Savunen, Tapio; Kekolahti, Pekka; Mähönen, Petri; Hämmäinen, Heikki; Kilkki, Kalevi

Mobile network operators' business risks in next-generation public safety services

Published in:
Telecommunications Policy

DOI:
10.1016/j.telpol.2024.102733

Published: 01/05/2024

Document Version
Publisher's PDF, also known as Version of record

Telecommunications Policy 48 (2024) 102733

Contents lists available at ScienceDirect

Telecommunications Policy

journal homepage: www.elsevier.com/locate/telpol

Mobile network operators' business risks in next-generation public safety services

Tapio Savunen *, Pekka Kekolahti, Petri Mähönen, Heikki Hämmäinen, Kalevi Kilkki

Aalto University, School of Electrical Engineering, Department of Information and Communications Engineering, Finland

ARTICLE INFO

Keywords:
Mobile network operator
Public safety
Business risk
Risk model
Mobile broadband

ABSTRACT

Field of research: This research falls under the field of mobile broadband 4G/5G networks for public safety communications and focuses specifically on the public safety services business of mobile network operators (MNOs).
Purpose: This research contributes a qualitative model of MNOs' business risks in providing public safety services. The risk assessment covers the business model used in European public safety mobile broadband projects.
Methods and data: A qualitative method was chosen for the research. The risk model used was an influence diagram with the causal taxonomy of risk, which is commonly used for qualitative and quantitative causal models based on Bayesian networks. The Delphi method was employed through the use of an expert panel to create the risk model. The expert panel's risk assessment was conducted using a case study that followed the model of European public safety projects.
Findings: The risk model shows that business risks are, in many ways, a threat to the financial goals of MNOs' public safety business. These risks could result in additional costs, contractual penalties, and lost service revenue. Additionally, there is potential for negative impacts on MNOs' regular business, which can lead to a loss of market share and revenue.
Value: This research provides new insights into MNOs' business risks in next-generation public safety services. Procurement authorities are advised to use the results in the business model and contract planning for public safety procurements. MNOs can gain advantages from these results by enhancing their understanding of the potential business risks, their consequences, and how to control and mitigate them in public safety projects.

1. Introduction

Wireless communications that meet the needs of public safety – police, fire and rescue services, and paramedics – are in the middle of a technological paradigm shift. Traditional public safety wireless communications have been based on narrowband networks, such as Terrestrial Trunked Radio (TETRA), Project 25 (P25), and Tetrapol (Fantacci et al., 2016). Public safety agencies are now gradually moving to standardised 4G/5G mobile broadband technologies. This is enabled by technological advancements and driven by the evolving needs of public safety organisations. Voice-based group communication, often called push-to-talk (PTT), is the main service of

* Corresponding author.
E-mail addresses: tapio.savunen@aalto.fi (T. Savunen), pekka.kekolahti@aalto.fi (P. Kekolahti), petri.mahonen@aalto.fi (P. Mähönen), heikki.hammainen@aalto.fi (H. Hämmäinen), kalevi.kilkki@gmail.com (K. Kilkki).

https://doi.org/10.1016/j.telpol.2024.102733
Received 21 September 2023; Received in revised form 19 December 2023; Accepted 23 February 2024
Available online 24 March 2024

narrowband radio systems, but they cannot meet the new requirements of public safety users, which include, for example, video transfer between field operations and control centres, access to operational databases, and applications providing useful information to first responders, such as maps and floor plans (Peltola & Hämmäinen, 2018; Yarali, 2020).

Public safety mobile broadband services enhance the efficiency of mission-critical field operations and improve the safety of both first responders and citizens. This is of value to society as a whole, as making public safety operations more efficient reduces costs, saves lives and property, reduces injuries, and contributes to crime reduction through preventive measures (Peltola & Martikainen, 2015). Peltola and Hämmäinen (2018) estimated the socioeconomic value of new public safety broadband services in Finland to be 40–94 euros per inhabitant annually. In the United Kingdom, public safety mobile broadband services could improve police productivity by 10% (Grous, 2013). In the European Union, more efficient public safety services in emergencies would represent an annual savings of 5%, or 24 billion euros (Forge et al., 2014).

The 4G/5G technologies that public safety organisations are moving towards are the same technologies that mobile network operators (MNOs) use in their networks. This development presents new business opportunities for MNOs. With certain enhancements – extended coverage and network hardening – MNOs' radio access networks (RANs) can be used to serve public safety agencies. Network hardening entails improving security and resilience, such as making improvements to radio site power supply backups and transmission network resilience. Hardening measures may pertain to technology, processes, competencies, and human resources (Peltola & Hämmäinen, 2018). The quality of service, prioritisation, and pre-emption (QPP) features provided by 4G/5G technologies allows for the services offered to public safety users to be differentiated from the services offered to an MNO's regular customers, which is necessary because they use the same mobile network (Hallahan & Peha, 2013). Another technology available in 5G networks to serve users in the same network with different service quality needs is network slicing. Network slicing covers core, transmission, and radio networks. Prioritising public safety users ensures that they can get proper service even in a congested network (Höyhtyä et al., 2018).

The transition of public safety agencies towards 4G/5G technologies offers an additional opportunity for governments and regulatory authorities: It eliminates the need for government investments in dedicated public safety networks, and regulators do not need to allocate dedicated frequency bands for public safety, since MNO frequency bands can be used (Productivity Commission, 2015; Norwegian Directorate for Civil, 2018).

MNOs have identified the new customer segment that public safety organisations represent. Savunen et al. (2023) analysed the ongoing nationwide public safety mobile broadband projects in which MNOs are involved and that are at least in the implementation phase – Emergency Services Network (ESN) in the United Kingdom, First Responder Network (FirstNet) in the United States, Réseau Radio du Futur (RRF) in France, Safe-Net in the Republic of Korea, and VIRVE 2.0 in Finland. They found that the MNOs' basic source of revenue in public safety projects was enhanced RAN. RAN enhancements also provide added value to MNOs' regular customers. Therefore, these enhancements give MNOs the opportunity to expand their market share, increase revenue, and reduce churn in the mobile communications market. Depending on the business model, other revenue opportunities may also be available in the public safety market, such as application services and device sales.

The ongoing nationwide public safety mobile broadband projects are each based on a contract between one or two MNOs and a public procurement authority (PPA) for the provision of mobile services to public safety agencies. One portion of the contract pertains to either extending and enhancing the existing MNO's RAN or, as in the case of Safe-Net, building a new network. Projects are organised by PPAs (Hankintailmoitukset, 2019; TED, 2019a, 2020). The PPA can be, for example, a government ministry, such as the Home Office[1] in the United Kingdom or the Ministry of the Interior in France; several government ministries, such as the Ministry of the Interior, the Ministry of Oceans, and the Ministry of Land, Infrastructure, and Transportation in the Republic of Korea; an independent government organization, such as the First Responder Network Authority in the United States; or a government-owned public safety operator, such as Erillisverkot in Finland (Savunen et al., 2023). The ranking criteria for offers vary, but price is usually an important factor. The role of a PPA is similar to the role of a government entity in public–private partnerships (PPP). PPAs must be able to channel the requirements of public safety agencies into negotiations as requirements for MNO services, evaluate the price in relation to the services offered, commit public resources to the contract, agree on the transfer of risk from the government to the MNO, and sign the contract on behalf of the government (World Bank, 2017).

Entering a new market exposes MNOs to new business risks. One such source of risk is that public safety organisations are often an unknown customer segment to MNOs, and the MNOs' business goals differ from those of public safety organisations. The goal of MNOs is to maximise revenue and profits, while public safety organisations' priorities lie in protecting life, property, and the state (Yarali, 2020).

Another source of risk is that public safety users have more demanding service needs than regular MNO customers. The availability, reliability, and security of these services must be very high (Yarali, 2020), and RAN enhancements are therefore needed. These are known as mission-critical (MC) requirements. A challenging combination for the profitability of the business includes demanding user requirements with significant investments and a relatively small customer segment (Savunen et al., 2023).

A third source of business risk is the contractual and regulatory framework between private and public parties in telecommunications projects. The public party can use its regulatory power to change the regulation in its favour after the contract is signed. This can endanger the operator's service revenue (Howell & Sadowski, 2018). The projects targeting next-generation nationwide public safety services are based on public procurements organised PPAs, who often also participate in organising public safety services alongside MNOs and may therefore have two different roles (Savunen et al., 2023). In addition, the improper allocation of financing

[1] 'The Home Office is the lead government department for immigration and passports, drugs policy, crime, fire, counter-terrorism and police (Home Office, 2021).'

and demand risk to the parties can be a source of operational unsustainability (Díaz, 2022).

If there are several actors in the project, MNOs should also pay attention to the organisation of the project. In such a project, it is essential that one actor has the role of system integrator to ensure end-to-end functionality. The length of the contract period also deserves MNOs' attention, as a long PPP contract is expected to support investments and foster innovations (Savunen et al., 2023).

The materialisation of risks based on these or other business risk sources would endanger the profitability of MNOs' public safety business. Therefore, if an MNO intends to enter the public safety market, these risks must be carefully managed. An appropriate risk-management method enables companies to take greater risks in their strategies, and it is a competitive advantage over competitors with less effective methods (Kaplan & Mikes, 2012).

The contribution of this research is a qualitative model of MNOs' business risks in the public safety service market. The business model of European public safety mobile broadband projects was chosen for the risk assessment. In these projects, MNOs' RANs are shared with public safety users. Other actors are responsible for other areas, such as MC applications and user devices. The goal of all European projects is to replace the existing technology by migrating from nationwide narrowband systems to broadband communications (Savunen et al., 2023).

The qualitative risk model follows the causal risk taxonomy proposed by Fenton and Neil (2018) for Bayesian networks; the taxonomy categories are risk triggers, risk events, risk controls, consequences, and mitigants.

The following are the research questions.

- What are MNOs' business risks in national public safety mobile broadband projects following the European business model and what are the underlying reasons for these risks?
- What are the potential consequences of these risks if they materialise?
- How can these risks be controlled and mitigated?

The paper has several targets: 1) introduce a risk model outlining MNOs' business risks in public safety mobile broadband projects involving MNOs and PPAs, 2) provide a practical tool for procurement processes for both MNOs and PPAs, 3) improve the understanding and visibility of MNOs' potential business risks in public safety projects and encourage open dialogue between PPAs and MNOs during the bid process and contract negotiations, and 4) address the current research gap in this area, as there has been limited research on public safety mobile broadband projects from the perspective of the MNOs' business interests.

The paper is organized as follows: Section 2 describes the research methods and data; Section 3 presents the case study used in the risk assessment; Section 4 presents the results of the research, the qualitative risk model, and its sub-models; Section 5 discusses these findings and their implications; and Section 6 provides a conclusion.

2. Research methods

2.1. Qualitative research

Out of the five nationwide public safety mobile broadband projects involving MNOs, only two have progressed to the production stage and currently serve the public safety sector (Savunen et al., 2023). As a result, the sources of quantitative data are limited. Furthermore, due to the emergent stage of research on the MNOs' business interests in public safety services, there is no existing theoretical framework. These were the primary motivations for choosing a qualitative research model.

The data collection and analysis process is described in Sections 2.3 and 2.4, and the method of presenting the results – the risk model – is described in Section 2.2.

2.2. Influence diagram using causal risk taxonomy

Methodologically, the qualitative risk model of this research is an influence diagram, a directed acyclic graph (DAG) consisting of nodes and arcs. Nodes are connected to one another by directed arcs, where an arc from one node to another indicates a causal relationship between them. Influence diagrams can be used in decision analysis to illustrate probabilistic dependencies (Howard & Matheson, 2005). In DAGs, the absence of cycles prevents the presence of circular decision-making pathways (Fenton & Neil, 2018).

