TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies
Department of Software Science
Centre for Digital Forensics and Cyber Security

Luisa Caretta Hopp 202107IVCM

APPLICATION OF THE METAGRAPH TO THE AVIATION SUPPLY CHAIN: A CASE STUDY

Master's Thesis

1st Supervisor
Olaf Manuel Maennel
Tenured Full Professor
Tallinn University of Technology
University of Adelaide

2nd Supervisor
Benedict Gross
PhD - LMU München, Germany
Senior Manager - PwC Germany

Tallinn 2023

TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies
Department of Software Science
Centre for Digital Forensics and Cyber Security

Luisa Caretta Hopp 202107IVCM

METAGRAAFI RAKENDAMINE LENNUNDUSE TARNEAHELAS: JUHTUMIUURING

Master's Thesis

1st Supervisor
Olaf Manuel Maennel
Tenured Full Professor
Tallinn University of Technology
University of Adelaide

2nd Supervisor
Benedict Gross
PhD - LMU München, Germany
Senior Manager - PwC Germany

Tallinn 2023

Author's declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature, and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Luisa Caretta Hopp ..... (signature)

Date: May 15, 2023

Abstract

Supply chains have increasingly become targets for various types of cyber attacks. However, they have been difficult to influence beyond direct suppliers with regard to cyber security requirements. This thesis introduces the graph-theoretic construct of the conditional metagraph to enhance cyber security maturity in the supply chain. The conditional metagraph is able to represent the supply chain as a system of systems on which algebraic calculations can be performed. Additionally, it allows the integration of supplier and component characteristics, which include cyber security properties. The graph-theoretic construct of the supply chain is tested for its applicability through a case study on the aviation industry. The illustration of five scenarios demonstrates how the use of the conditional metagraph increases the cyber security maturity of the supply chain choice and whether it provides support in the event of successful cyber attacks on suppliers. With the help of experts from the aviation industry, the applicability of the conditional supply chain is validated and challenged.

Annotatsioon

Tarneahelad on muutunud üha enam erinevat tüüpi küberrünnakute sihtmärgiks. Siiski on neid olnud raske mõjutada küberturvanõuete osas väljaspool otseseid tarnijaid. Käesolevas magistritöös tutvustatakse tingimusliku metagraafi graafikuteoreetilist konstruktsiooni, et tõsta küberturvalisuse küpsust tarneaehelas. Tingimuslik metagraaf suudab kujutada tarneahelat kui süsteemide süsteemi, millel saab teha algebralisi arvutusi. Lisaks võimaldab see integreerida tarnijate ja komponentide omadusi, mis hõlmavad küberturvalisuse omadusi. Tarneahela graaf-teoreetilist konstruktsiooni testitakse selle kohaldatavuse suhtes lennundussektori juhtumiuuringu abil. Viie stsenaariumi illustratsioon demonstreerib kuidas tingimusliku metagraafi kasutus tõstab küberturvalisuse küpsust tarneahela valikus ning kas selle kasutamine pakub tuge tarnijate vastu suunatud edukate küberrünnakute puhul. Lennundustööstuse ekspertide abil valideeritakse ja vaidlustatakse tingimusliku tarneahela kohaldatavus.

List of abbreviations and terms

AC domain	Access Control Domain (CMMC)
A-ISAC	Aviation Information Sharing and Analysis Center
AMC	Acceptable Means of Compliance
APT	Advanced Persistent Threat
B2B	Business to Business
BSI	Federal Office for Information Security (German: Bundesamt für Sicherheit in der Informationstechnik)
C3PAO	Third Party Assessment Organisations
CAAC	Civil Aviation Administration of China
CSASC	Cyber Security Across Supply Chain
CMM	Component Maintenance Manual
CMMC	Cyber Security Maturity Model Certification
COTS	Commercial-Off-The-Shelf
C-SCRM	Cyber Supply Chain Risk Management
CUI	Controlled Unclassified Information
DIB	Defence Industrial Base
DoD	Department of Defence
DSS	Decision Support Systems
EASA	European Union Aviation Safety Agency
ECCSA	European Centre for Cybersecurity in Aviation
ENISA	European Union Agency for Cybersecurity
FAA	U.S. Federal Aviation Administration
FCI	Federal Contract Information
HCI	Human-Computer Interaction
ICT	Information and Communication Technology
IEC	International Electrotechnical Commission
IPC	Illustrated Parts Catalogue
ISO	International Organisation for Standards
ISMS	Information Security Management System
ITU	International Communication Union
MRO	Maintenance, Repair, and Operations

