Evaluating non-functional qualities in railway by applying the quality triage method - A case study

Eivind H. Okstad

SINTEF Digital, Norway. E-mail: eivind.h.okstad@sintef.no

Ola Løkberg

SINTEF Digital, Norway. E-mail: ola.lokberg@sintef.no

Robert Bains

SINTEF Digital, Norway. E-mail: robert.bains@sintef.no

The railway industry is undergoing modernization and development with increasing use of new technology and digitalisation. In addition to physical security requirements, systems need to be secured against cyberattacks from outsiders. In addition, there are other quality requirements like scalability, reliability, availability, and sustainability that need attention. This paper presents results from testing the quality triage method, which has its origin from software development, on railway projects. The quality triage method aims to balance several quality requirements for decision making in development projects. Cybersecurity is an example of these quality requirements. A discussion of cost elements and benefits from applying the method within the railway domain has been outlined. As a main conclusion, the authors see new opportunities of addressing quality requirements more explicitly in projects by applying the quality triage approach to railway projects.

Keywords: Quality requirements, Functional requirements, Cybersecurity, Railway safety

1. Introduction

Railway projects traditionally focus on success factors like cost-effective deliverables and achievement of functional requirements from the infrastructure manager's or railway operator's point of view. In addition, passenger safety is much emphasised as the main societal requirement to any transportation means, and that is closely followed up by the regulatory authorities. However, there are other qualities that could benefit from attention in projects from stakeholders and related work processes, like security (cybersecurity), scalability, reliability, availability, and sustainability. Cybersecurity and security management become important issues in railway projects and operations with technology development and implementation of new railway technology. Such qualities may gain less attention in projects but come to surface later, typically after the system is put in service. Each quality could, and as usually done, be addressed by applying separate methods, although it may be demanding.

The quality triage method (Brataas et al., 2020b) was introduced as a simplified, low-demanding approach to decision support. It applies 'user stories' as basis for identifying quality risks and making multiple quality areas explicit. The original motivation for the quality triage method in this context is experiences from software (SW) development projects applying agile development that have been prone to neglecting quality requirements (Alsaqaf, et al., 2017). The quality triage method intends to meet these challenges in a way that makes it easier to balance and prioritise between different qualities in progress-, or regular project meetings.

The present article argues this way of thinking could be valuable in other domains than SW-development as well, and not only valuable for agile development projects. A case study presents results from testing the quality triage method in a railway-project environment (non-agile development). A light-rail company was contacted, and some experiences were shared with the research team on how cybersecurity issues usually are treated, and how the railway company plan to deal with cybersecurity as a quality requirement in upcoming projects.

1.1. *Background*

The railway industry is facing challenges when it comes to project efficiency and quality management during project execution, also taking into concern the multiple stakeholders involved in decision making. Challenges also become more prominent in a rapid changing world that requires implementation of new technology with increased digitalisation. New control, command and signalling systems (CCS) in railway might thus, be more vulnerable to cyber threats, which typically change at a faster pace than pure safety threats. New threats could even occur after the system is put into service. Due to the comprehensive and often static processes of safety-approval, cybersecurity e.g., as one important quality, needs a somewhat different handling than functional safety, preferably separated from the safety-approval regime (Okstad, et al. (2021).

Safety for passengers and goods is an important requirement set by the authorities in connection with development and operation of railway systems. Other non-functional requirements should as well be reflected. In addition to safety, requirements for uptime and service level will fulfil the railway business purpose.

Proceedings of the 32nd European Safety and Reliability Conference
Edited by Maria Chiara Leva, Edoardo Patelli, Luca Podofillini, and Simon Wilson

ISBN: 981-973-0000-00-0 :: doi: 10.3850/981-973-0000-00-0_esrel2022-paper

However, safety in operation may influence on other quality requirements. To balance different non-functional requirements, the authors want to test the quality triage method on light-rail projects where priorities and plans are made in frequent project meetings. The purpose is to achieve flexible and efficient decision-making processes with non-functional requirements and thus, saving time and costs that quite often become a challenge for the industry.

