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

Conference Paper

Mobile Network Operators' Business Risks in Next-Generation Public Safety Services

32nd European Conference of the International Telecommunications Society (ITS): "Realising the digital decade in the European Union – Easier said than done?", Madrid, Spain, 19th - 20th June 2023

Provided in Cooperation with:

International Telecommunications Society (ITS)

Suggested Citation: Savunen, Tapio; Kekolahti, Pekka; Mähönen, Petri; Hämmäinen, Heikki; Kilkki, Kalevi (2023) : Mobile Network Operators' Business Risks in Next-Generation Public Safety Services, 32nd European Conference of the International Telecommunications Society (ITS): "Realising the digital decade in the European Union – Easier said than done?", Madrid, Spain, 19th - 20th June 2023, International Telecommunications Society (ITS), Calgary

This Version is available at:
https://hdl.handle.net/10419/278017

Mobile Network Operators' Business Risks in Next-Generation Public Safety Services

Tapio Savunen[1]
Aalto University, School of Electrical Engineering, Department of Information and Communications Engineering
tapio.savunen@aalto.fi

Pekka Kekolahti
Aalto University, School of Electrical Engineering, Department of Information and Communications Engineering
pekka.kekolahti@aalto.fi

Petri Mähönen
Aalto University, School of Electrical Engineering, Department of Information and Communications Engineering
petri.mahonen@aalto.fi

Heikki Hämmäinen
Aalto University, School of Electrical Engineering, Department of Information and Communications Engineering
heikki.hammainen@aalto.fi

Kalevi Kilkki
Aalto University, School of Electrical Engineering, Department of Information and Communications Engineering
kalevi.kilkki@aalto.fi

Abstract

Field of research – This research is in the field of public safety communications in mobile broadband 4G/5G networks. Its specific focus is mobile network operators and their business risks in the public safety market.

Purpose – This research is intended to provide a qualitative model of MNOs' business risks in the public safety business. The risk assessment covers the business model used in European public safety mobile broadband projects, which is used in three of five ongoing projects.

Methods and data – A qualitative method was used for the current research. The risk model is an influence diagram, which is a directed graph consisting of nodes and arcs. The risk model uses the causal taxonomy of risk, which is commonly used for qualitative and quantitative causal models based on Bayesian networks. An expert panel and the Delphi method were used 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 a threat to the financial goals of MNOs' public safety business. The potential consequences of the risks are additional costs, contractual penalties, and lost service revenue. They can also have a negative impact on the MNO''s regular business, which in the worst case can lead to a loss of market share and revenue. All of these have a negative impact on the MNOs' financial results.

[1] Corresponding author

Value – This research brings new knowledge about MNOs' business risks in next-generation public safety services. Procurement authorities can use the results when planning public procurements in the field of mobile broadband public safety services. MNOs can benefit from these results by gaining a better understanding of potential risks, their consequences, and their control and mitigation in public safety projects.

Keywords: mobile network operator, public safety, business risk, risk model, mobile broadband

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 wireless communications for public safety have been based on narrowband solutions, such as Terrestrial Trunked Radio (TETRA), Tetrapol and Project 25 (P25; Fantacci et al., 2016). Public safety agencies are now gradually moving to standardised 4G/5G mobile broadband technologies. This is enabled by technological evolution and driven by the new needs of public safety organisations. Voice-based group communication, often called push-to-talk (PTT), is the main service of narrowband radio systems. The new needs of public safety users include, for example, video transfer between field operations and control centres and applications providing useful information to first responders in the field, such as maps and construction drawings (Peltola & Hämmäinen, 2018; Yarali, 2020).

New public safety broadband services improve the efficiency of field operations and the safety of first responders and citizens. In Finland, the socioeconomic value of these new services is estimated to be 40–94 euros per inhabitant per year (Peltola & Hämmäinen, 2018). In the United Kingdom, public safety mobile broadband services could improve police productivity with savings of 5–10% (Grous, 2013). In the European Union, when public safety services work more efficiently in emergencies, the annual savings of 5% would equal 24 billion euros (Blackman et al., 2014).

The 4G/5G technologies that public safety organisations are moving to are the same technologies that mobile network operators (MNOs) use in their networks. This development presents new business opportunities for MNOs; with certain enhancements, their networks can be used to serve public safety agencies (Peltola & Hämmäinen, 2018). This is also an opportunity for governments and regulators, as it negates the need for both government investment in dedicated nationwide public safety networks and the allocation of radio spectrum by regulators (Productivity Commission, 2015; Norwegian Directorate for Civil Protection, 2018).

MNOs are used to provide services to consumers and enterprises. Public safety services are a new opportunity for MNOs. However, entering a new market exposes MNOs to new business risks. Public safety organisations are often an unknown customer segment. The business objectives of MNOs differ from those of public safety organisations; the goal of MNOs is to maximise revenue and profits, while public safety organisations are to protect life, property, and the state (Yarali, 2020).

Compared to regular MNO customers, public safety users have more demanding service needs. The services' availability, reliability, and security – known as mission-critical (MC) needs – must be very high (Yarali, 2020). As such, mobile networks designed for consumers and enterprises cannot meet the needs of public safety organisations. Typically, coverage must be extended, and network security and resilience must be hardened (Peltola & Hämmäinen, 2018). 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).

One additional source of business risk in public and private sector telecommunications projects is the contractual and regulatory framework between private and public parties. The projects targeting next-generation nationwide public safety services are based on public procurements organised by public authorities, who often also participate in organising public safety services alongside MNOs and may therefore have two different roles (Savunen et al., 2023). The public party can use its regulatory power to change the regulation in its favour after the contract is signed. This can threaten the operator's service revenue (Howell & Sadowski, 2018). In addition, improper allocation of financing and demand risk to the parties can be a source of operational unsustainability (Díaz, 2022).

The materialisation of these or other business risks would jeopardise the profitability of MNOs' public safety business. Public safety services may also adversely affect services for MNOs' other customers, as the same network is shared between different user segments. 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 strategy, and it is a competitive advantage over competitors with less effective risk-management methods (Kaplan & Mikes, 2012).

Savunen et al. (2023) conducted a review of the five known ongoing public safety mobile broadband projects in which MNOs participate that are in at least the network implementation phase: VIRVE 2.0[2] in Finland, Réseau Radio du Futur (RRF) in France, Safe-Net in the Republic of Korea, Emergency Services Network (ESN) in the United Kingdom and First Responder Network (FirstNet) in the United States (Erillisverkot, 2021c; Carmona, 2021; Yarali, 2020; Home Office, 2021a; FirstNet Authority, 2021b). They analysed the MNO business models, including a comparison of two key models. Although the focus was not on business risks, a few risks were identified. MNOs should pay attention to the project organisation if the project follows a multi-actor business model in which there are several actors. In such a project, the role of the system integrator is essential (Savunen et al., 2023). The length of the contract period also deserves MNOs' attention, as a long public-private partnership (PPP) contract is expected to favour investments and innovations (Roumboutsos & Saussier, 2014).

Other research on public safety services and 4G/5G technologies conducted in recent years has mostly focused on technological questions. Some of these also have a connection with MNOs, although not directly with their business aspects. Topics include, for example, how to manage MNOs' radio-network service quality when the network is shared between different users with different needs (Höyhtyä et. al., 2018; Hallahan & Peha, 2013) or the analysis of security threats and measures to improve security of MNOs' 5G networks when used for public safety services (Suomalainen et al., 2021). The socioeconomic value of different implementation options for public safety networks, including MNO networks, has also been analysed (Peltola & Hämmäinen, 2018).