NATO	North Atlantic Treaty Organisation
NIST SP	National Institute of Standards and Technology Special Publication
OEM	Original Equipment Manufacturer
OPM	U.S. Office for Personnel Management
OSINT	Open Source Intelligence
Part-IS	Implementing Regulation (EU) 2023/203 of Information Security
PSOA	Private Sector Offensive Actors
RCT	Randomized Controlled Trial
SMBs	Small to medium-sized businesses
SoS	System of Systems
USA	United States of America
VPN	Virtual Private Network

Table of Contents

List of Figures

This version of the document is for digital distribution only,
as some of the figures are not legible in print.

List of Tables

1. Introduction

In December 2020, the attack on SolarWinds' product Orion caused a global outcry across industries. Supposedly secure organisations (as e.g., the Pentagon) that were secured to regulatory standards and above were compromised by an attack on their supply chain via an infected software update.[1, 2] Although many organisations have achieved cyber resilience on an organisational and technical level at various stages of maturity through cyber security certificates, the supply chain had not previously been in scope.[1, 2] In the EU and at NATO level are no certification standards tackling cyber security in the supply chain until the day of submission of this thesis. Organisations are confronted by the need to understand a system that was accepted as a black box and exploited as a cost-saver. The attack on SolarWind also demonstrated the potential of economies of scale by choosing key suppliers. By integrating malicious code into the production process of the IT management software solution Orion, the attackers were able to penetrate 18.000 companies.[1, 2] However, this is not the first incident in which the supply chain has been exploited. Other attacks focused on targeting selected companies with higher maturity through multiple less secure suppliers, e.g., small to medium-sized businesses (SMBs) as they don't have the financial budget to invest in cyber security. Airbus was the victim of several sophisticated espionage attacks around 2018.[3] By breaking into suppliers' virtual private network (VPN) connections, the attackers were able to penetrate Airbus' internal system and obtain sensitive and militarily confidential information on the design structures of engines and avionic details.[3] In addition to the corruption of integrity and confidentiality of products, the availability of service can be affected through the supply chain. This happened to Boeing in November 2022, where a ransomware attack on a supplier led to flight disruptions. As the supplier's responsibility lies in the navigation and flight planning tools, this resulted in pilots not being informed of potential hazards on given flight routes. However, flight safety reportedly was not in jeopardy.[4] To better understand and analyse supply chain attacks, the European Union Agency for Cybersecurity (ENISA) published a taxonomy which is described in the threat landscape of supply chain attacks from 2021.[5] It states that half of the supply chain attacks were conducted by Advanced Persistent Threat (APT) groups which are well-known in the security community.[5] Additionally, other actors exist on the market, such as Private Sector Offensive Actors (PSOAs), who sell exploits to governments and are held responsible for the SolarWind malware, among other APTs.[4] Thus, a high niveau of sophistication and unlimited

resources can be assumed on the attackers' side. The situation is alarming, especially for critical infrastructures that can put people's safety at risk. However, in industries such as aviation, safety regulations have been in place for several decades.[6] The integration of cyber security in the aviation industry is just a recent transition which will be ongoing for the next three years. Safety and (emerging) cyber security properties of indirect aviation suppliers are tackled based on a trust relationship with direct suppliers. ENISA points out that 62% of the attacks on customers benefit from exploiting trust in their suppliers.[5] Hence, even if an aircraft manufacturer has implemented cyber security, how can they determine with certainty that the globally interconnected supply chain has the required cyber security maturity?

