Supporting Failure Mode and Effect Analysis: A Case Study with Failure Sequence Diagrams

Christian Raspotnig and Andreas Opdahl

Department of Information Science and Media Studies, University of Bergen
NO-5020 Bergen, Norway
{Christian.Raspotnig,Andreas.Opdahl}@uib.no

Abstract. [Context and motivation] In air traffic management (ATM) safety assessments are performed with traditional techniques such as failure mode and effect analysis (FMEA). **[Question/problem]** As system modelling is becoming an increasingly important part of developing ATM systems, techniques that integrate safety aspects and modelling are needed. **[Principal ideas/results]** This paper proposes an approach for thorough failure analysis of ATM systems that consist of several interacting components and similar systems. The new technique is called failure sequence diagrams (FSD) and supports FMEA in modelling failures and their effects through interactions between system components. FSD has been used in a case study by safety and system engineers in three different ways. **[Contribution]** The study suggests that FSD was easy to use and supported FMEA well, but did not cover its weakness in analysing multiple failures.

Keywords: Failure analysis, safety, sequence diagrams.

1 Introduction

Air traffic management (ATM) in Europe is about to undergo the most extensive technological change in its history through the Single European ATM Research (SESAR) program [1]. A part of the change is describing the current and future systems of ATM, where modelling is becoming crucial. Modelling languages such as UML [2] are widely used in many domains, and the ATM community in Europe is becoming increasingly interested in using modelling for systems development.

The current safety assessments conducted in the European ATM community are following methods such as Eurocontrol's Safety Assessment Methodology [3], which includes the Functional Hazard Analysis [4]. This method can include traditional techniques, such as Hazard and Operability studies (HazOp) and Failure Mode and Effect Analysis (FMEA) [5], which are used at lower abstraction levels. While these techniques sometimes use models as an input, they typically use worksheets to discuss and document the hazards and failures. However, using models more actively in safety assessments can give benefits, such as better discussions and understanding of the system under assessment, along with integration of model-based system engineering. For ATM systems that consist of several interacting components, there is a need for a thorough failure analysis of the interactions, which are not easily analysed with the traditional techniques.

B. Regnell and D. Damian (Eds.): REFSQ 2012, LNCS 7195, pp. 117–131, 2012.

The purpose of this industry case study is to obtain real experiences on combining FMEA with Failure Sequence Diagrams (FSD), a specialized version of Misuse Sequence Diagrams (MUSD) [6] from the security field. FSD is a new technique in the safety field and in this paper the technique and the results obtained when combining the technique with FMEA in a safety assessment are presented.

The paper is structured as follows; in section 2 the background for the research is described along with the relevant work. Section 3 describes the research method used for obtaining the results presented in section 4, which are analysed in section 5 and further discussed in section 6. Finally, in section 7, we conclude upon the research and look ahead at further work, before we direct our acknowledgements.

2 Background

A system failure is defined as "an event that occurs when the delivered service deviates from the correct service" [7]. The relationship between fault, error and failure is described together with how it relates to interacting system components in [7]. FMEA is not only used for identifying the failure modes of system components and their effects, but also for finding the causal factors causing the failure to occur and thereby follows the idea with respect to faults, errors and failures. Although FMEA relates failure modes to system components and to the complete system, it does not address interactions between components. Most FMEA worksheets contain information about local or immediate effect and system effect, where the latter is a description of the failure propagated to system level. However, there is no support by FMEA to investigate failure propagation, except reasoning about the local and system effect of a failure mode.

FSD addresses failures and propagation between the interacting components. In Fig. 1 the notation for the FSD is presented, showing how the notation extends UML sequence diagrams. The notation includes current control and recommended action (indicated by dashed/green symbols), also referred to as mitigations. FSD also includes a notation for indicating component failure that can be used to differentiate whether a component fails (indicated by red/dashed symbols) to deliver its service, or if the failure only propagates through the component (indicated by a black/solid component symbols) without causing it to fail.

In Fig. 2 the use of FSD is presented by an example that is similar to the system that was analysed in the case study with FMEA. It shows that a corrupted flight coordination message, indicated by a red/dashed arrow, is sent into the system and not detected by the router or the LAN. When the corrupted message is received by the flight processor (FP) component, it causes the FP to crash and the FP is not able to send an alert to the monitoring system (MON). The MON continuously sends heartbeat messages to FP as current control. It registers that no response is given by the FP. Although the MON has a current control of sending an alert message (last message in the diagram) to the supervisor (SUP), a recommended action is to include new messages through the flight display (FD) to alert the air traffic control officer (ATCO) of the failure of the FP.