The current paper describes 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. This model is used in three of the five ongoing projects, which all have multiple actors. MNOs' radio access networks (RANs) are

[2] There are two different names in public use: Virve 2 and Virve 2.0. This paper uses Virve 2.0.

shared with public safety users, and while MNOs provide MC RAN services, other actors are responsible for other areas, such as MC applications and customer service. The goal of all European projects is to migrate from a narrowband system to broadband communications and replace the existing technology with a new one. 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 research questions are as follows:

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

The structure of the paper is 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 Section 6 provides a conclusion.

These results can be of use to MNOs considering entry into the public safety market and to government authorities planning procurement for public safety services. The paper also supports further research on MNOs' business in the context of next-generation public safety services.

2. RESEARCH METHODS

2.1. Qualitative Research

Only two of the five MNO-involved nationwide public safety mobile broadband projects have reached the production stage and are available to users in 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 this topic, there is no existing theoretical framework. These are the primary motivations for choosing a qualitative research model.

In this context, qualitative research is understood as 'an iterative process in which improved understanding to the scientific community is achieved by making new significant distinctions resulting from getting closer to the phenomenon studied'. This definition refers to the way of doing research and the results of the research: using empirical data in an iterative process to gain a better understanding of ideas new to academia (Aspers & Corte, 2019, p. 155).

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. It is a directed graph consisting of nodes and arcs, with nodes that are connected to one another by directed arcs. An arc from one node to another indicates a causal or other influential relationship between the nodes. Influence diagrams can be used in decision analysis to illustrate probabilistic dependencies (Howard & Matheson, 2005). An additional constraint in this case is that there are no cycles in the graph, so there are no circular decision-making links (Fenton & Neil, 2018).

In addition to influence diagrams, the risk model incorporates the causal taxonomy of risk, a method proposed by Fenton and Neil (2018) for Bayesian networks. In 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 the five categories, a cumulative node has been added, which sums the values of the consequence nodes.

Figure 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 itself and a consequence of risk triggers. It may contribute to only one consequence or to several. 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).

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 on 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.

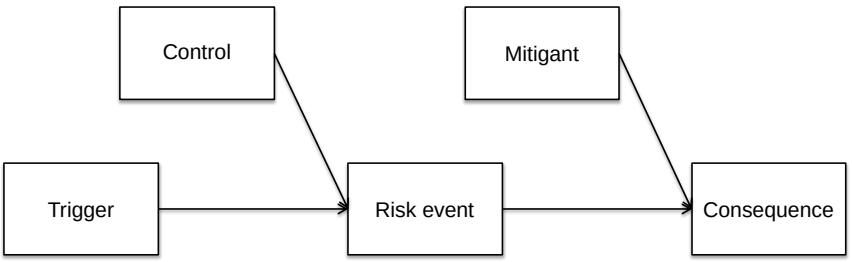

Figure 1. Causal taxonomy of risk (Fenton & Neil, 2018)

2.3. Expert panel and Delphi model

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

The Delphi method was chosen for working with experts. The Delphi method was originally developed 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).

The careful selection of experts is an important task in the Delphi method. One of the most critical requirements for experts is a deep understanding of the research area (Okoli & Pawlowski, 2004). On the other hand, diversity in the experts' backgrounds and areas of expertise is also needed so that opinions vary sufficiently.

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 an independent expert 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 phase. The background of the eight expert groups was as follows: academia – 1; public administration – 2; consulting – 2; industry – 1; and operator – 2. According to Hallowell and Gambatese (2010), eight experts is a sufficient number 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-assessment. The expert panel's average knowledge of cyber security was lower than that of other areas, and no one on the expert panel had expert-level cybersecurity knowledge (Rating 3). This limitation represents an opportunity for future research.

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

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. It was described by Schmidt et al. (2001) in their research identifying risks in software projects. The described process has three phases: 1) brainstorming for important factors, 2) narrowing down the list of factors, and 3) ranking the list.

Figure 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 to the experts with the necessary materials and templates, 2) independent work of experts (or expert groups), 3) analysis of the expert contributions, and 4) feedback on the panel's contributions. The feedback was presented in a way that guaranteed the anonymity of the answers.

All expert meetings were arranged online. This was to ensure that all experts had the same information needed for the next assignment. Following the model suggested by Kekolahti (2011), materials and templates, as well as expert contributions, were exchanged by email, which guaranteed the anonymity of the answers, and spreadsheet templates were used for structured expert contributions. There were also open-ended questions that the experts responded to by email.

The first assignment was the risk assessment of a case study (see Section 3). The purpose of the case study was to provide the experts with an equal starting point for the assessment of MNOs' business risks. The introduction of the assignment included a detailed case study description. The experts were asked to provide the most significant business risks for the case study on a spreadsheet template. The template included all five categories for each risk – risk triggers, risk events, risk controls, consequences and mitigants. The first assignment resulted in 112 different risks, a few 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 requested to give each risk a score between 0 and 3, with 0 being the least and 3 the most relevant. The result of the second assignment was the ranking of risks, using the average of scores 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 variants of the same risk, so they were combined into a total of 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, which comprised a combination of the sub-models, was also presented. The sub-models were also all explained in detail.

The third and final assignment was the prioritisation of the sub-models. Experts were asked to define the most significant and the least significant sub-models with consideration to MNOs' risks in the public safety business. The 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' order is according to the experts' prioritisation.

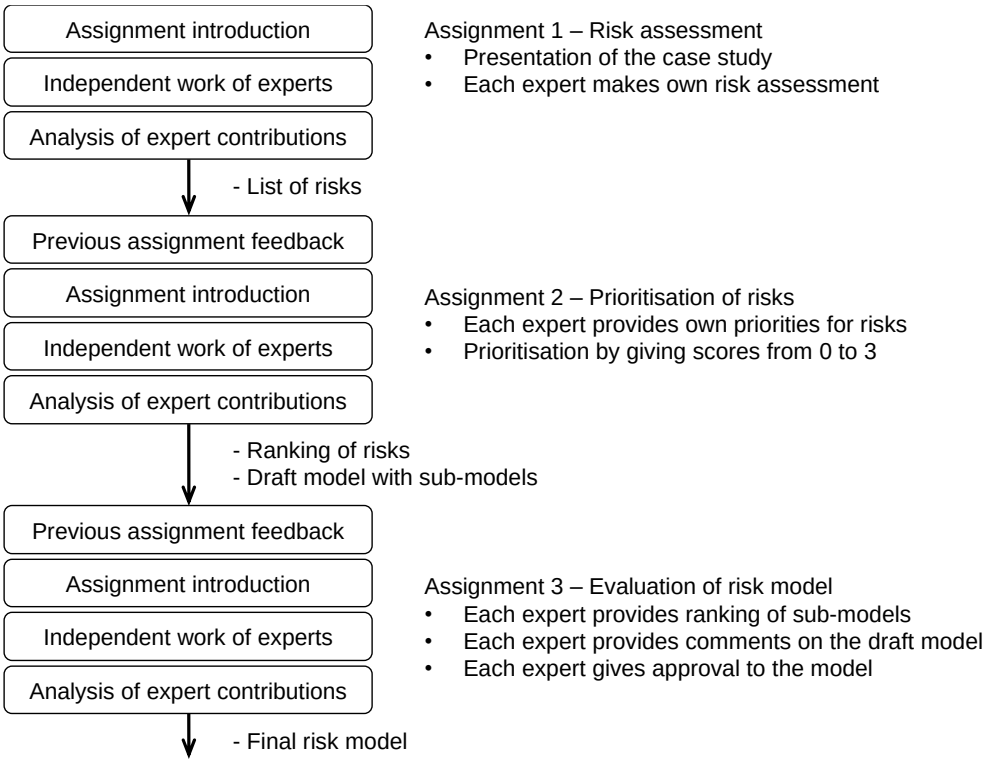

Figure 2. Data collection and analysis and the creation of a risk model

3. CASE STUDY

3.1. Business Model

The target of the research was to assess the MNOs' risks in a typical nationwide public safety mobile broadband project and 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 are 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 based on the number of actors responsible for providing public safety services, either 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, consumers and enterprises.

