Classification and Argumentation Maps as support tools for liability assessment in ATM

Giuseppe Contissa, Giovanni Sartor,
Migle Laukyte, Hanna Schebesta
Law Department, European University Institute (EUI)
Florence, Italy
giuseppe.contissa@eui.eu, giovanni.sartor@eui.eu,
migle.laukyte@eui.eu, hanna.schebesta@eui.eu

Paola Lanzi*, Patrizia Marti*•,
Paola Tomasello*
*Deep Blue - Rome, Italy
•University of Siena – Siena, Italy
paola.lanzi@dblue.it, patrizia.marti@dblue.it,
paola.tomasello@dblue.it

***Abstract* — In this paper we present an application of argument maps for assessing the liability impact of ATM systems. Such application has been recently developed within the ALIAS Project (Addressing the Liability Impact of Automated Systems). Such maps are used for presenting legal concepts and norms to lawyers and non lawyers (engineers, software developers, human factors specialists and other technical personnel), within the cooperative design and assessment of new technologies for ATM.**

Argumentation maps; legal risk; liability assessment; Air Traffic Management

I. INTRODUCTION

Communication of legal concepts is often a very difficult task, especially between lawyers and experts who have no legal background, yet whose professional activities frequently intersect with serious legal questions. The difficulties increase when legal norms must be applied to complex socio-technical systems (STSs): such systems can be seen as norm-governed systems, which strongly depend on legal and social institutions. Moreover, STSs are exposed to serious legal risks in case of adverse events. A mutual understanding among technical experts and lawyers is therefore crucial, and Air Traffic Management (ATM) is an example of this: on the one side, technicians and operators have difficulties in grasping different layers of norms (international, supranational, national legislation, technical rules, certification procedures, contractual clauses, etc.) regulating the system, on the other side, lawyers do not have the background needed to understand the technical infrastructure and the processes carried out by automated systems and human operators.

The ALIAS Project has recently developed the Legal Case (LC), a novel and innovative methodology which helps an interdisciplinary team, made of legal experts, engineers, human factors specialists and other technical personnel, to foresee and mitigate the legal problems that an automated technology under construction might cause. Thanks to the ALIAS methodology the need for changes in the allocation of legal liabilities can be identified at the project stage, and problems can be identified and addressed before deployment, through convenient technological adaptations or legal arrangements. The methodology promotes the integration of legal and safety culture, by embedding the technological risk assessments into the evaluation of legal risks and consider how legal arrangement contribute to the overall safety.

The proposed analytical methodology is based on a novel set of classification and argument maps, enabling legal analyses to complement risk analyses and safety arguments. In particular the maps are modelling tools for the legal risk analysis, acting as:

- Connecting tool: the maps structure and connect information about the system and its possible failures on the one side, and the applicable legal framework on the other side: failures are mapped according to consolidated approaches adopted by the human factors domain [1][2], and connected to a mapping of possible liabilities, according to an actor-based framework of liabilities in ATM developed within the project;
- Communication tool: the maps foster the process by which the lawyers and other stakeholders build their legal and technical knowledge, and also work as a powerful communication tool between stakeholders from different backgrounds, as the visual representation improves reasoning and analysis of complex issues;
- Assessment tool: the maps provide a support for the legal risk analysis carried out in the LC because they help to identify and evaluate the legal risks.

Two kinds of maps are used in the LC: classification maps and argumentation maps.

Classification maps provide taxonomies of the objects within a certain domain. They consist in boxes linked simply by lines in either the direction top-down or the direction left-right, and can be expanded and collapsed at different levels, since the classification maps can be multi-level. The goal of these maps is to help the Legal Analyst to structure his thinking and to focus his attention on specific level of classification. In the LC process we use two kinds of classification maps: the failures maps and the legal risks maps. The **failures-maps** (engaged in step 1.3 of the LC) map and

This work is co-financed by EUROCONTROL acting on behalf of the SESAR Joint Undertaking (the SJU) and the EUROPEAN UNION as part of Work Package E in the SESAR Programme. Opinions expressed in this work reflect the authors' views only and EUROCONTROL and/or the SJU shall not be considered liable for them or for any use that may be made of the information contained herein.

classify the possible failures and damages resulting from the use of an automated technology. The **legal risks maps** (engaged in step 2.1 of the LC) link each failure to hypotheses of liability and propose one or more hypotheses of liability for the involved actors;

Argumentation maps, instead, are visual representations of the structure of arguments, and are represented as diagrams with boxes corresponding to propositions and arrows indicating relationships between them. The goal of the argumentation maps is to link the premises (reasons) to a conclusion, either by supporting the conclusion or by attacking the premises (reasons) or the inference which brings to the conclusion. We use two kinds of argumentation maps: the legal analysis maps and the legal design maps. The **legal analysis maps** (engaged in step 2.2 of the LC) help the Legal Analyst to analyse the legal arguments which could support the attribution of liability, taking into account the applicable legal framework, and the factual circumstances of the accident resulting from the failures. The **legal design maps** (engaged in step 3 of the LC) enable the users to validate the legal design measures to mitigate the liability risk identified in the previous step.

