Fault Trees vs. Component Fault Trees: An Empirical Study

Tim Gonschorek[1(✉)], Marc Zeller[2], Kai Höfig[2,3], and Frank Ortmeier[1]

[1] AG Software Engineering, Faculty of Computer Science, Otto-von-Guericke-University Magdeburg, Magdeburg, Germany
{tim.gonschorek,frank.ortmeier}@ovgu.de
[2] Siemens AG, Corporate Technology, Munich, Germany
marc.zeller@siemens.com
[3] University of Applied Science Rosenheim, Rosenheim, Germany
kai.hoefig@fh-rosenheim.de

Abstract. When dealing with structural safety analysis, one of the most popular methodologies is Fault Tree Analysis (FTA). However, one major critique is the rapid increasing of the complexity, and therefore incomprehensibility, when dealing with realistic systems. One approach to overcome this are Component Fault Trees (*CFT*), presenting an extension to standard *FT*, allowing the separation of the analysis into less complex parts on the level of system components. *CFT*s are proposed to be more structured and partly reusable and therefore also claimed to be more straightforward to use by engineers with little safety domain experience.

In this work, we aim at getting an idea of the validity of presented theses and started an initial experiment with 13 computer science students, being asked to execute *CFT* or *FT* method on a given case study. Due to the number of participants, we focused on their empirical statements, the analysis solutions, and empirical results collected using a questionnaire.

Although the empirical impression has been that the resulting *CFT* models are better to use and more comprehensible than the FT models, the qualitative results have not supported this. Moreover, the component-wise modeling seams to mislead the students such that they have overseen failures outside the component structure, e. g., Common-Cause, Cross-Component, or external failures.

1 Introduction

Fault Trees (*FT*) [4,14] are widely used in industry to calculate hazard occurrence probabilities in the safety assessment process, e. g., according to IEC 61508 [5] or ISO 26262 [6]. This is done in a top-down way by analyzing the propagation of faults through a system, identifying causes (events) of the hazards, and calculating the hazard's likelihood from the occurrence probabilities of the basic events.

With the advent of model-based system engineering [3], which is introduced to tame the complexity, also the use of models in safety engineering processes

B. Gallina et al. (Eds.): SAFECOMP 2018 Workshops, LNCS 11094, pp. 239–251, 2018.
https://doi.org/10.1007/978-3-319-99229-7_21

has gained increasing attention in the last decade [1,7,10–13]. On of them is the approach of Component Fault Trees (*CFT*) [9] a model- and component-based methodology for Fault Tree Analysis, supporting a modular and compositional safety analysis strategy.

Like the other mentioned approaches, however, *CFT*s are not widely used in the industry yet. One reason for this might be the lack of experience in their applicability and evidence for the claimed improvements. An interesting starting point to overcome this gap is to (i) apply them to realistic system specifications and (ii) provide empirical evidence for their proposed improvements. One attempt to (i) is given in [2], where two realistic case studies are analyzed applying both, *FT* and *CFT* method to compare their benefits and drawbacks. For (ii) a controlled experiment with experienced practitioners from aerospace industry and Ph.D. students has already been performed [8]. The accumulated outcome is that it cannot be proven that *CFT* models imply significant more correct results than *FT*. Though, the subjective perception of the authors and the participants is that *CFT*s can reduce the problems of complexity, maintainability, and model consistency between system and safety model.

In this paper, we want to analyze the possible benefit from another point of view: one specific problem of development projects for critical systems is, in addition to the safety measure's applicability for experts, the communication between safety and system engineer. The system engineer is often inexperienced in the application of safety measures whereas the safety engineer is not aware of every specific problem of the system. Therefore, good communication is necessary. Unfortunately, often this is at least in need of improvement. In our point of view, this improvement can be enforced by a safety modeling methodology, that can be easily understood even by engineers that are inexperienced in this specific methodology. Hence, the goal of our case study is to provide data about whether using *CFT* lead to "better" analysis results when used by inexperienced users. We investigate both, the quality of the analysis results but also the collaborative aspect. This means whether *CFT* models are more comprehensible to other inexperienced engineers, working on the same analysis, than *FT* models. From this, we can draw our conclusion to the initial problem of the interdisciplinary exchange between safety and system engineer.

