Addendum to: "Combined Assessment of Software Safety and Security Requirements — An Industrial Evaluation of the CHASSIS Method"

Christian Raspotnig[1 2], Peter Karpati[2], and Andreas L. Opdahl[1]

[1] Department of Information Science and Media Studies, University of Bergen, N-5020 Bergen, Norway
[2] Software Engineering Department, Halden Reactor Project/Institute for Energy Technology, P.O. Box 173, N-1751 Halden, Norway

Abstract. This addendum contains further details about the two case studies reported in our paper *Combined Assessment of Software Safety and Security Requirements — An industrial evaluation of the CHASSIS method.*

1 The Radio Systems Case

1.1 Participants

In this case the two participants took part in all the activities. We will refer to them as *Informant-1-RadioSystemsSupplier* and *Informant-2-RadioSystemsSupplier* (participants in case 1, person 1 and 2).

Informant-1-RadioSystemsSupplier and *Informant-2-RadioSystemsSupplier* had 25 and 15 years of working experience from the IT industry. They were both experienced in system modeling and safety assessments, but had no practical experience with the hazard and operability study (HAZOP) method. They had both tried modeling with UML and conducting security assessments, but were not experienced.

1.2 Advance-prepared UC and feedback on T-UC

Before the evaluation, the first author created D-UC, T-UC and SD of a typical radio system used in ATM, based on his experiences with ATM and radio systems. The D-UC included an air-traffic control officer as an actor and use cases of transmit and receive radio message. These were further described by a T-UC. A SD was created prior to the meeting to show the components involved in the transmission of a radio message.

We presented the advance-prepared D-UC and T-UC to collect feedback on the realism of our descriptions. The D-UC and T-UC were compared to the system developed by the company, in order to change incorrect parts. We had also

Name	Transmit radio message
Iteration	1
Summary	An air-traffic control officer is transmitting a radio message to an aircraft
Basic path	bp1. Pushed transmit button activates radio client modulation bp2. Radio client records information bp2.1. Radio client transforms voice to digital signal (packets) bp2.2. Radio client sets frequency to transmit on bp3. Radio client sends packets to radio server bp4. Radio server identifies frequency to send on bp5. Radio server sends packets to correct radio bp6. Radio converts to AM (amplitude modulated) signal and sends to the antenna
Alternative paths	ap1. Replaces bp3,4,5: Radio client sends directly sends to radio ap2. Replaces bp3,4,5: Has analog interface to the channel (would be done with other boxes)
Exception paths	ep1. Affects all bps. Failure in network, will not have any communication. Dual network.
Extension points	
Triggers	tr1. Transmitter button pushed
Assumptions	as1. Systems work as expected as2. If failure of system, air-traffic control officer will be made aware of it. Side tone.
Preconditions	preC1. Setting the correct frequency preC2. Radio channel is free for communication
Postconditions	postC1. Radio message was sent to antenna.
Related business rules	
Authors	*Informant-1-RadioSystemsSupplier* and *Informant-2-RadioSystemsSupplier*
Date	27.03.2012

Table 1. A T-UC describing the transmit radio message from the *RadioSystems* case.

prepared three SDs in advance, but did not prioritize the walkthrough of these with the participants. This was because the participants were able to correct the T-UC in such a way that the SDs could easily be modified accordingly.

D-UC: The D-UC was just briefly shown to the participants, and they did not have any particular comments to it.

T-UC: There was a comment in the T-UC on the terminology used, i.e., they would use the term *radio server* instead of *radio central*. They did also comment that the radio system would communicate with a radio mast. Another comment was that the radio mast broadcasts an analog signal and that the conversion from digital to analog signal would have to be done before the radio mast was broadcasting the analog signal. Except from these few corrections, they found the basic path description as a realistic example of how their system would work.

During the introduction, we completed the alternative path, the exception path, assumptions, pre- and post-conditions together with the participants. The participants did not need much facilitation in order to understand and provide information to complete parts of T-UC. For the pre- and post-conditions there were some changes after a discussion on what it actually expected. Another T-UC named *receive radio message* was filled fast by reusing the information from the *transmit radio message* T-UC. While filling the exception path of the former T-UC, we noticed that the participants began to discuss and give information on failures of different components of the system, and we commented that we would look into this while going through the safety MUC and FSD. There was some confusion related to alternative paths and exception paths. Moreover, exception paths were perceived as a part of T-UC where failures could be documented.

1.3 Safety assessment

D-MUC: The safety D-MUC session produced three misuse cases: *communication failure*, *double transmission* and *interference*. A flip over was used to draw the D-MUC and the photo of the resulting safety D-MUC is shown in Figure 1. This part of the case study took about 17 minutes.

The first misuse case *communication failure* was identified through a discussion of how to interpret the guideword late together with the use case transmit. Based on the discussion about the possibilities of delays in their system, it was suggested to use the guideword "no" instead to fit with the identified misuse case *communication failure.* The participants discussed technical details about the communication system, i.e., the protocol the system would have to use in order to have a delay. *Informant-2-RadioSystemsSupplier* raised a question about the abstraction level of the communication channel, which was answered by *Informant-1-RadioSystemsSupplier* and confirmed by us to be at a higher abstraction level. The *communication channel (CC)* is drawn as the misactor in the D-MUC.

We further facilitated the D-MUC session by asking for more failures and the next misuse case *double transmission* was suggested by *Informant-1-RadioSystemsSupplier*. He explained that this misuse case has the same effect as communication failure, but that it cannot be mitigated so easily. A discussion followed on whether the *double transmission* misuse case threatens both the *transmit* and the *receive* UCs. First, *Informant-1-RadioSystemsSupplier* and *Informant-2-RadioSystemsSupplier* agreed that it threatens both. However, after drawing the line indicating that it also threatens the *transmit* UC and moving on to identify other misuse cases, *Informant-1-RadioSystemsSupplier* returned to the drawn D-MUC and stated that it only threatens the *receive* UC. We agreed taking a whole system view and that in such a view the *double transmission* would threaten both UCs. The air-traffic control officer (ATCO) and *flight crew (FC)* were identified as the possible causes.

The last misuse case *interference* was identified after we referred to the guideword "no" again and combined it with the *receive* UC. Details on the cause for interference were given and drawn as a misactor.

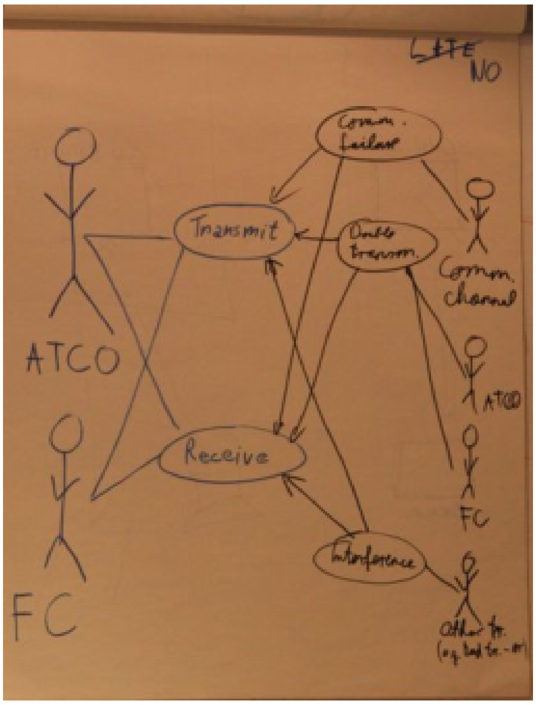


Fig. 1. The created safety D-MUC by use of the guideword "no".