The risk model incorporates the causal taxonomy of risk, a method proposed by Fenton and Neil (2018) for Bayesian networks. In

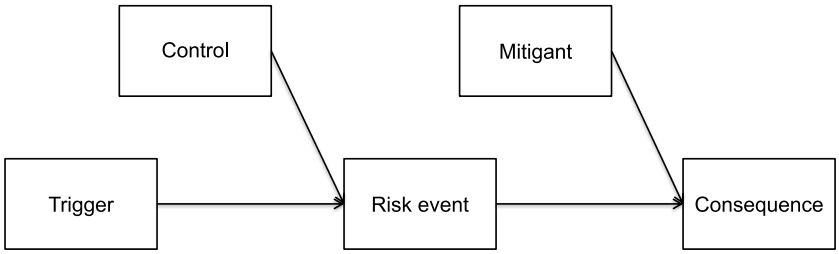


Fig. 1. Causal taxonomy of risk (Fenton & Neil, 2018).

the causal taxonomy of risk, nodes belong to five different categories: 1) risk triggers, 2) risk events, 3) risk controls, 4) consequences, and 5) mitigants. An assumption is that the causal relationship between nodes is probabilistic. In addition to these five categories, a node totalling the values of the consequence nodes was added.

Fig. 1 depicts the relationships between the different categories of nodes. Risk triggers are sources of risk events; in other words, they initiate risks. A risk event is a risk in itself and a consequence of risk triggers. With the help of risk control, the materialisation of a risk event can be prevented, in whole or in part. The consequence characterises the negative impact of a risk event if it fully or partially materialises; however, the final consequence can still be reduced by mitigants (Fenton & Neil, 2018). Additional information on Bayesian network modelling can be found in e.g., Kekolahti (2019).

Fenton and Neil's (2018) causal taxonomy was applied to Peltola and Kekolahti's (2015) research on public safety service risks in wireless networks, the focus of which was TETRA and MNO networks. According to the research, the most effective ways to control availability risks are the duplication of radio site transmission links, power supply backup, and real-time mobile traffic monitoring.

2.3. Expert panel and delphi model

An expert panel was the source of the data for this study. The task of this group of experts was to identify MNOs' potential business risks in public safety mobile broadband services and prioritise them. The expert panel also approved the risk model.

The Delphi method was chosen for working with experts. The Delphi method was originally devised by the RAND Corporation to support expert group work and consensus building through structured communication and feedback (Dalkey & Helmer, 1963). In the Delphi method, each expert has an equal opportunity to express their opinion, and everyone is then given feedback on the group's common view. Individual contributions are anonymous to support the free expression of opinions, and the experts can change their opinions during the process, which supports reaching a consensus (Linstone & Turoff, 1975). Structured interactions using questionnaires also support the experts' independent and gradual opinion formation. Further, direct confrontations, which can produce closed opinions and reject new ideas, can be avoided (Dalkey & Helmer, 1963).

Careful selection of experts is essential when using the Delphi method. One of the most critical requirements for experts is a deep understanding of the research area (Okoli & Pawlowski, 2004), but it is additionally imperative to ensure adequate diversity in the experts' backgrounds and areas of expertise, so as to include a sufficient variety of perspectives.

The expert panel consisted of 12 experts in eight groups. One group had four experts, one had two experts, and the other six groups had one expert each. Each group was treated as a collective unit and made its own contribution, all of which were treated as equal. The experts were from three different European countries, each of which had a public safety mobile broadband project in either the implementation or planning phases. The backgrounds of the eight expert groups were as follows: academia – 1; public administration – 2; consulting – 2; industry – 1; and operator – 2. According to Hallowell and Gambatese (2010), eight is a sufficient number of experts for an expert panel using the Delphi method.

Table 1 lists the key competence areas that were estimated to be the most significant in this research's business risk assessment. The distribution of the competences of the expert panel is also presented, which was based on the experts' self-assessments. The expert panel's average knowledge of cybersecurity was lower than that of other areas, and no one on the panel had expert-level cybersecurity knowledge (Rating 3). This limitation represents an opportunity for future research.

2.4. Data collection and analysis

The process for collecting and analysing data and creating a risk model in collaboration with an expert panel was created by applying the Delphi process proposed for 'ranking-type' surveys. This was described by Schmidt et al. (2001) in their research identifying risks in software projects. The described process includes three phases: 1) brainstorming for important factors, 2) narrowing down the list of factors, and 3) ranking the list.

Fig. 2 illustrates the steps of the process used in this research, consisting of three expert panel assignments. Each assignment included 1) introduction of the assignment with the necessary materials and templates, 2) independent work by the experts (or expert groups), 3) analysis of the experts' contributions, and 4) feedback on the panel's contributions. The feedback was presented in a way that preserved the anonymity of the experts' answers.

All expert meetings to introduce assignments were arranged online. This was done to ensure that all of the experts had the same information needed for each assignment. Following the model suggested by Kekolahti (2011), materials and templates, as well as the experts' contributions, were exchanged by email, which guaranteed that the answers could be given anonymously, and spreadsheet

Table 1
Distribution of competences on the expert panel.

Competence area	Average	Minimum	Maximum
Telecommunications	2.8	1	3
Critical communications, including public safety	2.6	2	3
Cybersecurity	1.4	1	2
MNO business	2.3	1	3
Business development	2.0	1	3

Rating: 0 = No knowledge; 1 = Basic knowledge; 2 = Good knowledge; 3 = Expert-level knowledge.

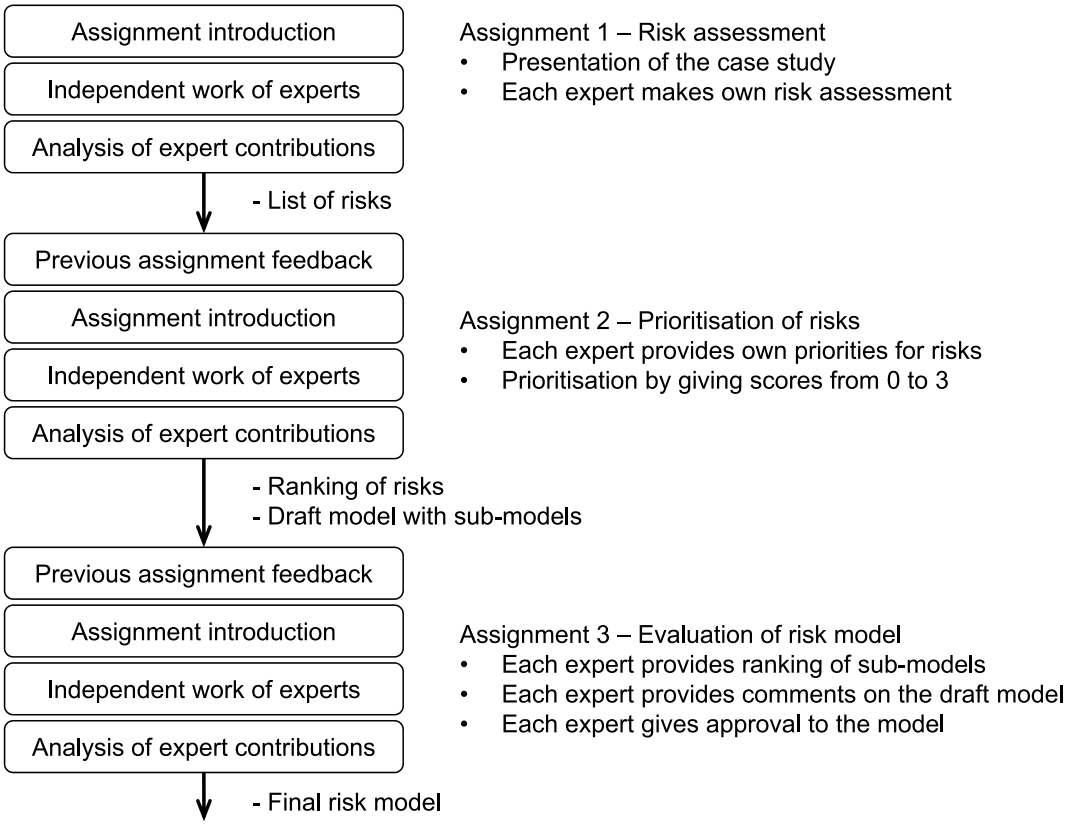


Fig. 2. Data collection and analysis and the creation of a risk model.

templates were used for structured expert contributions (see Appendix 1). There were also open-ended questions, to which the experts responded by email.

The first assignment was the risk assessment of a case study (see Section 3), and the experts were asked to provide the most significant business risks on a spreadsheet template. The template followed a given structure based on the causal taxonomy of risk (see Appendix 1; Fenton & Neil, 2018). The purpose of the detailed case study was to provide the experts with an equal starting point for the assessment of MNOs' business risks. The first assignment resulted in 112 different risks, some of which were similar enough to be combined, resulting in 106 risks.

The second assignment was to identify the most relevant business risks and prioritise them. The experts (or groups) were asked to give each risk a score between 0 and 3, with 0 being the least relevant and 3 being the most relevant. The experts were advised to consider the following factors when assessing risk relevance and scoring:1) Whether the consequence of the risk has monetary value (i.e., it has a financial impact on the MNO's business); 2) The probability and effect of each risk, where the total impact of the risk is the probability of the risk event multiplied by the value of the risk consequence; and 3) Whether the causal relationship between different risk elements is clear (e.g., risk triggers cause risk events and risk events can be managed with the help of risk controls; see Fig. 1).

The results of the second assignment were the basis for the ranking of risks using the average score received by each risk. The highest average score was 2.31, the lowest was 0.50, and the median was 1.42. The 22 risks with the highest average scores were selected to create risk sub-models; many of these were different variations of the same risk, which were combined, resulting in seven sub-models. The second assignment feedback to the experts included a list of risks with their average scores and an influence diagram presentation of each sub-model. A complete risk model comprised of a combination of the sub-models was also presented.

The third and final assignment was the evaluation and prioritisation of the sub-models. Experts were asked to define the most significant and the least significant sub-models with regard to MNOs' risks in the public safety business. Experts' approval and comments were also requested for the risk model. In the risk model and sub-models presented in Section 4, the experts' comments were taken into account, and the sub-models were organised according to the experts' prioritisation.

3. Case study

3.1. Business model

The objective of this research was to assess MNOs' business risks in a typical nationwide public safety mobile broadband project

and to build a corresponding risk model. To facilitate the expert panel's ability to contribute to the risk model, a case study was created describing the context in which MNOs' business risks were assessed. The case study contains descriptions of the MNO and the public safety mobile broadband project.

A key feature of the case study is the project's business model. The business model here refers to the setup of the project, including the project actors and their responsibilities. Naturally, from an MNO's point of view, the key questions are related to the MNO's own role and responsibilities.

The business model of the ongoing MNO-involved nationwide public safety mobile broadband projects can be defined using two dimensions, each with a two-value attribute. The first dimension categorises projects according to the number of actors responsible for delivering public safety services: a single-actor model or a multi-actor model. The second dimension categorises the projects based on the type of primary RAN: In a dedicated network, only public safety users use the network, and in a shared network, it is also used by the MNO's regular customers. Using these dimensions and their respective values, business models can be divided into four quadrants (Savunen et al., 2023).

The multi-actor shared-network model was chosen for the case study. All European projects – ESN, RRF, and Virve 2.0 – follow this model. The role of the MNO in these projects is to deliver shared MC RAN services and, potentially, some core network services (Savunen et al., 2023). As it is currently the only model used in Europe, there will likely be more projects based on this model in the future.

3.2. Project

The case study description follows the principles of the European nationwide public safety mobile broadband projects using a combination of the features of these projects (for a review of the ongoing projects, see Savunen et al., 2023). The stated goal of the project was to provide next-generation public safety mobile broadband services to public safety authorities. The project was assumed to be based on a public bid organised by a PPA.

The project was divided into two parts: MC RAN services provided by an MNO and public safety services and devices provided by a service operator. For end-to-end public safety services, both the services of the MNO and the service operator are required.

