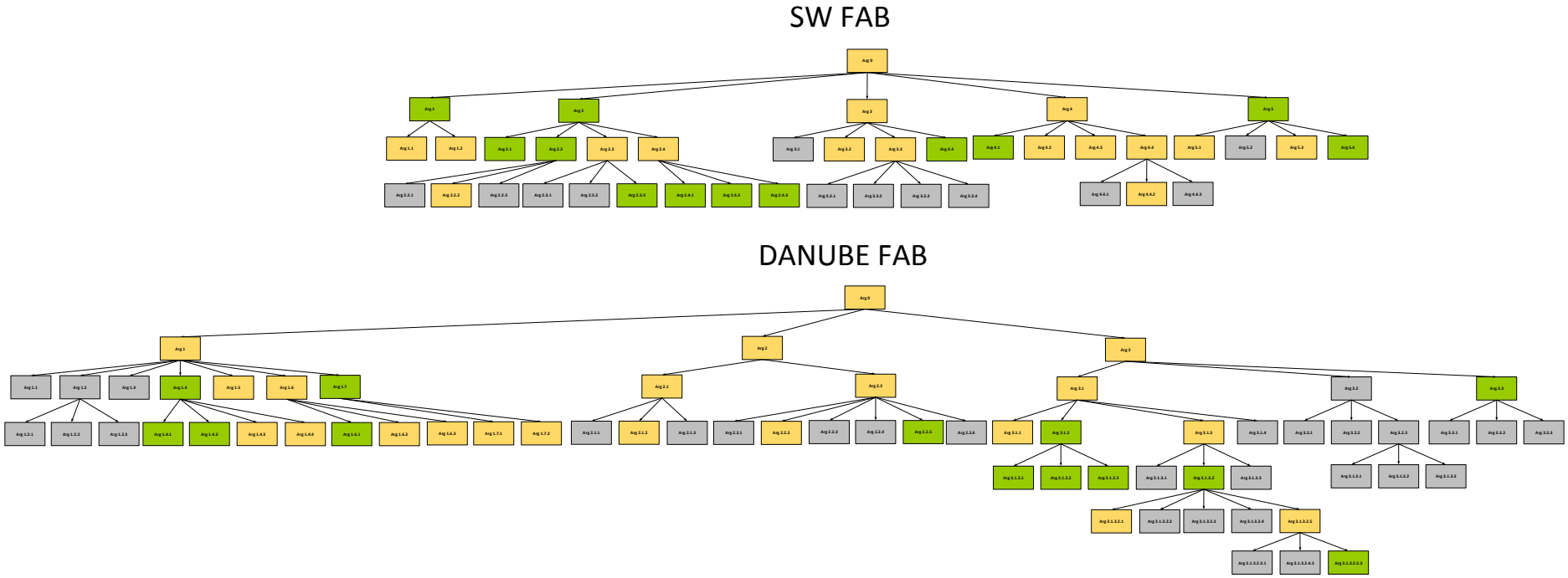

Figure 29 SW FAB Safety Case vs. Danube FAB Safety Case without connections between analogous elements