In the following, we want to present our analysis results: necessary background on the *CFT* method is provided in Sect. 2. After that we present our case study in Sect. 3 and discuss the results in Sect. 4. In Sect. 5 we conclude our paper.

2 Background

A *CFT* is a Boolean model associated to system development elements such as components [2,9]. It has the same expressive power as classic fault trees [4,14]. *CFT*s (as well as classic fault trees) are used to model the failure behavior of safety-critical systems. This failure behavior is used to document that a system is safe and can also be used to identify drawbacks of the design of a system.

In *CFT*s, a separate *CFT* element is related to a component. Failures that are visible at the outport of a component are models using *Output Failure Modes* which are related to a specific outport. To model how specific failures propagate from an inport of a component to the outport, *Input Failure Modes* are used. The internal failure behavior that also influences the output failure modes is modeled using the Boolean gates such as *OR* and *AND* as well as *Basic Events*.

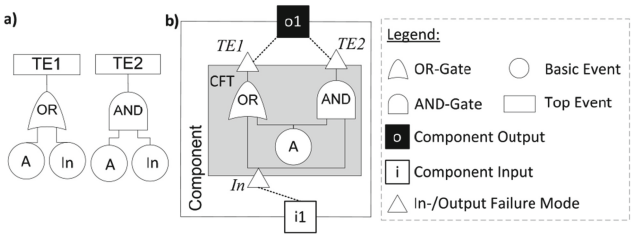

Fig. 1. Classic Fault Tree (a) and Component Fault Tree (b) [8].

Every *CFT* can be transformed to a classic fault tree by removing the input and output failure modes elements. Figure 1 shows on the left side a classic fault tree and on the right side a component fault tree. In both trees, the top events or output events *TE1* and *TE2* are modeled. The *CFT* model allows, additionally to the Boolean formula that are also modeled within the classic fault tree, to associate the specific failure modes to the corresponding ports where these failures can appear. Top event *TE1* for example appears at port *O1*.

3 Investigating the Analyzing Experience of Component Fault Trees

The goal of our research is to answer the following research questions:

> ***RQ***1: *"How do inexperienced engineers evaluate the comprehensibility and utility of another group's model for the same analysis task?"*

This leads us to N-version-styled safety analysis and serves as an indication for the question whether the resulting models are interpretable by other engineers inexperienced in dealing with *CFT* and *FT* (comparable to the sketched inter-communication problem between safety and system engineer). To answer ***RQ1***, we asked the participants to answer questions about the applied method and its usability for an iterative N-version-styled process. Further, we have instructed each of them to exchange their results with a different group and have asked questions about the participant's opinion on the quality of their model and their

received model to get an idea whether the internal and external comprehensibility of a model is close. This would also be a hint on the model consistency. Based on this, we formulated the following hypotheses:

H1: E{*CFT is useful for the analysis process*} ≠ E{*FT is useful for the analysis process*}
H2: E{*external perception of CFT*} ≠ E{*external perception of FT*}

For the comparison of the methods, we do not only take the impressions of the participants into account but also the qualitative results. Further, we were interested in the confidence of the participants whether they have found all failure combinations.

RQ2: *"Does using CFT leads to better analysis results than using traditional FT methods, especially when used by inexperienced system engineers?"*

H3: The quality of the analysis with CFT is higher than for FT.
H3.1: #(*critical cut sets CFT*) ≠ #(*critical cut sets FT*)
H3.2: E{*confidence for having found critical cut sets CFT*} ≠ E{*confidence for having found critical cut sets CFT*}

For the planning of our case study, we strongly oriented ourselves on [15].