Fig. 3 illustrates the division of the responsibilities in the case study project between the MNO and the service operator according to the chosen multi-actor shared-network business model. The MNO is responsible for providing MC RAN services to public safety users. The coverage of the MNO's RAN must be extended, and the network's resilience and security must be hardened to meet the requirements of public safety users (Peltola & Hämmäinen, 2018). Since the MNO's network is shared among different users with different service needs, the QPP features of 4G/5G technologies are necessary (Hallahan & Peha, 2013; Höyhtyä et al., 2018).

The service operator is responsible for the services of the dedicated MC core network, MC services (MCS), including MCPTT, MCVideo, and MCData (Lair & Mayer, 2017), devices and accessories, customer operations and services, and sales and marketing. The service operator therefore controls the customer interface for public safety users, including 24/7 support centres.

Fig. 4 illustrates the phases of the project from the MNO's point of view. The terminology follows that used by PPPs. The design of the network should already be explored during the bid process to better estimate the MNO's project costs, which are required for the MNO's bid. If the MNO is awarded the contract, the design process continues, followed by network building. Once the network building is complete and the RAN is ready for service, the operation and maintenance phases follow (World Bank, 2017). In the case study, the contract period for the project was 10 years, which was divided into two phases. The first phase, design and building, takes three years. The second phase, operation and maintenance, takes seven years.

The pricing model is fixed, with payment milestones for network building and maintenance. In practice, the MNO is paid for building and maintaining a RAN that meets public safety needs. RAN 3GPP technology upgrades are included in the network building and maintenance price. The pricing model for RAN services is subscriber-based and therefore dependent on the number of users.

The contract guarantees the MNO's exclusive right to provide public safety services. This means that during the contract period, only one MNO provides MC and classified RAN services to public safety authorities. However, not all public safety users will necessarily subscribe to the RAN services of the selected MNO. For example, if some user organisations consider the quality of the service insufficient, they may decide to postpone the use of the service. Alternatively, if they consider the price of the service too high, they can reduce the number of users from the original estimate and continue to use, for example, standard 4G/5G services for less critical users.

The MNO has the right to use the extended radio coverage for its regular customers. The service level of public safety services is defined in a service-level agreement (SLA), which sets penalties for unsatisfactory services.

3.3. MNO

The MNO defined in the case study description is not an existing MNO; similar to the project description, it follows the pattern of MNOs participating in ongoing public safety mobile broadband projects.

The RAN services requested in the project would be based on the MNO's existing LTE network. The LTE network cannot be used as such, and network coverage extensions and hardening are required. Additionally, in the MNO network, public safety users must be given priority over consumers and enterprise users to ensure good service quality, even in congested networks.

The direct business opportunities for the MNO are the project's revenue and profits. The number of new subscribers is relatively small compared to MNO's subscriber base. In the current national projects, the share of public safety users in relation to the total number of mobile phone users in the country varies between 0.4% and 0.8% (Savunen et al., 2023).

The project is strategic for the MNO due to indirect business opportunities based on improved network coverage and service

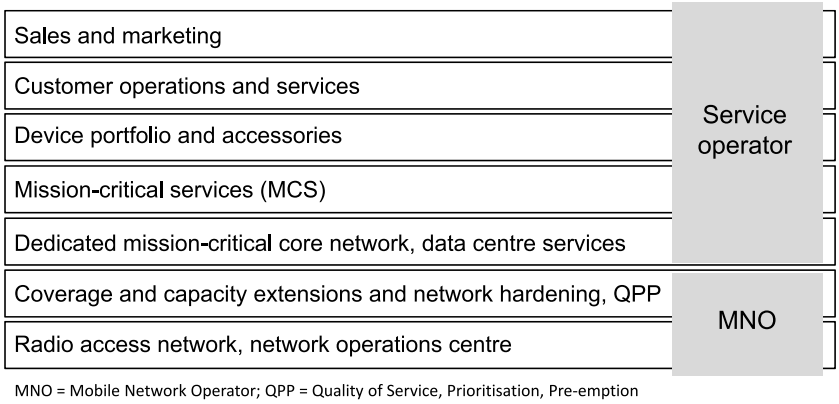


Fig. 3. Share of responsibilities for the case study.

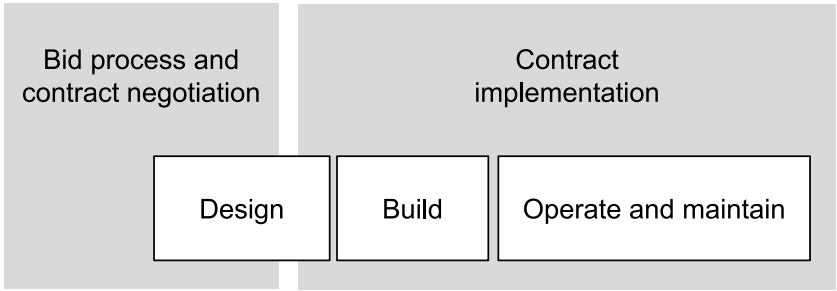


Fig. 4. Project phases of the case study, following PPP terminology (World Bank, 2017).

availability, which would be an advantage for the operator's other customer segments. The MNO would be able to increase its market share, reduce the churn rate, and potentially increase its average revenue per user (ARPU). For example, AT&T has reported that the enhanced network quality resulting from FirstNet's improvements has had a positive impact on its market share and customer churn within the mobile service market (Reardon, 2020). A network with better coverage and service quality than its competitors would also be a good basis for other new vertical businesses, such as the energy network communication market, fuelled by the growth of renewable electricity generation (Leligou et al., 2018).

Because the demanding coverage requirements of public safety necessitate a considerable number of new radio sites, the network building cost comprises a major portion of the total cost. The hardening of the transmission lines and backup power supply of radio sites also affect the network building cost when the goal is to meet the needs of public safety (Peltola & Hämmäinen, 2018).

The project's pricing model is a fixed price for network building and maintenance and a subscriber-based price for RAN services, allowing the MNO to set separate prices for these elements. Because the project is strategic for the MNO, it has decided to set a lower gross margin target for network building and maintenance than for RAN services, allowing the MNO to lower the total price. As price is one of the most important criteria when choosing an offer, the price set by the MNO has a significant impact on the competitiveness of its bid.

4. Risk model

4.1. Sub-models

Each of the risk model's sub-models represents its own risk domain and is an independent and complete entity. The key element of

Table 2
Sub-models of the risk model.

Sub-model	Risk domain
Contract	Unprofitable business due to the contract between MNO and PPA
RAN service does not meet needs	Poor service due to insufficient RAN operation
Cybersecurity	Cybersecurity risks cause unsatisfactory service and data breach
End-to-end solution not ready	Lost service revenue due to delayed end-to-end solution
RAN building not on time or not on budget	Network building causes losses and additional cost
Poor service to other customers	Poor service impacting other business segments
Physical attack	Physical attacks on infrastructure cause service breaks
Financial risk value	Cumulative financial business risk value of the model

each sub-model is one or two risk events that define the sub-model's risk domain. Other elements – risk triggers, controls, consequences, and mitigants – complement the sub-model and are aligned with risk events.

There are seven sub-models that each represent their own risk domain and a cumulative sub-model that sums up their combined financial risk. The sub-models are shown in Table 2, listed in the order of importance, as ranked by the expert panel.

The risk model is not exhaustive; the experts also found other risks, as described in Section 2.4. When building a model, one of the key questions is the complexity of the model; specifically, consideration must be given to the number of variables and the number of connections between them. Every effort was made in this study to include the most important risks in the model while retaining a level of detail that would enable the reader to readily adopt it and practitioners to easily apply it in practical projects. It should also be noted that risks and their prioritisation depend on practical projects and the terms of the contract.

4.2. Contract

The public safety business is a new venture for MNOs. The customer segment and its requirements differ from those of consumers and enterprises, which are MNOs' regular customers. In addition, the contract periods – 10 years in the case study – are usually relatively long. This could pose challenges in the flexibility of the contract, should there be any changes during the contract period.

The risk event in this sub-model is an unprofitable business caused by an inflexible contract and triggered by negative changes in the business environment. In the case study, the price model of the MNO's contract with the PPA was subscription based for services. The MNO estimated subscription-based revenue with certain assumptions about the ARPU and the number of subscribers. Either of these factors being lower than expected would trigger this risk, and the impact would be lost service revenue (Fig. 5); the two corresponding triggers are decreasing ARPU and a reduced number of users.

The third risk trigger is unfavourable political or regulatory changes that could challenge the business model, such as the MNO's exclusive right to public safety services. The PPA has legislative power that it can use to change regulations in its favour after the contract is signed, especially in the case of long contracts (Howell & Sadowski, 2018). The PPA can also be involved in organising public safety services, and can thus have two different roles (Savunen et al., 2023).

This sub-model has four controls, all of which are related to the contract. By defining the minimum level of ARPU and the minimum number of users in the contract, two potential reasons for unprofitability can be managed. The third control is a flexible contract that supports changes and negotiations during the contract period.[2] The fourth control is a different pricing model for services. In negotiations, the MNO can propose changing the contract from a subscription-based contract to a fixed-price contract.

Lost service revenue and additional service costs are the consequences of the materialised risk event. The mitigant for this event is contract renegotiation. A flexible contract supports renegotiations better than the more rigid structure of a transactional contract; therefore, there is a relationship between flexible contract control and the contract renegotiation mitigant.

4.3. RAN service does not meet needs

Public safety users have rigorous requirements for RAN services. They must be available everywhere and at all times, with high security and without any service breaks. It is challenging for an MNO to provide demanding public safety services on a mobile network originally designed for consumers and enterprise users with lower service-level requirements. The different levels of services need to be properly managed.

The risk event in this sub-model is poor service for public safety customers, such as holes in network coverage or service breaks.

This risk event has three triggers (see Fig. 6). The first is incorrect QPP operations. This refers to the service-level management functions of 4G/5G networks, which make it possible to differentiate the quality of service in the same network for different customers. Public safety users must be given higher priority than other users, which ensures appropriate services for these users, even in a congested network (Höyhtyä et al., 2018). If the QPP functions do not work properly – due to incorrect configuration, for example – poor service may result.

Another trigger is major power outages. Natural disasters, such as storms, wildfires, and floods, can cut power lines over a wide area and interrupt the power supply for several days. If radio sites are not equipped with batteries or other backup power sources, the communication service may be interrupted. For example, large storms caused long power outages in Finland in 2010, resulting at its worst point in 1050 out-of-order mobile network radio sites (Onnettomuustutkintakeskus, 2010).

The third trigger is poor coverage. Even with careful network design and building before the network operation (see Fig. 4), the radio network may still have blind spots, such as those that can result from large changes in elevation.

This sub-model has three risk controls. Two of these controls aim to ensure that the MNO's responsibilities for RAN services are clearly defined. In other words, in the case of service deviations, the MNO is not responsible for deviations outside of its commitments. The first control is an SLA with exact requirements to ensure that the contract clearly defines the level of service for which the MNO is responsible. The second control is complete acceptance testing of the RAN service after the network building. This is to obtain formal customer acceptance for the RAN building and ensure that it meets the requirements, including coverage extension and network hardening.

The third control is the implementation of thorough service testing and monitoring to ensure that services are functioning properly.

[2] One example of a flexible contract model is a relational contract, which is based on partnerships and mutual trust between the parties and supports negotiations throughout the contract period (Macaulay, 1963; Macneil, 1985).