The aim of the current paper is to provide detailed information on how the classification and argumentation maps are engaged in the LC methodology. In line with this, the paper is organized as follows: Section II provides an overview of the LC methodology, addressing the description of each step and highlighting where the maps should be used across the whole process. Section III provides information on how the maps are engaged in the steps of the proactive application. Finally, Section IV provides conclusive remarks about the innovative value of the classification and argumentation maps as a way to structure and connect information about system failures and legal discipline.

II. THE LEGAL CASE: OVERVIEW OF THE METHODOLOGY

As anticipated, the LC is the methodological tool built to facilitate the integration of the highly automated technologies into complex STSs, which in our case, deal with ATM. In particular, the goal of the LC is to address the liability issues resulting from the interaction between humans and automated technologies, in such a way that these liability issues would not hinder the design and development of these technologies.

The LC methodology is basically a legal risk management process. The 'legal risk management' approach considers legal risk as one of the components of risk management [3]. By legal risk we mean the probability and the severity of an unwanted legal outcome, being triggered by uncertain factual circumstances and/or uncertain future legal decisions. The legal risk management approach provides a systematic structure to identify, describe, analyze, evaluate and provide feedback on legal risks. In particular, the LC provides for a participatory and interactive model for legal risk management. This, on one hand, favours an interdisciplinary perspective; on the other hand, it facilitates communication and integration of the legal risk management into the overall risk management procedures.

The LC offers two ways in dealing with the legal risk associated to the ATM systems: proactive and retroactive. The proactive perspective addresses the legal risks during the design phase of the system's lifecycle and is meant to prevent or mitigate legal risk, that is, it is anticipatory. The retroactive perspective addresses the legal risks which arise at the deployment phase of already existing automated technologies and intends to offer a strategic response to legal risks that have already taken place (or may take place in the future) thus providing a structure for their containment.

In line with this, the LC can ideally be applied to any automated system, both under development or in operation. We assume that both proactive and retroactive applications of the LC will be performed under the guidance of a *Legal Analyst*, namely, a person having a legal background in aviation and liability law which enables him/her to understand the legal issues involved in a project or accident. Obviously, the Legal Analyst will need to call on other skills available within the project or outside of it, in case further technical knowledge is required. In fact, legal knowledge is necessary to deal with the liability topics while engineering knowledge and human factors are essential for the understanding of the technical and operational features of the object of the analysis, i.e., the automated process under examination. Thus, the Legal Analyst is assumed to be a member of an interdisciplinary project team dealing with the design or deployment of automated technologies. In this respect, the LC can be conceived not only as a legal risk management tool, but also as a communication channel between different expertise and domains of knowledge. We also assume that the end-users of the LC results could be the decision-makers, who could profit from the results of the LC to make decisions and plan investments. In this sense the LC can be considered a decision support and planning tool.

The generic process of the LC consists of four steps:

1. Understand the context: we collect the background information about the object (which may be an operational concept, a system, a service, or an accident in which a piece of technology played a crucial role);
2. Identify liability issues: we define the legal implications of the object on the basis of the understanding of its socio-technical aspects.
3. Perform the analysis: we analyse the stakeholders' acceptability of the legal implications defined in previous step, propose ways to deal with all involved legal risks, including possible mitigations and recommendations for the design.
4. Provide results and recommendations: we present the results of the study, highlighting the liability issues associated with the object, the ways to deal with legal risks and further recommendations.

Each of the 4 steps is centered around the use of sets of argument maps developed using Rationale by Austhink (http://rationale.austhink.com/): these maps play a crucial role in the construction of a LC for a new technology, by enabling the Legal Analyst to capture the logic of the legal issues, to explain them to non-lawyers, and make possible solutions understandable and subject to deliberation. The UML activity diagram in Figure 1 shows the workflow of the LC. Rounded rectangles represent actions, i.e., substeps within each step of the LC. Square-edged green rectangles represent a flow of objects from one action to another, that is, the flow of the information produced in each substep of the LC. Bold arrows represent the main workflow. Light arrows represent other connections between object and actions, that is, the information used as an input for each substep. The LOAT table, the R-LOAT table, and the complete set of maps used in the process (Failures maps, Legal Risks maps, Legal Analysis maps, and Legal Design maps) are also inputs and appear as yellow boxes.