3.1 Case Study Structure

To gather data about the modeling process and the comprehensibility of the models when exchanged with other modelers, we structured the analysis process in three iterations. After each iteration, the participants, meanwhile split into groups, filled in a questionnaire about their personal opinions. After that they exchanged their model with another group without knowing who will receive their model (*cf.* Fig. 3). We asked the participants to update their analysis model, based on potentially additional information derived from the received model.

Before starting the experiment, we have had to bring up the students on a comparable knowledge level. Therefore, a 3 h lecture on what is safety analysis and how to use *FT* and *CFT* measure has been given by safety experts.

3.2 Participant Constellation

We have executed this case study with the help of 13 students of computer science and related courses of study of one of our seminars at the Otto-von-Guericke-University Magdeburg, which we have seen as an initial starting point for a broader analysis on this topic. We are aware of the fact that a case study with 13 students cannot be representative for reliable conclusions. However, we think that this is sufficient for getting an intention whether using *CFT*s can improve

the safety analysis. Students as participants, in particular, are interesting since they are representative for inexperienced (safety) engineers. Since most of the students have only about one year until finishing their graduated Master's degree, the results might allow conclusions about how entry-level safety analysts would cope with the methods.

The participant group consists of nine graduate students and four undergraduate, which were at least in the fifth semester of their seven semesters bachelor's program. We split them into three groups: Two of them where asked to use the *CFT* method and one group to use the *FT* method. Table 1 shows an overview of the participants, their validation on their experience on programming, software quality, safety analysis, and fault trees. To increase the student's concentration, we informed the students about the case study after(!) the experiment. We only explained to them that the results they produce are the base for their grading of the seminar.

Table 1. Distribution of the student's individual, subjective experience.

Experience	CFT 1	CFT 2	FT
Programming	3.25	4.25	3.60
Software quality	3.25	3.25	2.80
Safety analysis	3.00	1.75	2.80
Fault trees	3.25	2.50	3.00
Mean	3.19	2.94	3.05

3.3 Example System: Adaptive Cruise Control

As an exemplary system for the case study, we have chosen an Adaptive Cruise Control (*ACC*) system. The *ACC* function automatically adjusts the vehicle speed to maintain a safe distance from vehicles ahead. It allows the vehicle to brake when it detects that the car is approaching another vehicle ahead and accelerates the car when traffic allows. In our example, the *ACC* functionality is realized based on two redundant radar sensors, a dedicated *ACC* Electronic Control Unit (ECU), which implements the control function, the motor ECU to control throttle, and the brake ECU to control the car's brakes (see Fig. 2).

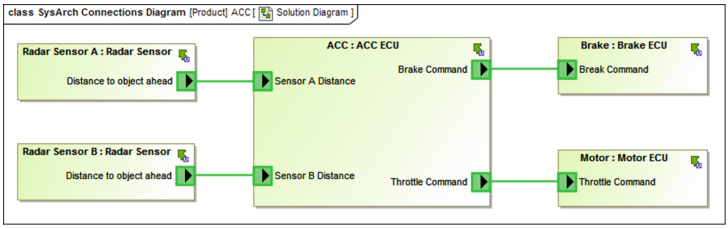

Fig. 2. System architecture of the exemplary *ACC* system.

The two hazards we defined for the students are:

- Collision (Car does not brake automatically, potential collision with an object ahead)
- Driver Disturbance (sudden braking without human interaction, potential harm by collision with other vehicles or wrong reaction of the driver)

3.4 Data Collection

For the analysis, we collected data from both, the analysis results, i. e., the cut sets of the resulting models, and the results of the questionnaire. We developed our question on an ordinal five-point Likert scale (1=strongly disagree to 5=strongly agree). The particular procedure which group received which model after which iteration is depicted in Fig. 3. Since all groups are meant to model *CFT* and *FT*, their modeling results are comparable by the cut sets resulting from qualitative FTA. The *FT* group has given away the complete *FT* whereas the *CFT* groups only exchanged the *ECU* component.