1.2. *Literature*

The present study aims to test the 'quality triage method' method of Brataas et al. (2020b) on a railway case. The method itself describes an approach for engineering of quality requirements by assigning appropriate priorities to quality requirements in large, complex, and agile engineering projects. The origin of the method is agile[a] (sprint) software development processes that was introduced by Behutiye et al. (2019) and others.

The concept of a quality triage is borrowed from emergency medicine, where a doctor quickly determines if a person requires immediate treatment or can wait (Brataas et al., 2020b). It is well documented that neglecting non-functional requirements is common in agile development (Behutiye, et al. (2019) and Ramesh, et al. (2010)). As an example, the systematic mapping study (N=156) of quality requirements in agile and rapid software development by Behutiye et al. (2019) identified the following top five challenges:

i. A limited ability of agile software development to handle quality requirements
ii. Time constraints due to short iteration cycles
iii. Limitations in testing quality requirements,
iv. Neglect of quality requirements
v. Lack of an overall picture of quality requirements

Several of these challenges can be said to be of a general nature in any development project, regardless of domain. Ramesh et al. (2010) pointed to customers' focus on core functionality and their lack of recognition for the importance of non-functional requirements at early stages. They concluded that inadequate attention to non-functional requirements made it harder to incorporate them late as the system grows through successive development cycles. Also, without clear specification of quality requirements, developers may make design choices that are arbitrary, and it becomes difficult to assess whether the system meets real requirements.

Basically, the quality triage method addresses a set of selected quality requirements and makes the process of controlling fulfilment of the quality requirements manageable. Examples of quality requirements to cyber-physical systems are Scalability, Safety, Reliability, Availability and Security as demonstrated in Brataas et al. (2020b). Cyber-physical systems in this context are integrations of computation, networking, and physical processes. The relevance of the method is linked to its simplicity and practical approach to cross disciplinary teamwork.

A quality triage is a label of an expert-group meeting for identifying challenges of quality concerns where further effort and improved coordination are required. The intention is to quickly identify and prioritise areas, or challenges of quality concerns at present stage. The concrete approach will address such qualities from the early project stages of, and throughout the project making the process manageable. The method is for practitioners in projects and needs to be tested in an industrial setting. One limitation may be the method's somewhat simplified approach to criticality ranking, but we believe the benefits of frequent team discussions will balance any drawbacks of simplicity.

The empirical study of Alsaqaf et al. (2019) uses exploratory qualitative interviews of practitioners. Challenging situations as experienced by practitioners in engineering of quality requirements within a context of large-scale distributed agile projects are identified. The method applies a qualitative coding[b] for data analysis and identification of challenging situations. In addition, the coding supports description of the mechanisms behind challenges and identifies different practices in use by agile teams to mitigate possible impacts of the identified challenges. Even though the method of Alsaqaf et al. (2019) address qualitative coding as the core method, it is highly relevant to the engineering of quality requirements in projects, like the approach of Brataas et al. (2020b). Both approaches focus on the practitioners' experiences as main input to decision making. An important result from the article of Alsaqaf et al. (2019) is the presentation of a comprehensive set of challenges, mechanisms, and practices currently in use to mitigate impact of reported challenges.

Another example of a method for managing quality requirements is the Six-Step Model (SSM) of Amro et al., (2020) that enables capturing the relationships between cyberattacks and component failures, assessment of safety and cybersecurity countermeasures, as well as the synergy between safety and cybersecurity. It aims to analyse safety and security risks and study the implications that security poses to safety. It is rather a holistic approach to assessing the interdependencies. The method facilitates collaboration of safety and security experts in the comprehensive safety and security analysis. Originally, the SSM was proposed by Sabaliauskaite, et al. (2016) to analyse, both safety and security aspects of cyber-physical systems.

2. The Quality Triage Method

This section explains the quality triage method more detailed, how it can be performed in practice, and how it would fit into an agile development practice (Brataas et al., 2020b).

[a] 'Agile': Flexible processes, fewer formal milestones

[b] 'Qualitative coding': Classification of qualitative statements

Figure 1 illustrates the principles of the quality triage method, exemplified by the four quality dimensions scalability, security, safety, and availability. Availability may depend on the other three dimensions to a certain degree: A condition for a system to operate (being available) may be that the requirements with respect to scalability, security and safety are fulfilled. In that context, availability will be a kind of meta-requirement compared to the other three. Also, relations between the other quality requirements may be possible.