Informant-2-RadioSystemsSupplier commented on the abstraction level of the MUC; there were many causes for communication failure and it made sense not to further break it down at this stage. There was a short discussion on which misuse case to use for further safety assessment. *Informant-1-RadioSystemsSupplier* argued that the double transmission was the most critical, as it would be harder to detect and mitigate. *Informant-2-RadioSystemsSupplier* did point out that there were several other communication failures that could go undetected and therefore are critical. But, it was agreed to use the double transmission for the further safety assessment.

T-MUC: The next step in the safety assessment was to use the T-MUC to detail the misuse case *double transmission.* Because of time constraints, only the most essential part of the T-MUC was filled. In Table 2 the resulting T-MUC is shown.

As seen in the Table 2, the T-MUC details the misuse case drawn in the safety D-MUC. However, the T-MUC was not filled right after the D-MUC session because it was suggested to switch to the FSD. During the FSD session, we recorded some information in parallel in the T-MUC, but then involved the participants after the FSD session to confirm the collected information and to fill the remaining fields. The total time used to discuss the T-MUC and then fill

Name	Double transmission
...	...
Basic path	bp1. flight crew and air-traffic control officer initiate the transmitting at the same time bp2. Other flight crew might receive the double transmission bp3. flight crew and air-traffic control officer releases the transmitting button at the same time
Mitigation points	mp1. If another flight crew hears double transmission and makes air-traffic control officer/flight crew aware of the double transmission mp2. If double transmission happens less than specific timeframe, receiver recognizes it and informs the voice-communication system. mp3. Procedure for re-transmit after a certain amount of time
Assumptions	as1. In bp1: Same length of transmission as2. In bp1: Communication channel is simplex as3. In mp2: double transmission does not happen at same time (resolution of some miliseconds)
Preconditions	preC1. flight crew and air-traffic control officer ready to transmit on the same time
Postconditions	postC1. The air-traffic control officer and flight crew not aware of the double transmission
Misuser profile	air-traffic control officer and flight crew (communication channel)
Authors	*Informant-1-RadioSystemsSupplier* and *Informant-2-RadioSystemsSupplier*
Date	27.03.2012

Table 2. The safety T-MUC for double transmission from the *RadioSystems* case.

out the fields was 27 minutes. However, it should be kept in mind that parts of the T-MUC was filled during the FSD session.

A few corrections were made to the already collected information. The participants used their domain knowledge to point out that a second aircraft could hear a double transmission, as amplified modulation of the VHF (very-high frequency) signal will give a tone and the message, as opposed to FM (frequency modulation), where one will not hear or recognize such a tone and message. This was then recorded as the first mitigation in the *mitigation point* field in Table 2.

We also observed how new assumptions were identified and recorded during the discussion about mitigations. There was also a discussion whether the mitigation for detecting the double transmission could lead to new hazards, and false alarms were mentioned by *Informant-1-RadioSystemsSupplier* and discussed by *Informant-2-RadioSystemsSupplier*.

As the misuser profile field had not been used for safety before, we had problems relating it to the components, actors or misactors from the D-MUC and FSD. Because of time limitations, we decided to move on with filling the HAZOP table.

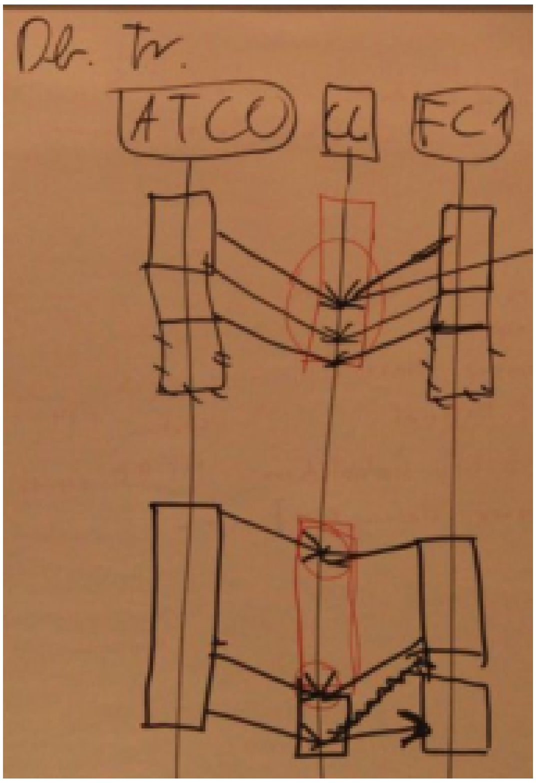
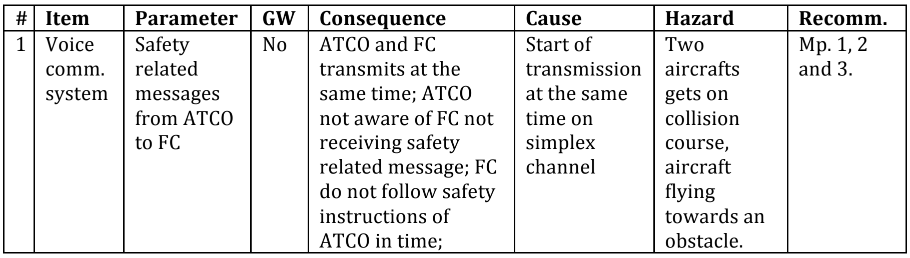


Fig. 2. The FSD representing the double transmission from the *RadioSystems* case.

FSD: The FSD session resulted in one FSD, which is shown in Figure 2. The session was partly facilitated by *Informant-1-RadioSystemsSupplier*, after we had facilitated the transition from D-MUC to FSD by drawing the *air-traffic control officer (ATCO)* and the *flight crew (FC)* as actors and *communication channel (CC)* as the system component on the flip over. This part of the case study lasted for about 12 minutes.

Informant-1-RadioSystemsSupplier was not sure whether to use the black or red color markers for drawing in the activation boxes and messages. However, when *Informant-1-RadioSystemsSupplier* was helped to draw the first activation boxes and messages on the FSD, he started using the FSD to explain concurrency of the transmissions from *air-traffic control officer* and *flight crew.* He also facilitated a discussion on how it could be detected.

Although the FSD was a simple example, it was not easy for *Informant-1-RadioSystemsSupplier* to draw the FSD. He was not familiar with the idea that time is represented downward in the diagram, by the lifeline of the components. Furthermore, he did not naturally think of using the red color to mark where the failure would happen in the FSD.



#	Item	Parameter	GW	Consequence	Cause	Hazard	Recomm.
1	Voice comm. system	Safety related messages from ATCO to FC	No	ATCO and FC transmits at the same time; ATCO not aware of FC not receiving safety related message; FC do not follow safety instructions of ATCO in time;	Start of transmission at the same time on simplex channel	Two aircrafts gets on collision course, aircraft flying towards an obstacle.	Mp. 1, 2 and 3.

Table 3. The HAZOP table created in the *RadioSystems* case.

However, *Informant-1-RadioSystemsSupplier* used the FSD to facilitate a discussion that gave new details on the double transmission. The FSD gave a good reference to discuss the misuse case and to represent the concurrency. In a discussion of whether to use the FSD at a more detailed level, *Informant-2-RadioSystemsSupplier* suggested splitting the FSD into a higher-level diagram for the consequences and a more detailed diagram for the causes. We suggested recording the new details of the double transmission scenario in the safety T-MUC.

HAZOP table: The final part of the safety assessment was to extract information for the HAZOP table, which resulted in Table 3[3]. Parts of the information had already been filled in the T-MUC and could be referred to, e.g., *Recomm. (recommendation)* in HAZOP referring to the *mitigation point* field in T-MUC. However, some clarifications were needed in order to specify the *consequence*, *cause* and *hazard*. In particular, we discussed that the hazard must be specified as a scenario at a higher level, in which the radio system is embedded in a larger ATM system.

Summary of safety assessment in the RadioSystems case: For the D-MUC, the participants initially went into technical details, but that they later realized that the technique should be used at a higher abstraction level at that stage of the safety assessment. The guideword helped the participants to brainstorm for hazards and three misuse cases were identified in 17 minutes. No mitigations were drawn (Figure 1), but some initial ideas on mitigation emerging during the discussions.

