On groupthink in safety analysis: An industrial case study

Yang Wang
University of Stuttgart
yang.wang@informatik.uni-stuttgart.de

Stefan Wagner
University of Stuttgart
stefan.wagner@informatik.uni-stuttgart.de

ABSTRACT

Context: In safety-critical systems, an effective safety analysis produces high-quality safety requirements and ensures a safe product from an early stage. **Motivation:** In safety-critical industries, safety analysis happens mostly in groups. The occurrence of "groupthink", under which the group members become concurrence-seeking, potentially leads to a poor safety assurance of products and fatalities. **Objective:** The purpose of this study is to investigate how groupthink influences safety analysis as well as how to reduce it. **Method:** We conducted a multiple case study in seven companies by surveying 39 members and interviewing 17 members including software developers, software testers, quality engineers, functional safety managers, hazard/risk managers, sales, purchasing, production managers and senior managers. **Results:** The TOP 10 phenomena of groupthink in safety analysis are: (1) The managers are too optimistic on the plan of safety analysis from norms. (2) The technical members overestimate their capability on avoiding risks. (3) The non-functional department is under negative stereotypes in safety analysis. (4) Non-technical members keep silence during safety analysis. (5) Team members keep consistent opinions with senior safety experts. (6) The team rationalizes the safety analysis solutions. (7) The safety analysts spontaneously freeze the safety-related documents. (8) The safety analyst has an illusion of invulnerability during verification. (9) The internal safety assessor rationalizes the safety assurance to a third party. (10) The team rationalizes the safety analysis for providing safety evidences. Furthermore, we found reasons like "cohesion" and "group insulation" and solutions like "inviting external expert" and "making key members impartial". **Conclusion:** There is groupthink in safety analysis in practice. Practitioners should look for the phenomena and consider solutions. However, the cases are limited to the investigated domains and countries.

CCS CONCEPTS

• **General and reference** → *Empirical studies*; • **Software and its engineering** → *Software organization and properties*; *Software safety*;

KEYWORDS

Groupthink; Safety Analysis; Case Study

ICSE-SEIP '18, Gothenburg, Sweden

DOI: 10.1145/3183519.3183538

ACM Reference format:
Yang Wang and Stefan Wagner. 2018. On groupthink in safety analysis: An industrial case study. In *Proceedings of 40th International Conference on Software Engineering: Software Engineering in Practice Track, Gothenburg, Sweden, May 27-June 3, 2018 (ICSE-SEIP '18),* 10 pages.
DOI: 10.1145/3183519.3183538

1 INTRODUCTION

To develop safety-critical systems, safety analysis[1] is used to identify potential causes of accidents. The causes can be eliminated or controlled in design or operations before damage occurs [20]. Popular safety analysis techniques include Failure Mode and Effect Analysis (FMEA), Fault Tree Analysis (FTA), Hazard and Operability Analysis (HAZOP) and the novel System Theoretic Process Analysis (STPA). To analyze the safety of a system, they are able to provide initial faults and causal factors in a qualitative way, as well as identifying the level of risks and evaluating their effects in a quantitative way. They are either inductive techniques like FMEA or deductive techniques like FTA. Most of them are based on reliability theory, while STPA is based on system theory to cover today's complex software-intensive, sociotechnical systems.

Although these safety analysis techniques are different, one commonality is that they are all performed with a lot of group work, especially in modern software development processes [1][28]. Safety analysis requires a sophisticated engineering approach because inadequate, incomplete or misunderstood requirements are recognized as a major cause in many accidents [30]. In general, performing safety analysis in practice, apart from the individual part, has to be discussed with the whole development team and cooperated with other functional departments, such as quality assurance department and production. The safety analysis needs a final assessment before delivery by an internal safety assessor and a third party company. Group safety analysis (GSA)[2] with cross-functional departments makes the analysis more comprehensive and the execution more productive [15]. Group members could share safety knowledge across different departments, whereas the management and customers become more satisfied when they could be a part of GSA.

However, group work encompasses additional psychological effects [18]. An inappropriate control of these effects might lead to an ineffective group work. Groupthink [17] is one of the most notorious. People under groupthink begin to think alike and do not tolerate new ideas. It leads a group to conform rather than search for an optimal decision. In GSA, groupthink might cause a sub-optimal or unsafe design decision, as revealed in the NASA disaster operation report of the Columbia space shuttle [11].

[1] We use "safety analysis" to cover "hazard/risk/safety analysis".
[2] We use "group safety analysis" to include all hazard/risk/safety analysis activities in groups.

In this article, we aim to investigate groupthink in GSA in software-intensive systems. We start from collecting current industrial practices corresponding to GSA. Furthermore, we derive the TOP 10 phenomena within aforementioned practices and analyze their reasons and solutions.

Contributions:

(1) We provide the TOP 10 phenomena of groupthink in seven GSA.
(2) We investigate possible reasons for the TOP 10 phenomena.
(3) We propose solutions on how to handle the TOP 10 phenomena in safety-critical system management.

2 BACKGROUND AND RELATED WORK

Groupthink [17], as a psychological phenomenon, was introduced by Janis in 1972. It is a linear model of how seven antecedents[3] increase the likelihood of premature concurrence seeking, which leads to eight psychological symptoms[3] of groupthink and a defective decision-making [23]. It has been initially investigated in the political area [16] and military contexts [19] as a causal factor for a defective decisions during a war or a political event. Recently, Rose [24] did a literature review, which covers in total 60 scholarly articles including case studies, experiments, literature reviews, applications and modifications on groupthink. The authors summarized diverse perspectives of groupthink including both "for" and "against". The application areas are extended to jury decision-making or ice hockey team performance. To this end, some problems and possible modifications, such as the assessment and test on groupthink are summarized.

In software engineering, practitioners have noticed groupthink [3]. De Snoo, Van Wezel and Jorna [8] mentioned the phenomenon about "dream team" (invulnerability) and "managers have not taken employees preferences into account" (unanimity) on groupthink when performing planning and scheduling. Manz and Sims [21] introduced three cases in studying autonomous work group decision processes. Five symptoms were explained in real contexts. Brockman et al. [2] investigated interpersonal cohesiveness in external new products (market success etc.) and internal new products (team member satisfaction etc.). Groupthink, as an outcome of cohesiveness, has a directly negative impact on external new products. The authors have also proposed the causal factors to cohesiveness, such as clan culture or political dominance of one department. Tennant [29] conducted an exploratory study and verified that the risk of groupthink causes ineffective decision making in emergency scenarios during operation management.