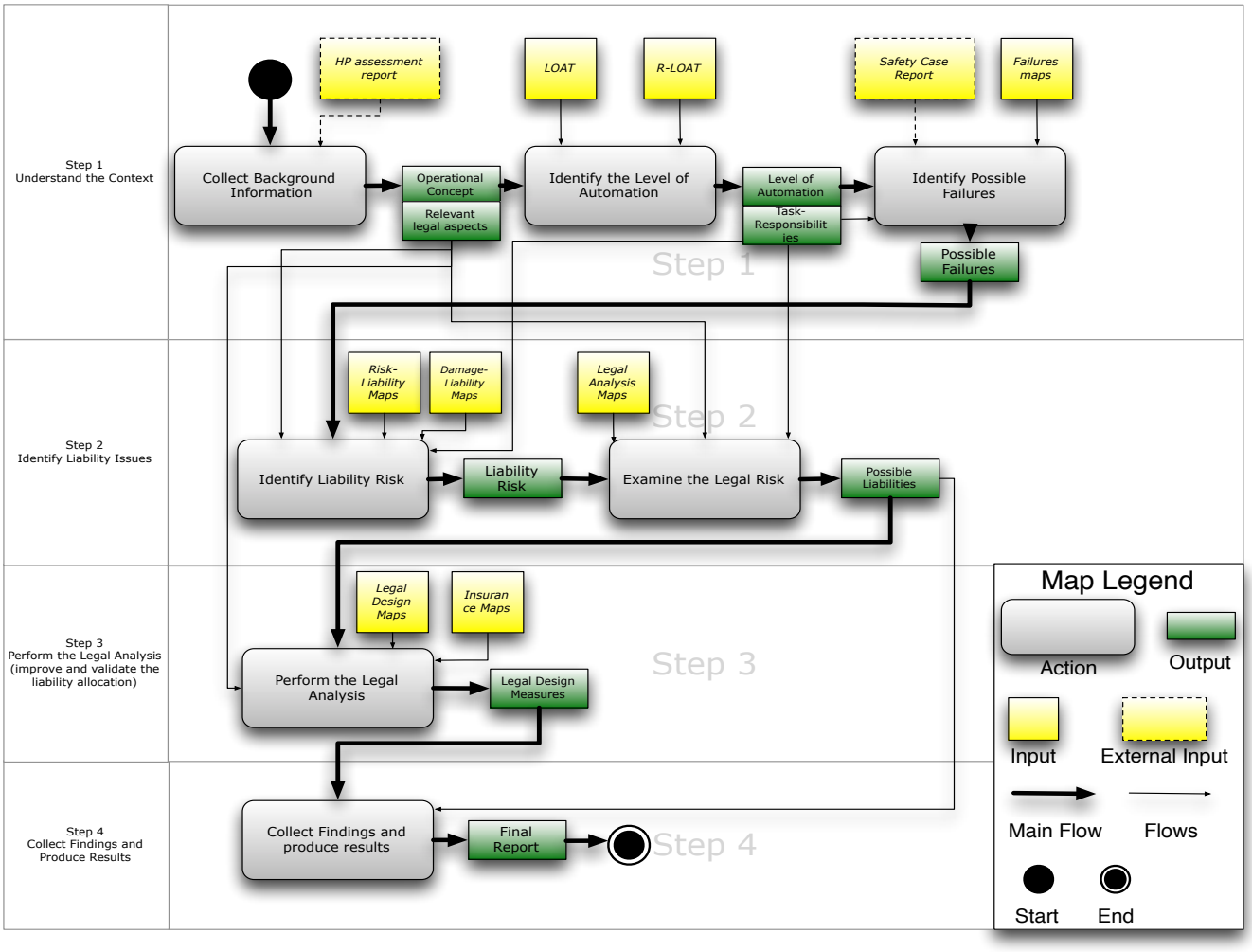

Figure 1 - The Legal Case process

As it is possible to see in the figure, the workflow shows the allocation of the complete set of maps (Failures maps, Legal Risks maps, Legal Analysis maps and Legal Design maps) across the whole process, thus also highlighting how each of them serves as relevant input for the following actions.