The mitigation idea became more concrete in the FSD. Still, no mitigations were drawn in the FSD. *Informant-1-RadioSystemsSupplier* partly facilitated the session; whereas he created good discussions by using the FSD as reference, explaining his and others' ideas, he did not succeed well in drawing the FSD. There was also a discussion about the level of detail in the FSD, and it was recognized that one could break the FSD down into a more detailed FSD. However, the FSD allowed discussing more details on concurrency, which we recognized as a break down of the misuse case at a lower abstraction level.

[3] The Risk and Comments column was removed to save space, as they were not used.

In the T-MUC, the concrete mitigation idea from the FSD was recorded as a mitigation point. The T-MUC was well suited to record the ideas from the discussions taking part during the D-MUC and, in particular, FSD sessions. Furthermore, assumptions were made both during the FSD and T-MUC sessions, and recording these in the T-MUC was seen as important to the participants and us.

Although the T-MUC collected and structured the information from the FSD and partly from D-MUC, the HAZOP table was useful for extracting the more general information, such as the *consequence* and *hazard* the *double transmission* could create. For the *recommendation* on how to avoid or treat the hazard, the *mitigation points* from the T-MUC could directly be referenced in the HAZOP table.

We noticed that the flow of information and ideas between the techniques was working well in the safety assessment. Although time was limited, hazards were identified and analyzed from different view points and abstraction levels.

The overall time spent for the safety assessment was 1 hour and 4 minutes. This included creating D-MUC, T-MUC, HAZOP table and FSD. Most time was spent on creating the T-MUC.

1.4 Security assessment

D-MUC: Security assessment started with the security D-MUC. When initiating the session, *Informant-1-RadioSystemsSupplier* listed some of the HAZOP guideword before they were shown with the projector to the participants. We chose the guideword “other” for the session and in combination with the UCs *transmit (Tr.)* and *receive (Rec.)*, the three misuse cases *simulating air-traffic control officer*, *initiating double transmission (regularly)* and *block normal communication* were created. These three misuse cases were investigated for *confidentiality, integrity and availability (CIA)*, which resulted in more detailed information for each of the three misuse cases. The result of applying the security D-MUC is shown in Figure 3. For this part of the case study, we used about 23 minutes.

For the D-MUC, *Informant-2-RadioSystemsSupplier* took an attacker point of view when he suggested that the attacker has an own communication system and directs it towards the *flight crew.* Furthermore, *Informant-2-RadioSystemsSupplier* continues with the thought of an attacker is attacking from a remote location, communicating with the *flight crew* without being recognized by the *air-traffic control officer*. The D-MUC starts out like a scenario and not like a higher-level threat against the UCs. When the participants are asked to associate the attack with the guideword, *Informant-1-RadioSystemsSupplier* suggests that the attacker pretends being the *air-traffic control officer* and associates it with the *integrity* attribute of the CIA triad. The participants brainstorm for how an attacker can block the communication to and from the air-traffic control officer and many ideas were created and associated with the CIA triad and other guidewords, such as “no”. This brainstorming session resulted in the misuse cases *simulating air-traffic control officer* and *initiating double transmission regularly.*

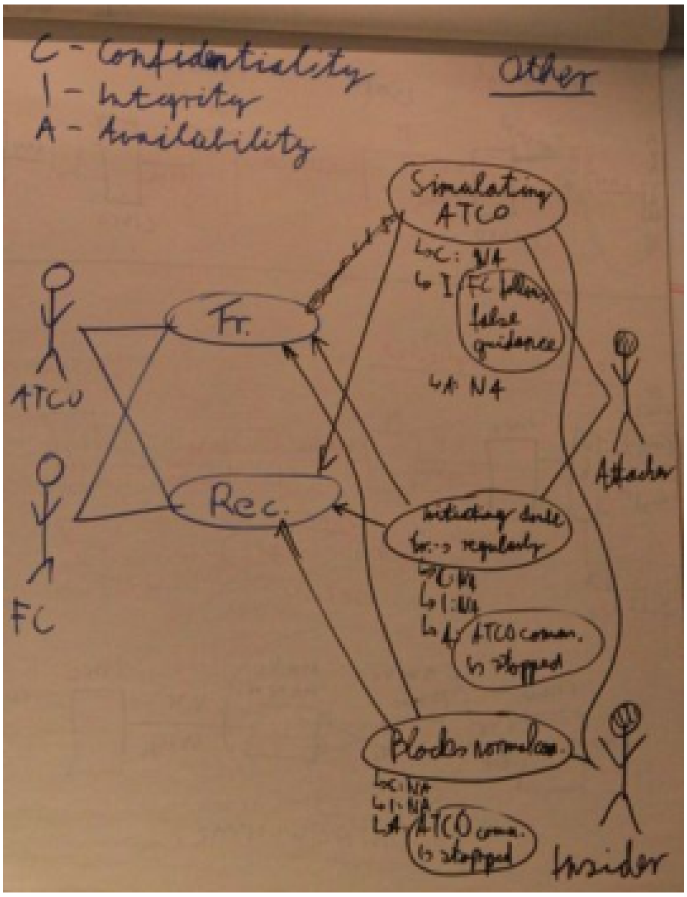


Fig. 3. The security D-MUC from the *RadioSystems* case.

The participants were asked which UCs the two identified misuse cases threatens, as they have not been associated with the UCs yet. Then *Informant-2-RadioSystemsSupplier* uses the guideword "other" and relates it to a scenario where somebody has access to the system from inside, which may allow blocking the air-traffic control officer and accessing the system directly. An *insider* is suggested as misactor and drawn together with the misuse case *blocks normal communication* to the D-MUC. *Informant-1-RadioSystemsSupplier* joins the idea and the two participants brainstorm how this could happen. At some stage in the brainstorming they stop and reflect on all the *assumptions* they have made for the scenario. *Informant-2-RadioSystemsSupplier* continues elaborating on the scenario, but suggests that the knowledge and means needed by an insider would make the scenario impossible. Finally, *Informant-2-RadioSystemsSupplier* states that the scenario is becoming quite complex and it is suggested to move on with the MUSD.

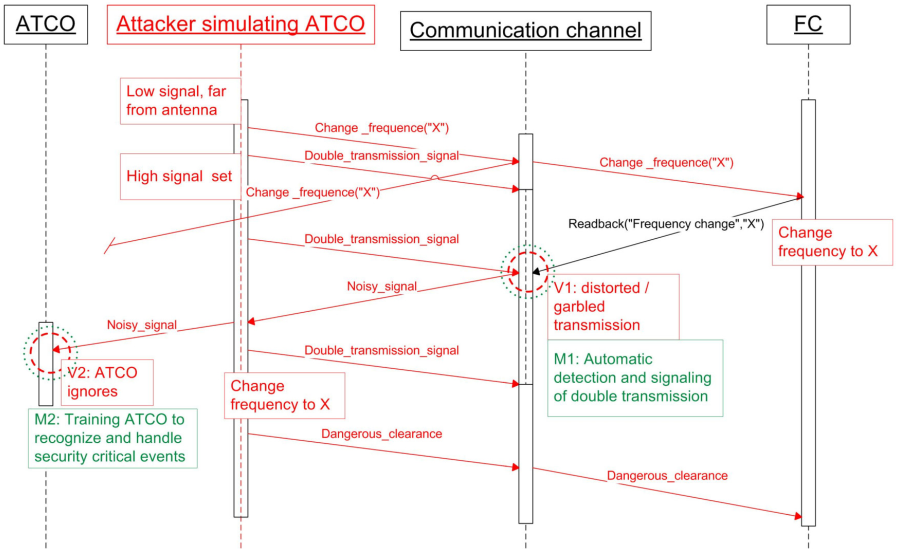

ATCO
Attacker simulating ATCO
Communication channel
FC
Low signal, far from antenna
Change _frequence("X")
Double_transmission_signal
High signal set
Change _frequence("X")
Change _frequence("X")
Readback("Frequency change","X")
Change frequency to X
Double_transmission_signal
Noisy_signal
V1: distorted / garbled transmission
Noisy_signal
Double_transmission_signal
M1: Automatic detection and signaling of double transmission
V2: ATCO ignores
Change frequency to X
M2: Training ATCO to recognize and handle security critical events
Dangerous_clearance
Dangerous_clearance

Fig. 4. The MUSD where an outsider is simulating the air-traffic control officer from the *RadioSystems* case.