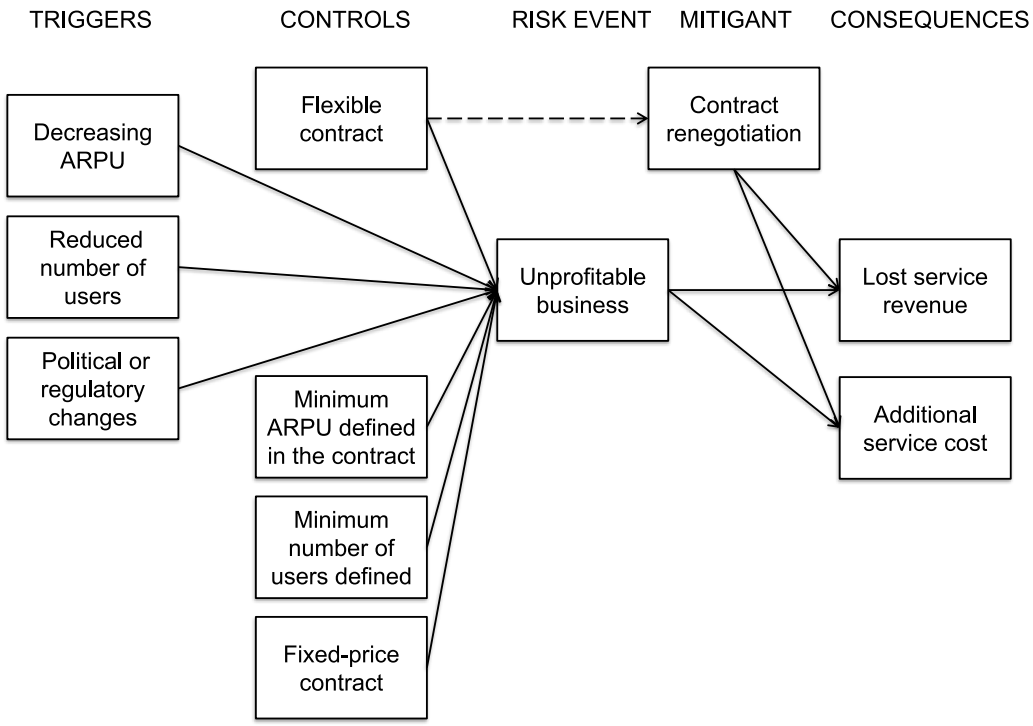


Fig. 5. Contract sub-model.

Potential service deviations must also be identified as soon as possible. By reacting quickly to service deviations, negative customer effects can be minimised.

The consequences of poor service are lost service revenue and service penalties when services do not meet the SLA. Correcting network deficiencies, such as poor coverage and insufficient backup power supply, induces additional RAN maintenance costs.

The mitigants of the risk are partly to improve service resilience to network problems and partly to correct the identified network deficiencies to avoid future service deviations. National roaming with other MNOs enables radio access through another network if the MNO's network is unable to provide services (Weedage et al., 2023). Tactical bubbles are deployable networks that provide temporary local coverage in the event of network service outages (Suomalainen et al., 2021). The other two mitigants, QPP operation tuning and improving network coverage and hardening, serve to correct the identified deficiencies of the network. One concrete example of hardening the network is equipping radio sites with longer-lasting backup power sources, such as diesel generators or fuel cells.

4.4. Cybersecurity

Cybersecurity threats pose a risk to public safety communications due to the authorities' strict information security requirements. Information in public safety communications must, without exception, be kept confidential, and data breaches are impermissible. Cybersecurity risks may also cause service deviations due to network intrusion (Suomalainen et al., 2021).

The risk event in this sub-model is unsatisfactory service and data breaches. The risk event has three triggers (see Fig. 7). The first trigger is a cyberattack motivated by public safety business. Because public safety activities contain sensitive information, public safety communications are an attractive target for cyberattacks. Data breaches related to public safety would also attract high-profile media coverage, and some attackers may target public safety communications seeking publicity.

Another trigger is network vulnerabilities that could enable successful cyberattacks. For example, the RAN is used by both the MNO's regular customers and public safety users, which could provide an attack surface for cyberattacks. Conversely, a core network is dedicated to public safety users (Section 3.2).

The third trigger is unethical behaviour, especially by MNO personnel, who could cause or contribute to cyberattacks and data breaches inside the organisation.

This sub-model has three controls. The first is cyber-resilience, which meets the needs of public safety. This challenges the MNO to assess its cyber-resilience capabilities as they pertain to public safety requirements – technologies, processes, and competencies – and to make any necessary investments and conduct appropriate development activities.

The second control is the appropriate screening of the MNO's public safety operations personnel. The MNO must define certain

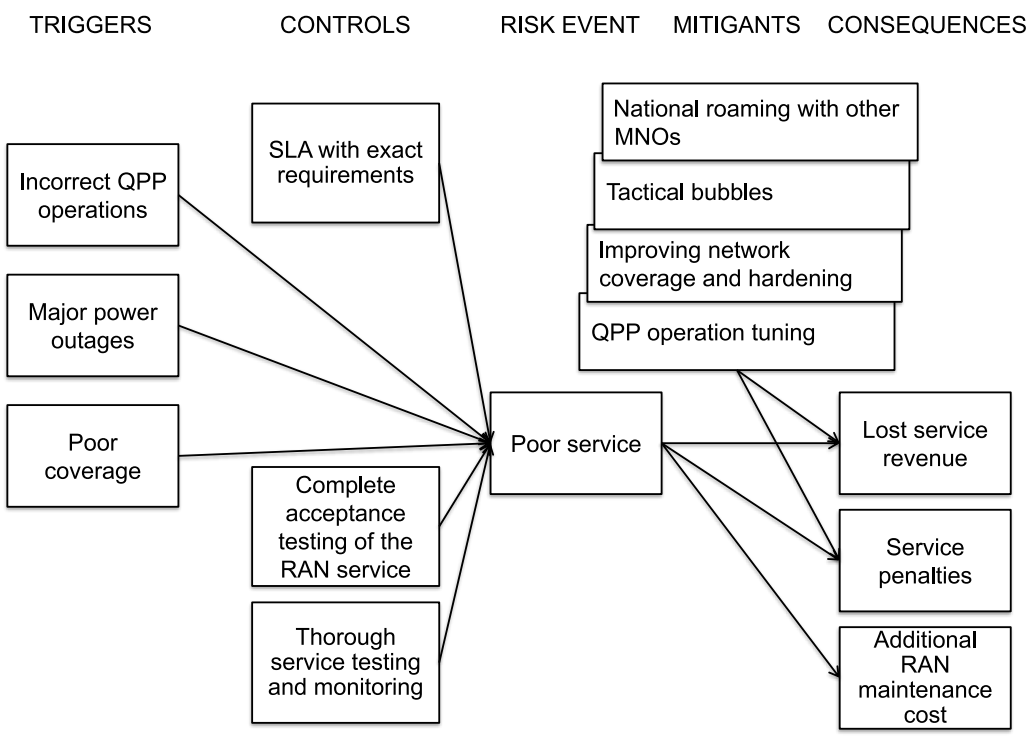


Fig. 6. RAN service does not meet needs sub-model.

requirements to be considered for and accepted in public safety service positions. This may also require the recruitment of new employees.

The third control is the MNO's compliance management, which meets the needs of public safety. This refers to the MNO's compliance management system and practices, including policies, employee training, monitoring, and other procedures. Senior management communication supporting key compliance practices is an integral part of compliance management.

The consequences of unsatisfactory services and data breaches are lost service revenue, service penalties, and an impact on other business segments.

This risk can be mitigated by improving cyber-resilience capabilities and through national roaming arrangements with other MNO operators. These measures serve to correct identified deviations and improve service resilience, which helps in managing longer service breaks caused by the risk.

4.5. End-to-end solution not ready

End-to-end functionality is essential for public safety users. This includes devices with accessories, MCS applications, RAN services, the core network, communications with command and control rooms, and user provisioning. A service consisting of all of these elements must always be available, cyber-resilient, and easy to use (Suomalainen et al., 2021; Yarali, 2020).

According to the multi-actor shared-network business model, the MNO is responsible for RAN services only. However, RAN services cannot be used without the integration of all the other elements. This creates the risk that the introduction of the MNO's services will be delayed.

The risk event in this sub-model is a delay in the end-to-end solution. There are five triggers (see Fig. 8). The first is that MCS applications do not meet user needs. Generally, users migrate from a narrowband solution, such as TETRA, Tetrapol, or P25, to services based on 4G/5G technologies. A smooth transition phase without major changes in public safety field operations, such as police and paramedic services, is a mandatory requirement. This requires new services to be similar to existing narrowband services. If new services provided by the MCS application do not meet the needs of end users, this may cause delays in service introduction.

Another trigger is the land mobile radio (LMR)/MCS gateway not being ready. The LMR/MCS gateway is a functionality needed for migration from a narrowband solution to a new broadband-based solution. Migration can take years, and during migration, group communications must be able to take place across both systems. When some users are using a narrowband solution and others are using a broadband solution, these users must still be able to communicate with one another. Without a properly functioning gateway, service migration cannot begin.

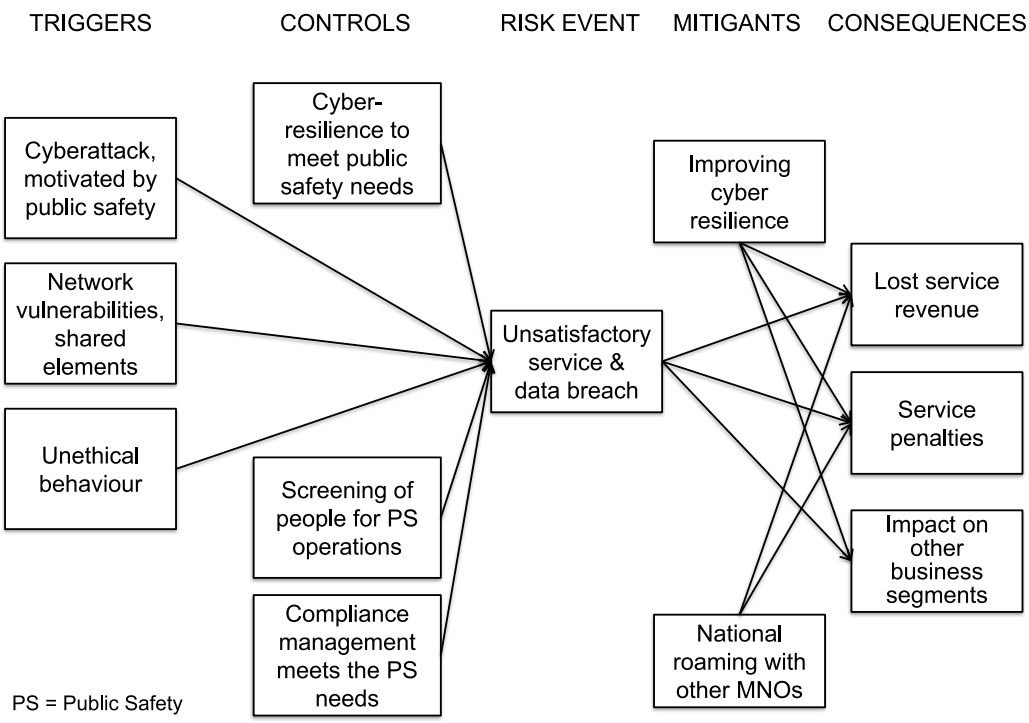


Fig. 7. Cybersecurity sub-model.

The third trigger is devices that do not meet user needs. Public safety operations require special user devices. In general, they must be capable of withstanding water, shocks, and drops; they must also be useable with gloves, and their form factor is larger than that of consumer phones. Another important requirement is direct device-to-device communication without RAN support. The crucial nature of this service can be seen in its use by fire and rescue operations inside buildings without network coverage, for instance (Fodor et al., 2014).

The fourth trigger is control room integration not being ready. Public safety communications systems must be integrated into control room solutions. In the current solutions, the control room interfaces are vendor-specific because they have not been standardised. Large nationwide networks can have dozens or even hundreds of different control rooms that need to be integrated into the communications system. They must also work with both the old and new solutions during migration. The integration of control rooms is usually a prerequisite for service introduction, and thus for the MNO's RAN services (National Audit Office, 2019).

The fifth and final trigger is no user engagement. User organisations, such as police and fire and rescue services, make the final decision on migration to new services from existing narrowband networks. For this, they must trust that the new services will fully support their operations.

This sub-model has one control: the delay compensation defined in the contract. The aim is to include in the contract the compensation to be paid to the MNO if the end-to-end solution is not ready on time and the MNO is not responsible for the delay. Ideally, the MNO would receive compensation comparable to the lost revenue due to the delay.