Using these dimensions and their respective values, business models can be divided into four quadrants (Savunen et al., 2023).

Figure 3 illustrates the positioning of the ongoing nationwide public safety projects on the business model map. All European projects – ESN, RRF and Virve 2.0 – follow the multi-actor shared-network model. The role of the MNO in these projects is to provide shared MC RAN services (3rd Generation Partnership Project [3GPP], 2020) and, potentially, some core network services as well (Savunen et al., 2023).

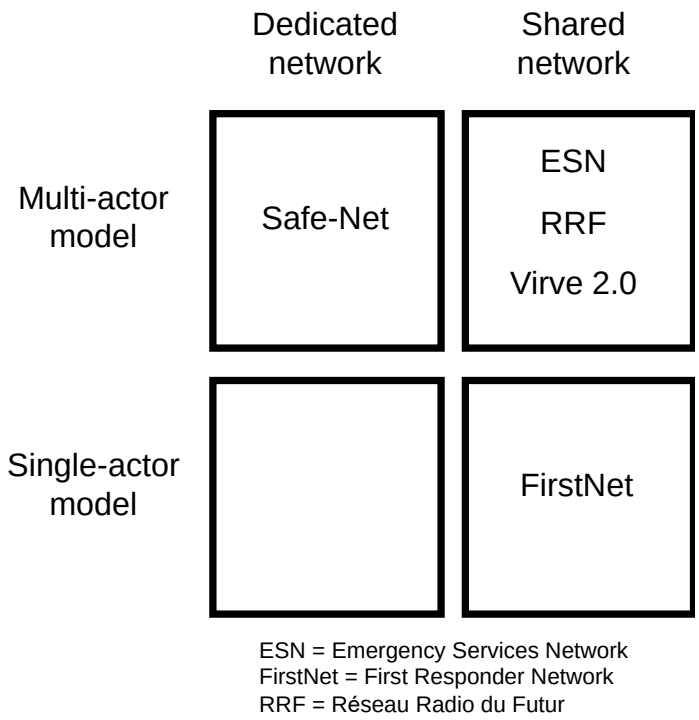

Figure 3. Ongoing nationwide public safety projects on the business model map

The multi-actor shared-network model was chosen for the case study. As it is currently the only model used in Europe, there will likely be more projects based on this model in the future. Furthermore, as the most complex model, it is likely to reveal a wealth of risks.

3.2. Project

The case study description follows the principles of the ongoing European nationwide public safety mobile broadband projects, using a combination of the features of the projects. A review of the ongoing projects can be found in Savunen et al. (2023).

The project is assumed to be based on a public bid organised by a *public procurement authority* (PPA; Hankintailmoitukset, 2019; TED, 2019b; TED, 2020). The ranking criteria for the offers vary, but price is usually an important factor.

The goal of the project is to provide next-generation public safety mobile broadband services to public safety authorities. The project is divided into two parts. One part is MC RAN services provided by an MNO. The second part is public safety services and devices provided by a service operator. For end-to-end public safety services, the services of the MNO and the service operator are required.

Figure 4 illustrates the division of the responsibilities in the case study project between the MNO and the service operator. The MNO is in charge of MC RAN services that meet the needs of public safety users. Since the MNO's existing network is used for public safety services, the coverage of the MNO's RAN must be extended, and the availability and security of the network must be hardened (Peltola & Hämmäinen, 2018). In addition, the quality of service, prioritisation, and pre-emption (QPP) functionalities of 4G/5G technologies are required to enable sufficient service quality for public safety users in the MNO's shared network (Hallahan & Peha, 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.

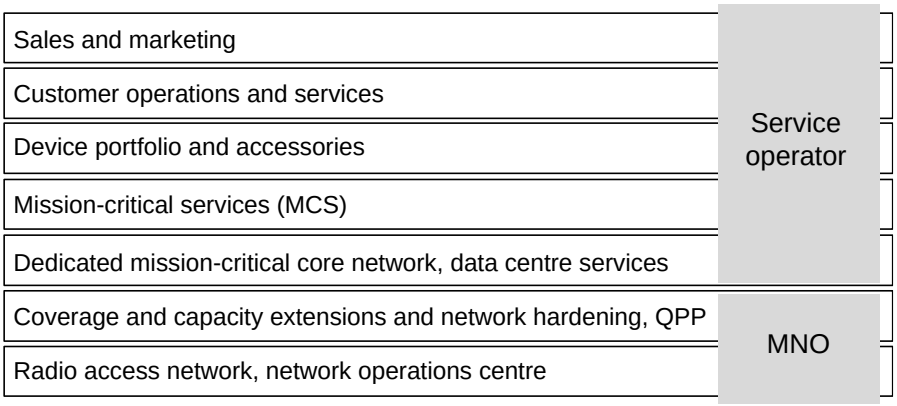

Figure 4. Share of responsibilities for the case study

Figure 5 illustrates the phases of the project from the MNO's point of view. The terminology follows that of 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 of the project is 10 years, which is divided into two phases. The first phase, including 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 network maintenance. In practice, the MNO is paid for building and maintaining an RAN that meets public-safety needs. The pricing model for RAN services is subscriber-based and therefore dependent on the number of users.

The contract guarantees the MNO's exclusive rights 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 to be insufficient, they may decide to postpone the use of services. Or, if they consider the price of the service too high, they can reduce the number of users from the original estimate.

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

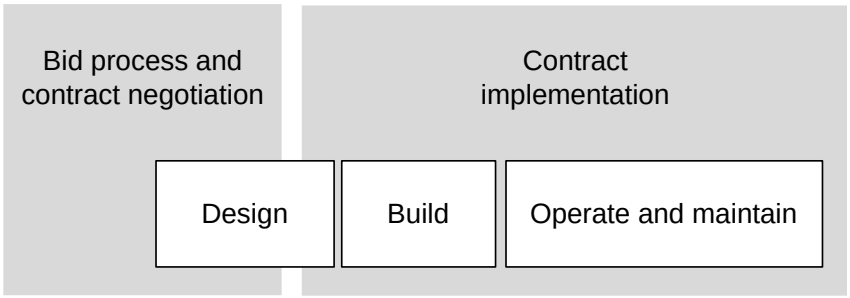

Figure 5. Project phases of the case study, following PPP terminology (World Bank, 2017)

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 the 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 a congested network.

The direct business opportunities for the MNO are the project's revenue and profit. 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). However, the churn rate of public safety users is likely to be low.

For the MNO, the project is strategic due to the indirect business opportunities based on improved network coverage and service availability: These would be an advantage for the operator's other customer segments. The MNO would be able to increase its market share and reduce the churn rate, as well as potentially increasing their average revenue per user (ARPU). For example, AT&T has stated that the higher quality network resulting from FirstNet's improvements has

positively affected its market share and churn in 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 smart grid market, driven by decentralised renewable electricity generation (Leligou et al., 2018).

The MNO has estimated the costs of network extensions and hardening, as well as the cost of RAN services. 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.

Appropriate risk management is important for an MNO to improve the competitiveness of its bid. When business risks are understood and modelled well, the offer does not require oversized risk reserves, and the MNO can also take higher risks. Therefore, the offer can be more competitive than competitors' offers due to more effective risk management (Kaplan & Mikes, 2012).

4. RISK MODEL

4.1. Sub-models

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

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 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

4.2. Contract

Public safety business is supposed to be a new business for MNO. The customer segment and its requirements differ from those of consumers and enterprises, which are MNO's regular customers. In addition, the contract period, 10 years in the case study, is a relatively long customer contract for an MNO.