In this session, the participants created the D-MUC faster and understood and adapted the technique better. The participants quickly adapted the attacheds mindset and contributed many ideas along the way.

T-MUC: Due to time limitations, it was agreed with the participants that the MUSD should be prioritized instead of making the T-MUC.

MUSD: We thus proceeded to explore use of the MUSD based on a scenario where an *outsider simulating the air-traffic control officer* was chosen based on the previous identified misuse case *simulating air-traffic control officer*. In the resulting MUSD session the focus was to facilitate a good discussion by using the MUSD technique. With the time limitations in mind it was agreed that a MUSD would only be sketched in the session and then completed by the authors after the session, to be sent and reviewed by the participants. The completed MUSD is shown in Figure 4. Time limitations did not allow using more than 10 minutes on this part.

The main actors and components involved in the scenario were sketched up in the MUSD. Both *Informant-1-RadioSystemsSupplier* and *Informant-2-RadioSystemsSupplier* took the attacker point of view, and they got involved in elaborating on how an *outsider* would *simulate the air-traffic control officer*, and at the same time avoid the air-traffic control officer noticing or being able to take back control of the situation. However, they also elaborated on mitigations, such as how an air-traffic control officer would be able to detect such a scenario and his possibilities of regaining control. The participants outlined a complete scenario, by building on each others ideas.

Summary of security assessment in the RadioSystems case: For the security D-MUC, the participants were taking the attackers point of view and elaborating on a scenario where an *attacker is simulating the air-traffic control officer* and *blocking normal communication* between the *air-traffic control officer* and the *flight crew.* The HAZOP guidewords worked well for security, and the CIA triad gave some more detailed ideas on what the attacker would do in the scenario. At some stage of the brainstorming, the participants stated that the scenario was becoming complex, which created a natural transition to MUSD.

The MUSD was used to facilitate the discussion with detailed focus on how an attacker could simulate the air-traffic control officer, thereby continuing the scenario from the D-MUC. The participants still took the attackers point of view, built on each others ideas and brought in elements from the D-MUC for further elaboration. At this stage they also identified possible mitigations.

Less time was spent on security than on safety assessment, about 35 minutes in total. Most time was spent on the security D-MUC. T-MUC was skipped. For the MUSD, there was not enough time to draw the diagram in detail.

1.5 Summary of the Radio Systems Case Study

For the use of the techniques, the participants understanding of techniques improved during the security assessments when compared to safety assessments. Whereas some time was used for the participants to understand the elements of each technique in the safety assessment, the use of techniques was more straightforward for the security assessment. It became particularly clear when starting the security D-MUC, where *Informant-1-RadioSystemsSupplier* listed some of the HAZOP guidewords before they were shown with the projector to the participants. Although we did not use the same guidewords for safety and security D-MUCs, we recognized that the participants related the guideword for security more easily to the UCs than the case was for the safety D-MUC. Also for the MUSD, their skills in modeling improved compared to FSD. We do, however, not consider this as a valid result as *Informant-1-RadioSystemsSupplier* drew the FSD whereas we drew the MUSD.

Their knowledge of the system and possible failures from the safety assessment was reused as vulnerabilities in the security assessment. The participants reused their knowledge of the *double transmission* from the safety assessment in the security attack scenario. Since they had already built a common understanding of the system, the discussions during the security assessment were more focused on the security parts. Also the double transmission detection, which was discussed as mitigation in the safety assessment, was brought into the security assessment as one way to detect the threat scenarios created by security D-MUC and MUSD.

We did not observe any confusion among the participants regarding separating the safety and security assessments. When the participants reused knowledge from the safety to the security assessment, they also translated the knowledge into a security setting.

2 The Airport Lights Case

2.1 Participants

In this case the three participants took part in all the activities (a fourth person was also present in parts of the sessions, but he was only observing without interfering and has not been included in the data collection). We will refer to them as *Informant-3-AirportLightsSupplier*, *Informant-4-AirportLightsSupplier* and *Informant-5-AirportLightsSupplier*.

Informant-3-AirportLightsSupplier, *Informant-4-AirportLightsSupplier* and *Informant-5-AirportLightsSupplier* had 22, 20 and 10 years of working experience from the IT industry. They were all experienced in safety assessments, but had less practical experience with security assessments. *Informant-3-AirportLightsSupplier* was experienced in HAZOP, while *Informant-4-AirportLightsSupplier* had tried it and *Informant-5-AirportLightsSupplier* had heard about it. Both *Informant-4-AirportLightsSupplier* and *Informant-5-AirportLightsSupplier* had tried modeling with SD, whereas *Informant-3-AirportLightsSupplier* was experienced in SD. However, none of the participants were experienced in modeling with UC and only *Informant-3-AirportLightsSupplier* claimed to have some experience with UML.

2.2 Advance-prepared UC and an updated SD

Because the system contained too many functions to model in the evaluation session, the authors decided to only model the control of airport lights. The first author modeled UC and SD of the system function based on his experiences from ATM in general, and from doing safety assessments of such a system in particular.

The advance-prepared D-UC, T-UC and SD of their system were presented to the participants in order to collect feedback on the realism and to change the incorrect parts.

SD: As shown in the photo of the projected SD in Figure 5, some changes were made to the SD.

When going through and correcting the SD, they easily understood the SD and were directly able to recognize their system and discuss the interactions. They immediately noticed that we had misunderstood their system configuration, which we errouneously had taken to include the *servers*. One of the participants stated that “it is a very good example and it is very easy to see how it works” when going through, discussing and correcting the SD. We asked whether the specific SD was clear to them and if it provided a good way to display and clarify how their system works, to which all participants agreed. Furthermore,

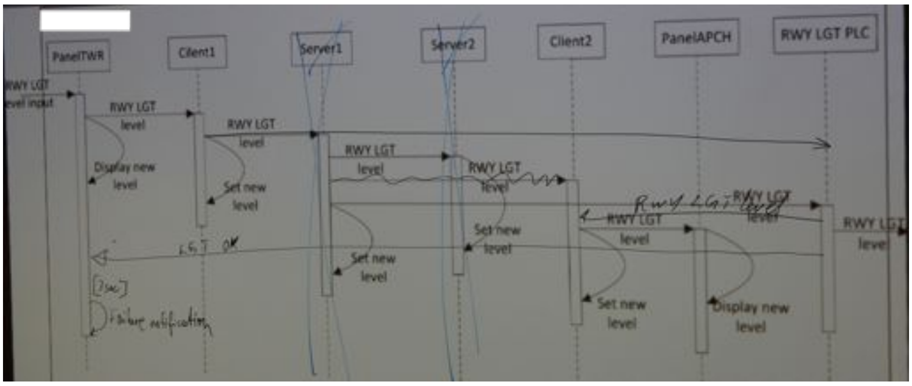


Fig. 5. SD in *AirportLights* case corrected by the participants. (RWY-LGT: Runway Lights, PLC: Programmable-Logic Controller, APCN: Airport Communication Network)

the participants discussed and corrected each others understanding of the system. The participants started discussing how their system could fail, and that SD provided a good starting point for failure analysis.