The consequence of this risk is lost service revenue, and the mitigant is the contract renegotiation. If full compensation is defined in the contract, no mitigant is required. There may also be a combination of both a control and a mitigant. For example, the contract specifies that if the end-to-end solution is delayed, the MNO is entitled to compensation, which will be negotiated when it occurs.

4.6. RAN building not on time or not on budget

RAN coverage extensions and network hardening are the technical basis for meeting public safety customers' availability and security requirements. These also require significant investments by the MNO (Savunen et al., 2023). As coverage extension and network hardening are also significant sources of the MNO's revenue in the project, there are risks associated with significant costs and revenues. In addition, a delay in RAN building would also delay the start of the RAN service.

Possible deviations in the RAN building are divided into two risk events (see Fig. 9), both related to the network design work included in the MNO's bid preparation (see Fig. 4). The purpose of the bid preparation is to estimate the costs of building the RAN for the MNO's bid. Underestimated costs in the bidding phase would endanger the profitability of the project.

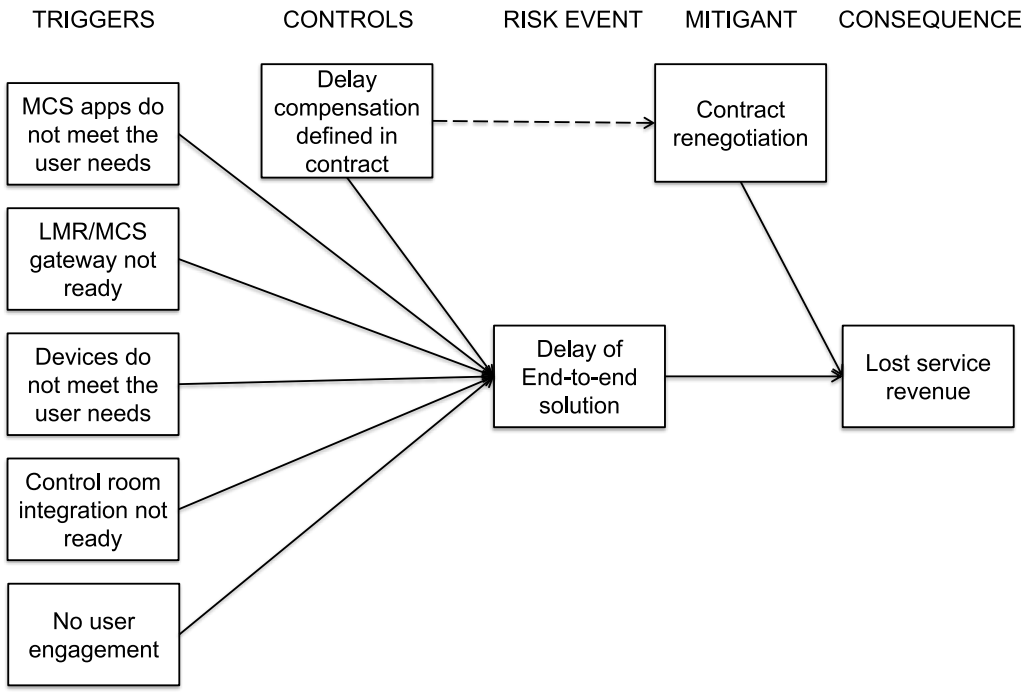


Fig. 8. End-to-end solution not ready sub-model.

The first risk in this sub-model is that the extension of the radio coverage area is not on time or not on budget because more radio sites are needed than expected. The other risk is that the hardening of the network is not on time or not on budget because the implementation of the duplicated links is more difficult than expected. This is related to the duplication of transmission connections between radio and core sites. The controls for these risks are a conservative coverage and hardening design related to cost estimates in the MNO's bid preparation. The MNO must not underestimate them, as can happen when trying to improve the competitiveness of the bid.

The consequences of both risk events are additional RAN building costs, lost service revenue, and RAN-building penalties due to the delayed start of RAN services. The mitigant is national roaming with other MNOs. In the case of delayed RAN building, the resilience provided by multiple RAN networks would reduce the service deviations caused by unfinished network extensions and network hardening.

4.7. Poor service to other customers

The public safety customer segment is only a small fraction of MNOs' regular customer segments (Savunen et al., 2023). If public safety services have a negative impact on service for the MNO's regular customers, the latter may switch to competitors, leading to a reduction in the MNO's market share. The negative financial impact can be significant, perhaps even surpassing what could be offset by the public safety business. This would also have a negative impact on the MNO's reputation, and customers may lose faith that the MNO is able to provide high-quality service.

The risk event in this sub-model is poor service to other customers, and it has two triggers (see Fig. 10). The first trigger is incorrect QPP operations. This is also a trigger for poor service to public safety customers. When QPP operations are used to differentiate the quality of service for different customers on the same network, incorrect operations can cause service-level deviations for different customer segments, including consumers and enterprises.

The other trigger for this event is a high need for local capacity. A large public safety operation may require a lot of mobile communication capacity in a small area. This can lead to a lack of network capacity and poor service to lower-priority users, namely consumers and enterprises. In the worst-case scenario, these lower-priority users would be disconnected.

This sub-model has three controls. The first is QPP operation testing. Taking measures to ensure that QPP functions work properly can prevent unnecessary limitations in network capacity for the MNO's regular customers.

The second control is thorough service testing and monitoring, which is also a control for poor service to public safety customers. Here again, the goal is to minimise service deviations through proper testing and detect such deviations as soon as possible through

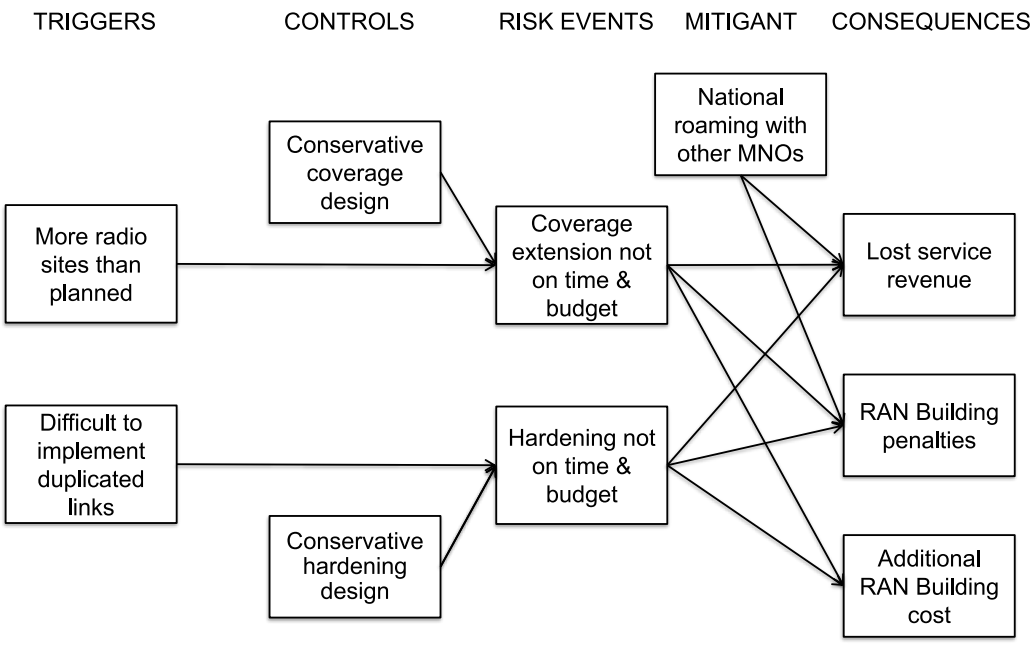


Fig. 9. RAN building not on time or not on budget sub-model.

service monitoring.

The third control is a capacity quota for other customers. This ensures that while the capacity required for public safety operations may be high, the entire capacity is not exclusively allocated to them. Instead, a portion of the capacity remains available for the MNO's regular customers.

The consequence of this risk is its impact on other business segments. In the worst-case scenario, this would mean a decrease in the MNO's market share in the consumer or enterprise segment, perhaps even both, if existing customers switch to competitors due to poor service.

The mitigants of this risk are QPP operation tuning and additional capacity. There is a relationship between the QPP testing control and the QPP tuning mitigant, where the mitigant serves to correct any malfunctions in QPP operations. Additional capacity is needed if the network is constantly congested in certain areas. Of course, this is also a question of the available spectrum, meaning whether the MNO has unused frequency bands available.

4.8. Physical attack

Attacks on physical infrastructure can damage the MNO's network centres and cause major disruptions to the operator's services. Attacks may not necessarily be targeted at the MNO's infrastructure, but they can still have significant effects; for example, physical attacks can affect the power supply of network centres and thus cause service breaks.

The risk event in this sub-model is a service break caused by a physical attack on the infrastructure (see Fig. 11). The risk controls are geo-redundant infrastructure and physical security that meets the needs of public safety. Geo-redundant infrastructure refers to duplicated network centres located in different geographical locations that back up one another in the event of a service outage. Physical security that meets the needs of public safety is intended to prevent potential attacks. For MNOs, this can mean additional investments.

This sub-model has four consequences. Three related consequences are lost service revenue, service penalties, and the impact on other business segments. Unsatisfactory services for consumers and enterprises could result in these customer segments switching to competitors. The fourth consequence is additional RAN maintenance costs related to correcting the identified network deficiencies.

Mitigants are tactical bubbles and national roaming with other MNOs. Both of these measures would help improve the resilience of services.

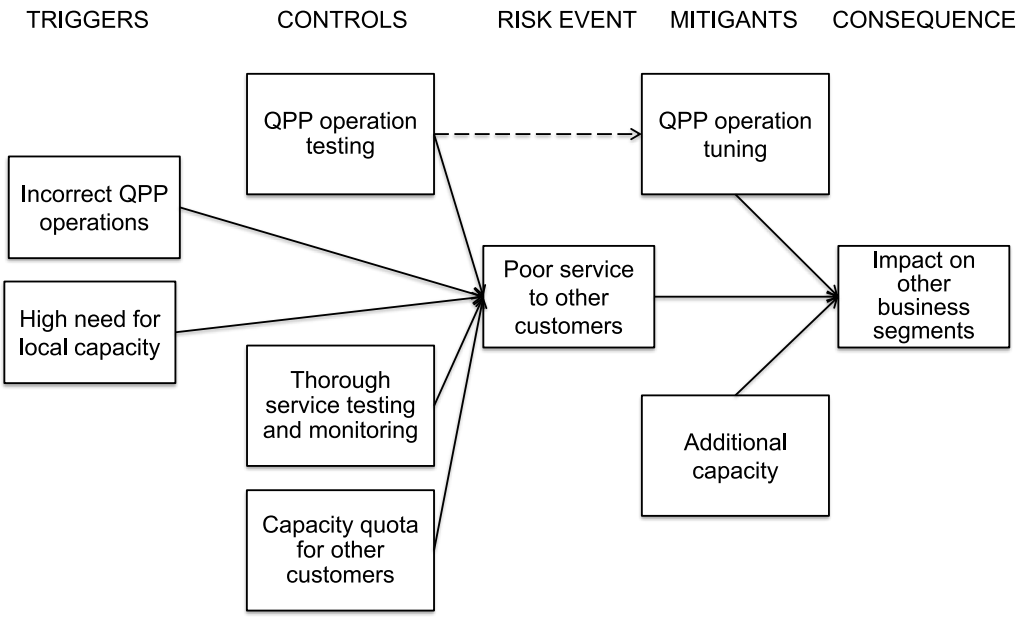


Fig. 10. Poor service to other customers sub-model.

4.9. Financial risk value

All of the business risk consequences of the model represent financial values. These are 1) additional costs, 2) contractual penalties, which are usually additional costs, 3) lost service revenue, and 4) impact on other business segments, which can be lost market share, leading to lost revenue. By adding all of these consequences, as shown in Fig. 12, one financial risk value can be created to illustrate the financial business risk of the model.