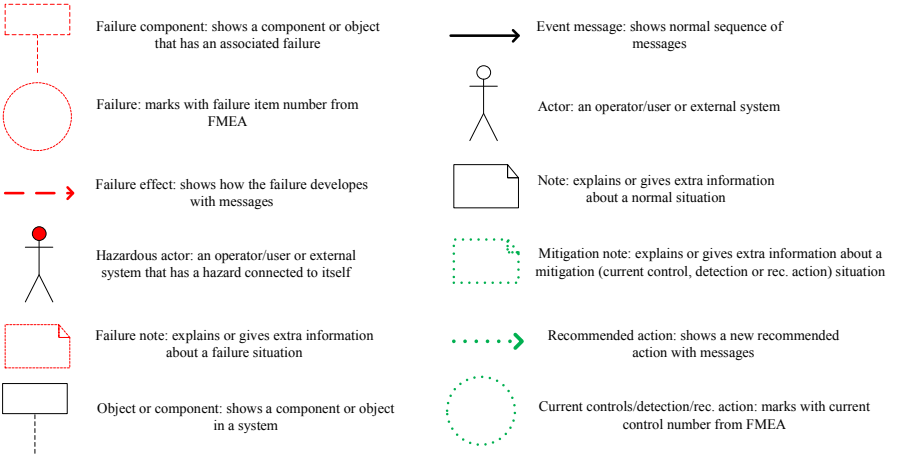

Fig. 1. Notation for the Failure Sequence Diagrams

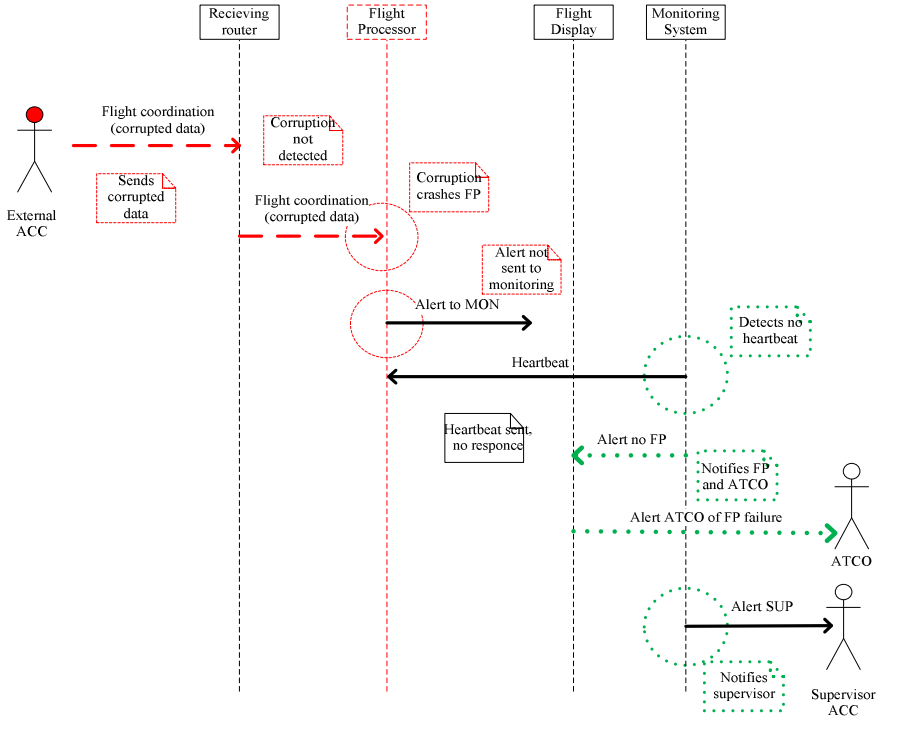

Fig. 2. Example in the use of the FSD

There are several related works to ours: on combining UML and failure identification has been done before, e.g., using FMEA on UML models for improving the interaction between design and dependability analysis [8], comparing system sequence diagrams with textual use cases in an experiment, for evaluating what is better for identifying hazards related to a system [9], or, closest to our work, the use of UML diagrams for safety analysis of a medical robot [10]. In the latter work, FMEA is used together with sequence diagrams and errors are modelled. However, in comparison to our work the three approaches do not extend the UML diagrams with an own notation for supporting FMEA specifically. To our knowledge they do also not attempt to improve the FMEA process with focus on interactions and failure propagation. Finally, they do not evaluate the optimal combination of interactive failure visualization and a structured use of a worksheet.