T-UC: For the T-UC, it was not that easy to relate SD and T-UC. The facilitator had to remind the participants of what the *alternative path* was about and the secretary had to write the *alternative path* example without much contribution from the participants. As the T-UC was used by the facilitator to summarize the discussion of the participants from the SD session, the participants did not contributing much with information.

2.3 Safety assessment

The safety assessment was started right after finishing the T-UC, by displaying the D-UC with a projector and presenting the guidewords to the participants. About 1 hour and 6 minutes were spent on the safety assessment part.

D-MUC: As shown in Figure 6, the D-UC are displayed with a projector to the left in the photo, whereas the corresponding D-MUC is drawn by hand and shown to the right. Two D-MUCs were created in this part of the safety assessment, which lasted for about 26 minutes. The first D-MUC took about 15 minutes to create and the second D-MUC about 10 minutes.

The guideword “no” and “late” were used to develop two D-MUCs, after some initial discussions about the guidewords. *Informant-3-AirportLightsSupplier* suggested using the guideword “fails”. Furthermore, “other” and “slow” guidewords were discussed instead of the “late”.

The misuse cases *no adjustment of runway lights* and *delayed adjustment of runway lights* were quickly identified and agreed upon. However, the participants

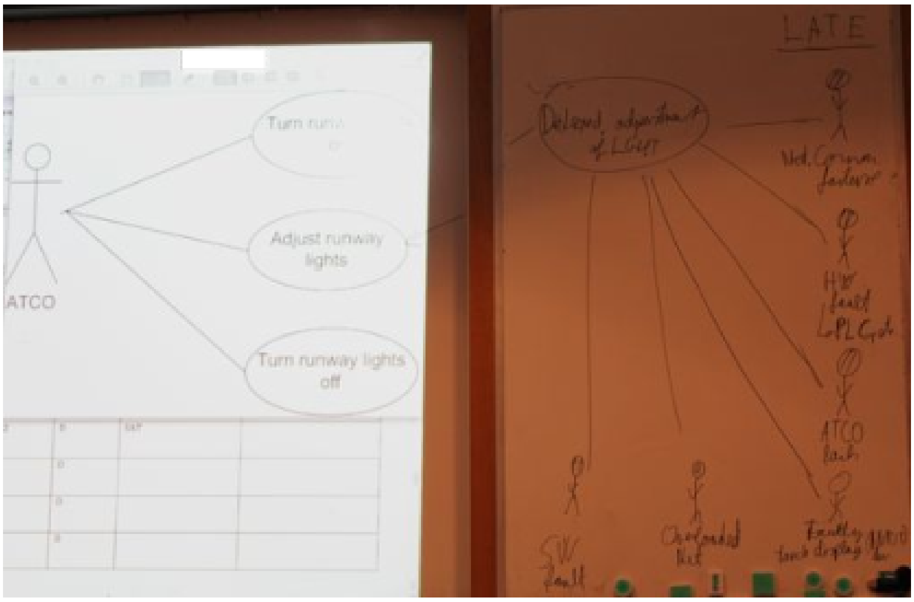


Fig. 6. Advance-prepared D-UC and created D-MUC for the guideword late in the *AirportLights* case.

also came up with conditions for the misuse cases, e.g., low visibility at an airport and the final approach phase for aircraft landing at the airport. Furthermore, the participants also explored different scenarios of not being able to adjust runway lights when they were at high intensity or low intensity. Domain knowledge was used to discuss the operating procedure for the air-traffic control officer adjusting runway lights and for aircraft in case no adjustment would be possible. The participants also used system knowledge when an "auto-lights" function was identified and discussed for relevance to the *adjustment of runway lights*.

Many potential causes for the two misuse cases were identified, which were put as misactors in the D-MUCs. It was also discussed at which level the misactors should be. They identified many parts of the architecture as misactors, and that they became more detailed in identifying causes, e.g., *software and hardware faults*. Furthermore, the participants discussed how it could happen that the *air-traffic control officer* would not be able to adjust runway lights. This was taken further in the second misuse case (*delayed adjustment of runway lights*), when the participants discussed the *human-machine interface* and how a delay of adjusting runway lights might affect the behavior of the *air-traffic control officer*. The participants also came up with a performance requirement from a standard.

T-MUC: Because of time limitations, there was no T-MUC created in the *AirportLights* case. However, there was a discussion on whether to continue with

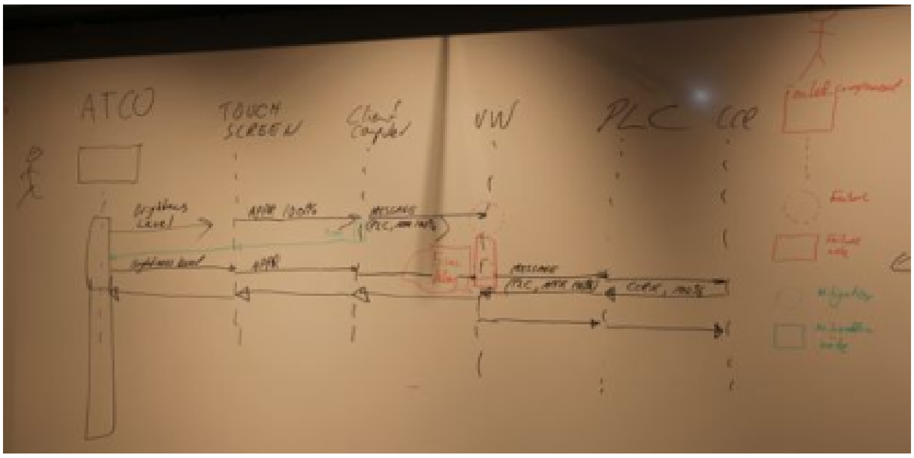


Fig. 7. The resulting FSD from the safety assessment in the *AirportLights* case.

FSD or T-MUC after the D-MUC session. We asked the participants to let us know their opinion on what they preferred and why. For T-MUC it was argued by *Informant-5-AirportLightsSupplier* that was believed to be better if one were alone, to write down the steps of D-MUC. He did, however, believe that FSD would be better suited in a group setting. *Informant-4-AirportLightsSupplier* argued that T-MUC would give more information. After a vote it is decided by the participants to continue with the FSD. However, due to the time limitations we did write T-MUC.

FSD: There was one FSD created during the safety assessment, which was partly facilitated by *Informant-3-AirportLightsSupplier*, who was experienced in SD and safety assessment as described in Section 2.1. A photo of the resulting FSD is shown in Figure 7. This part of the case study took about 33 minutes.

As shown in Figure 7, the notation for the FSD (right part) was drawn on the whiteboard before *Informant-3-AirportLightsSupplier* started facilitating the safety assessment with the FSD. In short, the FSD was created through the following steps:

1. Drawing and discussing the actors, system components and their interactions
2. Identifying the failure in the system for the scenario
3. Drawing the failure and analyzing the failures effect in the system and on the actors
4. Identifying mitigations for the failure and discussing both failure and mitigations for effectiveness

The resulting FSD in Figure 7 represents the scenario of *delayed adjustment of runway lights.*

We supported *Informant-3-AirportLightsSupplier* in the initial drawing of the SD, i.e., how to represent the *air-traffic control officer*, *network* and the lifeline with activation for the components. However, after some initial explanations, *Informant-3-AirportLightsSupplier* facilitated a good discussion on what components to include and how these interact in the system. All participants got involved in detailing the system, and they added on each others explanations while discussing. After being helped to draw the failure, we witnessed that the participants discussed several aspects of the failure, considering how the system would react and what the different actors would do if they would recognize the failure. They also considered environmental and operational settings, combining these settings into various scenarios.

All participants were involved in elaborating on the details about the failure and systems reaction. The causes for the failure were discussed, and some of the causes identified earlier in the safety D-MUC were used in the discussions. Mitigations were identified and analyzed in parallel with the failure, considering mitigations by the system and the actors.