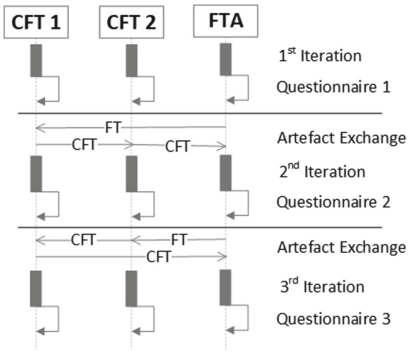

Fig. 3. Sketch of the sequence for the execution of the experiments.

$Q_1.4$	The modeling methodology used has supported me very well to structure the problem and to perform my analysis.
$Q_{2\|3}.4$	My own model was very well-suited to represent modifications or to compare the own model with the one received by the other group.

Fig. 4. Questions for for hypothesis **H1**.

For the analysis we asked the following questions correlated to **H1** (*cf.* Fig. 4). For verifying the proposition of hypothesis **H2**, we analyzed the questions presented in Fig. 5. We have separated them into two different parts: an internal and an external view and therefore compared them depending on the correlations of the exchanged model. Internal questions are about the comprehensibility of the own model whereas external questions are about the model, the group received. For analyzing our propositions for hypothesis **H3**, we collected the data from the question given in Fig. 6, using the qualitative verification results in the form of the minimal cut sets and the following questions. Based on this data, we can analyze what influence the different methods have on the results and the confidence in the results.

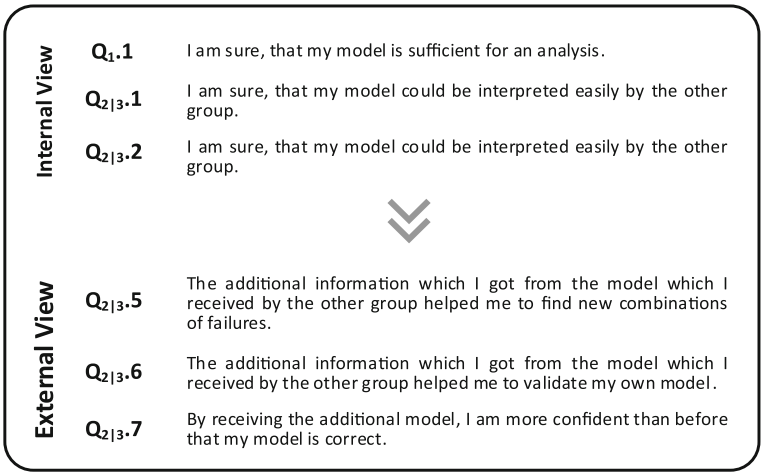

Fig. 5. Questions for for hypothesis **H2**.

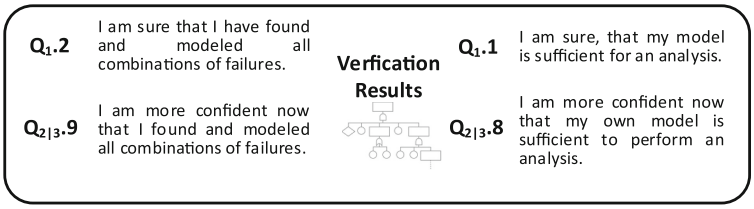

Fig. 6. Questions for for hypothesis **H1**.

4 Discussion of Results

In the following, we discuss our hypotheses based on the qualitative results of the analysis, the data from the questionnaire, and, in particular, the subjective impressions and statements we have collected from the participants[1].

For measuring the statistical significance, we analyzed the test values using the two-tailored Wilcoxon signed-rank test with a significance level $\alpha = 0.05$ and the correlation coefficient r. Therefore, the calculated z-values must be outside the interval $[-1.96; 1.96]$.

4.1 General Opinion on the Methods

When we analyze whether the methodology is sufficient and supportive for the applied safety assessment process, we find out that the overall perception of the participants is yes. The values of Table 2 supports this intention. Here, we

[1] The raw data and the modeling results are available under https://cse.cs.ovgu.de/cse-wordpress/wp-content/uploads/2018/03/sc2018_raw_data_anonymized.zip/.

compare whether the participants think that the methodology is supportive of the task (Q1.4).