A supply chain is a global integrated complex system of systems (SoS) but still seen in "a chain-like fashion"[7, 8]. Thus, certifying supply chains or designing a supply chain security standard is proving difficult. The major challenge with regulating a supply chain is that a cyber security maturity (which comes in different forms (e.g., ISO[9] or NIST[10])) of suppliers in a complex globally distributed network is to be imposed by a single supplier (e.g., an organisation which provides a critical infrastructure and thus falls under a certain cyber security regulation). However, this imposing supplier has often no knowledge and no influence over indirectly allied suppliers (e.g., the supply chain as part of the competitive advantage). This thesis addresses an approach to make the seemingly intangible property of cyber security of the suppliers tangible and influenceable by applying a graph-theoretical construct onto the SoS.

The graph-theoretic construct of a conditional metagraph integrates cyber security maturity on the supply chain and applies algebraic calculations on the graph to select suppliers above a certain threshold for cyber security maturity or to analyse data breaches in the supply chain. As the aviation industry has implemented traceability through its safety-related regulations, the industry allows to identify producers of components in finalised products even years after construction.[6] This feature is beneficial to realistically apply a graphic structure on an exemplary supply chain. Further, it lays the foundation for a feasible implementation of a conditional metagraph in the aviation industry on its transition to comply with the new cyber security regulation as, e.g., the Part-IS[11]).

Hence, the thesis represents an intersection of three disciplines: The aviation industry, supply chain cyber security, and graph theory which are explained in Chapter 2. An overview of the three fields holds the next subsection by introducing the research gap and novelty of this thesis. Chapter 3 introduces the structure of the case study and the final mapping of the graph structure to the aviation supply chain is explained in Chapter 4 and illustrated through scenarios in Chapter 5.

1.1 Research Gap and Novelty

Regulators at national and inter-governmental levels are increasingly focusing on supply chain cyber security. The Department of Defense (DoD) of the USA implemented the first supply chain certification model (Cyber Security Maturity Model Certification (CMMC)) which aims for a minimum level of cyber hygiene in their Defense Industrial Base (DIB).[12] This standard is convertible to international standards of Information Security Management System (ISMS) implementation (ISO 27001[9], NIST[10], or IT Baseline Protection Manual[13]). Critical infrastructures as military organisations complying with the CMMC benefit from early regulatory requirements regarding protection against system failures. This has encouraged them to address cyber security at an organisational level from early days on.[12]

However, the civil aviation industry entered its transition to cyber security integration in response to a rise of cyber incidents in the industry, as systems in the aviation industry are also increasingly based on software (e.g., aircraft or airport systems).[14] In addition to digitalisation, the aviation supply chain is characterised by rationalisation to a few close aircraft component suppliers which are given more responsibility by the aircraft original equipment manufacturer (OEM). This comes hand in hand with the OEM focusing on core capabilities and internationalisation through a global operating supply chain.[7]

The metagraph structure allows to represent complex structures through the use of non-sequential, parallel paths (the so called metapaths consisting of multiple simple paths) and elements which have multiple dependencies towards each other (instead of elements, sets of elements are integrated to the edges' vertices). Propositions complement edges and are filtered to create different views on top of the graph structure. Hence, the mapping of component properties, suppliers' cyber security maturity niveaus, and the information exchange between suppliers is represented through a conditional metagraph.[15]

The following research gaps have been identified: Increasingly sophisticated attackers emerge through the supply chain, particularly through SMBs or through highly connected suppliers. On the one hand, we have in the context of aviation an industry's sluggishness due to certification procedures of safety regulations that is counter-intuitive to cyber security controls.[6] On the other hand, the industry has the feature of traceability.[6] The identified research gap in the aviation industry is a missing cyber security implementation which must be fulfilled in the upcoming years.[11] The traceability capability makes the industry attractive to graphic application. Further, we have a global supply chain that includes different regions with diverse cyber security standards to meet. Additionally, the relationship of trust between suppliers has no real evidence that indirect suppliers

implement cyber security and is exploited by attackers.[5] So we have a harmonisation potential and the lack of certification standards scoping the supply chain. Finally, we have a graph-theoretic construct that has the potential to map interconnected organisations, but has not yet been applied to supply chains.[15, 16]

Based on the research gaps discovered, the following research questions arose, which will be answered subsequently in this thesis:

1. How does the conditional metagraph apply to the aviation supply chain?
2. How can the metagraph integrate cyber security on the aviation supply chain?
3. Has the metagraph benefits which enhance cyber security maturity of the aviation supply chain?