The participants used FSD more than D-MUC during the discussions. More often, they referred to the components drawn on the whiteboard, in particular when discussing details about the failures and mitigations in the system. Whereas *Informant-5-AirportLightsSupplier* was mainly contributing in the discussions about the system and internal failures, *Informant-4-AirportLightsSupplier* was more active in providing domain knowledge of the environment and actors involved. *Informant-3-AirportLightsSupplier* took part in and facilitated both types of discussions. At several occasions *Informant-3-AirportLightsSupplier* pointed out assumptions that were made, in particular when elaborating on reactions from actors involved in the FSD.

Informant-3-AirportLightsSupplier summarized the use of FSD as "a very good way to discuss" and "go into the details and find out what is really how the system works." The participants agreed that FSD would be a good means to facilitate discussions with other stakeholders, for example air-traffic control officer and flight crew, not part of the safety assessment, in order to analyze the scenario further.

Summary of safety assessment in the AirportLights case: The FSD part of safety assessment was partly facilitated by the *Informant-3-AirportLightsSupplier.* In the safety D-MUC session, the participants were able to suggest many causes for the misuse cases. The participants quickly adopted an operational mindset (about air traffic control situations), narrowing the scenario down to a specific phase of operation and bringing in environmental effects, such as weather and time of day as factors.

It was possible to create a scenario with FSD that corresponded to one of the safety D-MUC. The participants reused their understanding created during the safety D-MUC session in the FSD session. In particular, they reused domain knowledge of environmental and operating conditions.

Only one cause of failure was used in the FSD, whereas in the safety D-MUC many causes were identified. However, we noted that the causes identified with D-MUC were on different level of abstraction. If more FSDs had been created, more causes would have been identified and modeled.

We also observed that many of the discussions during the D-MUC and FSD sessions brought up information that could have been directly recorded in the T-MUC fields, such as *pre-conditions* about weather, time of the day and flight phase, *assumptions* about air-traffic control officer and flight crew operations, *stakeholders and the risks* involved. This points in the direction of using T-MUC in parallel in these sessions to record the information given by the participants, so that it is not lost. Just a few things were recorded in the D-MUC and FSD, but compared to T-MUC they did not facilitate the recording of such information well.

A total of 1 hour and 6 minutes was spent on safety assessment. Most time was spent on the FSD.

2.4 Security assessment

D-MUC: Two security misuse cases were created in this first part of the security assessment, shown in Figure 8. The two misuse cases were created using the guideword “other”. They were similar to each other as both considered an *insider controlling the runway lights*. Whereas the first misuse case was providing the notion of an insider controlling the runway lights from an airfield lighting control substation[4], the second misuse case considered how the runway lights could be controlled through the airport computer network. The misuse cases were created in less than 10 minutes.

There was no confusion about the security D-MUC activity, even though a different guideword was suggested and short time was used to explain the guideword and how to proceed. However, there was a slight confusion for the guidephrase, as the guideword “other” and the use case could be combined in three ways: (1) *other adjustment of runway lights*, (2) *adjustment other runway lights* and (3) *adjustment of runway lights other*. Each of them gave different associations; the resulting misuse case was formed as a combination of the first and last guidephrases.

The participants did contribute with information that could have been structured with a T-MUC. They gave information about the *preconditions* for an attack, the *misuser profile* by stating needed technical equipment and knowledge. Furthermore, the participants were discussing about other possible scenarios, e.g., how an insider could enter the airport and get access to the airfield lighting from the sub-stations and alternative ways of getting access to the runway lights through the airport computer network.

T-MUC: Because of time limitations, there was no T-MUC created for the security assessment in the *AirportLights* case. However, it was observed that several of the fields contained in a T-MUC could have been used to record and structure the information given about the misuses described with D-MUC and MUSD.

[4] The sub-station is on the airfield and provides direct access to controlling the various taxiway and runway lights on the airport.

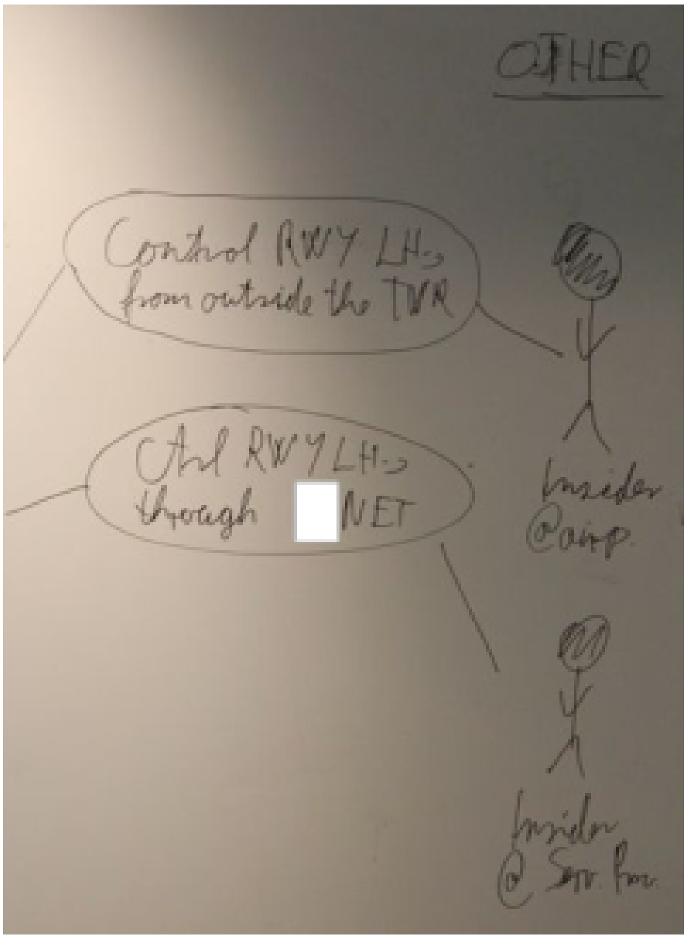

OTHER
Control RWY LH-> from outside the TWR
Ctrl RWY LH-> through [redacted] NET
Insider @airp.
Insider @ Sw. Pow.

Fig. 8. The security D-MUC created in the *AirportLights* case. (TWR: TOWER, NET: NETWORK)

MUSD: Both misuse cases were further described or explored with MUSD, but the misuse case where an insider is controlling the runway lights from the substations was given most focus and time. We did, however, observe that the participants were able to quickly and easily make the second MUSD, by adapting the information from the first MUSD to the second misuse case. About 19 minutes were spent on the MUSD.

Informant-3-AirportLightsSupplier took the role as the facilitator and drew both MUSDs. The initial discussion with the MUSD was how and where the *insider* would access the airfield lighting system. The next step was to draw the components between the access point and the actual runway lights, where they already had a clear idea of the components involved. Thereafter, a discussion followed about the insider preventing the air-traffic control officer from interven-

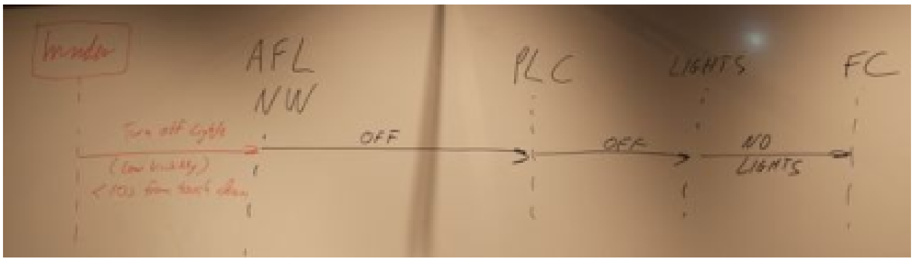


Fig. 9. The first MUSD drawn in the *AirportLights* case. (AFL NW: Airfield Light Network, PLC: Programmable-Logic Controller)

ing in shutting off the runway lights. Furthermore, there was a brief discussion on other light systems at the airport, and the possibility of the insider attacking the stop-bar lights[5] as well as the runway lights. Because of time constraints, we asked the participants to concentrate on the simpler scenario with only runway lights involved.