Basically, the triage[c] is about focused meetings (or sprints) in a project-development environment to balance the quality requirements (Brataas et al., 2020a). The quality triage method implies the following two steps:

i. Individuals, and group of experts to evaluate user stories/features from each quality's point of view.

ii. To identify and evaluate influences of different qualities and support decisions on mitigation tasks.

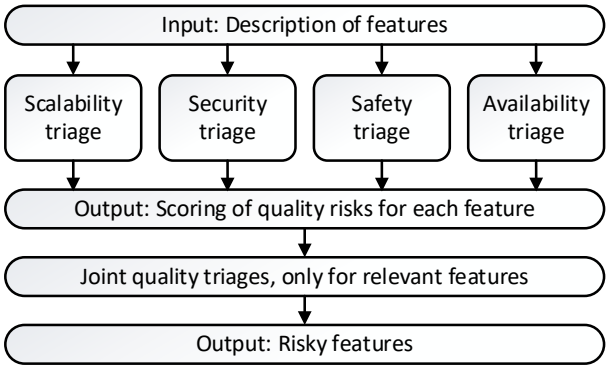

Figure 1. The quality triage method (Brataas et al., 2020b)

2.1. *Railway application of the method*

The quality triage method is not only suited for agile development projects or for projects where rapid decision support is critical. The authors believe the method is equally valuable as a means of assigning appropriate priorities to quality requirements in large and complex engineering projects (which is typically the case for railway projects).

For railway application, the following example illustrates one type of problem: If safety is threatened and hazards are related to automated functions, the railway operator typically switch to manual operation with reduced availability. Then the following dilemma occur: If you set too strict safety requirements for the system, which means more frequent manual operation, the operator also drive more often without the built-in safety barriers, which by time can lead to lower safety, in addition to lower availability. This aspect is not explicitly shown in Figure 1.

2.2. *Method guidance – as adapted to railway*

A step-by-step guideline has been prepared as a support to the case study that can be applied to long-distance railway and light rail/metro systems. The main reason for preparing such a guideline is that the original concept, and much of the notation else, has its origin from software engineering.

When introducing e.g., a new signalling system, carrying out modification of existing systems or significant upgrade, it might well introduce new features and concerns and hence, implying much work to analyse in detail all the quality-/non-functional requirements in addition to safety. The quality triage method here intends to emphasise the most important non-functional quality issues (prioritising) during the project work.

The quality triage method suggests to the project management the following steps, which are the main tasks taken from the method description of Brataas, et al. (2020b):

i. Provide a system description with limitations and constrains for the affected (new) system under study.

ii. Identify the relevant non-functional qualities (multiple) of the system.

iii. Describe a set of overall goals (epics) and related user stories[d]/features to address in those.

iv. Carry out individual triages: Domain (quality) experts are to evaluate criticality of user stories/features to the relevant quality from their own (single) point of view.

Select 1-3 factors for each quality dimension to aid in assessing the important-level scores.
Use a five-point scale to evaluate each factor that is to be calibrated by the experts according to the project at hand. *Classification of the effect from factors on user stories: VL-Very Low, L-Low, M-Medium, H-High, VH-Very High*
Assign scores based on discussions of the user stories/features and what are the prominent quality issues and dependencies.

Four basic outfalls are relevant in assessing effect of a user story/feature on quality dimensions:

1. User story/feature has **No unacceptable risk** for any of the quality dimensions.
2. User story/feature has **Unacceptable risk for one quality dimension**, and **the mitigation causes no problems** for other quality dimensions.
3. User story/feature has **Unacceptable risk for one quality dimension**, and **the mitigation causes more risks** for other quality dimension.
4. User story/feature has **Unacceptable risk for two or more** quality dimensions. Quality experts need to work together to coordinate solutions.

v. After individual triages, the experts gather for a short meeting (quality triage) where issues are flagged, dependencies between qualities identified, and solutions proposed.

[c] 'Triage' is about short decision meetings, or rapid sprints.