When comparing *FT* and *CFT* it can be seen that the overall mean evaluation of the usability of *CFT* (3.65) is higher than for the *FT* (3.33), especially, since it is so close because of one outlier in Iteration 2 for *CFT*.

This leads us to the point where we can say that the participant's perception is that *CFT* are more appropriate to be used in a process dealing with iterations and data exchange between different groups.

When calculating the z-value for Wilcoxon test, we get z=0.52 (r=0.21) lying with the critical interval. Therefore, we cannot reject the null hypothesis **H1**: E{*CFT is useful for the analysis process*} = E{*FT is useful for the analysis process*}.

4.2 Participant's Perception on Exchanging Models

Table 2. The participant's answers to the question whether the methodology is applicable when used in a shared process. For the overall values the data from the *CFT* groups were grouped.

	CFT1	CFT2	FT
Q1.4	4	3.5	3.4
Q2.4	3.5	3.25	3.4
Q3.4	4.5	2.25	3.2
Overall mean		3.65	3.33
Overall variance		0.96	1.52
Overall median		4	4

In the following, we want to analyze the participant's impression on exchanging the analysis results as an intermediate step. In particular, it is interesting which kind of input is interesting for a group. Either *CFT* or *FT*, or, e. g., just a model represented in another modeling formalism.

As we can see in Table 3 the evaluation of the helpfulness of an additional model is overall positive. When we have a close look at the different input variants, we see that the *FT* group evaluates the received *CFT* model with the highest values (3.77). It is, in particular, remarkably higher than the internal evaluations of the *CFT* teams (3.21).

Further, utilizing the *overall means*, we have found out that, in mean, the external evaluation for getting a *FT* model or a *CFT* model is the same (3.5). However, when we compare those values to the internal evaluation of the modeling group, we have a positive external rating for *CFT* models as input for a *CFT* group, since the internal rating (3.46) is lower than the external rating (3.5). In contrast to this, we see the opponent trend for *FT*. Here, the evaluation trend is negative, i. e., the internal rating (3.6) of the *FT* modeler is higher than the external evaluation of the *CFT* group (3.5).

When we have a closer look at the comments of the participants, this tendency gets underlined. As a remark from the *CFT* groups, we have received the feedback that the *FT* model is not well structured and complex to understand compared to the *CFT* models. Moreover, when exchanging the models, we had the problem that the *FT* has been drawn on four sheets of paper whereas the component model required just one. Further, the amount of exchanged components also had an impact. For the *CFT*, only the component ECU has been exchanged, however, for the *FT* this was not possible at all, since every time

Table 3. Internal and external perception of the helpfulness of a given analysis model being exchanged between groups using either different methodologies ($FT \leftrightarrow CFT$) or same methodologies ($CFT \leftrightarrow CFT$). The overall values where computed from the data of all constellations where a CFT group received a FT, the FT group received a CFT, and a CFT group received a CFT.

	Different methodology				Same methodology	
	Internal	External	Internal	External	Internal	External
	FT	CFT	CFT	FT	CFT	CFT
Iteration 1	3.60	3.42	2.75	3.87	3.50	3.42
Iteration 2	3.60	3.75	3.25	3.67	3.38	3.58
Overall mean	3.60	3.50	3.21	3.77	3.46	3.50
Overall variance	0.69	1.30	1.15	1.36	1.54	0.96
Overall median	4	4	3	4	3	3.5

the complete fault tree has been exchanged. This, of course also increased the subjective complexity. To support this, even members of the FT group claimed that their model was more complicated to be analyzed compared to the CFT. However, to normalize this remarks, we have to keep in mind that the analysis has been done with paper and pencil.

Overall, these results show that it can have a positive effect when receiving another model as input to compare the own results with. Moreover, at least for our participants, getting a CFT model as input seems to be the better alternative than a FT model.