By answering the research questions, the thesis introduces the following novel intersection of the three combined disciplines: The aim is to build a conditional metagraph structure which establishes cyber security maturity in the exemplary supply chain of the aviation industry and which holds the following properties:

- Integration of different cyber security certification standards from a global supplier base
- Calculation of purchasing options which are more secure than others based on different thresholds of cyber security maturity
- Integration of supply chain components and communication between suppliers as foundation for the thresholds of cyber security maturity
- Calculation of alternative purchase options in case a supplier loses its certification or brakes down
- Adjustment of purchase decisions in case a supplier increases in cyber security maturity
- Analysis in case an attacker has infiltrated a supplier from perspective of component security (integrity), information exchange (confidentiality), and overall importance for the supply chain (availability)

Therefore, this thesis tries to close the identified gap through a graph-theoretic analysis: As the importance of SolarWinds' lack of cyber security maturity in combination of its component criticality would have been visible before it was too late; the supplier of Boeing would have needed to at least include employee training against e.g., ransomware attacks to get accepted as Boeing's supplier; and the identification of critical information exchanges between Airbus and its suppliers would have forced the suppliers to provide advanced interface and infrastructure security controls.

2. Related Work

This chapter introduces cyber security in supply chains in academia and continues with cyber security regulations. Special regulations of the aviation industry are shortly introduced but the main characteristics of the aviation supply chain are extracted from the interviews presented in Chapter 3.

2.1 Supply Chain Cyber Security

Cyber security and supply chains are not an unknown combined topic to academia. The first paper analysing cyber security and supply chains was published in 2000.[17] Through the years, the topic expanded in academic discourse.[17] Ghadge et al. (2019) examine the progress of supply chain cyber security over a period of 20 years up to 2019. They conduct a systematic literature review of 41 relevant papers.[17]

Several definitions around the notion of cyber security and the supply chain are represented in the literature.[17] Cyber security consists of a "collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organisation and user's assets. In which, organisation and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment"[18] according to the ITU definition.[19, 18] Based on the code of law of the USA (section 3542, Chapter 35, title 44), information security is also defined as "protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality and availability".[20] Gasser and Morrie add "[...] disruption or misdirection of the services they provide"[21]. The last definition includes explicitly purchased goods and services in supply chains, e.g., the navigation tool of the Boeing supplier and the Orion update.[4, 1] Further, best practices to obtain a cyber resilient environment define cyber security hygiene. These best practices include continuous routines on technical, organisational and economical level.[22, 23]

The supply chain is defined as "a collection of different organisations that align their

business processes, goals, objectives and some components of their systems to third party organisations, suppliers, consumers and partners"[24, 25]. It includes all services, goods, and information which are moved between the point of origin and the point of consumption.[24] Further, many authors use notions as digital supply chain, electronic supply chain, IT system or cyber supply chain.[26, 27, 28, 29] In summary, these conceptualizations describe the influence and integration of information and communication technology (ICT) in the supply chain. These terms are becoming increasingly blurred with the traditional term supply chain, as today's supply chain is hardly independent of ICT.[28] In the following, the thesis uses the term "supply chain", by which the author implies that the terms mentioned before are included. Sobb and Turnbull (2020) describe the supply chain as a SoS which is difficult to define or model. The use of global suppliers in combination with emerging technologies and growing agility enhances the aim of increasing timeliness, profitability, and efficiency. But it comes with the cost of depending on factors such as international logistics, personal relationships, integrated cyber-physical systems, artificial intelligence, smart contracts, and Internet of Things which let the supply chain suffer from unique cyber security risks.[8, 30, 14] As supply chains are the digital consolidation of different organisations through communication links [31], on the one hand, members on these chains become vulnerable through the shared security arrangements and information.[32] On the other hand, the increasing visibility, information exchange and agility caused by digital technology improve the accuracy of cyber attack defense measures.[33]