The risk event in this sub-model is an unprofitable business due to negative changes in the operating environment combined with an inflexible contract. In the case study, the price model of the MNO's contract with the PPA is subscription-based for services. The MNO estimated subscription-based revenue with certain assumptions about the ARPU and the number of subscribers. If either of these factors were lower than expected, it would trigger the risk as the impact would be lost service revenue (Figure 6); the corresponding triggers are decreasing ARPU and 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 the regulation in its favour after the contract is signed, especially in the case of a long contract (Howell & Sadowski, 2018). The PPA can also be involved in organising public safety services in addition to the MNO and thus can have two different roles (Savunen et al., 2023).

This sub-model has four controls. These controls 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 other controls are a flexible contract that supports changes and negotiations during the contract period[3] and a different contract model. In negotiations, the MNO can propose changing the contract model from a subscriber-based model to a fixed-price model.

[3] One example of flexible contract models is relational contracts, which are based on partnerships and mutual trust between the parties and support negotiations throughout the contract period (Macaulay, 1963; Macneil, 1985).

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

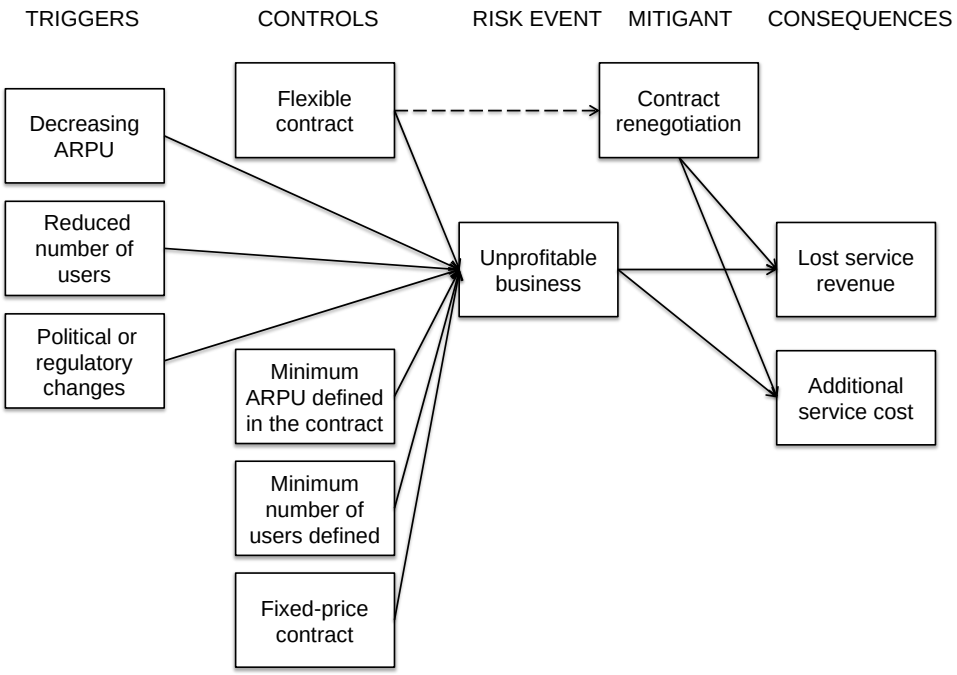

Figure 6. Contract sub-model

4.3. RAN Service Does Not Meet Needs

Public safety users have rigorous requirements for RAN services. They must always be available everywhere, with high security and without any service breaks. It is challenging for an MNO to provide demanding public safety services on a mobile network that was 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 the network coverage or service breaks.

The risk event has three triggers (see Figure 7). 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. For example, public safety users must get a higher priority than other users. This ensures appropriate services for public safety users, even in a congested network (Höyhtyä et al., 2018). On the other hand, if the QPP functions do not work properly – due to incorrect configuration, for example – poor service may result.

Another trigger is major power outages. Storms, for instance, can cut power lines over a wide area and may 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, in Finland in 2010, large storms caused long power outages, and at worst, a total of 1,050 mobile network radio sites were out of order (Onnettomuustutkintakeskus, 2010). In addition to storms, service interruptions can be caused by other natural disasters, such as earthquakes, floods, and forest fires.

The third trigger is poor coverage. Even if the planning and building of the radio network is careful, there may still be blind spots, such as large changes in elevation in the terrain.

This sub-model has three risk controls. Two of the controls aim to ensure that MNO's responsibilities for RAN services have 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 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. This is to obtain formal customer acceptance for the RAN building and 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. 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 because 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 the 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.

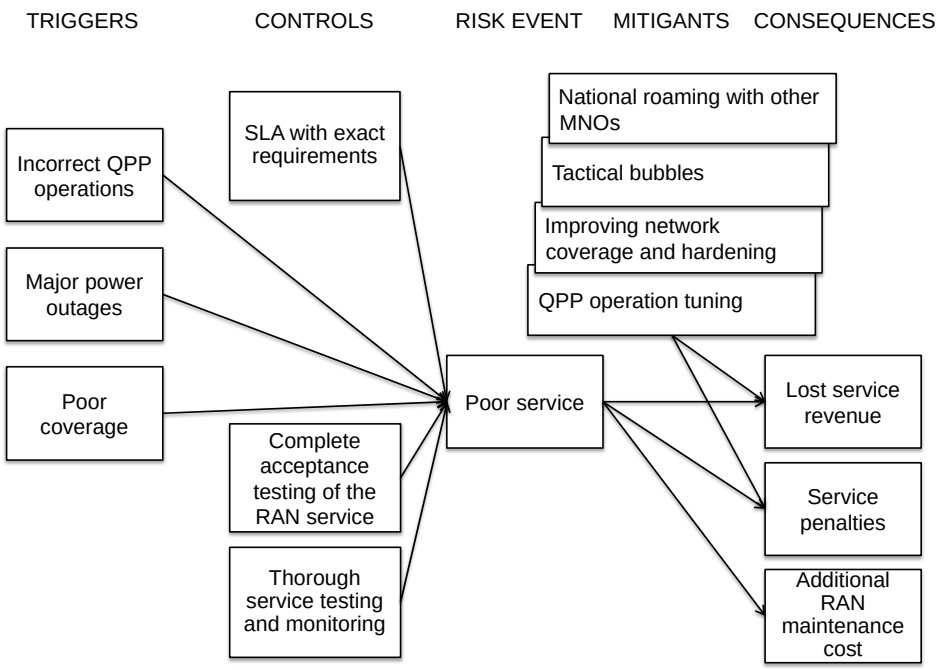

Figure 7. RAN service does not meet needs sub-model

4.4. Cybersecurity

Cybersecurity threats pose a risk to public safety communications due to the authorities' strict information security requirements. The information in public safety communications must be kept confidential in all situations, and data breaches are strictly forbidden. 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 Figure 8).

The first trigger is a cyberattack motivated by public safety users. Because public safety activities contain sensitive information, public safety communications are an attractive target for cyberattacks; in general the public administration and government sector (European Union Agency for Cybersecurity, 2022). Data breaches related to public safety would also be high-profile news in the media, 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 shared between public safety users and the MNO's regular customers, which could provide an attack surface for cyberattacks. Instead, the 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 MNO to assess its cyber-resilience capabilities in relation to public safety requirements – technologies, processes, competencies – and to make any necessary investments and conduct any necessary development activities.

The second control is appropriate screening of the MNO's public safety operations personnel. The MNO must define certain requirements to be considered for and accepted to public safety services 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 impact on other business segments.