When analyzing the statistical significance of our results for the null hypothesis **H2**: E{*external perception of CFT*} = E{*external perception of FT*} we get a z-value of -0.19 (r=0.21). This means, we cannot reject the null hypothesis for, and therefore, our impression is only empiric but not statistically relevant.

4.3 Qualitative Results and Confidence

The results of the minimal cut set analysis for the CFT or FT models created by the different groups are presented in Figs. 7 and 8. The FT group has only created a Fault Tree for the hazard *collision*, so the cut sets for the second hazard cannot be compared with the other results. Moreover, the FT group is the only group that changed their analysis model over time. However, they only split the basic failure events such that a sensor error has become either a distance too high or distance too low error. Nevertheless, this did not affect the failure propagation logic.

However, it is interesting that both CFT groups modeled the failure of the radar sensors in this detail. Discussion with the students has shown that this comes from the fact that they tried to model the behavior also outside the borders of the component, e. g., communication failures or loss-of-data.

Safety experts	CFT 1	CFT 2	FT
ACC ECU internal failure	Engine erroneous Behavior	Motor ECU fail	Radar sensor A distance too low
Brake ECU internal failure	Brake erroneous behavior	ACC ECU failure	Radar sensor B distance too low
Motor ECU interal failure	Radar Sensor B erroneous behavior	ACC ECU error	Brake ECU fails
Radar Sensor A internal failure, Radar Sensor B internal failure	ACC erroneous behavior	Radar A error	Radar sensor B distance too high
	ACC total failure	Brake ECU fail	ACC ECU error
	Radar Sensor A erroneous behavior	Radar Sensor A fail, Radar Sensor B error	Brake ECU error
	Brake total failure	Radar Sensor A fail, Radar Sensor B fail	ACC ECU fails
	Radar Sensor A total failure, Radar Sensor B total failure		Radar sensor A distance too high
			Radar sensor A fails, Radar sensor B fails

Fig. 7. Cut sets resulting form the CFT/FT model for the hazard "collision".

Safety experts	CFT 1	CFT 2
Brake ECU internal failure	Radar Sensor B erroneous behavior	Brake ECU fail
ACC ECU internal failure	Engine erroneous behavior	Motor ECUfail
Motor ECU interal failure	ACC total failure	Radar A error
Radar Sensor A internal failure	ACC erroneous behavior	ACC ECU failure
Radar Sensor B internal failure	Radar Sensor A erroneous behavior	ACC ECU error
	Brake erroneous behavior	Radar Sensor A fail, Radar Sensor B fail
	Engine total failure	Radar Sensor A fail, Radar Sensor B error
	Radar Sensor A total failure, Radar Sensor B total failure	

Fig. 8. Cut sets resulting form the CFT/FT model for the hazard "driver disturbance".

The cut sets show that all CFT groups have modeled more failures (failure and erroneous behavior) than in the solution created by safety experts, where all failures of the components are represented as an internal failure. This refinement of the internal failures of the components leads to more cut sets compare to the sample solution. When we have a closer look at the results, we find out that only the most inexperienced group CFT2 modeled the correct failure propagation.

For the FT group, we can observe a common situation since the model gets more complex than necessary and therefore they had two redundant subtrees. One of them directly leads to the hazard event and the second one is combined with the Motor ECU failure, i. e., in their failure propagation logic a motor fail does not lead to the crash of the car.

Another interesting aspect is the failure propagation of the CFT1 model. Here we can see that the *Radar Sensor B* is a single point of failure. The failure of this sensor, however, is only critical in combination with the failure of *Radar Sensor A*. This shows another problem of the *CFT* modeling for inexperienced modelers. *FT* pushes the engineer to keep the look on the complete system's behavior, whereas *CFT* more focus the view on single component's behavior. This can lead to a situation where the modeler loses the overview over the complete system, i. e., over cross-component-behavior, external failures, or common-cause failure, as for the radar sensors of the *ACC*. Due to this result, since both one CFT group and the FT group had a major error within their models, we cannot reject the null hypothesis for **H3.1** that $\#(\textit{critical cut sets CFT}) = \#(\textit{critical cut sets FT})$.