The cumulative financial risk value of the model represents the MNO's risk in the case study's public safety project. However, the financial risk value is not the only cost factor of the model. Risk controls and mitigants also represent their own costs. For example, the 'cyber-resilience to meet public safety needs' control likely means improved cybersecurity measures that must be put in place. This could be new security equipment and software or new security experts. The same applies to mitigants. For example, the 'tactical bubbles' mitigant requires equipment and software, and likely operating personnel and annual maintenance as well. All of these generate costs. In a quantitative model, these factors should also be considered.

4.10. Complete risk model

The complete risk model consists of the sub-models described in the previous sections. Figure B.1 in Appendix B illustrates the complete qualitative model, with the sub-models in columns and the different categories of nodes (triggers, controls, etc.) in rows. The nodes are connected to one another, as described in the sub-model presentations.

4.11. Underlying reasons for risks

The risk model shows that business risks are a threat to the MNO's financial goals in public safety business. The potential consequences of the risks are additional costs, contractual penalties, and lost service revenue; furthermore, they can have a negative impact on the MNO's regular business, which can lead to a loss of market share and revenue. All of these factors have a negative impact on the MNO's financial results.

Three underlying reasons explain the model's risks (see Table 3): 1) contractual arrangements, 2) the demanding service needs of public safety users, and 3) the special nature of the public safety segment.

Contractual arrangements in this context refer to the contractual and regulatory framework between the MNO and the PPA. One factor is the long contract period. In the case study, the contract period was 10 years, which is typical for ongoing MC public safety

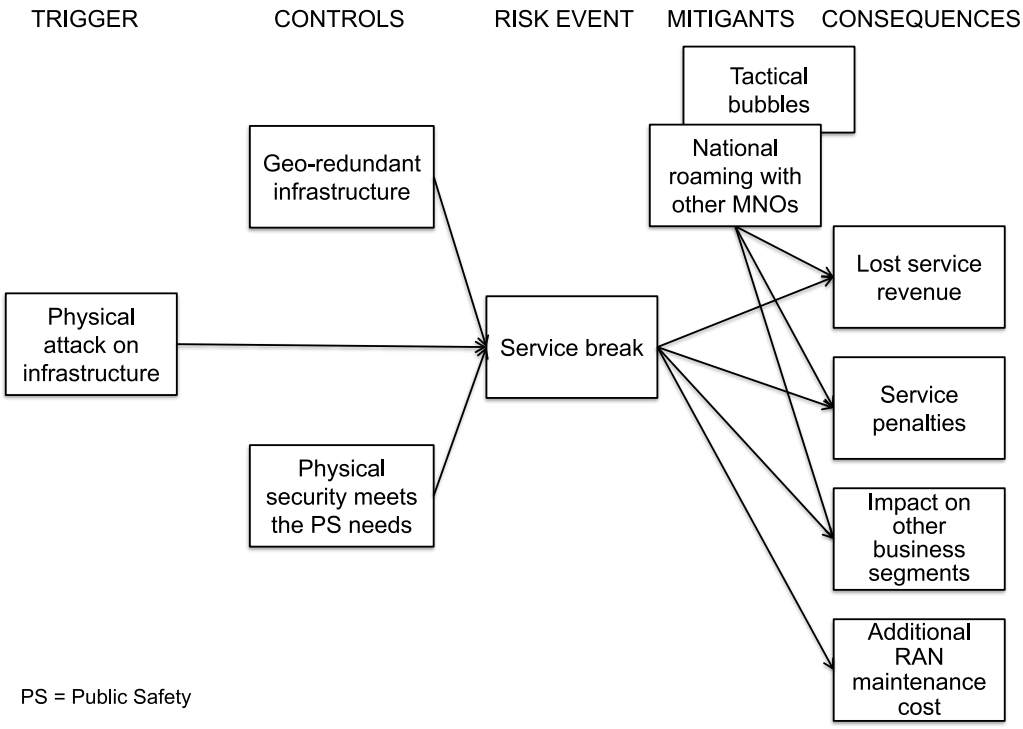


Fig. 11. Physical attack sub-model.

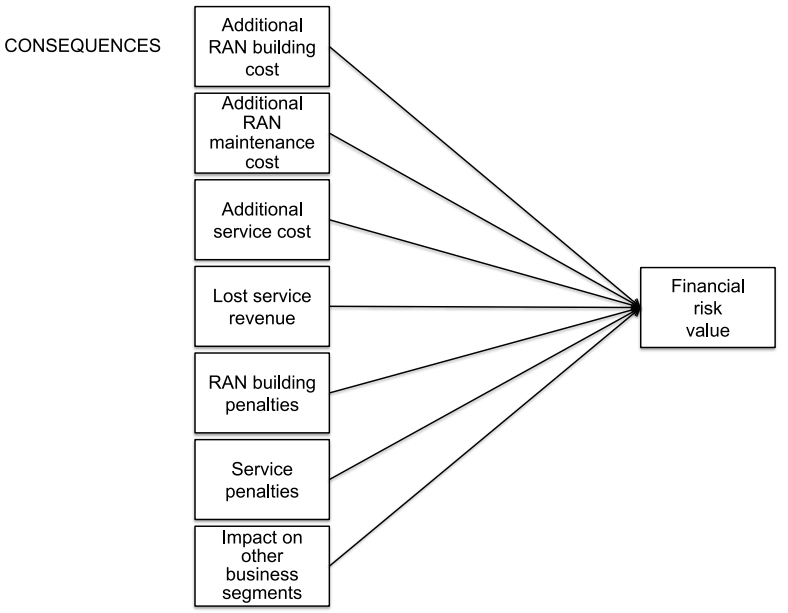


Fig. 12. Financial risk value sub-model.

Table 3
Underlying reasons for risks.

Reason	Risk domain
Contractual arrangements	Unprofitable business due to the contract between MNO and PPA
Demanding service needs of public safety users	Poor service due to insufficient RAN operation
	Lost service revenue due to delayed end-to-end solution
	Network building causes losses and additional cost
	Poor service impacting other business segments
Special nature of the public safety segment	Cybersecurity risks cause unsatisfactory service and data breach
	Physical attacks on infrastructure cause service breaks

projects (Savunen et al., 2023). This is motivated by significant network investments and the long payback period they require. However, a long contract period with a new customer segment with demanding requirements and developing technology is challenging for MNOs. An MNO may be vulnerable to substantial losses if the contract is inflexible and significant changes occur in the business environment or if the original assumptions of the number of users or ARPU are not correct. The PPA's role as a public actor can also be challenging. A PPA can use its power to change regulations in a way that weakens the MNO's position during the contract period (Howell & Sadowski, 2018).

The demanding service needs of public safety users refer to needs that meaningfully exceed the needs of the MNO's regular customers. Public safety users require communication services to be available everywhere, always, and with uncompromised security. Since the goal is to replace the existing technology and migrate from narrowband to broadband communications, services must be capable of meeting users' most demanding needs. Network coverage needs to be extended, and network resilience needs to be improved, including cybersecurity (Peltola & Hämmäinen, 2018). The network investments needed to accomplish this are significant, and there is a risk of exceeding budgetary and scheduling parameters and limitations. The financial risk this represents for an MNO depends on the business model. In the model of the case study, network building is one price element of the contract, and RAN services is another. Therefore, the MNO does not have to account for the depreciation of network investments in the pricing of services. This reduces the MNO's business risk.

The demanding needs of public safety users are also behind the service-level risks of the MNO's customers, including regular user segments. When serving multiple customer segments with distinctive service needs on the same mobile network, there is a risk that any and all segments may suffer from poor service. If customers are disappointed and SLAs are not met, this can materialise as financial losses, both in the public safety business segment and in the MNO's regular business operations.

The third risk area arising from demanding public safety needs is the complex end-to-end functionality required for these services. In the case study's business model, the MNO is responsible only for RAN services; however, all end-to-end functionalities must be in place before the MNO can start providing services and earning revenue. In this way, a delay in any essential end-to-end functionality is a financial risk for the MNO.

The special nature of the public safety segment refers to the differences in the unique needs of this customer segment compared to an MNO's regular customers. Public safety users are more vulnerable to cyberthreats due to the sensitive information associated with their operations and communications. According to the European Union Agency for Cybersecurity (2022), in 2021–2022, the public administration and government sector experienced the highest proportion of cyber incidents, accounting for 24.2% of all incidents. Furthermore, cyber incidents had the greatest impact on the public administration and government sector across various categories, including reputational, digital, financial, physical, and social impacts. In addition to cyberattacks, other possible cyberthreats include unethical behaviour on the part of the MNO's own personnel and physical attacks on the network infrastructure, and these can all cause service deviations and data breaches. Such security breaches can result in financial losses from both public safety and regular business segments.

4.12. Model validation

To validate the risk model, we used the evidence presented by the materialised risks observed in ongoing public safety mobile broadband projects. Do the risks observed in these projects confirm the findings of the risk model?

The risk model was primarily derived from the collective knowledge and insight of an expert panel. While this panel was well informed about ongoing projects, it is essential to acknowledge that the model itself does not explicitly depend on these projects for its formulation. However, as the panel members were aware of the unique challenges associated with these projects, this raises concerns about potential bias when using the same projects for model validation. Despite this slight methodological concern, the current lack of alternative similar projects provided limited options for model validation.

Given the unavailability of alternative projects, it is necessary to accept the situation, and ultimately, utilizing the knowledge from ongoing projects was the most practical approach to validate the model. The researchers remain confident, however, in the appropriate balance of the potential limitations against the need for model validation, while stressing that future research should include comparable new and not-yet-started projects for risk model refinement, thus ensuring the robustness and reliability of risk assessment models.

The case study followed the multi-actor shared-network model, the model of all ongoing European nationwide projects – ESN, RRF, and Virve 2.0 – so it is these projects that we will focus on first.

The procurement phase of the French RRF project ended in October 2022 and the implementation phase began (Donkin, 2022).

There has been no public information about the materialised risks of the project, which is understandable considering the short time between the beginning of the implementation phase and this writing.

The Virve 2.0 project in Finland was launched in 2018, and the suppliers of the core network and RAN services were awarded in 2020 (Erillisverkot, 2021a). MCS application procurement was also introduced, but it was suspended and scheduled to restart in 2024. The purpose of the postponement was to ensure seamless interworking services between the narrowband and broadband networks during the migration period (Erillisverkot, 2021b). This is one of the design goals of the project (Savunen et al., 2023). Postponing MCS procurement reflects the immaturity of the end-to-end solution and the related sub-model (see Section 4.5).

In 2011, the Home Office in the United Kingdom began a project to replace the TETRA-based Airwave network with the 4G/5G based ESN, with the aim of closing the Airwave network by the end of 2019. At the time of this writing in autumn 2023, the ESN is in the network-building phase due to many challenges in implementation. There have been challenges with the complex end-to-end solution, the share of responsibilities between different actors, and the engagement of user organisations. For example, the Home Office opted to change the deployment approach in 2018. They opted for an incremental model rather than a "big bang" transition, which allows the user organisations' priorities to be taken into account (National Audit Office, 2019).

There have also been challenges in radio-coverage building in the ESN project. EE, as the project's MNO, is in charge of extending its network to include 675 new radio sites. This was almost complete in 2022; however, EE found that an additional 92 radio sites may be necessary as radio coverage was found to be more limited than originally expected (National Audit Office, 2023).

The materialised risks in the ESN network-building phase reflect two sub-models – the 'end-to-end solution not ready' and the 'RAN building not on time or not on budget'. Although these risks have materialised at the project level, they have not had a significant impact on EE's business, which raises the question: Why?

EE was originally granted the ESN contract in December 2015, valued at 675 million GBP. The contract was to continue until 2021. As a result of project delays, the contract was renegotiated in 2019 and extended to December 2024. The value of the new extended contract was 895.7 million GBP. The higher price was due to the extended duration of the contract and the new incremental delivery model based on payment milestones (TED, 2019a). This demonstrates the importance of contract renegotiations when original assumptions change, as illustrated in the 'contract' sub-model.