3 Method

The purpose of the case study was to evaluate how FSD could be used together with FMEA. In particular, we wanted to gain experiences on the industrial use of FSD and the interaction between the two techniques.

3.1 Research Questions

For the case study design we developed three research questions with sub-questions to guide our observations in the meetings to obtain qualitative data on the usage of FSD together with FMEA.

1. Can FSD support FMEA?
    a. Is it possible to use FSD along with FMEA?
    b. Is it easy to use FSD in combination with FMEA?
    c. Can FSD improve discussions among participants?
    d. Can FSD increase understanding of the system?
2. How should the two techniques be used together?
    a. What are the pros and cons of the ways of combining the techniques?
    b. What is the optimal way to combine the techniques?
3. Can FSD cover the weaknesses of FMEA?
    a. Can FSD show multiple failures?
    b. Can FSD help relating failures and their effects to interactions?
    c. Integration of safety assessments and model-based system engineering?

3.2 Choice of Research Method

Case study as a method was discussed with the Air Navigation Service Provider (ANSP) organization according to their needs for safety analysis of system changes. A research method that would let them conduct the safety analysis as required, but at the same time could allow for research taking place within their organization, was seen as beneficial to both parties. Therefore, case study was selected for observing the use of the two techniques together in a real setting. In the following sub-sections the case study design is described.

3.3 The ANSP Case

We followed a European ANSPs assessing the safety of introducing the Flight Management Transfer Protocol (FMTP) [11], [12]. A procedure based on [3] was used for deciding the scope of the change, whether a safety assessment was required and which technique to use. The ANSP decided to use FMEA and to structure the safety assessment through FMEA meetings. An earlier safety assessment of the coordination function between air traffic control units was used to establish the required safety level and possible hazards.

Meetings were organized, taking place in a meeting room with the needed facilities, e.g., a big table, a video projector and a white board. An FMEA team was established, with a facilitator, a secretary, three systems engineers and an air traffic control officer. Several of the participants were familiar with UML, but only one of them had previous experience with sequence diagrams.

In advance all participants received a document describing the FMTP system and the overall system, relevant safety documentation and a procedure for conducting the FMEA. The latter consisted of a worksheet with the columns component number, component, failure mode, causal factor, immediate effect, system effect, current controls and recommended action. Furthermore, it included a list of typical failure modes for components and software as described in [5].

3.4 Procedure for Conducting the Case Study

During the case study we observed three strategies of using the two techniques together in the meetings. Below the activities taking place during each strategy is described and referred to as sessions:

1. First session (day one – five hours' meeting)
    a. Introduction of case study, purpose, techniques and basic usage
    b. Explaining a simplified notation without mitigation
    c. Conducting the FMEA
    d. Applying the FSD to the FMEA result
    e. Summarizing the FSD and FMEA session
2. Second session (day two and three – six and two and a half hours' meetings)
    a. Summary of the first session
    b. Explaining the full notation with example similar to Fig. 2
    c. Conducting the FMEA together with FSD
    d. Summarizing the FSD and FMEA session
3. Third session (day four – three hours' meeting)
    a. Repeating the full notation
    b. Conducting the FSD
    c. Summarizing the results with FMEA
    d. Summary of all sessions

3.5 Data Collection during the Sessions

In the first two sessions, the first author acted as an observer. The participants were encouraged to use FSD and FMEA as seen beneficial to their task. Whenever

experiencing difficulties, they were told to discuss among themselves and identify a natural solution. If they were not able to find a solution, they could ask the observer for advice. For the third session, the first author supported the facilitator and drew the FSDs as a participating observer, before taking a passive role with the FMEA.

For collecting relevant data, we decided to focus on three types of data:

1. Verbal – which questions were asked, e.g., to us or between themselves, discussions and general comments regarding the technique.
2. Interactions – how was the interaction with FSD, e.g., drawing, pointing, referring to, looking at while talking or thinking.
3. Notes – which parts of the notation were or weren't used, and which parts of the notation were used wrongly or correctly.

For the data types, all relevant observations from the sessions were written down. The sessions were also video-taped for extracting more information relevant to our data types. Pictures were taken of the FSD diagrams for each component, which we used together with our notes to reconstruct how the notation was used. The video recorder only captured the participant standing next to the white board and it was not possible to reconstruct the interaction of participants pointing to the drawing by analysing the video recordings.

In the last session the first author did not take notes as he facilitated the meeting and relied solely on the video recordings for the data collection. When summarizing the FMEA worksheet, we did not video record the worksheet and the participants. The video camera was directed towards the white board, only recording the use of FSD to support the summary. However, we reconstructed the discussions by using the audio part of the recording.