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

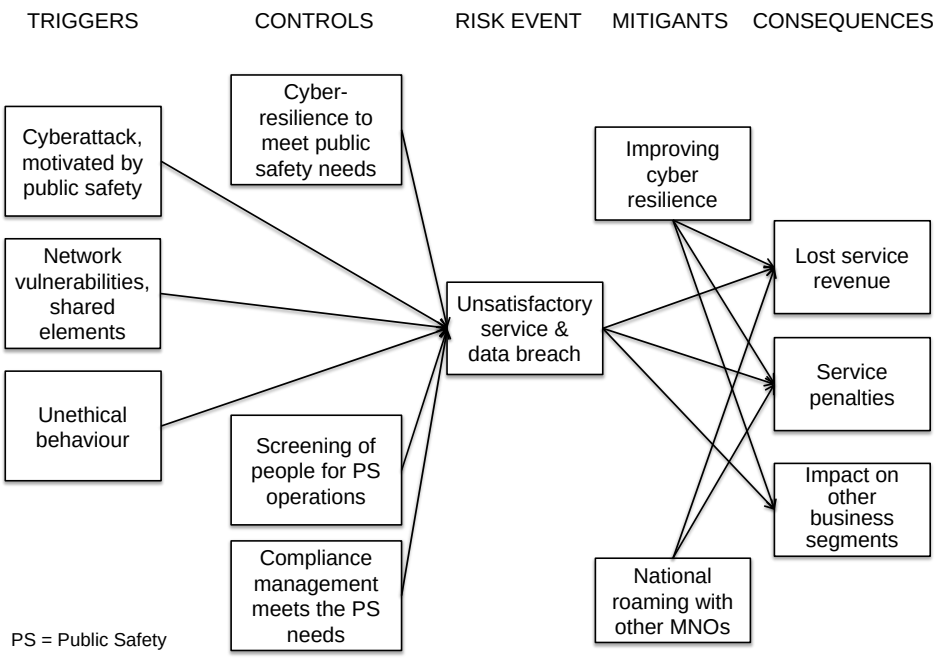

Figure 8. Cybersecurity sub-model

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, core network, communications with command and control rooms and user provisioning. The service

consisting of all these elements must always be available, cyber-resilient and easy to use (Suomalainen et al., 2021; Yarali, 2020).

The MNO is responsible only for RAN services. However, RAN services cannot be used without all other elements being integrated. This creates a 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 Figure 9). 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. New services must enable smooth migration without causing major changes in public safety field operations, such as for fire and rescue services. 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, it may cause delays in the 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 take place between both systems. Some users use a narrowband solution and some use a broadband solution, and these users must be able to communicate with one another. The LMR/MCS gateway is a solution for managing the migration process. Without a properly functioning gateway, service migration cannot begin.

The third trigger is devices not meeting user needs. Public safety operations require special user devices. In general, they must be protected from water, shocks and drops, they must also be usable with gloves and their form factor is larger than that of consumer phones. Another important requirement is device-to-device communications, which entails direct communication between devices without RAN support. The need for this can be seen in 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. These 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 also 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 the risk is lost service revenue due to the delay. 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.

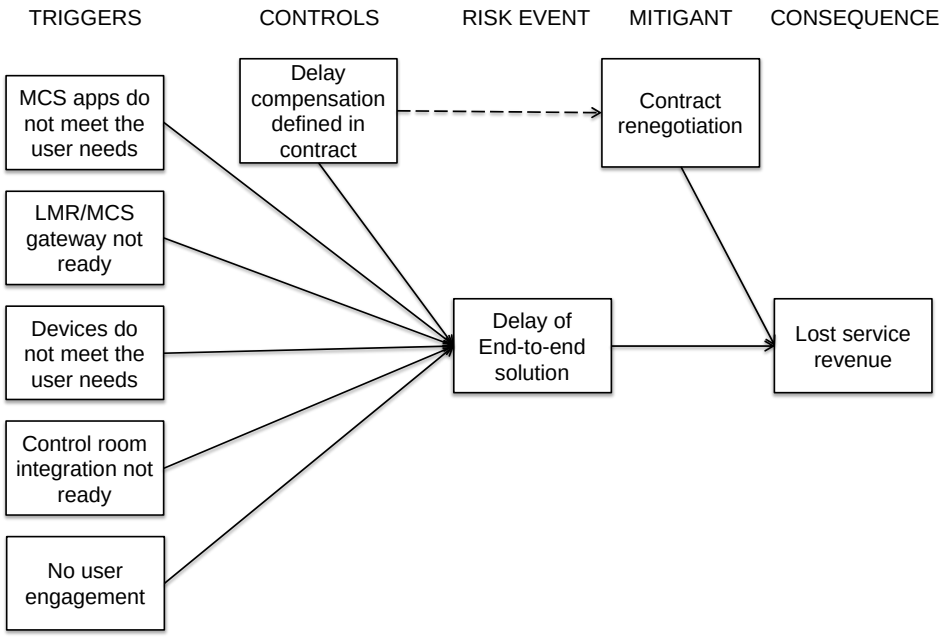

Figure 9. End-to-end solution not ready sub-model

4.6. RAN Building Not On Time or 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 from the MNO (Savunen et al., 2023). Coverage extension and network hardening are also a significant source of the MNO's revenue in the project; therefore, 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 Figure 10). Both are related to the network design work included in the MNO's bid preparation (see Figure 5). Its purpose 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.

The first risk in this sub-model is that the extension of the radio coverage area is not on time or 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 on budget because the implementation of the duplicated links is more difficult than expected. This is related to the duplication of the 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 in an effort 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 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.

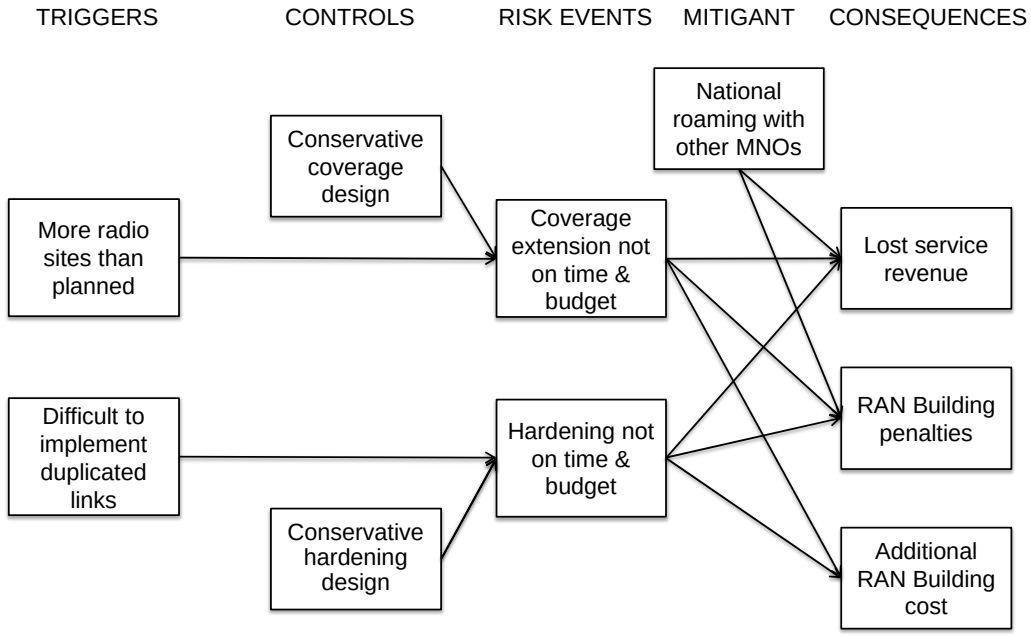

Figure 10. RAN building not on time or on budget sub-model

4.7. Poor Service to Other Customers

The size of the public safety customer segment is only a fraction of MNO's regular customer segments, i.e., consumers and enterprises (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.