The Safety Case Report [4] and the HP Assessment Report [5][6] are highlighted as external inputs. The arrow that connects them to the substeps of the LC is dotted, signifying that the LC can be applied without using those reports (if they are not available yet). It this latter case we assume that the LC report can be used as input for the subsequent application of Safety Case and HP assessment process.

In the following section we provide a description of these maps and how they are engaged in the concerned step of the proactive application of the LC methodology.

III. THE USE OF THE MAPS IN THE PROACTIVE APPLICATION OF THE LEGAL CASE

The first step of the analysis: the failures-maps

Step 1 – Understand the Concept – has the threefold purpose to i) collect background information about the ATM

concept being designed, ii) classify the level of automation of the associated system or technology, and iii) identify the possible failures of this new operational concept. We assess the level of automation of the system or technology (ii) with the help of the Level of Automation Taxonomy (LOAT) [5]. The LOAT is a tool which divides the human-machine interaction into separate tasks (information acquisition and analysis, decision and action selection, action implementation) showing in each of them how the tasks are divided between the human and the machine: how the tasks are divided between humans is shown in R-LOAT (Responsibility LOAT) which we developed to reveal the responsibilities of each human (user, developer and manager) involved in given process.

This step (iii) connects the LC with EUROCONTROL's Safety Case. The two cases share a common approach to, and understanding of, risks, faults, hazards, and consequences. This implies the possibility of a mutual exchange between the two cases, since the hazards identified in applying one case to a specific technology can be used as an input in applying the other case, and vice versa.

In the LC a set of classification maps has been developed in order to identify risks of failures related to the development, training, use and maintenance of automated technologies, and different types of damages that may emerge whenever such failures result in accidents. The failures-maps have been developed on the basis of the socio-technical framework developed within ALIAS, according to which failures are divided into latent conditions and active errors: latent conditions may be either technical or organisational, while active errors may be either technical or human. Active errors are those acts or events that can be directly linked to the accident, such as the unsafe actions on the part of the operators that ultimately led to the accident, or the malfunctioning of one of the hardware components, etc. Latent conditions are those that may lie dormant or undetected for hours, days, weeks, or even longer, until one day they contribute to a sequence of events resulting in an accident. Examples of the latter are bad organisation of work processes, bad maintenance of hardware components, bad management of safety or training, etc.

The failures-maps present the list of failures through a tree-shaped structure. The failures-maps structure is a multi-level set of predefined types of failures that serve as a basis for identifying the potential failures of the project in question. The structure is multi-level, being composed of the four top-level failures. For each kind of failure, a different branch of the map shows a set of different sub-types of failures. For instance in Figure 2 below we show how the latent technical conditions can come in the form of, for instance, the absence or insufficiency of (or even defective) maintenance of essential safety tools, or the malfunctioning of safety devices.

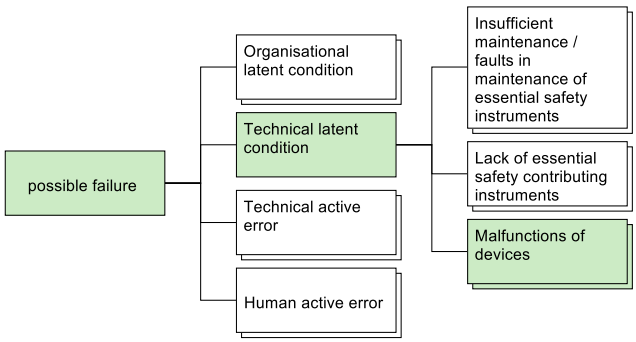

Figure 2 - Failures maps

Step 2: Legal Risk And Legal Analysis Maps

In the following step – Step 2: Identify the liability issues – we assess the risk of liability in the light of the existing legal framework. We perform this assessment with the help of two kinds of maps: legal risks maps and legal analysis maps.

A legal risk map is a support tool for highlighting the liability risks associated to the possible failures identified in the previous step. It links a particular factual constellation (in particular a kind of failure) to a possible legal liability. The purpose of legal risks maps is to suggest kinds of legal liabilities to be investigated for each possible failure identified in Step 1. The legal risks maps are classification maps: the main kinds of failures (first level of the mapping structure) are connected to the possible legal liabilities (second level of the mapping structure) resulting from them. In particular, each type of failure is linked to different hypotheses of attribution of liability to one or more of the subject involved (pilots, air traffic controllers, air carriers, air service providers, manufacturers, etc.).