3.6 Data Collection through Interviews

The first author interviewed the participants after the sessions as follows:

1. Explaining the purpose and procedure for the interview
2. Asking for their own comments
3. 11 questions based on Technology Acceptance Model (TAM) [13]
4. Asking for comments on a summary of our analysis

For the interviews it was only possible to conduct two face to face meetings. Of the remaining three participants we were able to interview two of them through email, with the same structure for the interview. The answers were returned and analysed along with the notes from the two other interviews. The last participant, a system engineer, was not able to respond due to time constraints.

In the interview they gave their general opinion on the usage of FSD to support FMEA, before answering the TAM questions regarding perceived usefulness, perceived ease of use and intention of use. In the end of the interview they discussed the summary of the case study and either agreed or disagreed with our findings.

4 Using FSD for Supporting FMEA

In this section we describe how the techniques were used in each session.

4.1 First Session

The participants started the regular FMEA process and discussed some components for clarification. FSD was used after finishing the FMEA analysis of the first component. There was a discussion on how to use the FSD, where the participants concluded to use it for supplementing FMEA. A natural start for them was to draw up all components identified in the FMEA worksheet, but they discussed this and also asked us as observers. Another issue discussed and questioned was to use one or more FSD diagram per failure mode. As they progressed some modifications were done, e.g., that power supply was not included as it seemed hard fit it to the FSD as a specific component. The participants agreed that a good start would be to draw the normal sequence of messages in the FSD, before analysing the failure, its causes, related effects and mitigations.

While drawing the normal sequence there were several discussions on the functions of the components involved. There were a number of clarifications, e.g., the role of a monitoring system and what kind of functionality that was allocated to this component. These clarifications led to statements such as “we are better in thinking around graphical notation” and “FSD gives us an overview of the system”. At the same time they commented on only using one FSD diagram per failure mode, or else “the FSD would become too complex”.

The participants used wrong notation on some occasions, e.g., not including message text above the arrows or using the lifeline for symbolizing an external actor. Furthermore, the only FSD specific notation used was the failure markings.

Several participants engaged in diagram drawing. In the beginning the task was left to one of the system engineers, but several times the facilitator and another system engineer participated in the drawing. All participants used the drawings when discussing, either by pointing to components or referring to them by name. Several of the participants went up to the white board when explaining details about the system.

4.2 Second Session

This session started with summarizing the advantages of using FSD for bringing clarity of components and how they interrelate, and giving a good overview of the system. The participants also discussed further use of FSD and it was decided that FSD should support FMEA in a more iterative manner. Furthermore, they discussed using FSD for identifying failure modes and causal factors, but concluded FMEA better suited for this. They used FSD for investigating the immediate and system effects, along with the current controls.

The participants used FSD from the beginning of the session and shortly discussed which messages to look at before using FSD to draw a normal sequence of messages in the system. They also marked the failure mode in the FSD, but used the FMEA worksheet to discuss the causal factors. Immediate effects and system effects together with the current control were usually discussed by use of FSD, with recommended

actions identified from these discussions. This continued throughout the session, where FSD and FMEA were used iteratively on the components.

Support for Discussion. Inclusion of both inbound and outbound messages in the FSD drawings was also discussed by the participants. Most of the discussions were on understanding the system and components, along with interactions, not on usage of FSD. Nevertheless, the facilitator found it hard to draw some of the messages, as different levels of the OSI model [14] were discussed with respect to corrupted data and detection of such data. In the end diagrams were drawn and notes were used to state at which level the messages were drawn. Sometimes they used an FSD as starting point for discussion on failures, but only marked the failure of a component in FSD and then summarizing it in the worksheet. They also commented that they did not see the need to draw diagrams of failures of the external system. However, they used FSD to draw and discuss how such failures would affect the system under analysis.

Use of Notation. The participants were able to use the notation for drawing situations of corrupted data going into the system, and wrote assumption as notes of the data going unnoticed through the system. Often they used the numbering from FMEA for failure modes and current control and also wrote names above the messages correctly. Still, for component failure they often only drew the initial failure marking and then used the FSD more for discussions than drawing the complete sequence of messages. Once they also left the FSD drawings and drew a sketch for explaining how the messages could be switched by the system. Moreover, the note notations were seldom used to comment their drawings. For current control green arrows were used instead of the combining green circles and black arrows. They repeatedly used a component symbol for representing an external system as opposed to the actor symbol suggested. Once they used the actor symbol, but did not include the name. The participants also suggested using a red cross over a message to indicate that it did not reach the receiver as intended, as a new notation. Later, when looking at specific part of the system, they did not draw all the components, but only those interacting with the specific component. In the beginning they used wrong notation for corrupted data, i.e., black arrows instead of red, but it was used correctly later.