Modern software development is becoming close-knit, which advocates more interactions and a collaboration mode to overcome some problems in software engineering [5]. Group work becomes prominent. Human factors are becoming deterministic. Thus, organization psychology has to be reconsidered. Gren, Torkar and Feldt [14] conducted a qualitative and quantitative investigation on eight large companies through surveys and interviews concerning group development and maturity when building agile teams. They propose the importance of considering group psychology in modern agile group development, such as the increase in job satisfaction and personality. Gren and Goldman [13] did further an experiment in terms of increasing adept application of agile practices by group development. They obtained an insignificant result. Nevertheless, it helps us to decide our investigation as a case study rather than an experiment due to the fact that the research in organization psychology requires much time. Besides a general group work exploration in modern agile projects, Coyle, Conboy and Acton [7] mentioned that groupthink is prominently a significant counter-arguments causing group process losses in agile software development. Other findings, such as "group member domination" and "members afraid to speak up" are also related with groupthink. McAvy and Butler [22] collected a number of groupthink symptoms during a longitudinal case study over two agile teams. Due to the cohesive agile teams, groupthink has a negative impact on decision-making. The authors suggested that the project manager should take a devil role to reduce this phenomenon. Other recent research also discussed the negative impacts of groupthink in modern software engineering [9][10]. Hence, to strengthen an effective group work, groupthink should be reconsidered in today's software engineering.

In developing safety-critical systems, the effects on groupthink are fatal. A defective group work on safety quality assurance leads to an unsafe product that threatens people's life. Ferraris and Carveth [11] investigated how groupthink affected a faulty decision-making, and further caused the Columbia accident. Due to a common organizational change, more complex communication issues arise to keep an on-time delivery. Some groupthink symptoms appeared in a real Columbia investigation, such as "some people are reluctant to raise certain issues of importance". Schiano and Weiss [27] focuses on groupthink in security-critical systems. The recommendations are at the group level, such as "the standard security must be integrated into meetings". The problems show similarities with safety-critical systems, such as "not following standards" and "just doing what the business asked for". However, they investigated groupthink only through one case concerning a failing system. As far as we know, the research on groupthink in safety-critical systems is scarce. ISO 26262-2 [12] mentioned "groupthink" as an indicator of a poor safety culture. Yet, this problem has not been solved and need to be considered in safety engineering. We focus on safety analysis.

3 STUDY DESIGN

We conduct a case study following the guideline from Runeson et al. [25] and Yin [32].

Fig. 1. Participants

[3]We list Janis's groupthink model in Appendix A, which includes eight symptoms, seven antecedents and nine recommendations.

3.1 Context

We conduct a multiple case study in seven safety-critical industries (three of them are from the same company - company A). We select company A (large) as our primary object (with 47 participants). We investigate in its three subsidiaries. To cover different sizes of companies, we include company C (medium) and company D (small). To expand our research domains (company A is an international automotive industry), we include company B (an international medical equipment industry) and company D (a local industry 4.0 based production system). The duration of the investigated projects vary from 6 months to 3 years. The safety assurance processes are following ISO 26262 (automotive), VDA (automotive), Automotive-SPICE, ISO 14971 (medical equipment), ISO 15004 (medical equipment) and IEC 60601 (medical equipment). The safety analysis is following the internal standards for FMEA, FTA and HAZOP. The safety analysis is mainly performed either in the development team or in the functional safety department. The execution of safety analysis shows similarities, while the interfaces between them are non-deterministic. We have overall 56 participants (17 participants took part in the interviews) to reach a wide range of positions, as shown in Fig. 1. The main participants are from the quality assurance area. They are quality managers to guide the safety analysis. More than half of the members are from a functional safety department. However, other roles like developer, analyst and leader, as well as the members in the area of sales, purchasing and production are also included.

3.2 Research question

The research goal is to investigate groupthink in GSA. We formulate four research questions to steer the design of our study, as shown in Table 1.

Table 1: Research questions (RQ 1 follows the standards. RQ 2 refers to Janis's symptoms, RQ 3 refers to Janis's antecedents, and RQ 4 refers to Janis's recommendations, as shown in Appendix A.)

RQ 1	What are the current practices in GSA?
RQ 2	What are the symptoms of groupthink during GSA?
RQ 3	How could these symptoms occur?
RQ 4	How to handle groupthink during GSA?

3.3 Data collection

We conducted three rounds of data collection, which took a period of three months involving the conduction of surveys, semi-structured interviews, direct observations and documentation review.

Before data collection, we pre-interviewed five experts from four companies by telephone to decide on a common objective, establish agreements and help designing the survey. Each interview lasted one hour. These five experts were further arranged to be the representative of each company.

In the first round, we used a survey[4] to collect both qualitative and quantitative data. The qualitative data cover the participant's background and the descriptions of phenomena. The quantitative data cover the participant's background and the frequencies of the occurrences of phenomena in GSA. The survey was running for two months. We sent the link to each representative via email, as well as the survey in electronic version to ensure that all the participants are able to receive them. During these two months, the first author checked the progress every two weeks through communicating with the representatives by videophone. The content included the distribution and the respondent's rate from the surveys, as well as the problems and feedback.

In the second round, we used semi-structured interviews to investigate the in-depth reasons and solutions. We selected the subjects based on the results from the first round survey.

Meanwhile, the first author reviewed a wide range of documents including R&D process development instrument, product development and process development quality management procedure, quality management handbook, R&D risk management instruction, FMEA/FTA guideline/working instruction, decision analysis and resolution in quality management and technical review. Other informal documents, such as screen-shot of the project management tool and message items, such as email or internal apps, were also reviewed.

The first author conducted also a direct observation in the safety analysis process and team meetings in company A. Beside the regular processes, the first author observed the verbal communication temporarily, as well as the members' field notes. In the third round, we designed a final interview with the specific experts to perform the validation of the solutions.

3.4 Data analysis

We use qualitative data for RQ 1, RQ 2, RQ 3, and RQ 4. We analyze the data by using the coding approach [4], since it is especially appropriate for investigating human aspects of software engineering. We use open coding to record the transcript line-by-line. After that, we use selective coding to choose the code related to groupthink. Finally, we use axial coding to relate the symptoms, reasons and solutions.