The confidence of the CFT1 group stays quite constant. For FT and CFT2 this is not the case. In the second step, after receiving the *CFT* from CFT2, the confidence of FT that all failure combinations had been found drops from 3.2 to 2. Whereas the confidence of CFT2 group rises from 2 to 3.5. When having a closer look at the results of the analysis and the comments of the participants the reason is clear.

The FT group had some problem with modeling all possible failure modes arising from the sensors of the *ACC*. Since, in contrast to the CFT groups, they had no methodology for modeling different outputs and error types of a systems element, their model only contains the failure modes "sensor error" and "sensor failure". However, the other groups differentiated between getting a sensor value representing a "too high" or "too low" distance for the measurement, which has the benefit of being able to define different influences on the erroneous braking and acceleration of the system. The result of CFT2 is a consequence of the effect that they are, on average, more skeptic with their model but after getting the model of CFT1 as input, the confidence increased.

Many participants stated as positive aspect of the *CFT* methodology the guidance they get (i) from the structured component point of view, where they model each element separately and (ii) from the different viewpoint since *CFT* components can be seen as interacting elements in the system with propagating failures whereas *FT* only convey a strict structural point of view.

In this sense, the given results support hypothesis **H3.2** that the structured methodology of *CFT* can support the confidence of inexperienced system analysts more than the less strict *FT* method does.

However, the null hypothesis **H3.2**: E{*confidence for having found critical cut sets CFT*} = E{*confidence for having found critical cut sets CFT*} cannot be rejected, since Z=−1.15 (r=0.47).

4.4 Threats to Validity

In this section, we want shortly discuss external and internal thread to the validity of case study and the drawn conclusions.

Internal Validity. For the internal validity of the case study, the number and constellation of the participants are of high interest.

One possible threat is the degree of experience of the participants. When we have a closer look on the research questions, we do not see this as a disadvantage for the study since we wanted to analyze the general comprehensibility of the methods without requesting any classification concerning the professional context of each participant. So, we focus only on the applicability and comprehensibility of the given example system. Moreover, we think that it could also be a light benefit because the subjective impression of the participants is not overlapped by personal positive or negative historical experiences.

A second point is the difference in the experience of the participants. To overcome this problem, we tried to split the undergraduate evenly throughout the groups, i. e., the group with two undergraduate students, the *FT* group, also

got one more member than the others. This lead, with respect to our measure (*cf* Table 1) to groups with comparable experience level. This comparability was also supported by the introductory lecture given by experienced safety experts.

The primary threat, of course, is the number of participants, which lead to the fact that our ordinal data does never show a statistical significance. However, to bridge this gap, we also took into account the personal statements of the participants that were not directly projected onto the ordinal scale. Moreover, we see this as a first step in the direction of a more considerable estimation, and therefore even this small sample size and the corresponding gained experiences are of value to us.

External Validity. The major threat to the external validity is the complexity of the example system, since *CFT* are claimed to be most effective when it comes to large, complex systems, or reusability of specific components. In fact, neither the *FT* nor the *CFT* fit on one page but were split over four A4 pages, and single subtrees had been substituted by proxy or virtual events. Therefore, in combination with the low level of practical experience, this seems to be a sufficient benchmark, especially concerning the limited amount of time. For consecutive studies, we will validate the applicability of more complex example systems.

5 Conclusion

In this paper, we have presented our investigation to the question whether applying Component Fault Trees (*CFT*s) can support the modeling process compared to common Fault Trees. In particular: *"How do inexperienced engineers evaluate the comprehensibility and utility of another group's model for the same analysis task?"* and *"Does apply CFT lead to better analysis results than using traditional FT methods, especially when used by inexperienced system engineers?"*

We found out that indeed we can answer the research questions with yes. Even though the results are not statistically significant for the small number of participants, the results, as well as the statements of the participants, give a clear trend. The usage of *CFT* can support, in particular, inexperienced engineers in analyzing a system. Even for the iterative process, where intermediate analysis results are exchanged between different groups, using *CFT* methodology seems to have an advantage over *FT* methods.