[d] 'User story' is about important applications or features that characterise the system.

vi. Elaborate on each quality dimension the scoring of the different quality criteria or factor for each user story/feature.

vii. Make plans for additional meetings (triages) to further coordinate and consult parties regarding the mitigation actions.

Quick evaluations are valuable in projects where limited resources (time, money, expertise) restrict any full analysis (if appropriate) of the system related to each quality dimension, and thus, might become a more targeted and time-efficient evaluation. In addition, it could explore and handle dependencies among quality dimensions at early stages. Based on experiences from applying the 'Protection Poker' method of Tøndel, et al. (2019), the five-point scale for assessing each factor was suggested.

Like what is done in Protection Poker, this scale needs to be calibrated to the project at hand, which means that the quality experts responsible for the analysis need to consider what is very high, or very low score related to the factors chosen, and evaluate the features/user stories, accordingly.

3. Case study – railway project

The authors believe in quality triage as a generic concept to facilitate and organise relevant project work in expert teams, and it might well fit other domains than SW development, like railway projects. In the railway business, infrastructure companies and railway operators are responsible for delivering cost-effective transport services to the public and are at the same time obliged to fulfil a set of quality requirements. Examples of such quality requirements are safety, security, availability, punctuality, and reliability of the railway system. The main benefit of applying the method in railway projects, is according to the author's view, not only as a flexible decision support, but rather a simplified means of assigning appropriate priorities to quality requirements in large and complex projects.

3.1. *Case description and analysis*

This section describes the CBTC-technologies that have been addressed in the case study, and the relevant features for scoring. The individual quality scoring is given in Section 3.2 as basis for the joint quality triage in Section 3.3.

3.1.1. *System description (CBTC)*

CBTC-technology (Communication Based Train Control) is the industry standard for managing and securing subway/metro traffic and has been in use for many years around the world. The CBTC-technology allows for wireless communication between trains, as well as between train and the infrastructure. It optimises both speed and distance between trains in interaction with the driver and the traffic-control centre. Trains running tighter with better flow implies that several trains can operate simultaneously in the subway/metro system. In Norway, actors plan to buy wireless communication as a service over the public mobile networks and must enter into agreement with tele companies as providers of the service. These agreements need to set strict requirements for accessibility and service level for the control systems, mobile coverage along the entire metro line, priority traffic in the mobile network, 24/7 monitoring, as well as sufficient assistance in connection with implementation and testing. Functional requirements for CBTC are fulfilled by implementation of automatic train protection (ATP) functions, automatic train operation (ATO), and automatic train supervision (ATS) functions.

When applying the quality triage method to a CBTC-system, the authors like to address the following three qualities: Safety, Availability and Security. Safety is an absolute concern. Availability relates to uptime and is about the service level offered to customers and cost-efficient operation. Security is about protecting the digitalised systems that could be exposed to cyber threats (cybersecurity). As aid in assigning the important level scores to user stories/features, two factors are selected for each quality dimension according to Table 1.

Table 1. Quality factors to rate

Quality	Factor	
Safety	-Possibility -Consequence	-The possible occurrence of the safety critical situation (event) -Potential loss in terms of loss of lives, expenses, or damage to the environment
Avail-ability	-Probability of failure -Restoration time	-Probability of functional failure given component redundancy -Time for the restoration of a failed system (unplanned maintenance)
Security	-Asset value -Exposure	-How valuable are the assets that this functionality touches upon? -To what extent does this functionality open-up for attacks?

The selected factors are based on Brataas et al. (2020b). Physical safety is the opposite of the term 'risk' that could be expressed as a function of consequence and likelihood of an unexpected event, or accident. For this study we select 'possibility' instead of 'likelihood' to convey a high-level evaluation (qualitative).

Availability builds on the Reliability, Availability, Maintainability and Safety (RAMS) process following the EN 50126-1 standard (CENELEC, 2017), and it can be increased by optimising reliability, minimising probability of failure and improving maintainability. Redundancy and restoration time are other important factors to availability. In this study we select the factors 'probability of failure' and 'restoration time' to score on availability.