The following map (Figure 3) shows a list of potential technical latent conditions, and related liabilities emerging from them. For instance, technical latent conditions, which could lead to an accident involving the Traffic Collision Avoidance System (TCAS), could be those regarding insufficient capacity of TCAS processors to compute advisories' updates. This could engender product, organisational or managerial liabilities. Technical latent conditions could also threaten the functioning of Remotely Piloted Aircraft Systems (RPAS) in case in which the software calculating avoidance manoeuvres was malfunctioning, because it was not adequately tested. Here organization, managerial and product liability may be at issue, with regard to user, maintainer and the developer.

Another set of maps links damage to liability: usually liability is triggered by a damage (civil liability may be seen as the obligation to compensate for a damage). Moreover, according to the legal framework of ATM, different kinds of damages (on board, on the ground, to passengers, to baggage, to third parties, above or below different values, etc.) may trigger different kinds of liability for the different actors involved in the event from which the damage arises: the Figure 4 shows the hypothesis of liability emerging from damages

arising from accident taking place on board of the aircraft (SDR stands for Special Drawing Rights, that are supplementary foreign exchange reserve assets defined and maintained by the International Monetary Fund (IMF). 1 SDR is about 1.5 US dollar).

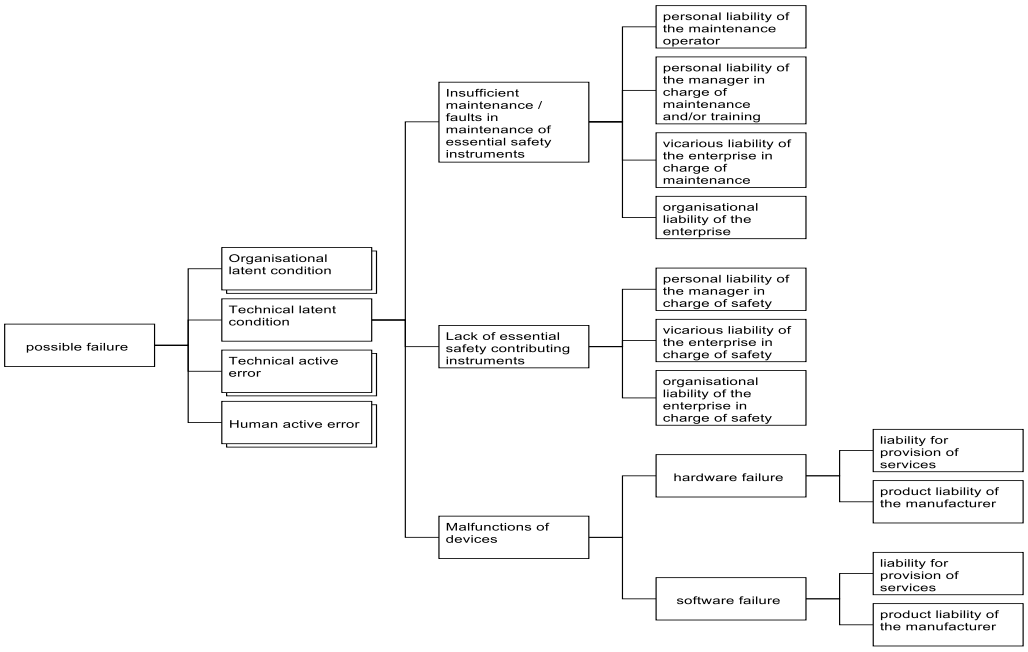

Figure 3 - Risk Liability map for technical latent conditions

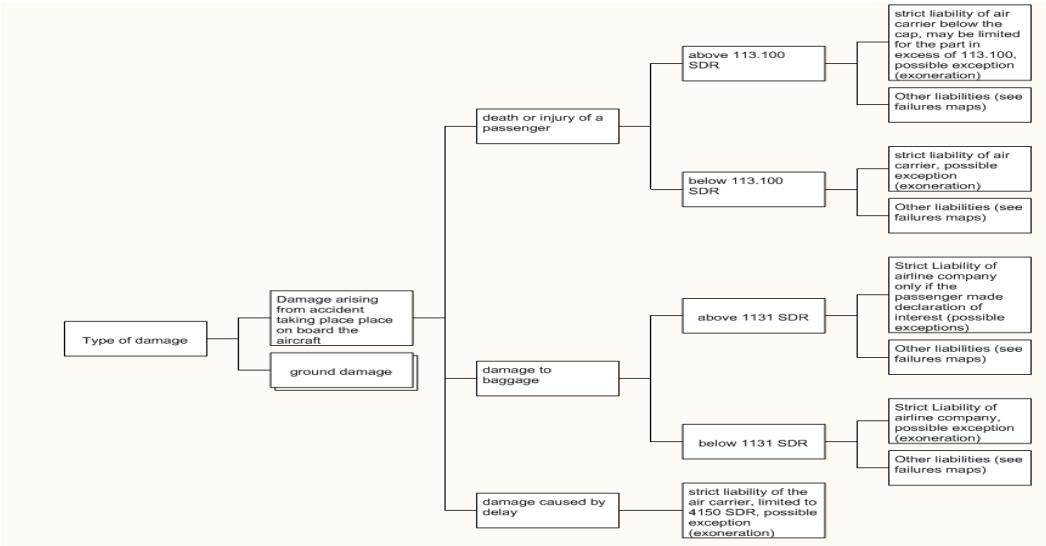

Figure 4 - Damages map

After having built the legal risk map, the Legal Analyst needs to examine the possibility that a legal risk concerning a particular actor occurs in different contingencies. To do this, he can rely on the legal analysis maps (supported by the relevant legal and empirical knowledge).

Legal analysis maps reflect our understanding of the law on liability as it is represented in the current legal framework concerning air law, product liability, insurance and contract law. The answer which the Legal Analyst looks is whether there is the risk of a particular kind of liability: this is established by checking whether the conditions for that kind of liability may exist under certain circumstances. Initial hypothesis of attribution are validated with the help of an extensive set of argument maps, which cover different types of liability (personal liability, enterprise liability, product liability, special cases of liability such as air carrier liability, etc.). In such maps arguments supporting the attribution of liability are combined with 1-level counterarguments attacking (by rebuttals and under cutters) the liability arguments, with further level counterarguments, providing attacks against 1-

level counterarguments, and so on. In this way a dialectical tree is built for each potential liability.

For example, the map shown below (Figure 5) explains the underlying legal logic of finding a product manufacturer liable in case of a defective product. The first thing to do is to check whether the technology is a product or a service from the legal point of view, and this map shows that we assumed that the technology in question is a product. The map shows that the defectiveness of a product might be related to the unreasonably dangerous design and, with the help of the Legal Analyst, the interdisciplinary team consults the jurisprudential texts on this matter to understand what the concept of unreasonably dangerous entails.

The legal analysis map also shows two possible defences against product liability: the first is that the product was designed according to the current state-of-the-art in particular technological field, and, the second is that the technology was built in compliance with the technical standards and regulations. However, compliance with a standard is not enough to exonerate a producer from liability claims.