However, we have to keep in mind that both modeling techniques, *CFT* and *FT*, can cause trouble during the analysis. The problem with a *FT* is the rapidly increasing complexity of the tree when applied to real systems. This can often lead to redundancies and therefore can shadow other failure modes and cut sets if they have been combined with a redundant subtree. However, a benefit is the need to overview the complete system while modeling the *FT*.

In contrast to that, *CFT*s help focusing component-wise on separated and less complex system elements. Nevertheless, this can even be a source of problems since it can easily shadow the view for cross-component dependencies or external failure events. Hence, it can increase the loss of common cause failure relation,

which may lead to both, under and over-specification of the failure propagation logic.

To get more reliable data, we plan to repeat the experiments on a larger group of participants, e. g., from one of our larger courses with about 200 students and more complex models.

Acknowledgment. Parts of the work leading to this paper was funded by the Framework Programs for Research and Innovation Horizon 2020 under grant agreement n.732242 (DEIS).

References

1. Filax, M., Gonschorek, T., Ortmeier, F.: Building models we can rely on: requirements traceability for model-based verification techniques. In: Bozzano, M., Papadopoulos, Y. (eds.) IMBSA 2017. LNCS, vol. 10437, pp. 3–18. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-64119-5_1
2. Höfig, K., Joanni, A., Zeller, M., Montrone, F., Rothfelder, M., Amarnath, R., Munk, P., Nordmann, A.: Model-based reliability and safety: reducing the complexity of safety analyses using component fault trees. In: RAMS (2018)
3. INCOSE: Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities. John Wiley & Sons (2015)
4. International Electrotechnical Commission (IEC): IEC 61025: Fault Tree Analysis (FTA) (1990)
5. International Electrotechnical Commission (IEC): IEC 61508: Functional safety of electrical/electronic/programmable electronic safety related systems (1998)
6. International Organization for Standardization (ISO): ISO 26262: Road vehicles - Functional safety (2011)
7. Joshi, A., Miller, S.P., Whalen, M., Heimdahl, M.P.: A proposal for model-based safety analysis. In: 24th DASC (2005)
8. Jung, J., Jedlitschka, A., Höfig, K., Domis, D., Hiller, M.: A controlled experiment on component fault trees. In: Bitsch, F., Guiochet, J., Kaâniche, M. (eds.) SAFECOMP 2013. LNCS, vol. 8153, pp. 285–292. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-40793-2_26
9. Kaiser, B., Liggesmeyer, P., Mäckel, O.: A new component concept for fault trees. In: Proceedings of the 8th Australian Workshop on Safety Critical Systems and Software (2003)
10. Lisagor, O., McDermid, J., Pumfrey, D.: Towards a practicable process for automated safety analysis. In: ISSC 24 (2006)
11. McDermid, J., Kelly, T.: Software in safety critical systems: achievement and prediction. University of York, UK (2006)
12. de Miguel, M.A., Briones, J.F., Silva, J.P., Alonso, A.: Integration of safety analysis in model-driven software development. IET Softw. **2**(3), 260–280 (2008)
13. Papadopoulos, Y., McDermid, J.A.: Hierarchically performed hazard origin and propagation studies. In: Felici, M., Kanoun, K. (eds.) SAFECOMP 1999. LNCS, vol. 1698, pp. 139–152. Springer, Heidelberg (1999). https://doi.org/10.1007/3-540-48249-0_13
14. Vesely, W.E., Goldberg, F.F., Roberts, N.H., Haasl, D.F.: Fault Tree Handbook. US Nuclear Regulatory Commission (1981)
15. Yin, R.K.: Case Study Research and Applications: Design and Methods. Sage Publications, Thousand Oaks (2009)