Security as a quality is inspired by Protection Poker (Williams, et al. 2010 and Tøndel, et al. 2019). Here, the more traditional factors 'consequence' and 'likelihood', typically used in security risk analysis, are replaced with 'exposure' and 'value'. This is to be better aligned to the feature as a unit of analysis if facing a potential cyberattack incident.

3.1.2. *Description of features*

Each CBTC-application installed on a new-, or existing subway/metro implies hundreds of new functions or features. It will simply be too much analysing in detail every quality implication of those features. The idea is thus, to identify and focus the attention on the most critical features (against qualities goals) of the CBTC-technology viewed as a system.

The overall goals including the underlying features of the CBTC-system are identified and described based on the CBTC-standard (IEEE, 2005). These features have been discussed through an internal Table-Top, with input from railway companies. The following 'epics' (overall goals) are adapted to the case study based on descriptions of the CBTC-technology in the IEEE-standard. The level of features (e.g., A1-A3) for which, the method is to be applied can be adapted to the actual application and any specific focus areas.

A. **Automatic train protection (ATP).** A CBTC-system shall be capable of providing bidirectional ATP. The wayside and train-borne vital processing of train status and control data allow for- and provide continuous automatic train protection (ATP). Important features of ATP are the following:

   A1. Train location/train speed determination: Establish the location, speed, and travel direction of the CBTC-equipped train operating in a CBTC-territory. Establish the location of both the front and rear of the train. Train location determination function shall be self-initializing and automatically detect id. and location of each CBTC-equipped train.

   If the CBTC train location/speed determination function is dependent upon wheel rotation, the CBTC-system shall correct for position errors induced by the slipping or sliding of wheels and shall correct for position errors caused by variation in wheel size due to wear, trueing, or replacement.

   A2. Safe train separation: Provide safe train separation between CBTC-equipped trains based upon the principle of an 'instantaneous' (brick wall) stop of the preceding train. For mixed-mode operation (trains without CBTC), safe train separation shall be provided through an auxiliary wayside system and/or through strict adherence to operating procedures, as specified by the authority having jurisdiction.

   A3. Overspeed protection and brake assurance: Speed limits and restrictions shall apply when any portion of the train is within the speed limit area. If the ATP profile speed at that location is exceeded, the CBTC-system shall initiate an immediate brake application. During service brake situations (not emergency brake) the CBTC-system shall monitor the achieved brake rate to ensure an acceptable brake rate is achieved within a predetermined time frame.

B. **Automatic train operation (ATO).** For operation of trains without any crew, a CBTC-system shall, be capable of providing several ATO-functions. It implies e.g., to automatically operate trains in accordance with the prescribed operating criteria and within safety constraints imposed by the ATP.

   B1. Automatic speed regulation: Automatic control of speed, acceleration, deceleration, and jerk rates within specified passenger comfort limits (as defined by the authority having jurisdiction). Train speed stays below the overspeed limits imposed by ATP.

   B2. Platform berthing control: Implements a set of specified platform-berthing control modes.

   B3. Door control: Automatic control of train doors (and platform edge doors, where fitted) during passenger boarding and discharging.

C. **Automatic train supervision (ATS).** If specified by the authority having jurisdiction, a CBTC-system may interface to, or be integrated with an ATS-system.

   C1. ATS user interface with information and action controls: Each ATS-interface displays information and implements all the control actions within acceptable latencies as specified by the authority having jurisdiction.

   C2. CBTC train identification and train tracking: Automatic tracking, maintaining records of, and displaying on the ATS user interface the locations, identities, train schedule, and other pertinent data for all the CBTC-equipped trains in the CBTC-territory.

   C3. Train routing: Manual and automatic routing of trains based on CBTC-train location reports and in accordance with the train service data, predefined routing rules, and any ATS user-directed service strategy.

To support the above vital functions, the CBTC-system allows for determination of train location to a high degree of precision, independent of track circuits, and geographically continuous train-to-wayside and wayside-to-train data communications.

3.2. *Scoring of quality risks*

Table 2 shows the scores given to the different quality criteria for each of the features. It is followed by a brief justification based on descriptions found in IEEE (2005) and engineering judgement among the authors (based on the authors' experience and knowledge of common implementation of those features).