We use quantitative data for RQ 2 to show the occurrence of each groupthink symptom in each GSA in Fig. 3. In the survey, the participants could select the symptoms that they noticed in the seven GSA and give the number of frequency ("1", "2" and "3" mean "low", "medium" and "high"). We use the Shapiro-Wilk test for a normal distribution. Since the data are all non-normally distributed, we use Pearson's r to show the degree of correlation between each symptom and GSA, as shown in Table 2. To this end, we summarize the most frequent symptoms in each GSA, from which we investigate further to generate the Top 10 phenomena in Table 3.

4 RESULTS

4.1 RQ 1: What are the current practices in GSA?

As we can see in Fig. 2, we walked-through the standards like ISO 26262, ISO 14971 and IEC 60601, as well as FMEA, FTA and risk management internal standards. We divide the safety analysis activities to seven general GSA. We reviewed these seven GSA together

[4]This survey is available online: https://zenodo.org/record/885231#.Wnlgj66nFaQ.

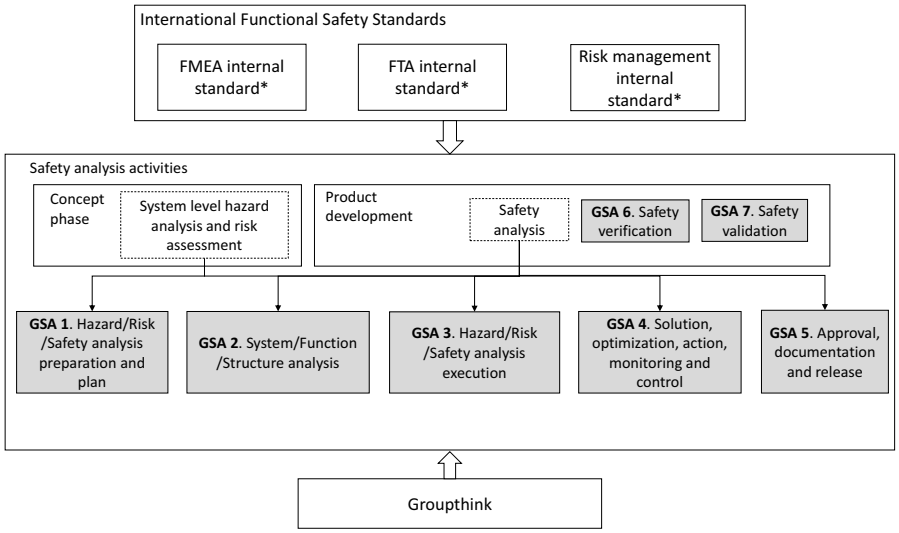

Fig. 2. Group Safety Analysis

with our industrial partners from the primary company A. Below, we introduce these GSA in detail:

1. Hazard/Risk/Safety analysis preparation and plan. This is the first step in safety analysis including making technical decisions and a safety analysis schedule. The processes and results of safety analysis must be proven for all the products and the production processes. Project manager should decide the moderator, contract and plan. The safety analysis plan (including updated plan) should be created with a specific tool (at least an English version). Cross-functional departments should join in this step. The safety analysis might include customers. A general negotiation has to be conducted.

2. System/Function/Structure analysis. This is the second step in safety analysis including determining the scope of the system (system limits, interfaces and boundary conditions), specifying the system (random) failures and type of the analysis for the systems (both qualitative and quantitative). The system determinations and boundary conditions shall be acknowledged by the customers.

3. Hazard/Risk/Safety analysis execution. This is the primary step of safety analysis. Depending on the different techniques, the execution is different. The most popular techniques are FTA, FMEA and HAZOP. FTA is a top-down method, which starts from identifying the top events and goes deeper to find causalities. The safety analyst draws the fault trees. FMEA is a bottom-up method, which finds and evaluates failure concerning the severity (S), probability of occurrence (O) and probability of detection (D). The safety analyst records the failures and effects, as well as measures the risks to provide solutions. HAZOP is a systematic risk analysis method, which identifies, assesses and manages risks at a system level. It happens mostly at the beginning of the projects and is combined with FMEA or FTA for analyzing the systems.

4. Solution, optimization, action, monitoring and control. This is the forth step in safety analysis. Following the investigation of causal factors including qualitative and quantitative interpretation, a decision can be made, which could be a solution for development, an action for operation or the monitoring and control for a risk. The moderator provides support in the interpretation.

5. Approval, documentation and release. This is the fifth step in safety analysis. The safety analysis execution process and results must be documented. The diagrams, tables and interpretations are necessary to be understood and evaluated. The results are diverse, such as the depth and the scope of safety analysis. The documents should focus on providing recommendations rather than requirements. The structure of a safety analysis report includes system overview, participants, detailed results, descriptions, list of assumptions, sources and attachments. The release has to be determined by customers to ensure that it includes no sensitive data.

6. Safety verification. After the execution of safety analysis. The requirements are to be verified. The purpose of the verification is to demonstrate that the embedded software satisfies its requirements in the target environment [12]. In the design phases, verification is the evaluation of safety requirements from safety analysis.

7. Safety validation. After the safety verification, the requirements need a validation at the system level. The first purpose of the safety validation is to provide evidence of compliance with the safety goals and that the functional safety concepts are appropriate for the functional safety of the item, while the second purpose is to provide evidence that the safety goals are correct, complete and fully achieved.