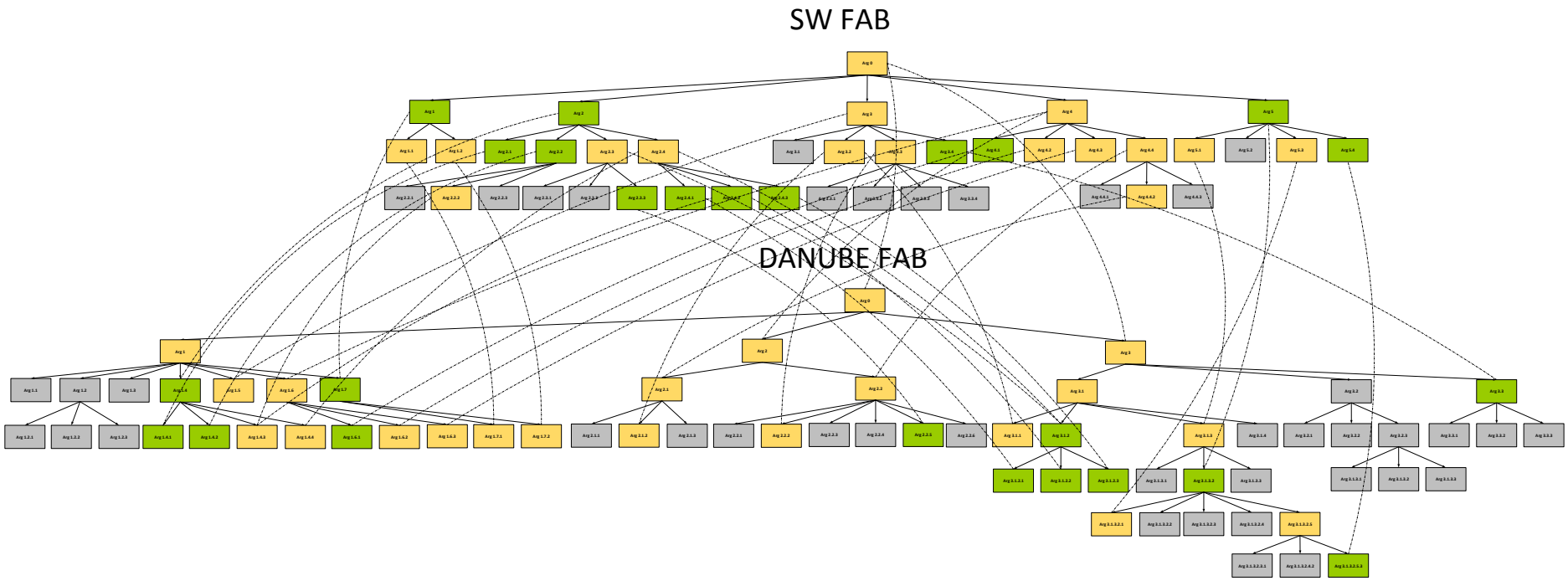

Figure 30 SW FAB Safety Case vs. Danube FAB Safety Case with connections between analogous elements