Combining the Techniques. In this session they combined FSD and FMEA in an interesting way. They often drew failure modes, but went back to the FMEA worksheet for discussing causal factors and immediate effects. FSD was still used in these discussions, either for looking at and referring to parts in the FSD or for letting the facilitator point out things in the drawings. All participants pointed to FSD for identifying components and messages in discussions, and for reasoning about messages at different levels in the OSI model. They also used FSD more systematically to show how corrupted data went unnoticed through the system and explaining intermittent loss of messages or handshake functionality. Once a recommended action was found by use of FSD, but usually the FMEA worksheet was used for this. Sometimes system engineers corrected the facilitator in drawing current control wrongly, but they also corrected each other's representations of message flow in the system. Although FSD was not used for drawing failure of power supply, they used it to get an overview of which components that would be affected by such a failure. Some participants also used FSD as reminder for further

discussions, when the secretary needed time to update the FMEA worksheet. In some circumstances they also asked each other for oral explanations, and used the FSD to follow the explanation given.

4.3 Third Session

Before the FMEA meeting started, small icons of the FSD notation was prepared by the first author on the sides of the white board. The participants and first author agreed to only use FSD for facilitating the meeting, but let the secretary note the discussions in the FMEA worksheet (not visible to the participants). After finishing the analysis with FSD, the worksheet was shown for further refinement. In this session we also analysed the software of some components, compared to the other sessions where the analysis was more concerned with components at a system level.

Although the first author drew the FSD with the defined notation it was not always straightforward. He found some problems drawing software components, as the decomposition feature of UML sequence diagrams [2] was not used. The diagrams became too complex, as software components were added to the lifelines with the specialized FSD notation. Often all the information would not fit on the white board. Nevertheless, the relevant FSD notation was used and a new alt operator [2] notation was introduced, which worked well for representing system effects of failure modes. The participants seemed to understand this operator as they referred to it as different scenarios of system effects. The participants also corrected the FSD, e.g., when the notation was used incorrectly or messages were drawn to the wrong components.

The session was facilitated by drawing the FSD and then asking for comments. Drawing the FSD in front of everyone allowed for corrections of everyone's understanding. Many corrections were also made by walking through the drawings, pointing to the flow of messages and asking the participants to explain accordingly. This was evident as the FSD was changed gradually, as discussions revealed new aspects both with respect to system effects of failures and functionality in the system. When the FMEA worksheet was brought up in the last part of the session, some corrections also had to be made here. The facilitator used FSD to point out these corrections to the secretary.

There were few discussions or questions on how to use the FSD, perhaps because the first author drew the diagrams and facilitated the meeting. Nevertheless, when he suggested drawing a recommended action the participants agreed that it was out of scope, but it was further discussed and noted in the FMEA worksheet. In the end everybody discussed facilitating with FSD and summarizing the results with FMEA worksheet. The participants had used the FSD repeatedly to understand the system and ensure a common understanding, but missed the structure of the FMEA worksheet and preferred to use it for brainstorming failure modes first and then using FSD. It was argued that with FSD only the focus became more on how the system works and the interaction of the components than on failure modes and causal factors.

5 Results

In this section we present the results from analysing the data from the previous section. We present the results for each research question from section 3.1.

5.1 Can FSD Support FMEA?

Verbal. We noted no direct questions related to whether FSD was able to support FMEA. Mainly there were discussions and general comments regarding the support. In the first and last session, the participants clearly stated that FSD gave an overview of the system and allowed for better reasoning due to use of graphical notation. Additionally, FSD ensured common understanding among the participants. This shows that using FSD supports FMEA. The participants were not being able to use FSD for representing failure of power supply. From this we conclude that the support is not possible for analysing all aspects of a system and is limited to the notation of sequence diagrams. This is further supported by the representation of corruption of messages at different layers in the OSI model.

Interactions. Although the main use of the FSD was to draw diagrams, the participants also used them actively in discussions, both in explaining to each other and for checking their understanding, by pointing at or referring to names of components or messages and the related failure notations in the drawings. Often they used the FSD to make all participants join the discussion. The FSD supported the FMEA by giving the participants a common overview of both system artefacts and the relevant failures aspects, which was used for discussions and understanding.
Notes. From the data collected we saw that the notation was improved gradually during the sessions. Although the participants did not use much time for learning the notation in advance, they applied it quite easily. From this we conclude that FSD is a light-weight technique that can easily be used to support FMEA. The entire notation was not used, but the notation that was used was helpful and adequate in supporting the FMEA.