They used the same environmental and operational conditions as for the FSD, and that these were written on the whiteboard as the interaction sequence from the insider was drawn. They did, however, add new domain knowledge into the discussions, e.g., different types of aircraft involved, the combinations of attacking the *integrated landing system* as well as the runway lights and other weather conditions such as strong side winds. *Informant-4-AirportLightsSupplier* brought in domain knowledge about the most critical period of the flight phase[6].

There was a slight confusion when drawing the messages, whether black or red color should be used, especially when drawing the last message, going from *lights* to *flight crew*, as shown in Figure 9. The participants questioned whether this was normal system behavior, and we discussed that on the one hand it is allowed system behavior, but on the other hand it should somehow be marked that the harm can happen.

At some stage of the discussion the participants also elaborated on possible mitigations, e.g., how the air-traffic control officer could notice that the runway lights would be turned off. They took the attacker point of view and came up with new attacker steps to avoid that the air-traffic control officer could interfere or how the runway lights could be turned off without the air-traffic control officer noticing.

Summary of security assessment in the AirportLights case: During the security D-MUC session, the generation of misuse cases was very dependent on the way the UC is phrased and how the guideword is applied with UC. We see the

[5] Stop-bar lights are used at the holding point before entering the airport. The air-traffic control officer uses it as a safety barrier, to prevent an aircraft from taxiing out on the runway, e.g., for take-off while another aircraft is landing on the same runway.

[6] It was stated to be the last 10 seconds before touch down on the runway.

potential for guidephrase generation, e.g., a list of the different combinations of guidewords and UC phrases. This could be automatic if ontologies are used. It could add to the completeness of the D-MUC modeling security.

In the transition from D-MUC to MUSD, the focus was put on how an attacker could access the airfield lighting system. The D-MUC session was kept at a higher abstraction level, as the participants were discussing the capabilities of an attacker and were he could attack. The MUSD was facilitated by *Informant-3-AirportLightsSupplier* and the participants came of up with several ideas for relevant operational and environmental factors. In the MUSD session the discussion were at a lower abstraction level, but at the same time the threat to the aircraft was put forward, which is at a higher abstraction level.

Just as for the safety assessment there was not enough time to use T-MUC, but much information was given during the D-MUC and MUSD sessions that could have been recorded in the T-MUC fields.

For the security assessment only 34 minutes were used. The MUSD session was the longest session during the security assessment sessions.

2.5 Summary of the Airport Lights Case Study

The participants reused many of the ideas from the safety assessment for the security assessment. The scenarios created by the participants, in particular during the FSD session, gave a common understanding, which was used in both safety and security assessments. In particular we noticed that they reused knowledge of the system, the domain, functionality, components, environment and assumptions. Although the interconnectivity of the airfield lighting system was the main aspect for the safety assessment, the network of the airfield lighting system became more important during the security assessment, and the participants gave more details when describing it.

In the security assessment, the participants knew what to do when using the techniques. *Informant-3-AirportLightsSupplier* continued to facilitate with the MUSD technique, so there was a learning effect from safety part, in particular from the FSD. Furthermore, they seemed to more naturally align to the scope of assessment and limitations, what to discuss and not, when applying the security assessment.

They were able to distinguish the safety part from the security part. We did, however, observe that *Informant-5-AirportLightsSupplier* once mentioned an example of a malicious act against the air-traffic control officer in the safety assessment part. This seemed more as a comment than a suggestion of cause and it was not followed up on, neither by us nor by *Informant-5-AirportLightsSupplier* in the post-study questionnaire.

3 Replies to the post-study questionnaire

The questions were sent to the participants after the sessions and returned in a few days. Four participants answered the questions, whereas participant

Informant-4-AirportLightsSupplier replied that he did not have time to give any answers. The questionnaire had two parts:

The first part contained 24 statements that we asked the participants to rank on a Likert-like scale ranging from 1—strongly disagree to 5—strongly agree. Table 4 shows the answers. The grey-marked questions in the questionnaire were concerned with issues that we did not introduce the participants to or have time for during the case study. We gave them the option of leaving them blank or, if they liked, they could give us their opinion of how they think it would, i.e., if they would have been introduced to it. When the statements were not ranked/left blank, we have put the participant(s) in the NA ("Not Answered") column to the right.

The section part contained 8 open-ended questions to the participants to allow them detailing their experiences with CHASSIS. The participants from the *RadioSystemsSupplier* chose to give their common answers, while *Informant-3-AirportLightsSupplier* and *Informant-5-AirportLightsSupplier* answered the questions individually.