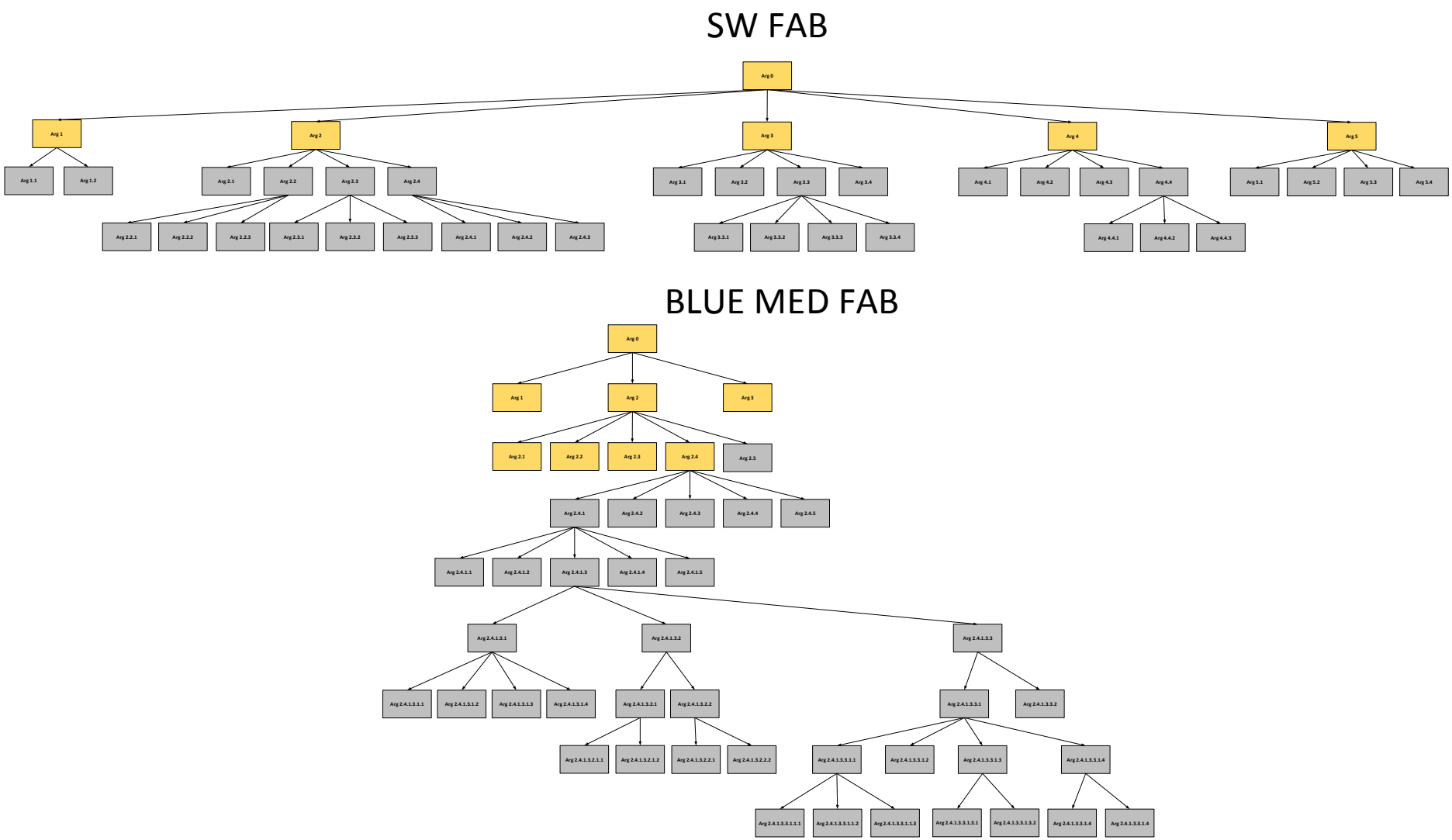

Figure 31 SW FAB Safety Case vs. BLUE MED FAB Safety Case without connections between analogous elements