5.2 How Should the Two Techniques Be Used Together?

Verbal. How FSD and FMEA can be used together was commented on several times in the three sessions. Firstly, there was a discussion about in which order the techniques should be applied, resulting in three strategies of using the techniques together: sequentially, with either technique being used before the other, or in parallel. The benefit from using the techniques in sequence, done in the first and second sessions, seemed lower than parallel use. The FMEA worksheet structure was missed when using the techniques sequentially compared to when using them in parallel. Secondly, it was discussed that the FMEA allowed for more specific brainstorming on the failure modes, which was neglected when only using FSD. From this we conclude that it is best to use the techniques in parallel. It allows for better brainstorming and a more structured approach through FMEA, while FSD offers the overview of components and details about their interactions, along with relevant failure effects.

Interactions. FSD was used interactively for explaining and exploring how the system works and for ensuring a common understanding among the participants. We could see from the increased common understanding of the participants that there was a benefit from first drawing the normal sequence of messages with FSD, then using the FMEA for brainstorming on the failure modes and causal factors, before going back to the FSD to

discuss and explore the effects of the failures. Whereas completing the FMEA worksheet first, and then using the FSD for drawing the results gave a good verification, the understanding of the system was not as good among the participants. Conversely, when using the FSD first and then summarizing with the FMEA worksheet, understanding was better, but there was a lack of structure and brainstorming. We conclude that using the two techniques in parallel gave the best results and the optimal use of the two techniques together.

Notes. Only parts of the notation were used and the notation that was used was not always used correctly during the first two sessions. For the last session more of the notation was used, as the FMEA worksheet was used after the FSD and not in parallel. However, for the parallel use the notation that was particularly useful was *failure*, *failure effect*, *component*, *event message* and *current control*. We conclude that the FMEA worksheet covered the need for the three types of notes and the recommended action.

5.3 Can FSD Cover the Weakness of FMEA?

Verbal. The previously described common understanding between the participants could be compared to the use of adequate system documentation as input to the FMEA without support from FSD. It is a general weakness of techniques that do not allow for interactively exploring a system while assessing it. The use of FSD generated discussions on how the system worked, especially how the components interact with respect to failures. Some of the discussions would not have taken place only using FMEA and system documentation. FMEA's weakness is that it does not allow for assessing multiple failures. The discussion suggests that FSD would become too complex for showing multiple failures in one diagram. Although multiple failures were not modelled with FSD, the discussions revealed that FSD gave a good overview and understanding of the system. Through the graphical notation and overview obtained it supports the participants in keeping other identified failures in mind.

Interactions. Much time was spent on investigating the interaction between components. In the first session FMEA was used before FSD. When the participants started using FSD they did not only draw the diagrams, but used the FSD for pointing, referring and explaining the interaction of components and how failure effects propagated through the system. Although FMEA had already been used, the interactive use of FSD, exploring and explaining to each other, increased the participants' understanding of the system failures and interaction between components in particular.

Notes. While our observations indicate that FSD is not suitable for modelling multiple failures, we find the use of the alt operator promising for showing multiple system effects. The effects of a failure propagating through the system could be connected to other failures identified in the system. Nevertheless, we conclude that FSD is limited in covering this weakness of FMEA.

5.4 Analysis of the Interview

The interviews mainly showed that the FSD increased the understanding among the participants of how the system worked, especially through the visual notation and

allowing for an interactive use. They preferred to use FSD and FMEA in parallel, not in sequence, but saw the benefit of using FSD first to ensure a common understanding of the system. They stressed that FMEA should be used to give the structure of the analysis. Some of the participants also stated that more time was spent, but that they felt more sure about the analysis being thorough.

From the answers to our questions we observed that the participants perceived the technique as useful. It indicated that FSD was easy to use, but that more time would be needed for learning the notation, and remembering it. All participants would use the technique again, but some made it contingent on using it in a group and if they believed that it would help making all participants understand the system under assessment. Most of the participants agreed with our findings from the case study, but some of them mentioned not always paying attention to use the notation correctly.

5.5 Threats to Validity and Reliability

There are several threats to validity of case studies [15] and in the following we discuss construct validity, external validity, internal validity and reliability.

A threat to construct validity is whether we identified the correct operational measures for the concepts being studied. To handle this threat we have focussed on using common, well-understood vocabularies that are common in the security, safety and modelling areas, and we have used the interviews to let the participants comment on our summary of the case study.