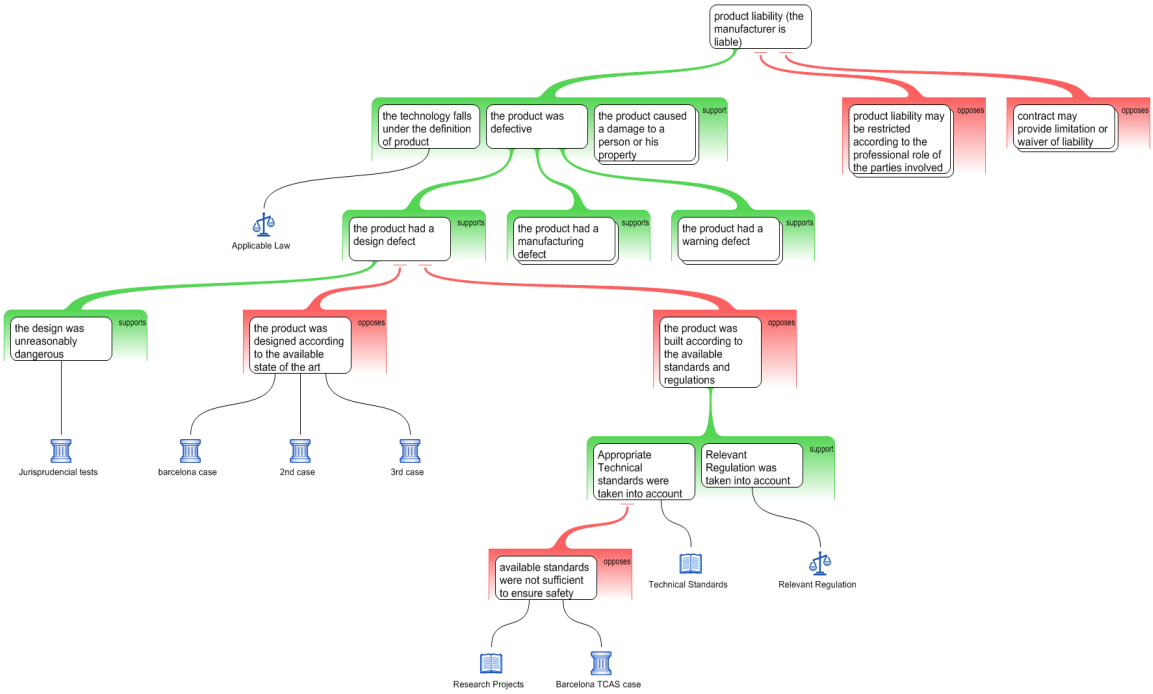

Figure 5 - Legal Analysis map for product liability

The Third Step, Perform the Legal Analysis: Legal Design Maps

The third step – Perform the legal analysis – consists in engaging in legal design on the basis of the results of the legal analysis performed in the previous step. By legal design we mean proposing possible mitigations and recommendations for the systems design. Such mitigations and recommendations are targeted towards optimal acceptability of the liability risks for all stakeholders. This involves complementing the outcomes of the legal responsibilities analysis with private (contractual) legal regulations meant to ensure an allocation of liabilities which is acceptable to the parties. Three fundamental liability-design measures can be decided upon at this stage: Liability mitigating measures; Liability enhancing measures; Liability displacing measures.

In this step the argumentation maps allow the user to design and validate the legal design measures that may mitigate such risks. This concerns making changes in the allocation of liabilities and considering what impact this has on the liability risks which are to be supported by each party.

In particular, we build Legal Design maps (Figure 6) which help to find suitable liability design measures, measures able to suggest different solutions to the problem of eventual liability for any failure that the technology in question could cause. The argumentation map represented in Figure 4 provides an example illustrating how liability-design measures could be used to help a Legal Analyst addressing software liability. The map deals with product