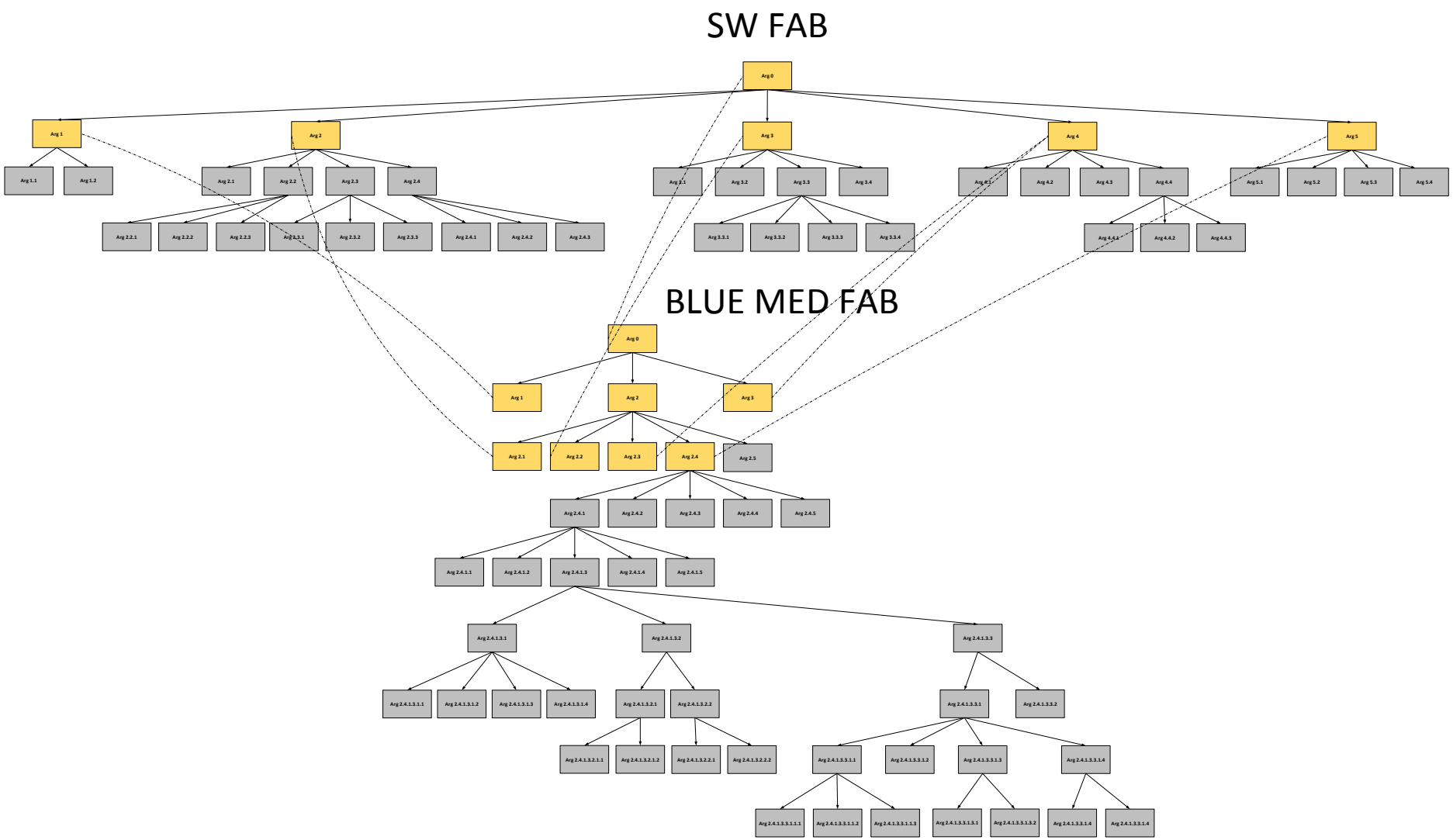

Figure 32 SW FAB Safety Case vs. BLUE MED FAB Safety Case with connections between analogous elements