Following Li et al. (2015) into economics, they suggest that financial performance is improved precisely through collaboration with organisations in the supply chain in terms of risk (information) sharing.[33] Simon and Omar (2019) analyse the differences of over- and underinvestment through uncoordinated cyber security investments in the supply chain by assuming strategic and non-strategic attackers. A coordinated cyber security investment indicates that every supplier in the supply chain invests at the supply chain optimal level into cyber security. This also indicates that organisations benefit from other suppliers' investments and having other suppliers' profiting from own cyber security investments. However, the ideal coordinated investment is dependent on an optimal central planner.[34]

To understand the need for cyber security, Ghadge et al. (2020) describe different "points of penetration"[17] within the supply chain. These points refer to vulnerabilities within the supply chain that are split into human, technical, and physical perspectives. An example of technical points of penetration are legacy systems or outdated software. Human vulnerabilities are the employees who can become victims of social engineering or attackers themselves. The physical point of penetration is the local access to physical infrastructure.[17] Environmental disasters mentioned in the literature are not considered here as they are not included in the definition of cyber security. The author limits the definition of

cyber security to malicious or unintentional attacks on systems that have been influenced by people or ICT. Further, Ghadge et al. (2020) address the impact of cyber attacks in the supply chain.[17] With reference to Dolgui, Ivanov, and Sokolov (2018) they describe the consequence as a "cascading ripple effect" from the organisation (primary propagation zone) into the supply chain (secondary propagation zone) and ending in the society (tertiary propagation zone).[17, 35] The primary propagation zone includes disruption in quality, continuity, or productivity of operations while the secondary propagation zone indicates damage to reputation and impairment of future cooperation. The tertiary propagation zone includes negative effects on the business sector or society as cyber incidents could influence the safety of products.[17, 35] Dolgui et al. (2018) end with a conceptual model for supply chain cyber security systems, which combines organisational, IT, and supply chain security systems and is shown in Figure 1.[17]

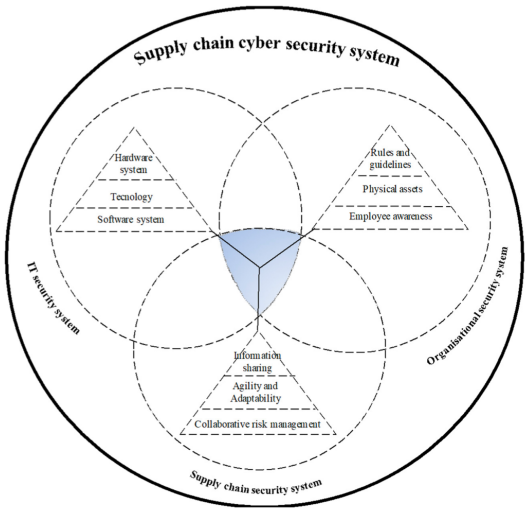


Figure 1. *Conceptual Model for Supply Chain Cyber Security Systems ([17, Fig.10, p. 233])*

A different perspective is the division of supply chain cyber security into logistic, organisational, and technical parts. This is supported by Urciuoli and Hintsa (2017) pointing out the most vulnerable part of the supply chain laying in the transit or logistics. This section of the supply chain should also be considered in terms of cyber security, as attackers could use logistics or cargo in transit for physical intrusion.[36]

Another important definition is the cyber supply chain risk management (C-SCRM) which is described as a combination of the expertise in cyber security, supply chain management and enterprise risk management. The overall aim of the C-SCRM is to contain the spread of supply chain attacks causing intellectual, and financial property theft, competitive espionage, or disruption of operations.[28] This term is filled by various standards published and prescribed by government actors, such as institutions or agencies (e.g. NIST or IT-basic protection).[25] Boyson et al. (2021) compared implemented practices and

procedures of the NIST cyber security framework (C-SCRM) in a longitudinal perspective of a decade. They showed that certain practices and procedures had a positive impact on enterprise breach profiles by focusing on their threat profiles.[28] Thus, the implementation of standards is a first step towards a cyber attack resilient supply chain. Le and Hoang (2016) conclude that maturity models are a foundation for a stronger security model as they are useful for management and security compliance. However, they lack the potential to measure quantitatively for an actionable assessment of security experts.[37] Cheung, Bell, and Bhattacharjya (2021) conducted a literature review on 98 papers about supply chains focusing on cyber security. They describe that different cyber security standards and policies for various sectors exist instead of an accepted standard for cyber security in supply chains.[38, 39, 19]. Relevant standards will be described in more detail in the next Subsection 2.1.1.