The risk event in this sub-model is poor service to other customers, and it has two triggers (see Figure 11). 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, also consumers and enterprises.

Another trigger is 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. This ensures that QPP functions work properly; for example, the network capacity of MNO's regular customers is not unnecessarily limited.

The other 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 deviations as soon as possible through service monitoring.

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

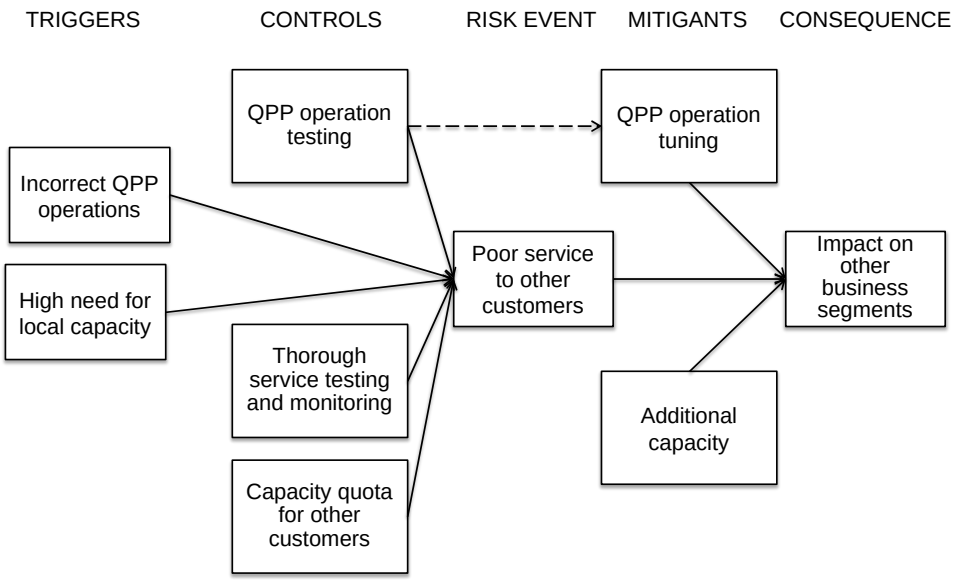

Figure 11. Poor service to other customers sub-model

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 Figure 12). 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 the MNO, this can mean additional investments.

There are four consequences in this sub-model. Three related consequences are lost service revenue, service penalties and 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. These serve to improve the resilience of services.

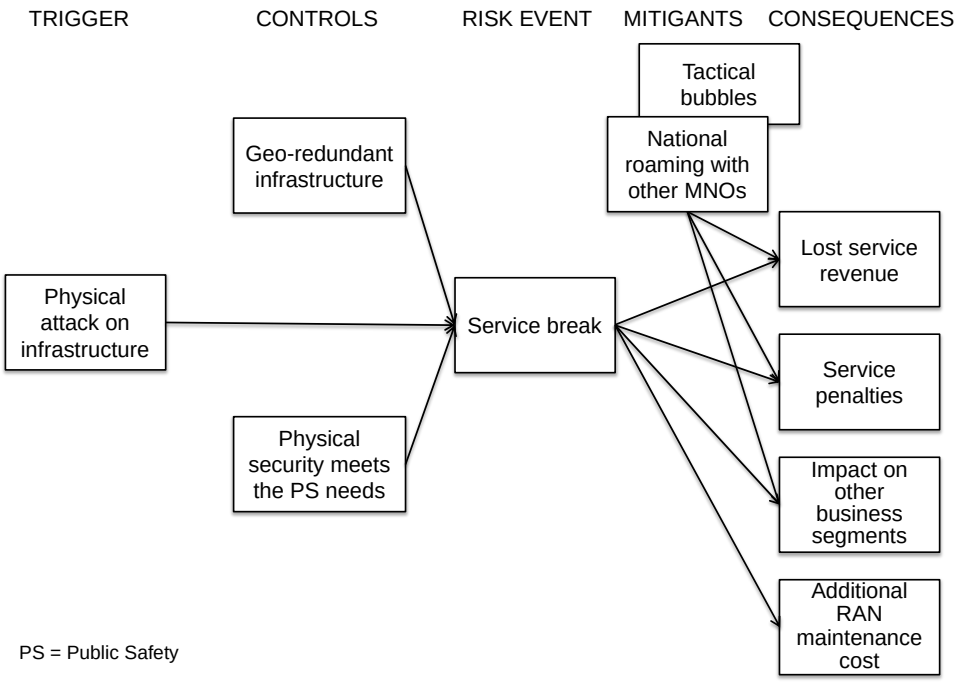

Figure 12. Physical attack sub-model

4.9. Financial Risk Value

All of the business risk consequences of the model represent financial values. They 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 up all of these consequences, as shown in Figure 13, one financial value can be created to illustrate the financial business risk of the model.

If a quantitative model is created, the figures should be scaled to make them comparable. To make the revenue-related figures – lost service revenue and impact on other business segments – comparable with cost-related figures, operating

expenses must be deducted from revenue; in practice, this is done by multiplying the revenue figures by the gross profit margin percentage.

The cumulative financial risk value of the model represents the MNO's risk in the case study's public safety project. However, 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.

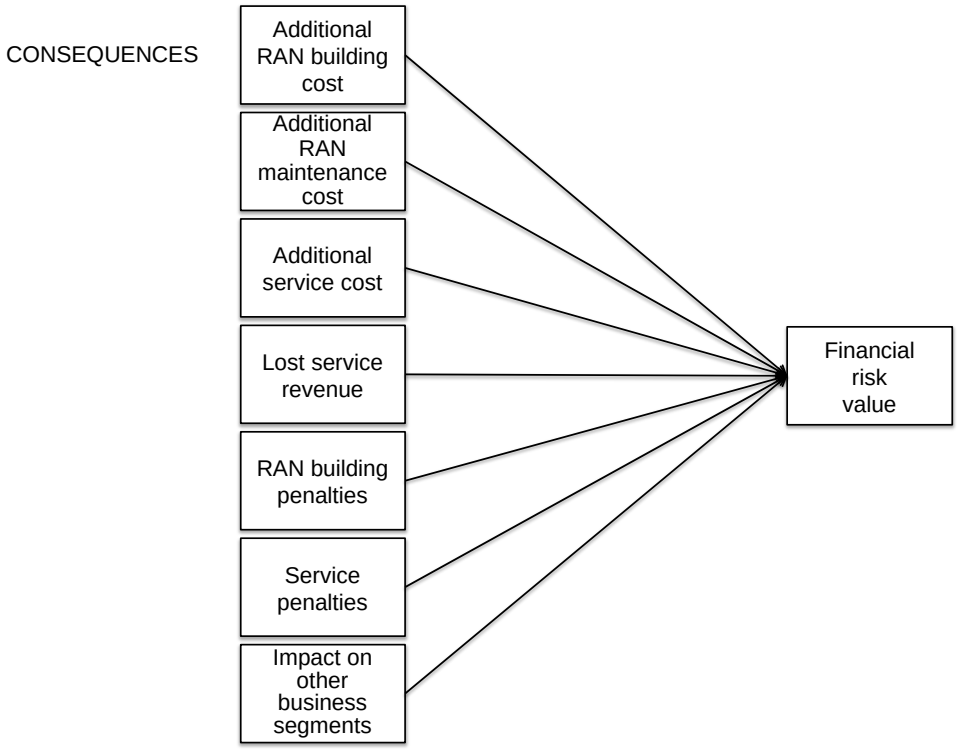

Figure 13. Financial risk value sub-model

4.10. Complete Risk Model

The complete risk model consists of the sub-models described in the previous sections. Figure 14 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.