liability for software failure (here we assume that a software system is deemed a product rather than a service). As discussed above, a product can be defective by reason of its design, its manufacture, or the warnings regarding its use. The argument for the defective product design could be defeated by claiming the state-of-the-art exception, which would apply if the product is designed according to the relevant rules and requirements, and complies with the state of the art in the relevant technological field. But the state-of-the-art exception may in turn not be applicable to the case at hand if the purchaser/user of the product (software) has agreed with its producer/seller that the producer is strictly liable for software defects. This is just an example of the numerous possible options on how to re-balance the burden of

liability among the stakeholders involved in design, development and deployment of highly automated technologies in the ATM.

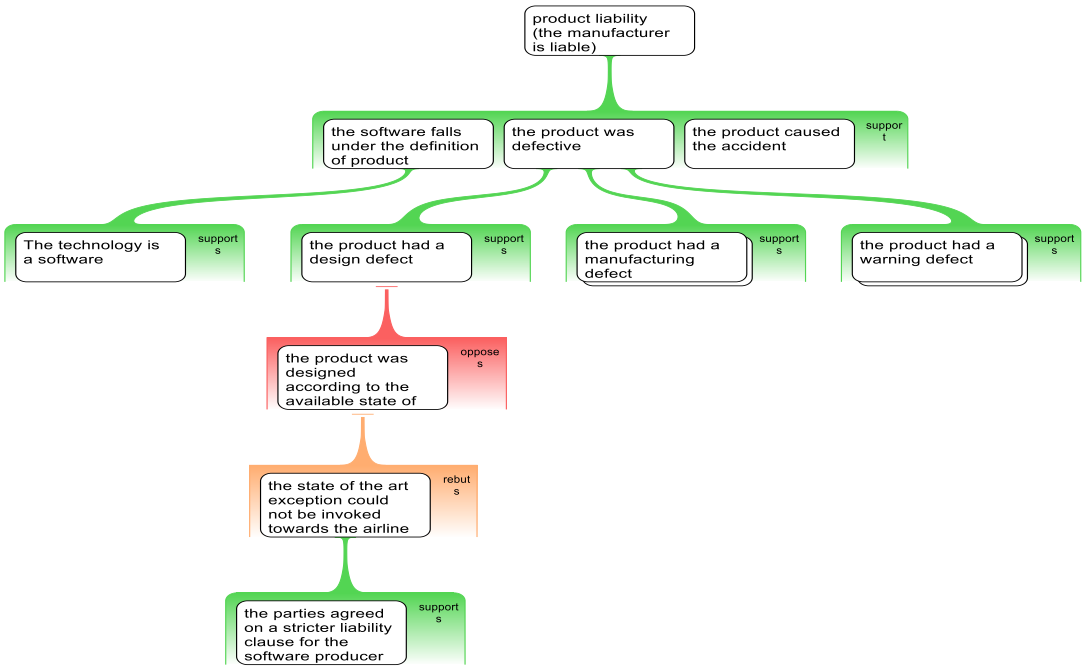

Figure 6 - Legal Design maps

In the last step – Step 4: Collect findings and produce results – the results of the analysis are presented to the stakeholders, highlighting the liability issues associated with the automated technology, the ways to deal with legal risks, and further recommendations. If all stakeholders agree with the results, this information will be included in the concept documentation, so as to be implemented into contractual and other private agreements. The stakeholders might not agree as well: for such cases we assume that the parties could think of a different legal design, different allocation of tasks and the deployment of the technology.