One additional materialised risk following the risk model can be found in FirstNet in the United States. In December 2020, there was a bomb attack in front of AT&T's facilities in Nashville. A number of telecommunications services, including FirstNet public safety services, were affected and eventually disrupted, both locally and in other states. FirstNet deployable network solutions – that is, tactical bubbles – were used to connect FirstNet users in problem areas (FirstNet Authority, 2021). This is illustrative of the risk described by the 'physical attack' sub-model and tactical bubbles as a measure to mitigate risk.

These examples demonstrate the materialised risks that reflect the different risk sub-models. The sub-models for which there are no examples are related to the project's operation phase. This is, of course, because the European projects are still in the network-building phase and not yet operational.

5. Discussion

This discussion covers three topics related to the risk model: 1) the relationships between the public safety mobile broadband business and an MNO's other business and the MNO's strategy, 2) how MNOs and PPAs can use the risk model, and 3) the limitations of the risk model.

The focus of the risk model was MNOs' business risks in public safety mobile broadband services. However, this does not exist in isolation from an MNO's regular mobile business with the consumer and enterprise customer segments. The key connection between public safety and regular business operations is the MNO's RAN, which is a shared resource. In the risk model, this is reflected in the 'poor service to other customers' sub-model, where the sharing of RAN can negatively affect the services of consumers and enterprises, and thus the MNO's business with these customers.

An MNO's business decision to enter the public safety services market is not only dependent on business risks, but also naturally on the revenue and profit opportunities of the public safety business and synergies with the MNO's other business segments. The extended network coverage opens new opportunities for the MNO, including the potential for increased market share and reduced customer churn in the regular customers' segment. The MNO's strategic goals also have an impact. The multi-actor business model is suitable for the MNO's market strategy, where the goal is to target several industries with similar service requirements as in public safety – extended coverage, high availability, and security (Savunen et al., 2023). One example is the energy network communication market, whose growth is driven by distributed energy production (Leligou et al., 2018).

If the MNO's strategy is to target a variety of customer segments with high service requirements, the public safety mobile broadband project would provide a good opportunity for the MNO to enhance its RAN. At best, the coverage extension and hardening

Table 4
Application of the risk model.

MNO	PPA
Assessment of operator's business risks	Planning of the business model and the contract for the procurement
Analysis of risk controls and mitigants	Understanding the operator's perspective on risks
Analysis of pricing models	Planning a balanced risk sharing between parties
Consideration of contractual risks	Balancing the risk transfer and the contract price

of the network would be paid for by the government, as in the case study of building and maintaining RAN with a fixed-pricing model. This would give the MNO an advantage over its competitors – even if not necessarily a sustainable one.

The second discussion topic concerns the application of the risk model. This is addressed from the perspective of two actors: the MNO and the PPA (see Table 4).

An MNO considering entering the public safety market, or one already in the bidding process for public safety services, can use the risk model as a tool to assess its potential risks in the public safety business. For example, the MNO can use the model as a basis for risk assessment or for comparison of its own view of business risks. Once the major risks have been identified, the controls and mitigants of the model can be analysed by comparing them to the operator's own capabilities. If there are options for different business models, the findings of the model can also be useful in comparing them. Further, MNOs can use the risk model when analysing contractual arrangements and pricing models during contract negotiations.

The recommended use of the risk model for a PPA is in the planning of the business model and the contract for the procurement of public safety services. The model can help the PPA to better understand the different business risks involved for MNOs. By evaluating different business models with consideration for MNO risks, it is possible to include risk control and mitigation measures for the most significant risks, both in the business model itself and in the contract.

PPAs can also use the risk model when assessing risk transfer and its balance between the parties. The more risk transferred to the MNO, the higher the risk premium, and the higher the price of the MNO's services. The PPA is also advised to have an open dialogue with MNOs during the bid process and contract negotiations to improve the visibility of the project's risks. A reasonable goal is to find balanced risk sharing between the parties.

The third discussion topic is the limitations of the risk model. Some of the limitations in this research pertaining to the risk model itself are related to it being a qualitative model. If an MNO wants to estimate the costs of different risks, a qualitative model cannot provide answers. The same thing is true if the MNO wants to compare different options to control the risks and choose the most effective option. However, all projects are different and have their own specific figures, and for this reason, the application and modifications of the model would be necessary in any case.

There are also limitations in the risk model related to the chosen business model for the case study. According to the multi-actor shared-network business model, the MNO is responsible for RAN services only. However, many other elements are needed for end-to-end public safety services, such as core network service, customer service, and sales and marketing (Fig. 3). Business risks related to these elements are not included in the risk model, as they are not applicable to the chosen business model. The notable exception to this is the 'end-to-end solution not ready' sub-model, which describes the business risk to the MNO if all elements of the end-to-end functionality are not available as expected.

6. Conclusion

The contribution of this research is a qualitative model of MNO business risks in the public safety services market. The risk model is based on the business model of European next-generation public safety mobile broadband projects. The model shows that business risks pose a threat to the financial goals of the MNO's public safety business in many ways. These risks could result in additional costs, contractual penalties, and lost service revenue. Moreover, if these risks materialise, they could negatively affect the MNOs' regular business, potentially leading to a loss of market share and revenue.

Three main sources of the MNO's risks are contractual arrangements, the demanding service needs of public safety users, and the special nature of the public safety segment. These underlying reasons explain the risks in the business risk model.

The risk model can serve as a tool for MNOs and PPAs in the procurement processes of public safety mobile broadband projects. MNOs can benefit from these results by better understanding the project's potential risks, their consequences, and their control and mitigation. Accordingly, it is recommended that PPAs use the results of this research in business model and contract planning for new public safety procurements.

This research provides new insight into next-generation public safety mobile broadband projects from the perspective of MNOs. Given the limited prior research on this subject, this study serves as a foundational contribution that can pave the way for future research.

One interesting and beneficial avenue for future research would be a financial analysis of MNOs' business opportunities in the field of next-generation public safety services. A financial analysis that includes estimated revenue potential, capital and operating expenditures, and profits would provide MNOs with a model with business figures to assess the market opportunities and their profitability. PPAs could use the results when planning new public safety procurements to better understand the financial constraints of the MNO business. A financial analysis could also be used to assess the effects of different business models and their sensitivity to business risks.

Declaration of interest

- Tapio Savunen works at Airbus Defence and Space, in the Public Safety and Security business
- Pekka Kekolahti, none
- Petri Mähönen, none
- Heikki Hämmäinen, none
- Kalevi Kilkki, none

Research funding sources

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

CRediT authorship contribution statement

Tapio Savunen: Conceptualization, Investigation, Methodology, Project administration, Visualization, Writing – original draft, Writing – review & editing. **Pekka Kekolahti:** Conceptualization, Investigation, Methodology, Validation. **Petri Mähönen:** Validation. **Heikki Hämmäinen:** Validation. **Kalevi Kilkki:** Validation.

Acknowledgements

The authors would like to thank the anonymous experts for their extensive contributions, as well as Dr. Matti Peltola and Dr. Jaakko Saijonmaa for their valuable comments.

APPENDIX A. DATA COLLECTION TEMPLATES

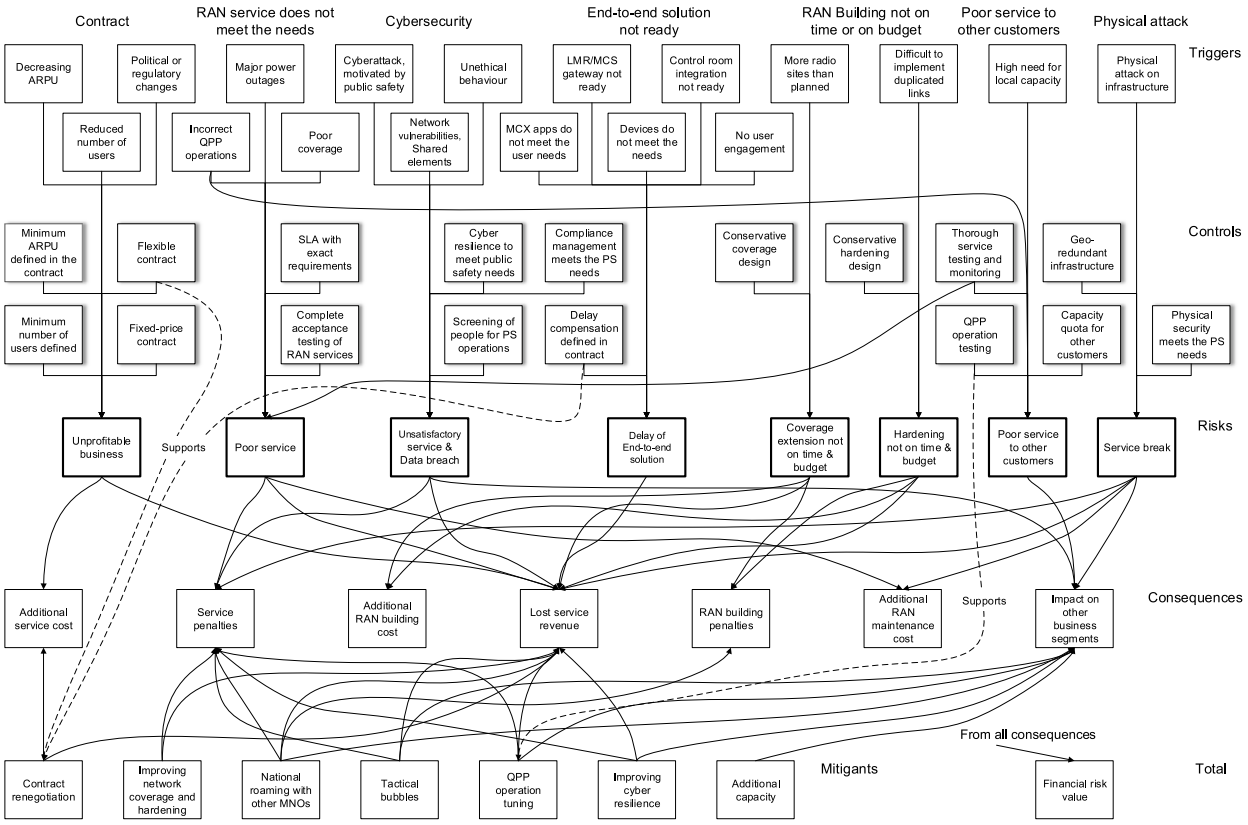
1. Risk trigger	2. Risk event	3. Control	4. Consequence	5. Mitigant
Example: Unpredictable user requirements	**Example**: High network build/maintenance cost	**Example**: Exact user requirements in the contract	**Example**: High cost, less margin, less profit	**Example**: Renegotiation of the agreement