Table 2. Scoring of quality risks for each feature

User story/ Feature	Safety		Availability		Security	
	Possibility	Consequence	Probability of failure	Restoration time	Asset value	Exposure
A1	L	VH	VL	H	VH	H
A2	L	VH	VL	H	VH	H
A3	L	H	VL	M	H	H
B1	VL	VH	VL	M	VH	H
B2	L	L	L	L	H	M
B3	H	H	M	L	L	M
C1	VL	L	VL	VL	M	VL
C2	L	L	L	VL	M	M
C3	L	L	VL	VL	M	M

Safety: ATP functions in a train provide fail-safe protection against collisions, excessive speed, and other hazardous conditions. ATP-functions shall thus, have precedence over both the ATO- and ATS- functions. Train location and safe train separation are considered as highly safety critical functions and are scored safety consequence 'Very High' by failure. However, as the design is well proved and the quality assurance and testing of the software are thorough, the possibility of safety related failures is considered 'low' for A1, A2 and A3. Automatic speed regulation provided by the ATO-function is indeed a safety critical function and scored 'Very High' to safety consequence. But as for the ATP, we believe the software is well proved and tested and consider the possibility of safety related failures to be 'Very Low'. The platform berthing control of the CBTC-system allows for different berthing modes depending on e.g., the platform length. However, the possibility and safety consequence of a failure is considered 'Low' because of an assumed low train speed when approaching the platform area, and a proved system. Door control is a bit more uncertain with regards to safety. The consequence may be 'High' if it fails, due to the possibility for passengers dropping into the platform or falling out of a train, still in motion. The ATS-functions are considered as only minor safety critical and are given scores 'low' and 'Very Low'. Among other factors, the ATS functions are not required to be implemented in a fail-safe manner according to clause 6.3.2 in IEEE (2005).

Availability: Probability of failure for the ATP-, ATO- and ATS-functions are given slightly lower scores (positive) for availability compared to the 'possibility' score related to safety. Probability of failure regards only the technical system (HW/SW-failures) and not any operational or human failure, which might be included in the safety factor 'possibility'. Restoration time concerns the mean time to repair/replacement of failed pieces of the CBTC-equipment (i.e., first-level repair) and will include on-site diagnostics, the replacement of failed components, and testing of repaired units, subsystem, or the whole system. A CBTC-system also includes maintenance- and diagnostic capabilities to detect and react to certain failures. Remote diagnostics capabilities and local built-in test equipment and other fault displays for troubleshooting, then facilitate timely identification of failed components and functions (clause 5.4.4 of IEEE, 2005). Restoration times are thus, scored 'high' to 'medium' for the ATP and 'Low' to 'Very Low' for the rest of the features in Table 2.

Security: Exposure to cyberthreats is obviously a concern when dealing with continuous, high capacity, bidirectional train-to-wayside data communications through the ATP- and ATO-functions. The exposure is, nevertheless, not that high taken into concern the appropriate measures implemented to protect the systems. Although, scores for exposure are conservatively set to 'High' for the ATP-system, and 'High' to 'Medium' for the ATO-features. Asset value is here about the assumed 'value' of equipment and consequence costs (injuries, loss of lives) of failures occurring due to cyberattacks. Then, train location/train speed determination and safe train separation is scored 'Very High' as these functions are vital to safe operation of the train. The same argument goes for the ATO, B1 automatic speed regulation. The rest of the features are scored 'Very Low' to 'Medium' and become less critical.

3.3. *Joint quality triage*

Given the scoring of factors in Table 2, the joint quality triage meeting (a 'Table-Top' in this case study) identified the following features where further coordination seems to be needed:

Safety and Availability: Several features of the ATP-system (A1, A2 and A3) scores 'very high' or 'high' on both safety consequence and availability. However, the 'probability of failure' factor affecting on availability is assumed 'Very Low' due to the well proven and reliable systems in railway designs. The possibility of failures implying safety consequences is therefore set to 'Low' for the ATP features. Another aspect is the procedure requirement of manual operation in case of safety related failures that may imply major availability consequences, and safety concerns at a longer run (see section 2.1). Such kinds of dependencies, or possible indirect influences on other qualities from safety concerns on availability are not that easy to catch with the current method. However, this may be elements to discuss in further work with developing the method.