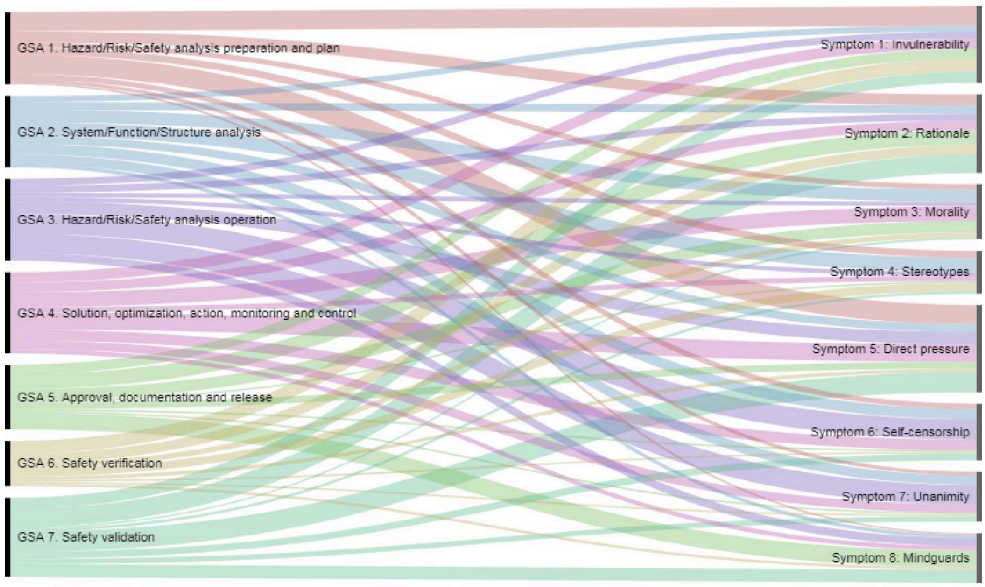

Fig. 3. Janis's groupthink symptoms in GSA (on the right side, we use the abbreviations of symptoms. All the symptoms are shown in Appendix A.)

4.2 RQ 2: What are the symptoms of groupthink during GSA?

This research question has both quantitative results (4.2.1) and qualitative results (4.2.2).

4.2.1 Janis's groupthink symptoms in safety analysis. Groupthink has eight symptoms[3]. Yet, different GSA encompasses different symptoms, as shown in Fig. 3. We list GSA 1 to GSA 7 on the left side and eight symptoms on the right side. The widths of the lines show the occurrence of each symptom. The thicker lines mean that the symptoms occur more in the GSA. In GSA 1 (hazard/risk/safety analysis plan and preparation), 56.4% of the participants mentioned the "invulnerability", while 56.4% of the participants mentioned "direct pressure". In GSA 2 (system/function/structure analysis), 41% of the participants saw the "stereotypes", while 35.9% of the participants saw the "morality". In GSA 3 (safety analysis execution), 59% of the participants found the "self-censorship", while 56.4% of the participants found the "unanimity". In GSA 4 (solution, optimization, action, monitoring and control), 51.3% of the participants mentioned the "direct pressure", while 43.6% of the participants mentioned the "morality". In GSA 5 (approval, documentation and release), 48.7% of the participants found the symptom "mindsguard", while 43.6% of the participants mentioned about the "rationale". In GSA 6 (safety verification), 38.5% of the participants saw the "invulnerability", while 28.2% of the participants saw the "rationale". In GSA 7 (safety validation), 59% of the participants found the "direct pressure", while 53.8% of the participants found the "rationale". The other symptoms show less importance in each GSA. We statistically calculate the symptoms and show the first two most frequent symptoms in GSA 1 to GSA 7 in Table 2. Pearson's r shows the correlations between each symptom and each GSA. The values are between 0 to 1, which indicate a positive linear relationship. The "unanimity" has the most positive relationship with GSA 3, while "rationale" has the worst positive relationship with GSA 7.

4.2.2 The Top 10 groupthink phenomena in safety analysis. As we can see in Table 3, based on the quantitative data of the fourteen symptoms in Table 2, we summarize the Top 10 groupthink phenomena in GSA. One phenomenon might cover two to three symptoms in each GSA.

4.3 RQ 3 & RQ 4: How could the Top 10 phenomena in groupthink occur and how to handle them?

1. The managers do not plan safety analysis activities in detail.

Description In GSA 1, the project managers plan the safety analysis following standards. All the members believe that they have a process to ensure safety and do not show more concerns on achieving safety goals. Yet, the norm needs a detailed adaption in different projects. That causes the groupthink symptoms "direct pressure" from the project manager on discussing the detailed plan and "invulnerability" on the existing plan from standards or procedures. One interviewee mentioned: *"Basically, we refer to the standards and internal procedures. The concrete execution shall have been described in the procedure documents by the procedure design department."*
Reasons and solutions *Reason 1: Lack of norm concerning the implementation and execution procedure.* The industries rely on norms for functional safety assurance. Thus, the project manager do not place emphasis on planning and preparing the implementation and execution activities. When we ask them: *"How do you perform safety*

Table 2: Statistic descriptive on the occurrence and influential of Janis's groupthink symptoms in GSA

GSA	Most frequent symptoms	N	Mean	St. Dev	St. Error	Min	Median	Max	95% CI lower	95% CI upper	Pearson's r
GSA 1	Direct pressure	22	2.091	0.848	0.136	1	2	3	1.737	2.445	0.654
	Invulnerability	22	2.045	0.928	0.149	1	2	3	1.658	2.433	0.712
GSA 2	Stereotypes	16	2.750	0.559	0.090	1	3	3	2.476	3.024	0.440
	Morality	14	2.500	0.732	0.117	1	3	3	2.117	2.883	0.622
GSA 3	Self-censorship	23	2.696	0.621	0.099	1	3	3	2.442	2.949	0.886
	Unanimity	22	2.727	0.617	0.099	1	3	3	2.470	2.985	0.978
GSA 4	Direct pressure	20	1.900	0.831	0.133	1	2	3	1.536	2.264	0.928
	Morality	17	1.471	0.696	0.111	1	1	3	1.140	1.801	0.897
GSA 5	Mindguards	19	2.421	0.815	0.131	1	3	3	2.054	2.788	0.833
	Rationale	17	2.824	0.513	0.082	1	3	3	2.580	3.067	0.725
GSA 6	Invulnerability	15	2.000	0.894	0.143	1	2	3	1.547	2.453	0.814
	Rationale	11	1.455	0.498	0.080	1	1	2	1.160	1.749	0.400
GSA 7	Direct pressure	23	2.565	0.712	0.114	1	3	3	2.274	2.856	0.483
	Rationale	21	2.952	0.213	0.034	2	3	3	2.861	3.043	0.370

Note: (1) GSA 1 is hazard/risk/safety analysis plan and preparation; GSA 2 is system/function/structure analysis; GSA 3 is hazard/risk/safety analysis execution; GSA 4 is solution, optimization, action, monitoring and control; GSA 5 is hazard/risk/safety analysis approval and documentation; GSA 6 is safety verification; GSA 7 is safety validation. (2) The evaluation is from 1 (occasionally) to 3 (frequently). (3) "95% CI lower" means 95% confidence interval lower bound level, and "95% CI upper" means 95% confidence interval upper bound level.