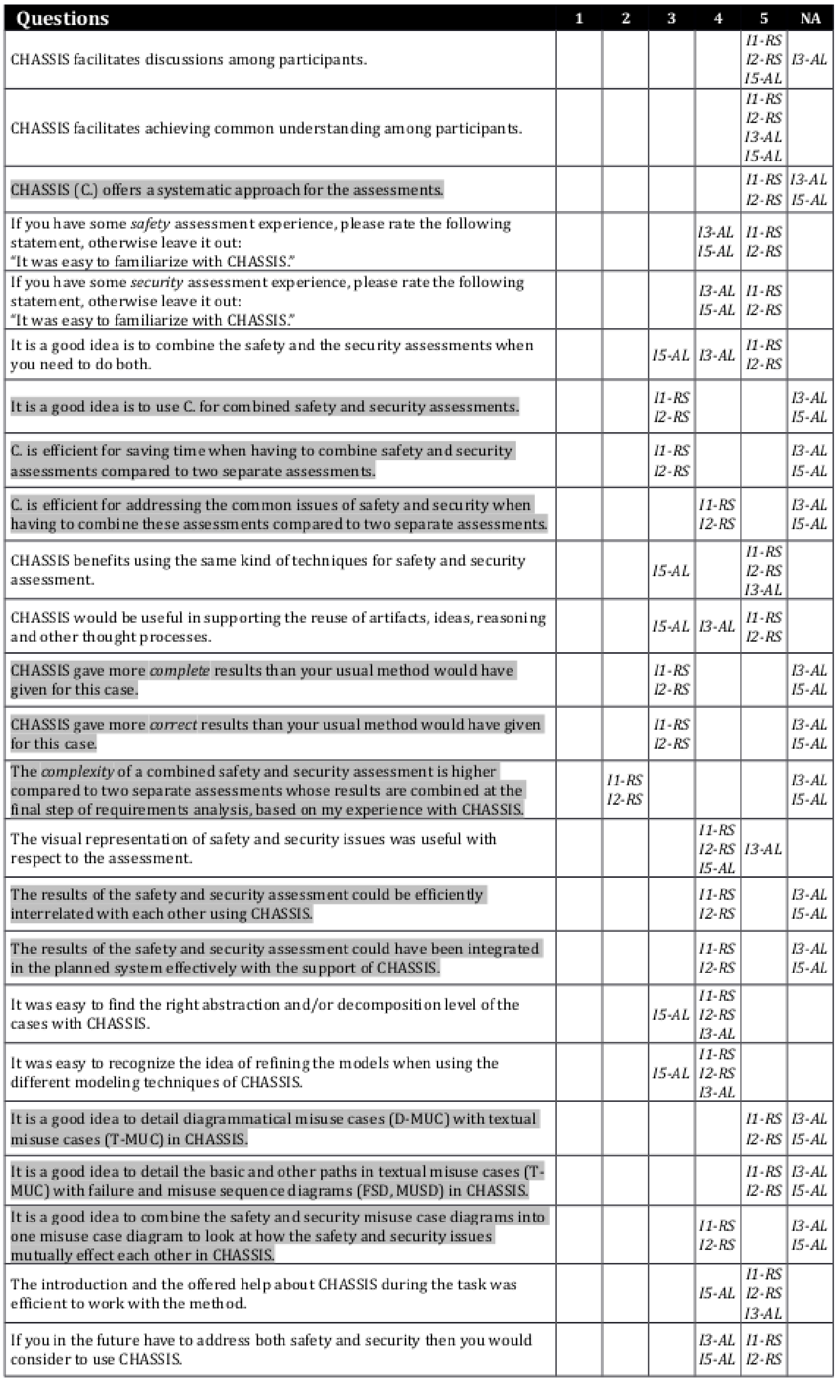
3.1 Ranking of statements

Of the issues we had introduced the participants to, they agreed most strongly that CHASSIS facilitated *discussions* and common understanding among participants. They also supported the statements that it was *easy to familiarize* with CHASSIS both from a safety and a security background, that it was efficient to work with the method, and that they would *consider to use CHASSIS again* in the future. None of the issues we had introduced the participants to received negative scores, although *Informant-5-AirportLights* was neutral (score 3) on 5 of the issues (while positive, score 4 or 5, on the rest).

Among the issues we did not have the time to introduce the participants too, the two who rated it both disagreed with the statement that *the complexity of a combined safety and security assessment is higher compared to two separate assessments whose results are combined at the final step* of requirements analysis.

3.2 Answers to questions

Asked about the *strengths of CHASSIS*, The participants from the *RadioSystemsSupplier* found the method easy to understand, to which *Informant-3-AirportLightsSupplier* added ease of use. The participants from the *RadioSystemsSupplier* also mentioned that the visual approach makes it easy to discuss and to distribute knowledge to others. *Informant-5-AirportLightsSupplier* agreed that the visualization of safety and secrity risks makes it easy for participants to understand and to participate in discussion. Considering what they *liked about CHASSIS*, *Informant-3-AirportLightsSupplier* liked that it presented both graphical and textual information of system to be analyzed. The diagrams were good to show during discussions. *Informant-5-AirportLightsSupplier* liked the sequence diagrams.



Questions	1	2	3	4	5	NA
CHASSIS facilitates discussions among participants.					I1-RS I2-RS I5-AL	I3-AL
CHASSIS facilitates achieving common understanding among participants.					I1-RS I2-RS I3-AL I5-AL	
CHASSIS (C.) offers a systematic approach for the assessments.					I1-RS I2-RS	I3-AL I5-AL
If you have some *safety* assessment experience, please rate the following statement, otherwise leave it out: "It was easy to familiarize with CHASSIS."				I3-AL I5-AL	I1-RS I2-RS	
If you have some *security* assessment experience, please rate the following statement, otherwise leave it out: "It was easy to familiarize with CHASSIS."				I3-AL I5-AL	I1-RS I2-RS	
It is a good idea is to combine the safety and the security assessments when you need to do both.			I5-AL	I3-AL	I1-RS I2-RS	
It is a good idea is to use C. for combined safety and security assessments.			I1-RS I2-RS			I3-AL I5-AL
C. is efficient for saving time when having to combine safety and security assessments compared to two separate assessments.			I1-RS I2-RS			I3-AL I5-AL
C. is efficient for addressing the common issues of safety and security when having to combine these assessments compared to two separate assessments.				I1-RS I2-RS		I3-AL I5-AL
CHASSIS benefits using the same kind of techniques for safety and security assessment.			I5-AL		I1-RS I2-RS I3-AL	
CHASSIS would be useful in supporting the reuse of artifacts, ideas, reasoning and other thought processes.			I5-AL	I3-AL	I1-RS I2-RS	
CHASSIS gave more *complete* results than your usual method would have given for this case.			I1-RS I2-RS			I3-AL I5-AL
CHASSIS gave more *correct* results than your usual method would have given for this case.			I1-RS I2-RS			I3-AL I5-AL
The *complexity* of a combined safety and security assessment is higher compared to two separate assessments whose results are combined at the final step of requirements analysis, based on my experience with CHASSIS.		I1-RS I2-RS				I3-AL I5-AL
The visual representation of safety and security issues was useful with respect to the assessment.				I1-RS I2-RS I5-AL	I3-AL	
The results of the safety and security assessment could be efficiently interrelated with each other using CHASSIS.				I1-RS I2-RS		I3-AL I5-AL
The results of the safety and security assessment could have been integrated in the planned system effectively with the support of CHASSIS.				I1-RS I2-RS		I3-AL I5-AL
It was easy to find the right abstraction and/or decomposition level of the cases with CHASSIS.			I5-AL	I1-RS I2-RS I3-AL		
It was easy to recognize the idea of refining the models when using the different modeling techniques of CHASSIS.			I5-AL	I1-RS I2-RS I3-AL		
It is a good idea to detail diagrammatical misuse cases (D-MUC) with textual misuse cases (T-MUC) in CHASSIS.					I1-RS I2-RS	I3-AL I5-AL
It is a good idea to detail the basic and other paths in textual misuse cases (T-MUC) with failure and misuse sequence diagrams (FSD, MUSD) in CHASSIS.					I1-RS I2-RS	I3-AL I5-AL
It is a good idea to combine the safety and security misuse case diagrams into one misuse case diagram to look at how the safety and security issues mutually effect each other in CHASSIS.				I1-RS I2-RS		I3-AL I5-AL
The introduction and the offered help about CHASSIS during the task was efficient to work with the method.				I5-AL	I1-RS I2-RS I3-AL	
If you in the future have to address both safety and security then you would consider to use CHASSIS.				I3-AL I5-AL	I1-RS I2-RS	

Table 4. Answers to statement with a five point scale (from 1—strongly disagree to 5—strongly agree, RS: RadioSystemsSuppliers, AL: AirportLightsSupplier).

When asked about the *weaknesses of CHASSIS*, The participants from the *RadioSystemsSupplier* wondered whether the diagram notations might become too complex for some cases, leading to loss of overview. *Informant-5-AirportLightsSupplier* was not convinced that CHASSIS was a better way to trap risks and hazards than conventional Failure Mode and Effect Analysis (FMEA). Asked what he *disliked about CHASSIS*, *Informant-5-AirportLightsSupplier* explained that the method did not did not seem to ensure that one really finds all the safety/security risks. Therefore, the method should perhaps be based more explicitly on the requirements list, and then all the requirements with any relation to safety/security should be considered. The risks should also be classified, so that all are listed, but only those that will have any impact are analyzed.

Concerning the *disadvantages of combining safety and security assessments*, The participants from the *RadioSystemsSupplier* answered that the result might be too complex for complicated cases.

When asked about *other issues that could not be easily fit into CHASSIS*, *Informant-5-AirportLightsSupplier* mentioned that safety and security elements that concerns other suppliers systems should also be noted and addressed. The "big picture" is important.

Finally, we asked the participants about the pros and cons of *integrating CHASSIS into their existing development processes*. The participants from the *RadioSystemsSupplier* thought that it will be a good idea to implement CHASSIS into the system development process. Since their products are usually embedded in more complex systems, it would be useful to do a complete analysis of the voice-communication system to evaluate and get assessments for all the various components. In this way it would be possible for their customer (the air-navigation service provider) to specify the correct safety and security level for the components. The participants from the *AirportLightsSupplier* were also positive. *Informant-3-AirportLightsSupplier* would like to acquire a tool for analyzing security, which was also integrated in the same process as safety *Informant-5-AirportLightsSupplier* mentioned the "great outputs", especially the diagrams, which would help document their safety and security assessments. At the same time, he cautioned that CHASSIS would need to be implemented in a way that keeps the process effective and sensible, probably by merging with other existing system analysis exercises. Otherwise it might become too time consuming and thus de-motivating.