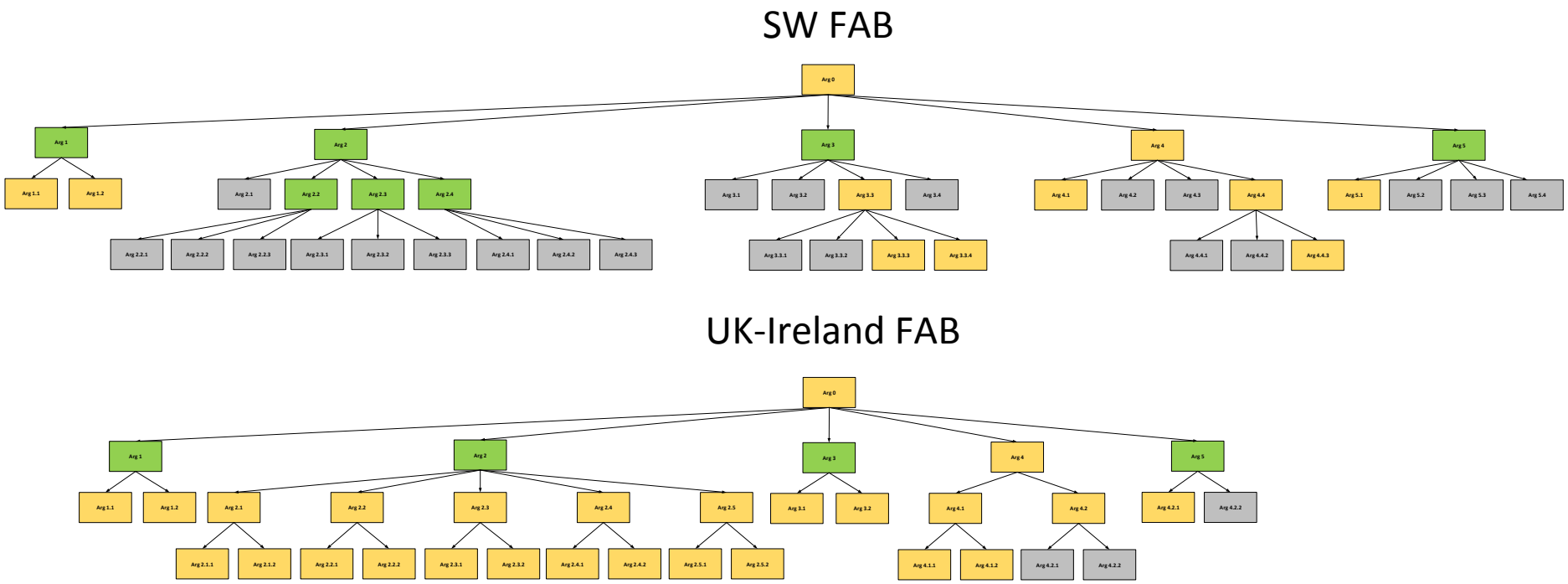

Figure 33 SW FAB Safety Case vs. UK-Ireland FAB Safety Case without connections between analogous elements

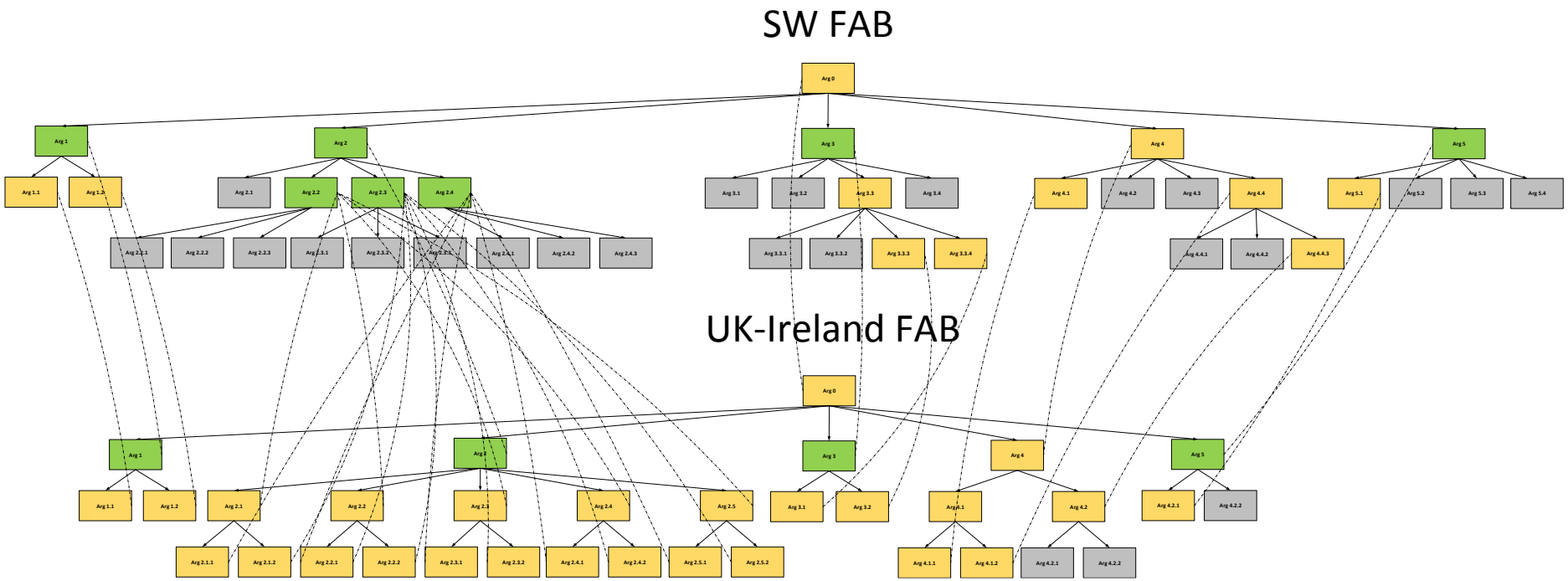

Figure 34 SW FAB Safety Case vs. UK-Ireland FAB Safety Case with connections between analogous elements