Threats to external validity are concerned with whether a study's findings can be generalized. As is common for a single case study, external validity is limited for our study, since we studied a specific system in a specific organization with only one project. However, there may be some generalizability because we used FSD together with a commonly used technique on a change in natural environments that will have to be implemented in all ATM systems of the European ANSPs.

In this work internal validity can be threatened when concluding on the data collected. To address this threat we have used video recording for analysing the data, allowing thorough data analysis. Nevertheless, the threat could have been further reduced if including more researchers in the analysis of the data, but was not possible due to the wish of the ANSP to be anonymous.

Reliability is concerned with whether the data collection can be repeated with the same data obtained. For this we have addressed our procedure for conducting the case study. As the ANSP organization preferred anonymity, it was not possible to include examples of the data collected. They did not wish the organization's procedures and documentation related to their systems to be published or referenced. However, most of the procedures are based on standards and guidelines which are commonly used by ANSPs in Europe.

6 Discussion

Previous sections show that the participants were able to use FSD with little prior training. In the first session they were enthusiastic about using the FSD. Several were involved in drawing and explaining by use of FSD. We observed that the mutual

understanding of the different components and their role in the total system increased when using the FSD. Furthermore, when developing the FSD in parallel with FMEA, we also saw their mutual understanding of the system increase. In the third session we witnessed the same, but it also became evident that not using the FMEA worksheet gave a disadvantage due to the lack of structure with respect to brainstorming for failure modes and causal factors. Although some information was recorded in the worksheet, the participants felt that it was important to have a brainstorming session, ensuring the complete set of failure modes and causal factors being assessed.

6.1 Sequence Diagrams and Failure Notation

One could argue that performing FMEA on a sequence diagram (SD) without the failure notation could give the same effect. From our observations however it is clear that the interaction between the participants when drawing the diagrams and including failure notation has an own benefit, particularly evident when modelling how the effects of a failure propagate through the system. The notation forces the participants to identify how the interacting components react to failures. Also the related notation for mitigations of the failures and their effects is valuable, as it makes the participants consider the different components for best possible failure mitigation. Although the notation was not used correctly in the beginning, it was clear that it improved and that the participants needed to gain experience. Their understanding of the notation also became clear as they corrected each other during the study. We conclude that FSD was easy to use for the participants. Using existing SDs as an input to FSD and extend them with the failure notation, would give a further benefit with respect to time and effort. The ANSP organization does model some of their systems with UML, but not with SD at the time. However, SD is utilized in ATM [16], and our work of integrating it with safety should be of particular interest. Other safety domains can also benefit of using our approach, especially those familiar with SD and FMEA.

6.2 The System Assessed and Decomposition

Only parts of the notation were used by the participants, but we do not conclude that there is no need for the full notation. The system analysed was only a small part of a system, and the analysis was only about a minor change of this system. Therefore, not all the parts of the notation fitted. If the analysis would be on a system under development we believe that, e.g., the use of recommended action would increase and current control decrease accordingly.

When using the notation we observed challenges caused by increased complexity when assessing software components with the FSD and recognize the necessity of reducing such complexity. SD offers this through decomposition and we see the need for incorporating decomposition into FSD when used for detailed assessment of software components. In this case the participants felt that such a detailed level was not necessary, since no major software changes were needed for introducing FMTP. Specialized versions of FMEA exist for assessing software, and FSD should be capable of supporting these if the decomposition feature is adopted.

6.3 Tool Support

While using FSD we also noted general comments about tool support. The participants perceived FSD as helpful, but pointed out that a tool would make it possible to integrate FMEA and FSD further. A tool could give FSD the needed structure from the FMEA worksheet and allow for collecting all the relevant information directly in the FSD. Although this was not within the scope of our case study, we believe it shows their interest for FSD and possible future use.

7 Conclusion and Further Work

In this paper we have presented the new technique FSD with the results of using it to support FMEA. This was done by a case study in an ANSP organization, where the introduction of FMTP was assessed with respect to safety. FSD, when used together with FMEA, allowed for an interactive failure-oriented approach, ensuring a mutual understanding among the participants on how the system would work and would not work during failures. It allowed for looking at failure propagation through the system, with particular focus on components and their interactions.

We have shown that it is possible to use FSD for supporting FMEA and outlined an optimal usage of the techniques together. FSD is not able to cover all weaknesses of FMEA, especially not the assessment of multiple failures. FSD addresses components and their interactions in particular, which we conclude is an improvement of the FMEA technique and the overall safety assessment.