Availability and Security: Security aspects in sense of cyberattacks on ATP and ATO features are highly relevant and scores 'Very High' and 'High' for the asset value and exposure, respectively. If some of these attacks effect on functionality, restoration time might be significant and are scored 'High'. Anyway, considering the fail-safe architecture and well protected ATP- and ATO-systems, the authors assume the safety implications of cyberattacks on the CBTC-system to be minor.

As a result of the joint quality triage, additional meetings are set up to coordinate the mentioned aspects. The product owner knows for which features additional measures are needed in the backlog, and which experts are responsible for suggesting solutions. Just as important, the product owner can proceed with the features where no quality additions are needed.

When the quality experts at a later stage recommend mitigations for the quality issues identified, the scoring in Table 2 can be used to identify quality experts that may need to be consulted to check that the mitigations do not cause further problems, or effects on other qualities. In this case, one example is the mitigations that end up being suggested by the safety and availability experts concerning feature A1 to A3. For these features, the quality triage identified the need for coordination due to possible interdependencies but did not provide any suggestion for which, mitigation that fulfilled those needs. When the experts later suggest solutions, these solutions may need to be checked by availability- and security experts to prevent any new problems, as these qualities have moderate scores for the related feature.

4. Discussion

As explained in the introduction, our goal has been to test the quality triage method on a relevant case from the railway business. The authors liked the idea of moving from quality requirements currently handled largely implicit in design process, to a new practise of understanding and managing quality requirements more explicitly during the project execution phases.

4.1. *Cost*

The quality triage method certainly comes with some costs, mainly involving the work needed to perform the joint quality triages. Quality experts, or member of the project, need to spend time to evaluate user stories/features from the point of view of their quality dimension, and discuss quality concerns with other quality experts. The way to succeed with this approach in railway may be to facilitate quality triage processes in connection with the frequent/regular project meetings.

Although, there is a cost of estimating risk of the features and possible interlinks between qualities, this is a task that strictly speaking should be done in any project. The quality triage method makes this task cost-effective by facilitating quick, traceable evaluations of key areas. The number of experts to involve may vary depending on the projects, and this will of course have impact on costs.

4.2. *Benefit*

Through a description of the CBTC-technology as applied in railway, the authors have demonstrated the potential and usefulness of the quality triage method to quickly identify where effort on quality should be put, and where the different quality dimensions and their responsible parties need to coordinate effort.

Since risks are identified earlier, mitigation actions can be done while the cost of such still is low. Evaluations may be slightly more relaxed for features attaining low risk. Hopefully, the enhanced evaluation of quality risks will increase the final quality of the CBTC-solution as selected and designed. Thus, the need for costly, and time-consuming modifications after the railway system is put in service, to a larger degree, could be avoided.

5. Conclusion

A case study of applying the quality triage method to a railway-project environment has been carried out. As described in the introduction part of the paper, railway projects, as well as projects in other domains, could benefit from improved management of quality concerns like e.g., the security aspects (here cybersecurity) along the way. Cybersecurity as a quality was focused in the paper due to new technology introduced in railway at higher pace, and digitalisation like it implies to the railway sector in general.

As explained, different methods exist for the industry to address any single quality requirements separately during project execution. The most common and recognized are truly the safety- and security assessment methods as they are applied in high-risk industries, critical infrastructures, including the public transportation industries. The quality triage method was here introduced from the software development environment, and it has fascinating features when it comes to its simpleness and intuitiveness, but even though, showed valuable contribution given the present context.

CBTC-technology was selected as the railway sub-system in the current case study. Cybersecurity was focused when analysing this train-controlling and signalling system. CBTC consists of three separate, but interconnected constituents: ATP, ATO and ATS that provide important functionality as well as take care of important safety functions of the train. As being electronical and digitalized components, they are highly exposed to cyber threats. Cyberattacks and related failures to these systems can therefore lead to severe safety and availability consequences.