Table 3: The Top 10 groupthink phenomena

#	The Top 10 groupthink phenomena in GSA
1.	The managers do not plan safety analysis activities in detail.
2.	The technical members overestimate their capability in functional development and ignore the importance of safety analysis.
3.	During system/function/structure analysis, the non-functional departments are under stereotype and are always absent.
4.	During safety analysis, beside developers and safety experts, the other members keep silence.
5.	During safety analysis, the team members always keep consistence with the opinions from senior safety experts.
6.	When providing safety analysis solutions, the team members prefer explaining the rationality of the existing solutions.
7.	The safety analysts spontaneously freeze the internal safety-related documents.
8.	During safety verification, the safety analysts set themselves as a "police" to blame the development team.
9.	During safety validation, the internal safety expert takes the role as a "lawyer" to rationalize their safety assurance to a third party.
10.	The team performs safety analysis aiming to provide the required evidence for certification (paperwork culture).

analysis", they answered: *"We have the standards. Yet, the implementation and execution are depending on the projects." Solution 1: Assign critical roles.* A minimum implementation and execution of the requirements in norms shall be established into each critical role or department. Each role or department has its responsibilities, authorities, execution methodology and the corresponding accountability [20]. *Solution 2: Provide a second chance meeting.* The arrangement of responsibilities or tasks could be established in a second meeting. That will not influence the original structure of the meetings. It aims to implement, update and enforce the execution of norms. *Solution 3: Invite external expert.* The plan and preparation of safety analysis could invite experts from the procedure design department. It helps the design on performing safety analysis in a specific project, whereas the specific project helps the procedure design department to make a general procedure for future work.

2. The technical members overestimate their capability in functional development and ignore the importance of safety analysis.

Description In GSA 1, some technical members are function-oriented and are kind of "super stars". They believe in their function development experiences, which could avoid risks. The voice concerning safety analysis is ignored, which causes groupthink symptom "invulnerability" on the capability of functional development. One interviewee mentioned: *"The functions can bring the largest profits. We have worked in this area many years and are able to avoid some basic risks. We have still safety testing in the end."*

Reasons and solutions *Reason 1: Cohesion.* In most safety-critical industries, the employee's mobility is relatively low. Most employees have been working for a long time in the same area and company. That increases cohesion. However, the cohesion decreases the capability to face change and accept outside suggestions, such as the suggestions from safety experts. *Solutions 1: Split groups.* More working groups could provide more ideas. The members in each group should be heterogeneous. In a small group, performing safety analysis is more productive than in a large group [31]. In addition, the competitive mechanism could stimulate passions. *Reason 2: Lack of norms concerning the interface between functional development and safety analysis.* Safety analysis and functional development shall be concurrent. Yet, the execution lacks a clear definition on the interfaces between them. One developer mentioned: *"In the project plan, we follow the functional safety norm. But the establishment is separated from us (development)." Solution 2: Invite external expert.* Some safety experts could be invited to the internal meetings of development teams. One solution that has not been mentioned by Janis[3] but specific for safety-critical systems is that an effective communication channel between functional development and safety analysis has to be designed in the safety analysis plan and preparation.

3. During system/function/structure analysis, the non-functional departments are under stereotype and are always absent.

Description In GSA 2, the non-functional departments like sales or purchasing are always absent. They do not provide suggestions and follow the technical members. This is a groupthink symptom called "stereotype" on the non-functional departments. As one system developer mentioned: *"We invite them to the meetings to analyze the system, but they always give some reasons like "I have not received the emails" and not take part in them. They said "I have no idea about development" and let us make decisions."*

Reasons and solutions *Reason 1: Group insulation.* Safety system working groups operate at different levels of organization [20]. The safety analysis concerning system/function/structure should not stop at the functional level. However, the safety analysis among groups is always isolated, which includes working places, tasks, responsibilities and organization/personal development management, which causes too many excuses on not taking part in the GSA 2. It seems a lack of conscientiousness. *Solution 1.1: Invite external expert.* In industry, the employees do not prefer working on the tasks that goes beyond their working scope. Some members are not full-time on safety analysis. The invitations are sometimes personal and non-regulated. As far as we know, these invitations happens mostly occasionally. As one interviewee mentioned: *"Before the meeting, we send the email to a sales manager. But we got no feedback."* The time, the channel and the complementary methodology are all indeterminate. The cross-functional departments should facilitate interactions and build connections, such as communication channels and interaction patterns. *Solution 1.2: Establish multiple groups.* All the departments including non-functional departments are able to provide suggestions on the system/function/structure from their perspectives. *Reason 2: Lack of norms concerning the requirements on joined departments.* The cooperation among groups could be improved by personally inviting external experts. However, to be more efficient, the practitioners should rely on some regulations. The existing procedures include few requirements on joined departments. *Solution 2:* The requirements on joined departments could be written into the procedures to standardize GSA.

4. During safety analysis, beside developers and safety experts, the other members keep silence.

Description In GSA 3, only developers and safety experts join in the discussion. This is called "self-censorship" in groupthink. One sales manager mentioned: *"They have more expertise and take the responsibility for this."* Hence, the sales manager follows other technical members.

Reasons and solutions *Reason 1: Temporarily low self-esteem.* Safety analysis is a window into systems, everyone could see and connect hazards in the daily work. The members from the sales department have more practical experiences on products. They can see the possible hazards from the end-users' viewpoint. The members from the purchasing department know more about the purchased components from suppliers. The possible hazards from these components and purchasing procedures could cause further accidents during the development. However, most employees, especially in functional safety, QA or functional development department, think safety analysis more technically in-depth. The non-technical members are not confident. One production manager said: *"What we mentioned during safety analysis is too high-level, which cannot really help the development of products and even the safety analysis. Even more, what they talked is apart from our knowledge areas."* *Solution 1.1: Assign critical evaluators.* Each one should be given his/her responsibilities to raise questions in his/her specific areas. Everyone's voice deserves respect. An "ad-hoc" brainstorming sessions are possible. *Solution 1.2: Provide a second chance meeting or feedback channels.* Someone, who does not want to raise questions in the meetings, could have a second chance through trustful feedback channels to provide suggestions. *Reason 2: High stress from external threats.* A non-professional voice will raise doubts on the employee's core competence. People like to join in the discussion in his or her area of expertise. Especially the employees who are already in the senior level. The fresh man also does not want to show his cons in front of his or her leader and other colleagues. *Solution 2: Improve feedback channels.* One interviewee mentioned: *"It would be great, if we could provide suggestions anonymously."* For example, an anonymous mailbox has been tried by some departments.