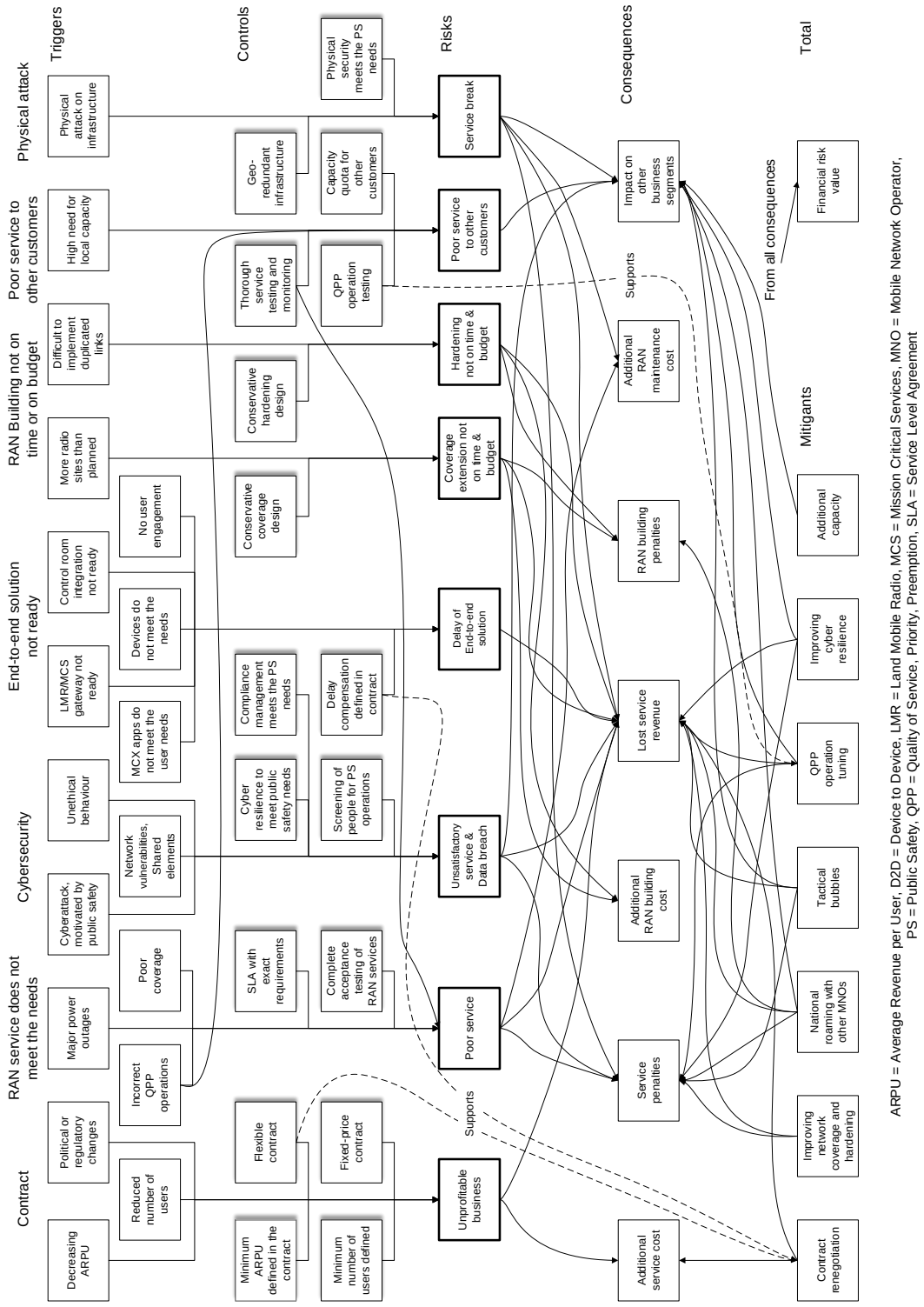

Figure 14. Complete risk model

4.11. Underlying Reasons for Risks

The risk model shows that business risks are a threat to the financial goals of MNO's public safety business, as described in the case study. 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 have a negative impact on the MNO's financial results.

Can we find the underlying reasons for the risks that can cause these negative impacts? Three key reasons that explain the model's risks are 1) contractual arrangements, 2) the demanding service needs of public safety users and 3) the special nature of the public safety segment.

Contractual arrangements here 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 is 10 years, which is a typical order of magnitude for ongoing MC public safety 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's business can be loss-making if the contract is inflexible and significant changes occur in the business environment or the original assumptions 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).

Another key reason for the MNO's business risks is the demanding needs of public safety users. They require communication services to be available always, everywhere and with uncompromised security. Since the goal is to migrate from a narrowband to broadband communications and replace the existing technology with a new one, the services must meet the most demanding needs. Network coverage needs to be extended and network resilience needs to be improved, including cybersecurity (Peltola & Hämmäinen, 2018). The network investments are significant, and there is a risk of exceeding the budget and schedule. The financial risk 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 are another. Therefore, the MNO does not have to allocate the depreciation of network investments to the prices of the services. This reduces the MNO's business risk.

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

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

The special nature of the public safety segment is the third key reason for an MNO's business risks. Public safety is a different customer segment than 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 number of cyber incidents, accounting for 24.2% of all incidents. Furthermore, cyber incidents had the greatest impact in the public administration and government sector across various categories, including reputational, digital, financial, physical, and social impact. In addition to cyberattacks, another possible cyberthreat is unethical behaviour of the MNO's own personnel. Physical attacks on the network infrastructure are also possible. All of these can cause service deviations and data breaches. This can result in financial losses from both public safety and regular MNO business segments.

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

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) the evidence provided by the materialised risks of ongoing public safety mobile broadband projects and 3) how MNOs and PPAs can use the risk model.

The focus of the risk model was the MNO's business risks in public safety mobile broadband services. However, this is not isolated from the 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 sub-model of poor service to other customers, where the sharing of RAN can negatively affect the services of consumer and business customers 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 naturally on the revenue and profit opportunities of the public safety business and synergies with the MNO's other business segments. The MNO can reap benefits from extended network coverage with regular customers, which presents an opportunity to increase the MNO's market share and reduce churn in the mobile services market. The MNO's strategic goals also have an impact. The multi-actor business model is suitable for the MNO's horizontal market strategy, where the MNO targets multiple Industries with similar service requirements in terms of extended coverage, high availability, and security (Savunen et al., 2023). An example is the wireless communications services needed by the smart grid market, driven by decentralised renewable electricity 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 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 is the evidence provided by the materialised risks of ongoing public safety mobile broadband projects. Do the materialised risks justify the risk model? The case study follows the multi-actor shared-network model, the model of all ongoing European projects – ESN, RRF and Virve 2.0. Therefore, we first focus on these projects.

The risk model is primarily derived from the collective knowledge and expertise of an expert panel. While this panel is 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, since the panel members are aware of the unique challenges associated with these projects, it raises concerns about potential bias when using the same projects for model verification. Despite this slight methodological concern, the current lack of alternative similar projects leaves us with limited options for model verification.

Given the unavailability of alternative projects, we have to accept the situation when using expert panels and utilizing the knowledge from ongoing projects becomes the most practical approach. We think that we have balanced the potential limitations against the need for model refinement, while stressing that the future research such focus finding new and not yet started comparable projects for risk model verification, thus ensuring the robustness and reliability of risk assessments models.

The procurement of the French RRF project was completed in October 2022, and the project entered the implementation phase (Donkin, 2022). There has been no public information about the materialised risks of the project, which is understandable, considering the short time that has passed since the beginning of the implementation phase.