The optimal use of FSD and FMEA is to draw SDs first, then use FMEA to do a structured brainstorming for failure modes and causal factors, before drawing the effects of the failures along with mitigations. Depending on the completeness of the FSD, it should be kept for documentation purposes and have clear relations to the FMEA worksheet. During our case study, the participants in some cases used the numbering of, e.g., failure modes and system effects from of the FMEA worksheet in the FSD. If done consistently, it is an adequate way of keeping the link between the FSD and FMEA and for documenting the joint results.

Even though not emphasized by the participants, the discussions showed that FSD supports visualization of error propagation very well. One goal of FMEA is to relate an identified failure's immediate effect with the system effect, in order to analyse whether the failure can lead to system hazards. By drawing this error propagation with failure effect messages in FSD, it allows for a very sound and structured way of following a failure through the system. In the interviews the participants emphasized that by using FSD they had higher belief of correctness and completeness of the identified effects of failures, than compared to only using FMEA.

The case study gives valuable industrial experience. It shows practical use of a new technique that may not only be used for drawing diagrams, but can facilitate discussions, explore and correlate the understanding among the participants. This is valuable input to our understanding of several practical aspects on the use of these techniques. However, the FSD was not evaluated for its effectiveness to identify failures, related effects and mitigations. Therefore, experiments on comparing it to other techniques would be valuable, such as [6].

Further work will explore the decomposition feature of SD and how it can be incorporated into FSD to support FMEA of software components. We will also investigate how FSD can support FMEA in analysing multiple failures, as the overview of components and their interactions should be suitable for this. Finally, we will conduct further evaluations by applying our approach to a system under development, to further investigate the techniques for mitigation identification.

Acknowledgement. We would like to thank Peter Karpati and Guttorm Sindre for sharing their observations and viewpoints. Furthermore, we thank Vikash Katta for sharing his ideas and material on MUSD. Finally, the Norwegian Research Council is thanked for financing our research.

References

1. SESAR Joint Undertaking, http://www.sesarju.eu/about
2. Unified Modeling Language, http://www.uml.org/
3. Eurocontrol: Air Navigation System Safety Assessment Methodology. Ed. 2.1 (2006)
4. Eurocontrol Safety Assessment Methodology Task Force: Functional Hazard Assessment – Guidance Material B1. Ed. 2.0 (2004)
5. Ericson, C.A.: Hazard Analysis Techniques for System Safety. John Wiley & Sons Inc., New Jersey (2005)
6. Katta, V., Karpati, P., Opdahl, A.L., Raspotnig, C., Sindre, G.: Comparing Two Techniques for Intrusion Visualization. In: van Bommel, P., Hoppenbrouwers, S., Overbeek, S., Proper, E., Barjis, J. (eds.) PoEM 2010. LNBIP, vol. 68, pp. 1–15. Springer, Heidelberg (2010)
7. Avizienis, A., Laprie, J., Randell, B.: Fundamental Concepts of Dependability. Research Report No 1145, LAAS-CNRS (2001)
8. David, P., Idasiak, V., Kratz, F.: Towards a better interaction between design and dependability analysis: FMEA derived from UML/SysML models. In: Proc. ESREL 2008 and 17th SRA-Europe Annual Conference, Valencia (2008)
9. Stålhane, T., Sindre, G., du Bousquet, L.: Comparing Safety Analysis Based on Sequence Diagrams and Textual Use Cases. In: Pernici, B. (ed.) CAiSE 2010. LNCS, vol. 6051, pp. 165–179. Springer, Heidelberg (2010)
10. Guiochet, J., Vilchis, A.: Safety analysis of a medical robot for tele-echography. In: Proc. of the 2nd IARP IEEE/RAS Joint Workshop on Technical Challenge for Dependable Robots in Human Environments, Toulouse, pp. 217–227 (2002)
11. Eurocontrol: EUROCONTROL Specification of Interoperability and Preformance Requirements for the Flight Message Transfer Protocol (FMTP). EUROCONTROL-SPEC-0100 (2007)
12. Commission of the European Communities: Regulation 633/2007 Laying down requirements for the application of a flight message transfer protocol used for the purpose of notification, coordination and transfer of flights between air traffic control units (2007)
13. Davis, F.D.: Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. MIS Quarterly 13, 319–340 (1989)
14. Stallings, W.: Data and computer communications. Prentice Hall, New Jersey (2000)
15. Yin, R.K.: Case Study Research. SAGE, California (2009)
16. Eurocontrol: EUROCONTROL Specification For On-Line Data Interchange (2007)