5. During safety analysis, the team members always keep consistence with the opinions from senior safety experts.

Description In GSA 3, at the beginning, almost all the members join in the discussion. When senior managers or safety experts express their ideas or suggestions, they seek consistence with them. It is called "unanimity" in groupthink.

Reasons and solutions *Reason 1: Impartial leader.* The execution of safety analysis is guided by a moderator, who guides the procedures as well as controls the time. Mostly, to limit the discussion about safety analysis, the senior managers or safety experts stand out and express their opinions to end the discussion. It makes the decision-making procedures partial. As one moderator mentioned: *"Sometimes there is a tough discussion between different opinions, we have to stop them, because of the time plan. I try to get in touch with some leaders or experts maybe through eye contact. They will provide a decision and we use it to finish this part."* That causes the decision overly relying on personal decision-making capability and integrating more non-technical considerations from managers, such as cost and schedule. *Solution 1: Make key member impartial.* First, a standardized safety analysis procedure with a defined, transparent and explicit decision-making procedure helps the moderator and experts to be impartial. One moderator suggested: *"We always like to use "high-risk priority" principle rather than directly adopting key member's decision."* That could avoid the bias from positions and thus concentrate on risks. Second, we have to ensure that those who are making safety-related decisions are fully informed and skilled [20]. Third, the decisions could be assessed and improved. *Reason 2: Cohesion.* This cohesion is between team members and senior managers or safety experts. Some team members were hired by the senior managers. They have been working for him or her for a long time and give the same voice with their managers. *Solution 2: Split groups.* The practitioners could spit the high-cohesive members into separate groups when performing safety analysis.

6. When providing safety analysis solutions, the team members prefer explaining the rationality of the existing solutions.

Description In GSA 4, the team members prefer using existing solutions for mitigating risks. As one interviewee said: *"When we got a risk, we would like to use the existing methods from the former projects or similar products. It saves more efforts and is more reliable to validate its feasibility of the existing one rather than to propose a new one."* We can see three groupthink symptoms from this case: "rationale", "morality" and "direct pressure".

Reasons and solutions *Reason 1: Lack of norms on change management procedure.* We reviewed an internal change management manual and advised one senior quality manager. He mentioned: *"We do the impact analysis when performing change management. Most of the time, we concentrate on the changed parts. Based on the experiences and expert opinions, we analyze the possible impacts. In safety analysis, we notice the requirements on change management in ISO 26262-8, part 8, but there is no mention of a systematic technique."* The members believe in the morality of the former solutions for the unchanged parts and try to rationalize them. *Solution 1: Enhance change management.* Establishing the management of change requirements for evaluating all changes for their impacts on safety systematically. *Reason 2: High stress from external threats.* The delivery deadline causes stress. That causes the team members using the existing solutions for mitigating risks and trying to rationalize them. One interviewee said: *"Before a deadline, we won't switch to developing new solutions. That increases risks on delivery. When we have an existing solution, we use it. The worst case, we could write the possible risks on the internal (for developers) or external (for customers) reports."* It shows that the existence of a solution is more important than the effectiveness of a solution under delivery pressure. *Solution 2: Devote a block of time to provide alternative scenarios.* Some alternatives or new solutions could be reserved and reconsidered. *Reason 3: Temporarily low self-esteem.* The team members are afraid of undertaking responsibilities. They do not believe in their capability to propose a better solution than the former one. Furthermore, they have to invest more efforts for new solutions. When there is an accident during the execution, they have to be responsible for it. A "blame culture" exists. *Solution 3: (Refer to solution 2) Devote a block of time to provide alternative scenarios.* In addition, the proposal of the opinions and the execution of them shall be divided. After accepting the new solutions, the team members shall share responsibilities. To this end, the practitioners need consider anonymity.

7. The safety analysts spontaneously freeze the internal safety-related documents.

Description In GSA 5, the safety analysts take the responsibility for the documents and freeze them to avoid review and modification. One interviewee mentioned: *"Sometimes I have a question about the results what we have discussed in the meeting. Later, I am not able to open such files anymore. When I ask the relevant person, he said that we have already discussed and decide in the meeting. The results are documented. If there are questions, I should ask other people."* That is called "mindguards" in groupthink symptoms.

Reasons and solutions *Reason 1: Lack of norms on the authority of safety-related documents.* The norms require a lot of documents for each activity. Yet, there is no description of authority. The documentation engineers protect the documents by themselves as to protect the decisions of groups. *Solution 1: Make key members impartial.* The generation of documents should be transparent. The documents should be appropriately open. To manage safety, there is a safety information system including safety analysis related documentation. They are not only for maintenance, but also for guiding safety audit and assessment. *Reason 2: Group insulation.* The management of safety-related documents including project related documents, organization related documents and process management documents is separate. That causes too many limitations on authority. *Solution 2: Discuss with trusted people.* In documentation management, the industry could consider some online documents management tools. The non-confidential documents are preferred to be open to project-related people.

8. During safety verification, the safety analysts set themselves as a "police" to blame the development team.

Description In GSA 6, the safety analysts sometimes overestimate their authority on a "police" role and neglect their responsibility as a "teacher" or a "doctor". They shall work on finding safety vulnerabilities and guide the development to ensure the safety. However, some of them are concerned only with finding vulnerabilities and even blaming. As one developer mentioned: *"They always point out our failures. That gives us a bad mood. When we ask further for a suggestion, they said that they are not clear about the detailed development, they care about if the development can satisfy these safety requirements. We cannot get any help."* It shows a groupthink symptom "invulnerability".