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, 2021c). MCS application procurement was also introduced, but it was suspended and scheduled to restart in 2024. The purpose of the postponement was to ensure a seamless interworking of services between the narrowband and broadband networks during the migration period (Erillisverkot, 2021d). 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 risk represented by the end-to-end solution not ready sub-model.

In 2011, the Home Office in the United Kingdom began a project to launch the ESN to replace the TETRA-based Airwave network with 4G/LTE services (National Audit Office, 2019). Two key actors, EE as the MNO and the supplier of public safety solutions, were awarded ESN contracts in 2015 (TED, 2019b; TED, 2019a). The original target was to close the Airwave network by the end of 2019. As of spring 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 decided

to change the deployment model in 2018. Instead of a 'big bang' migration, an incremental model was chosen, which allows the priorities of user organisations to be taken into account (National Audit Office, 2019).

In the ESN project, there have also been challenges in radio-coverage building. EE is in charge of extending its network to include 675 new radio sites. In 2022, this was almost completed; however, EE found that an additional 92 radio sites may be necessary where radio coverage was found to be weaker than originally expected. In addition to EE's radio coverage, the Home Office is responsible for the extended area service of 292 new radio sites. In 2022, none of these were operational (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 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: What is the reason for this?

EE was originally awarded the ESN contract in December 2015, which was due to run until 2021. The value of the contract was 675 million GBP. Due to project delays, the contract was renegotiated and extended in 2019, and it will expire in December 2024. The new value of the extended contract is 895.7 million GBP. The higher price is due to the extended duration of the contract and the new incremental delivery model based on payment milestones (TED, 2019b). This demonstrates the importance of contract renegotiations when original assumptions change, as illustrated by 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 wider areas. FirstNet deployable network solutions – that is, tactical bubbles – were used to connect FirstNet users in problem areas (FirstNet Authority, 2021a). This example illustrates the risk described by the physical attack sub-model and tactical bubbles as a measure to mitigate risk.

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

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

Assuming that an MNO is considering entering the public safety market or is already in the bidding process for public safety services, the risk model can be used as a tool to assess the MNO's 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, the MNO can analyse contractual arrangements and pricing models during contract negotiations.

A PPA can use the risk model for planning the procurement of public safety services. The model can help a PPA, for example, to better understand the business risks of MNOs, especially pertaining to different types of risks. The PPA can

also evaluate different business models from the point of view of the MNO, for example, if trying to avoid challenging models for the MNO.

With the help of the risk model, the PPA can also assess the 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. A reasonable goal is to find balanced risk sharing between the parties.

The risk model in this research has its limitations because it is 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; for this reason, the application of the model is needed in any case, even though we had a quantitative model.

Table 4. Application of the risk model

MNO	PPA
Assessment of operator's business risks	Planning of the public 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	Avoiding risks that increase the contract price

6. CONCLUSION

The current research produced a qualitative model of an MNO's business risks in the public safety service market, following the business model of European next-generation public safety mobile broadband projects. This model is used in three of the five ongoing MNO-involved nationwide mobile broadband projects, where the MNO's role is to provide MC RAN services. An expert panel and the Delphi method were used to create the risk model.

The risk model shows that business risks are a threat to the financial goals of an MNO's public safety business. The potential consequences of the risks are additional costs, contractual penalties, and lost service revenue. In addition, materialised risks can have a negative impact on the MNO's regular business, which could lead to a loss of market share and revenue. All of these have a negative impact on the MNO's financial performance.

Three underlying reasons that explain the MNO's risks are the contractual arrangements, the demanding service needs of public safety users, and the special nature of the public safety segment. In the risk model, these are behind the seven risk domains, which are realised as their own sub-models. By combining all the sub-models, a complete risk model was created.

The risk model follows the causal taxonomy of risk commonly used in causal Bayesian network risk models. Each sub-model includes risk triggers, risk events, risk controls, consequences and mitigants. With the help of risk controls, it is possible to stop or reduce the materialisation of the risk, and mitigants can be used to alleviate the consequences of risks that materialise.

The evidence provided by the ongoing European next-generation public safety projects, in the form of materialised risks, justifies several sub-models of the risk model. This is despite the fact that there are only three projects, one of which has only recently reached the implementation phase. However, there is still no evidence of sub-models related to the project's operation phase because the European projects are not yet in operation.

MNOs and PPAs can use the risk model in procurement processes for public safety mobile broadband projects. An MNO can use the model as a tool to assess the risks in the public safety business if it is considering entering the public safety market or is already in the bid phase of a project. The MNO can benefit by better understanding potential risks in the project, their consequences and their control and mitigation. Correspondingly, a PPA can use the risk model in planning the procurement of public safety services.

This research brings new knowledge about MNOs' business risks in next-generation public safety mobile broadband projects. There is very little previous research on the topic, so this study lays the groundwork for additional research. The results of this paper can also be used in practical projects by MNOs and PPAs.

In general, the migration of public safety agencies to broadband technologies is in its infancy, and the number of ongoing projects is very limited, with only two in operation. However, new projects are starting and new information enables further research to validate these results and expand the research topic.

Research Funding

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

Declaration of Interest

Tapio Savunen works at Airbus Defence and Space in the Secure Land Communications business; Pekka Kekolahti, none; Petri Mähönen none; Heikki Hämmäinen, none; Kalevi Kilkki, none.

Acknowledgements

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

References

3rd Generation Partnership Project. (2020). *3GPP TS 23.251 V16.0.0; Technical specification group services and system aspects; Network sharing; Architecture and functional description (Release 16)*. https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=830

Aspers, P., & Corte, U. (2019). What is qualitative in qualitative research. *Qualitative Sociology, 42*, 139–160. https://doi.org/10.1007/s11133-019-9413-7

Carmona, G. (2021). *Réseau Radio du Futur program, Status Update for TCCA*. https://tcca.info/documents/France-Broadband-update_Gerard-Carmona.pdf

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

FirstNet Authority. (2021b). *FirstNet: The history of our nation's public safety network*. https://www.firstnet.gov/about/history

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

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

Hankintailmoitukset. (2019). *Virve 2.0; Radioverkon (RAN) hankinta*. https://www.hankintailmoitukset.fi/en/public/procurement/16268/notice/18695/overview

Hoffman, M.-L. (2015). *FirstNet Board Oks program's final RFP, eyes January bid solicitation*. GovConWire. https://www.govconwire.com/2015/12/firstnet-board-oks-programs-final-rfp-eyes-january-bid-solicitation/

Home Office. (2021a). *Emergency Services Network: Overview*. GOV.UK. https://www.gov.uk/government/publications/the-emergency-services-mobile-communications-programme/emergency-services-network

Howard, R. A., & Matheson, J. E. (2005). Influence diagrams. *Decision Analysis, 2*(3), 127–143. http://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. http://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, July). 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

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, March 19–23). Smart Grid: A demanding case study for 5G technologies. *2018 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, Athens, Greece, 215–220. 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.

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. 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, August). 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

Productivity Commission. (2015). *Public safety mobile broadband*. Australian Government. https://www.pc.gov.au/inquiries/completed/public-safety-mobile-broadband/report

Reardon, M. (2020, October 22). *AT&T's wireless business thrives amid pandemic*. CNET. https://www.cnet.com/tech/mobile/at-ts-wireless-business-thrives-amid-pandemic/

Roumboutsos, A., & Saussier, S. (2014). Public-private partnerships and investments in innovation: The influence of the contractual arrangement. *Construction Management and Economics, 32*(4), 349–361. https://doi.org/10.1080/01446193.2014.895849

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), 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. (2019a). *Services - 2803898-2019*. https://ted.europa.eu/udl?uri=TED:NOTICE:280398-2019:TEXT:EN:HTML

TED. (2019b). *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, arXiv:2301.03250. https://doi.org/10.48550/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.