The results obtained from the joint quality triage showed some interesting aspects of safety and availability interaction concerning the ATP. Then, for interaction between availability and security, security aspects in sense of possibility of cyberattacks on ATP and ATO features were highlighted. Finally, it was mentioned that additional meetings should be set up for the responsible actors to coordinate the mentioned aspects.

The subsequent discussion showed that there are issues related to costs and benefits by applying the method. Even though the authors see clear benefits of applying the quality triage approach to railway project, there are some challenges linked to the method that can be improved. One example is the lacking ability of addressing more hidden dependencies, or possible indirect influences on other qualities. The example mentioned was the safety concerns (or measures, procedures) on availability and/or other qualities.

It was not that easy to catch in these kinds of sprint meetings, which characterise the quality triage method. However, this may be subjects for further work in developing the method.

Another aspect to address in further work would be to test the quality triage method in an actual railway project, considering a more detailed level of user stories/features. Applying the quality triage method on a more detailed level of user stories/features, could turn out to be even more beneficial than the case study in this paper suggests.

Acknowledgement

The work with this paper was funded by an internal research project in SINTEF. The authors also like to acknowledge the opportunity for valuable discussions with rail operators and colleagues at SINTEF Digital.

References

Alsaqaf, W., Daneva, M., Wieringa, R. (2017). Quality requirements in largescale distributed agile projects–a systematic literature review. In: *International Working Conference on Requirements Engineering: Foundation for Software Quality*. pp. 219–234. Springer.

Alsaqaf, W., Daneva, M., Wieringa, R. (2019). Quality requirements challenges in the context of large-scale distributed agile: An empirical study. *Information and software technology*, 110, 39-55.

Amro, A., Kavallieratos, G., Louzis, K. and Thieme, C.A. (2020). Impact of cyber risk on the safety of the MilliAmpere2 Autonomous Passenger Ship. The 3rd International Conference on Maritime Autonomous Surface Ship (ICMASS 2020). *IOP Conf. Series: Materials Science and Engineering 929*, 012018.

Brataas, G., Hanssen, G., Herbst, N., van Hoorn, A. (2020a). Agile Scalability Engineering: The ScrumScale Method. *IEEE Software.*

Brataas, G., Tøndel, I.A., Okstad, E., Løkberg, O., Jaatun, M.G., Hanssen, G.K., Myklebust, T. (2020b). The Quality Triage Method: Quickly Identifying User Stories with Quality Risks. *IEEE software.*

Behutiye, W., Karhapää, P., Lopez, L., Burgués, X., Martínez-Fernández,S., Vollmer, A.M., Rodríguez, P., Franch, X., Oivo, M. (2019). Management of quality requirements in agile and rapid software development: a systematic mapping study. *Information and Software Technology* p. 106225.

Cao, L., Ramesh, B. (2008). Agile requirements engineering practices: An empirical study. *IEEE software* 25(1), 60–67.

CENELEC (2017), EN 50126-1: The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 1: Generic RAMS process.

IEEE Std 1474.1 (2005). Standard for Communications- Based Train Control (CBTC) Performance and Functional Requirements, *IEEE-SA Standards Board*, The Institute of Electrical and Electronics Engineers, Inc.

Okstad, E.H., Bains, R., Myklebust, T., Jaatun, M.G. (2021). Implications of Cyber Security to Safety Approval in Railway. In *Proceedings of the 31th European Safety and Reliability Conference.* ESREL2021, Research Publishing.

Ramesh, B., Cao, L., and Baskerville, R. (2010). Agile requirements engineering practices and challenges: an empirical study. *Information Systems Journal*, vol. 20, no. 5, pp. 449–480.

Sabaliauskaite, G., Adepu, S. and Mathur, A. (2016). A six-step model for safety and security analysis of cyber-physical systems. In *Int. Conference on Critical Information Infrastructures Security*, pages 189–200. Springer.

Tøndel, I.A., Jaatun, M.G., Cruzes, D.S., Moe, N.B. (2017). Risk centric activities in secure software development in public organisations. *International Journal of Secure Software Engineering (IJSSE)* 8(4), 1–30.

Williams, L. Meneely, A., Shipley, G. (2010). Protection poker: The new software security game," *IEEE Security and Privacy*, vol. 8, no. 3, pp. 14–20.