Reasons and solutions *Reason 1: Group insulation.* The functional safety department and the development team are isolated. *Solution 1: Invite external expert.* The safety verification is preferred to be happening during the development phase. The development team could invite relevant members to take part in their meetings or daily work. Effective communication channels and feedback channels are useful. *Reason 2: Temporarily low self-esteem.* A strong attitude and blame are sometimes because of lacking confidence. The reason of the safety analysts taking the role as police to blame could be that they temporarily lack technical capability to teach and cure them. *Solution 2: Devote a block time to discuss the solutions.* A preparation time slot and a harmonious environment for cross-functional communication are vital.

9. During safety validation, the internal safety expert takes the role as a "lawyer" to rationalize their safety assurance to a third party.

Description In GSA 7, the internal safety expert shows partiality as a "lawyer". He or she sometimes does not aim to find the hazards rather to rationalize the safety assurance capability and pass a third party validation. That is a symptom called "rationale" in groupthink.

Reasons and solutions *Reason: Cohesion.* The internal safety expert is a member in the company. As one safety expert said: *"I am working for the company, what I should do is to validate that our process is safe enough to deliver a safe product."* The organizational

cohesiveness changes the objectiveness of safety validation. *Solution: Invite external expert.* One senior manager suggested inviting an external safety expert to validate the process and product before a third party validation. The external safety expert should be independent and might come from the same company, but different subsidiaries.

10. The team performs safety analysis aiming to provide the required evidence for certification (paperwork culture).

Description During the whole GSA, the team members perform safety analysis aiming to provide evidence for certification. That is called "rationale" in groupthink.

Reasons and solutions *Reason: Impartial leader.* The leader takes safety superficially. That causes the groupthink symptom that no other member is concerned with it. As one senior manager mentioned: *"We do safety analysis is because the norm requires it. By following the norms, we can get a certification in parallel with our products. That helps us to sale more products."* Another feedback from a developer is: *"We have no idea about the norms. We just follow the requirements from our leader. He takes care about the norm-related issues."* However, employees need to feel that they will be supported if they show concerns for safety.

Solution: Make key members impartial. A manager's open and sincere concern for safety in everyday can have a major impact on the reception given to safety analysis [20]. First, opening standards is important, as well as opening communication on the standards. Each team member needs to know "how" and even "what". "Leadership-collaboration" should replace "command-control management" [6]. Second, a thorough integration of safety culture is necessary from three levels: surface level cultural artifacts; organizational rules, values, practices; and values and deep cultural assumptions [26]. The surface level includes everyday practices. In the middle, it states the rules like policy, standards and guidelines. Lastly, values and deep cultural assumptions are used for making leaders with more emphases on safety.

5 DISCUSSION

5.1 Implications

This article notes the consideration on groupthink in safety analysis. From our viewpoint, the occurrence of conflicts, together with an effective decision-making, is positive for safety analysis. However, the occurrence of groupthink is potentially fatal. We investigate seven GSA according to the norms. We calculate the occurrence and frequential of groupthink symptoms in the GSA. We propose Top 10 phenomena, which happen in safety analysis and cause the results lacking group considerations. We find out the possible reasons and solutions which are specific for safety analysis to avoid groupthink referring to Janis's seven antecedents[3] and nine recommendations[3]. Eight symptoms[3] have all been found in our Top 10 phenomena. Six of seven antecedents are found with a specific form in GSA. "Lack of norms" concerning various aspects is the most proposed cause, which has been five times mentioned in the Top 10 phenomena. "Cohesion", "Group insulation" and "Temporarily low self-esteem" show three times. Yet, "homogeneous" has not been found in our cases. "Homogeneous" means the similarities of members' social backgrounds and ideology. In most safety-critical industries, they have a standardized organization development procedure. They have a regular hiring process according to the requirements from organization structure. The phenomenon of a "homogeneous" team is rare. They range the members from new employees to experts. The knowledge background is also diverse. We map eight of the nine recommendations in the proposed solutions. "Invite external expert" is the most popular one, while "make key members impartial" shows also its importance. Only the recommendation on "setting a devil role" has not been mentioned by the interviewees. It has some difficulties. Each one has his core area. The devil role is hard to cover a wide range of topics. In addition, the interviewees show also unwillingness. More than that, the interviewees mentioned two other suggestions: improve the communication/feedback channels and regular procedure requirements on joined members or departments and a systematical change management.

5.2 Threats to validity

5.2.1 Internal validity. First, the seven GSA cover only the major parts of safety analysis activities. We walked-through the norms and relevant literatures to summarize the GSA that happen in a group. Yet, such activities were observed more than thirty types [30]. Some of them are integrated into the development process. Thus, we use five main activities when performing safety analysis by using various techniques and two activities including safety verification and safety validation, which are directly relevant to the safety analysis. Other activities like safety audit, which concerns more on the safety assurance process, is not included in this article. Second, the survey questions could be incomplete. Groupthink is not a popular word in software engineering. To make it more understandable to the participants, we simplified the original descriptions from Janis and set the questions in an easy way. Thus, we propose the survey available online for review. During the interviews, it was possible to explain them in-depth. Third, the influence from culture can be a limitation. We performed the survey in four Europe companies. Two of them are international companies covering Asia subsidiaries. The participants are from both Europe and Asia. However, it is not enough to generalize the result. We hope to expand this study in a wider scope.

5.2.2 Construct validity. First, since the interviews were conducted with industries, the audio recordings were not allowed. We recorded the results only relying on the transcript by the first author. Concerning some missing points and confidentiality, we contacted the participants again and provided our protocol to ensure the results. Second, the results have many inconsistent terminologies. Some of them are internal terms in each company. We discussed our results and determined them with the primary company A.

5.2.3 External validity. First, the primary company is in the automotive industry. We generated our results for RQ 1 mainly from the automotive area functional safety standards ISO 26262. We referred to the safety standards ISO 14971 and IEC 60601 in medical equipment area as well. However, these two areas cannot stand for all the safety-critical industries. Second, the attitudes toward groupthink also rely on different roles. We aim to cover as many roles as possible. Most of the participants are from quality assurance departments, development teams and relevant managers. Some of

them are from sales, purchasing and production. The amount of participation is limited.

5.2.4 Reliability. Some contents concerning groupthink are sensitive, such as "impartial leadership". We designed and collected the survey anonymously. Yet, the participants may also reserve some results.