Fig. A.1. Spreadsheet template; assignment 1, risk assessment

Category	Sub-category	Score - 0,1,2,3	1. Risk Trigger	2. Risk Event	3. Control	4. Consequence	5. Mitigant
2 Operational	End-to-end solution	0	MCX apps (Mission Critical PTT etc.) do not meet the user needs	Delay of end-to-end solution	E2E service control agreed and organized in cooperation	Lost revenue	Renegotiation of the contract
2 Operational	End-to-end solution	0	Service outage due to fault in Service Operator solution	Impact on MNO Alpha perceived quality and reputation	SLA with requirements on Service Operator	Loss of commercial users (churn)	Message to media and market (from the Service Operator), supported by Service Operator, that the fault is with the Service Operator, not Alpha
2 Operational	End-to-end solution	0	Due major failure communication is not working	Vendor risk	Risk assessmet of vendor selection for critical part of CORE systems	1) Cause damages/casualties for user, 2) brand and reputation may be damaged by service failures	Change of vendor (might be difficult/expeensive)
2 Operational	End-to-end solution	0	unsuffucient redundancy in critical part of CORE components	Major Network failure	Redundancy is built in to critical part of CORE	PPDR field operation fails	Risk analysis of needend redundancy
2 Operational	End-to-end solution	0	Standardization process delays, deviations and proprietary features	System functionality gaps, adverse behaviour and/or service disruption	Extensive test and verification, operational system based on mutually agreed features, phased approach	System solution quality level and functionality degradation	Retesting and verification, reducing non-functioning elements
2 Operational	End-to-end solution / devices	0	Devices do not meet the user needs, e.g. no device-to-device comms.	Delay of end-to-end solution	E2E service control agreed and organized in cooperation	Lost revenue	Renegotiation of the contract
2 Operational	End-to-end solution / devices	0	Radio performance of terminals is not sufficient	Service area is less than predicted	Minimum reguirements for terminal procurement are focuren on best possible RF performance	disrupt service availability	thruthful communication for users about reason and planned solution to solve problems
2 Operational	End-to-end solution / devices	0	Specific mobile devices with user related features at MNO RAN needed	No or some specific end user features functioning, functionality compromised, dependency on specific supplier	Test and validation process before operational use, piloted approach in restricted area	More extensive system support needs, higher costs	Additional resourcing and work to provide functionality
2 Operational	End-to-end solution/ integration	0	Unstable service due to complex end-to-end structure	Delay of end-to-end solution	Compensation defined in contract	Lost revenue	Renegotiation of the contract
2 Operational	End-to-end solution/ integration	0	LMR/MCX gateway does not work (narrowband / broadband interworking)	Delay of end-to-end solution	Compensation defined in contract	Lost revenue	Renegotiation of the contract
2 Operational	End-to-end solution/ integration	0	Control room integration not ready	Delay of end-to-end solution	Compensation defined in contract	Lost revenue	Renegotiation of the contract

Fig. A.2. Spreadsheet template; assignment 2, prioritisation of risks (only some of the lines are shown, a total of 106 lines)

APPENDIX B. COMPLETE RISK MODEL



ARPU = Average Revenue per User, D2D = Device to Device, LMR = Land Mobile Radio, MCS = Mission Critical Services, MNO = Mobile Network Operator, PS = Public Safety, QPP = Quality of Service, Priority, Preemption, SLA = Service Level Agreement

Fig. B.1. Complete risk model

References

Dalkey, N., & Helmer, O. (1963). An experimental application of the Delphi method to the use of experts. *Management Science, 9*(3), 458–467. https://doi.org/10.1287/mnsc.9.3.458

Díaz, G. R. (2022). Private participation in government-led backbone network projects: Lessons from three Latin American experiments. *Telecommunications Policy, 46*(8), Article 102367. https://doi.org/10.1016/j.telpol.2022.102367

Donkin, C. (2022). *Orange, Bouygues among emergency network winners. Mobile World Live*. https://www.mobileworldlive.com/featured-content/top-three/orange-bouygues-among-emergency-network-winners/.

Erillisverkot. (2021a). Virve 2.0 mobile strategy, building safety together. *Erillisverkot*, 14. https://www.erillisverkot.fi/uploads/2021/04/virve-mobile-stragegy-2021-version-1.1_03_2021web.pdf.

Erillisverkot. (2021b). *Press release: Erillisverkot takes steps to secure the Virve 2.0 project targets – procurement of new application services postponed*. https://www.erillisverkot.fi/en/press-release-erillisverkot-takes-steps-to-secure-the-virve-2-0-project-targets-procurement-of-new-application-services-postponed/.

European Union Agency for Cybersecurity. (2022). *ENISA threat landscape 2022*. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022.

Fantacci, R., Gei, F., Marabissi, D., & Micciullo, L. (2016). Public safety networks evolution toward broadband: Sharing infrastructures and spectrum with commercial systems. *IEEE Communications Magazine, 54*(4), 24–30. https://doi.org/10.1109/MCOM.2016.7452262

Fenton, N., & Neil, M. (2018). *Risk assessment and decision analysis with Bayesian networks*. CRC Press.

FirstNet Authority. (2021). *FirstNet Authority provides update on Nashville bombing*. https://www.firstnet.gov/newsroom/press-releases/firstnet-authority-provides-update-nashville-bombing.

Fodor, G., Parkvall, S., Sorrentino, S., Wallentin, P., Lu, Q., & Brahmi, N. (2014). Device-to-device communications for national security and public safety. *IEEE Access, 2*, 1510–1520. https://doi.org/10.1109/ACCESS.2014.2379938

Forge, S., Horvitz, R., & Blackman, C. (2014). *Is commercial cellular suitable for mission critical broadband? Study on use of commercial mobile networks and equipment for "mission critical" high-speed broadband communications in specific sector: Final report*. European Commission: SCF Associates LTD. https://data.europa.eu/doi/10.2759/54788.

Grous, A. (2013). *The socioeconomic value of mission critical mobile applications for public safety: 2x10MHz in 700MHz, preliminary research results: UK and EU*. London: Professional LTE Conference, 10 October 2013.

Hallahan, R., & Peha, J. M. (2013). Enabling public safety priority use of commercial wireless networks. *Homeland Security Affairs, 9*, 13. https://www.hsaj.org/articles/250.

Hallowell, M. R., & Gambatese, J. A. (2010). Qualitative research: Application of the Delphi method to CEM research. *Journal of Construction Engineering and Management, 136*(1), 99. https://doi.org/10.1061/(ASCE)CO.1943-7862.0000137
Hankintailmoitukset. (2019). *Virve 2.0; Radioverkon (RAN) hankinta*. https://www.hankintailmoitukset.fi/en/public/procurement/16268/notice/18695/overview.
Home, Office. About us – the first duty of the government is to keep citizens safe and the country secure. GOV.UK. https://www.gov.uk/government/organisations/home-office/about.
Howard, R. A., & Matheson, J. E. (2005). Influence diagrams. *Decision Analysis, 2*(3), 127–143. https://doi.org/10.1287/deca.1050.0020
Howell, B., & Sadowski, B. (2018). Anatomy of a public-private partnership: Hold-up and regulatory commitment in Ultrafast Broadband. *Telecommunications Policy, 42*(7), 552–565. https://doi.org/10.1016/j.telpol.2018.05.001
Höyhtyä, M., Lähetkangas, K., Suomalainen, J., Hoppari, M., Kujanpää, K., Ngo, K. T., Kippola, T., Heikkilä, M., Posti, H., Mäki, J., Savunen, T., Hulkkonen, A., & Kokkinen, H. (2018). Critical communications over mobile operators' networks: 5G use cases enabled by licensed spectrum sharing, network slicing and QoS control. *IEEE Access, 6*, 73572–73582. https://doi.org/10.1109/ACCESS.2018.2883787
Kaplan, R. S., & Mikes, A. (2012). Managing risks: A new framework. *Harvard Business Review, 90*(6), 48–60. https://hbr.org/2012/06/managing-risks-a-new-framework.
Kekolahti, P. (2011). Using Bayesian belief networks for modelling of communication service provider businesses. In *Proceedings of the 8th Bayesian modelling applications Workshop*. https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=3bf9fa20bd9d564a91f708787d63e0d16f90a388#page=62.
Kekolahti, P. (2019). *Bayesian network analysis of mobile service and device usage [Doctoral dissertation*. Aalto University. https://aaltodoc.aalto.fi/server/api/core/bitstreams/d2b82c62-8ddb-4df8-86fa-a2da01eb22bc/content.
Lair, Y., & Mayer, G. (2017). *Mission critical services in 3GPP*. 3GPP. https://www.3gpp.org/news-events/1875-mc_services.
Leligou, H. C., Zahariadis, T., Sarakis, L., Tsampasis, E., Voulkidis, A., & Velivassaki, T. E. (2018). Smart grid: A demanding case study for 5G technologies. In *2018 IEEE international conference on pervasive computing and communications workshops* (pp. 215–220). Athens, Greece: PerCom Workshops. https://doi.org/10.1109/PERCOMW.2018.8480296.
Linstone, H. A., & Turoff, M. (Eds.). (1975). *The Delphi method*. Addison-Wesley.
Macaulay, S. (1963). Non-contractual relations in business: A preliminary study. *American Sociological Review, 28*(1), 55–67. https://doi.org/10.2307/2090458
Macneil, I. R. (1985). Relational contract: What we do and do not know. *Wisconsin Law Review, 4*, 483–526.
National Audit Office. (2019). *Progress delivering the emergency services network*. https://www.nao.org.uk/wp-content/uploads/2019/05/Progress-delivering-the-Emergency-Services-Network.pdf.
National Audit Office. (2023). *Progress with delivering the emergency services network*. https://www.nao.org.uk/wp-content/uploads/2023/03/progress-with-delivering-the-emergency-services-network.pdf.
Norwegian Directorate for Civil Protection (2018). Alternatives for mission-critical services in public mobile networks in Norway. Dsb Nødnett. 3. https://www.nodnett.no/bibliotek/alternatives-for-mission-critical-services-in-public-mobile-networks-in-norway/.
Okoli, C., & Pawlowski, S. D. (2004). The Delphi method as a research tool: An example, design considerations and applications. *Information & Management, 42*(1), 15–29. https://doi.org/10.1016/j.im.2003.11.002
Onnettomuustutkintakeskus. (2010). *Heinä-elokuun 2010 rajuilmat*. Tutkintaselostus S2/2010Y https://turvallisuustutkinta.fi/material/attachments/otkes/tutkintaselostukset/fi/muutonnettomuudet/2010/s22010y_tutkintaselostus/s22010y_tutkintaselostus.pdf.
Peltola, M., & Hämmäinen, H. (2018). Effect of population density and network availability on deployment of broadband PPDR mobile network service. *Digital Policy, Regulation and Governance, 20*(1), 78–96. https://doi.org/10.1108/DPRG-07-2017-0042
Peltola, M. J., & Kekolahti, P. (2015). Risk assessment of public safety and security mobile service. In *2015 10th international conference on availability, reliability and security* (pp. 351–359). IEEE. https://doi.org/10.1109/ARES.2015.65.
Peltola, M., & Martikainen, O. (2015). Valuation of mobile broadband PSE network for society. *Journal of NBICT, 1*, 1–22. https://www.riverpublishers.com/journal/journal_articles/RP_Journal_1902-097X_201411.pdf.
Productivity Commission. (2015). *Public safety mobile broadband*. Australian government. https://www.pc.gov.au/inquiries/completed/public-safety-mobile-broadband/report.
Reardon, M. (2020). *AT&T's wireless business thrives amid pandemic*. CNET. https://www.cnet.com/tech/mobile/at-ts-wireless-business-thrives-amid-pandemic/.
Savunen, T., Hämmäinen, H., Kilkki, K., & Kekolahti, P. (2023). The role of mobile network operators in next-generation public safety services. *Telecommunications Policy, 47*(3), Article 102489.
Schmidt, R., Lyytinen, K., Keil, M., & Cule, P. (2001). Identifying software project risks: An international Delphi study. *Journal of Management Information Systems, 17*(4), 5–36. https://doi.org/10.1080/07421222.2001.11045662
Suomalainen, J., Julku, J., Vehkaperä, M., & Posti, H. (2021). Securing public safety communications on commercial and tactical 5G networks: A survey and future research directions. *IEEE Open Journal of the Communications Society, 2*, 1590–1615. https://doi.org/10.1109/OJCOMS.2021.3093529
TED. (2019). *Services - 409374-2019*. https://ted.europa.eu/udl?uri=TED:NOTICE:409374-2019:TEXT:EN:HTML.
TED. (2020). *Services - 586641-2020*. https://ted.europa.eu/udl?uri=TED:NOTICE:586641-2020:TEXT:EN:HTML&src=0.
Weedage, L., Rangel, S., Stegehuis, C., & Bayhan, S. (2023). *On the resilience of cellular networks: How can national roaming help? arXiv preprint*. https://doi.org/10.48550/arXiv.2301.03250. arXiv: 2301.03250.
World Bank. (2017). *Public–private partnerships: Reference guide version 3*. World Bank Group. https://elibrary.worldbank.org/doi/abs/10.1596/29052.
Yarali, A. (2020). *Public safety networks from LTE to 5G*. John Wiley & Sons.