IV. CONCLUSIONS

Although being still in a prototypical version, the LC methodology is gathering great interest from the ATM community. Industrial suppliers, ANSPs, and authorities are unanimous in recognizing the need to address the liability impact of automated systems as early as possible during the project's lifecycle. While legal commentary addresses punctual doctrinal issues of liability, nothing has been devised so far which integrates a systematic legal assessment of legal risks in the innovation process. In so far, the LC methodology represents a completely innovative approach to deal with this kind of problems. Indeed, the LC methodology represents a new approach in bridging the technological innovation and the legal perspective, and may be considered a novelty also for the legal domain, where very few legal scholars have endeavoured to design, develop or study legal risk management methods [7]. Moreover, the LC facilitates communication between the legal experts and the technical experts involved in designing a new concept: to this end, the set of maps and tables representing and integrating the relevant technical and legal knowledge are the key asset for dealing with communication breakdowns that so often arise in highly technologically developed contexts.

Ultimately, the LC will provide an important tool also for policy makers. Multiple parallel or joint applications provide much needed information about the allocation of liability from different perspectives that comprise all relevant stakeholders. Where several projects discover similar liability misalignments these problems can be raised on a higher level. In the future, the potential of the LC to address systemic issues will be strengthened, supporting policy makers to take action at systemic level.

In the future, besides linking the maps to source materials (case law, legislation, other documents regarding technologies, accidents, stakeholders, etc.), and providing a more in-depth coverage of the most important and controversial subject matters, we intend to make the maps more interactive, enabling users to visualize and browse them on the web. The next release of the methodology will enable the users of these argumentation maps to change old and add new arguments, personal notes and other information. The models provided in the Carneades [8] and OVA (Online Visualisation of Arguments) will be particularly significant in this regard. The project will also consider providing automated assessment of the status of arguments, for instance according the semantics of Carneades [9] or of the ASPIC+ system [10]. Besides, the project will evaluate the integration of argumentation methods used in the LC to represent the legal risk, with certain methods used in risk analysis (Contingency Trees, Fault Trees):

analyses based on such methods may provide to the LC an assessment of the probabilities of accidents.

REFERENCES

[1] J. Reason, James, Human Error. Cambridge: Cambridge University Press, 1990.

[2] D. A. Wiegmann and S. A. Shapell, A Human Error Approach to Aviation Accident Analysis. Aldershot: Ashgate, 2003.

[3] L. Save and B. Feuerberg, "Designing human-automation interaction: a new level of automation taxonomy", in Proc. Human Factors of Systems and Technology 2012, 2012.

[4] EUROCONTROL, Safety Case Development Manual, edition 2.2, November 2006

[5] SESAR 16.4.1, HP assessment process for projects in V1, V2 and V3, 16.4.1- Del ID, 18.10.2013

[6] SESAR 16.5.1, Framework for HP Automation Related Good Practices, 16.05.01-003, 25.10.2011

[7] T. Mahler, "Tool-supported Legal Risk Management: A Roadmap", in European Journal of Legal Studies, vol 7, pages 175–198. European Press Academic Publishing, FIRENZE – ITA, 2009.

[8] T.F Gordon, "The Carneades web service", in COMMA, pages 517–518, 2012.

[9] T. F. Gordon, "An overview of the carneades argumentation support system", in C.W. Tindale and C. Reed, Eds., Dialectics, Dialogue and Argumentation: An Examination of Douglas Walton's Theories of Reasoning, pages 145–56. College Publications, London, 2010.

[10] H. Prakken, "An abstract framework for argumentation with structured arguments", in Argument and Computation, 1:93–124, 2010.

[11] ALIAS Project, D1.3 Framing the Problem, E-02-ALIAS-D1.3

[12] ALIAS Project, D3.1 Repository of Cases, E-02-13-ALIAS-D3.1

[13] ALIAS Project, D3.3 Case Based Analysis and Modelling, E-02-ALIAS-D3.3