6 CONCLUSION

In this article, we investigate groupthink in safety analysis. We conducted a case study in seven safety-critical companies. We investigated seven GSA concerning groupthink. We statistically summarized the most frequent symptoms through 39 surveys. We investigated further the Top 10 groupthink phenomena through 17 interviews. We investigated and mapped the reasons with Janis's theory. We generated further the solutions combining Janis' theory and safety system management. We found that the groupthink does exist in safety analysis. The practitioners should find phenomena and consider solutions. Our cases show limitations mainly on the domains and countries. It could be expanded in the future.

APPENDIX A JANIS'S GROUPTHINK MODEL

We list eight symptoms, seven antecedents and nine recommendations from Janis's groupthink model [17]:

Symptoms

(1) Illusion of *invulnerability*.
(2) Collective *rationalizations*.
(3) Belief in inherent *morality* of the group.
(4) *Stereotypes* of out-groups.
(5) *Direct pressure* on dissenters.
(6) *Self-censorship*.
(7) Illusion of *unanimity*.
(8) Self-appointed *mindguards*.

Antecedents

(1) *Cohesion*.
(2) *Group insulation*.
(3) *Impartial leader*.
(4) *Lack of norms*.
(5) *Homogeneous*.
(6) *High stress from external threats*.
(7) *Temporarily low self-esteem*.

Recommendations

(1) Leader should *assign each member the role of "critical evaluator"*.
(2) *Making key members impartial*.
(3) The organization should *establish multiple groups*.
(4) Each member should *discuss the group's ideas with trusted people* outside of the group.
(5) The group should *invite external experts* into meetings.
(6) At least one group member should be *assigned the role of devil's advocate*.
(7) The organization should *devote a block time to discuss conflict and provide alternative scenarios*.
(8) The organization could *slip the group*.
(9) The organization should *provide a second chance meeting*.

REFERENCES

[1] K. Beck. 2000. *Extreme programming explained: Embrace change*. Addison-Wesley Professional.
[2] B. K Brockman, M. E Rawlston, M. A Jones, and D. Halstead. 2010. An exploratory model of interpersonal cohesiveness in new product development teams. *Journal of Product Innovation Management* (2010).
[3] M. Brown. 2014. Groupthink in software engineering. *International Journal of Computing and Business Research* (2014).
[4] K. Charmaz. 2014. *Constructing grounded theory*. Sage.
[5] A. Cockburn. 2002. *Agile software development*. Addison-Wesley Boston.
[6] A. Cockburn and J. Highsmith. 2001. Agile software development, the people factor. *Computer* (2001).
[7] S. Coyle, K. Conboy, and T. Acton. 2013. Group process losses in agile software development decision making. *International Journal of Intelligent Information Technologies* (2013).
[8] C. De Snoo, W. Van Wezel, and R. J Jorna. 2011. An empirical investigation of scheduling performance criteria. *Journal of Operations Management* (2011).
[9] Meghann L. DG., Kieran C., and Tom A. 2017. Examining decision characteristics and challenges for agile software development. *Journal of Systems and Software* (2017).
[10] T. Dingsøyr and Y. Lindsjørn. 2013. Team performance in agile development teams: Findings from 18 focus groups. In *Proceedings of the International Conference on Agile Software Development*. Springer.
[11] C. Ferraris and R. Carveth. 2003. NASA and the Columbia disaster: Decision-making by groupthink?. In *Proceedings of the 2003 Association for Business Communication Annual Convention*.
[12] International Organization for Standardization. 2011. *Road vehicles - Functional safety*. ISO.
[13] L. Gren and A. Goldman. 2016. Trying to increase the mature use of agile practices by group development psychology training - An experiment. In *Proceedings of the 4th International Workshop on Quantitative Approaches to Software Quality*.
[14] L. Gren, R. Torkar, and R. Feldt. 2017. Group development and group maturity when building agile teams: A qualitative and quantitative investigation at eight large companies. *Journal of Systems and Software* (2017).
[15] L. Harms-Ringdahl. 2003. *Safety analysis: Principles and practice in occupational safety*. CRC Press.
[16] P. Hart. 1990. *Groupthink in government: A study of small groups and policy failure*. Swets & Zeitlinger Publishers.
[17] I. Janis. 2008. Groupthink. *IEEE Engineering Management Review* (2008).
[18] S. WJ Kozlowski and B. S Bell. 2003. Work groups and teams in organizations. *Handbook of Psychology* (2003).
[19] R. M Kramer. 1998. Revisiting the Bay of Pigs and Vietnam decisions 25 years later: How well has the groupthink hypothesis stood the test of time? *Organizational Behavior and Human Decision Processes* (1998).
[20] N. Leveson. 2011. *Engineering a safer world: Systems thinking applied to safety*. MIT press.
[21] C. C Manz and H. P Sims Jr. 1982. The potential for groupthink in autonomous work groups. *Human Relations* (1982).
[22] J. McAvoy and T. Butler. 2009. The role of project management in ineffective decision making within agile software development projects. *European Journal of Information Systems* (2009).
[23] B. Mullen, T. Anthony, E. Salas, and J. E Driskell. 1994. Group cohesiveness and quality of decision making: An integration of tests of the groupthink hypothesis. *Small Group Research* (1994).
[24] J. D Rose. 2011. Diverse perspectives on the groupthink theory - A literary review. *Emerging Leadership Journeys* (2011).
[25] P. Runeson, M. Host, A. Rainer, and B. Regnell. 2012. *Case study research in software engineering: Guidelines and examples*. John Wiley & Sons.
[26] E. H Schein. 2010. *Organizational culture and leadership*. John Wiley & Sons.
[27] W. Schiano and J. W Weiss. 2006. Y2K all over again: How groupthink permeates IS and compromises security. *Business Horizons* (2006).
[28] K. Schwaber and M. Beedle. 2002. *Agile software development with Scrum*. Prentice Hall Upper Saddle River.
[29] D. V. Tennant. 2011. Leadership in crisis situation - A case study. (2011).
[30] J. Vilela, J. Castro, L. E. G Martins, and T. Gorschek. 2017. Integration between requirements engineering and safety analysis: A systematic literature review. *Journal of Systems and Software* (2017).
[31] S. A Wheelan. 2009. Group size, group development, and group productivity. *Small Group Research* (2009).
[32] R. K Yin. 2013. *Case study research: Design and methods*. Sage.