The literature explicitly distinguishes between supply chain cyber security and cyber security across supply chains (CSASC).[40] On the one hand, supply chain cyber security focuses on solution approaches within an organisation that is part of a supply chain. Here, the focus is primarily on protecting assets according to confidentiality, integrity, and availability (C-SCRM)[41]. On the other hand, CSASC goes beyond corporate boundaries and involves the tertiary stage of Ghadge et al. (2020) and Dolgui et al. (2018) ripply effects (e.g. reputational damage).[40, 17, 35] In the academic literature, security has received less consideration due to its lack of quantifiability and the complexity of supply chains and cyber security until now.[40] The authors conclude by presenting a theoretic framework for CSASC aimed at cyber resilience throughout the supply chain. The framework is based on mandates and supplier relationships as well as supplier size and standards in cyber security. Special emphasis is given to the feedback loop, which allows the framework to adapt to changing attack environments.[40, 41]

A little digression into the grey literature shows the current state of CSASC in studies related to practice. A significant part of cyber attacks occur through supply chains.[42] SMBs (500 or fewer employees) are of particular importance here, as they have access to a proportionately large amount of important information in relation to their organisational size. In addition, SMBs often have less cyber security precautions due to lower resource availability.[43] However, it should be noted that SMBs offer fewer points of attack than larger suppliers due to their smaller size.[32] Wong et al. (2022) empathize a strong focus on employee cyber security hygiene (the human aspect w.r.t. Ghadge et al. (2020)[17]) as the backbone of SMBs lies within their human workforce.[44] Increasingly, companies conduct security audits with their business partners.[32, 40, 43] The use of standards is one way to introduce cyber security hygiene in the supply chain in an auditable way.[45, 22]

Topping et al. (2021) conduct an analysis of supply chain C-SCRM standards for critical infrastructure in the US, the UK, and EU. They conclude that a unified taxonomy for C-SCRM standards is missing for different regions and for different authorities. Based on a comparison of the different regulators and standards of the three regions mentioned above, they introduce a first taxonomy draft. This draft is a first step towards a unified C-SCRM framework and can be extended in the future.[46] The next subsection

2.1.1 Cyber Security Standards in the EU and the USA

There are standards established that are internationally recognized and those that are mandated at the national level by business partners or the government. If governments want to enforce standards, they first need a legal basis. ENISA sets minimum requirements for cyber security strategies of EU member states through NIS directives.[47] The NIS directive EU 2016/1148 is the first EU cyber security strategy adopted by member states in 2018.[48] Germany had already implemented some points of the NIS directive with its IT Security Act 1.0, which has been in force since 2015. With the entry into force of the IT Security Act 2.0, the focus is also placed on cyber security in supply chains.[49, 50] In addition, the EU commission has adopted in 2020 a NIS2 directive proposal which also focuses on the supply chain cyber security.[51] On national level, the first supply chain law passed in 2022 in Germany which addresses the supply chain but in the context of human rights.[52, 53] However, on the basis of a first supply chain law, it is now being tested to what extent it could also be applied in other areas, such as cyber security.

In Europe, standards in the area of information sharing, critical infrastructure protection, and basic risk management exist.[46] The ISO/IEC 27000 family is an internationally recognized standard for information security management systems.[45] This standard was adopted by Germany and further refined in the IT Baseline Protection Manual[1]. It further includes additional minimum requirements as e.g., for interface security controls which partly covers the interface between suppliers.[55] This standard is mandatory for operators of critical infrastructures, public authorities. Since the enactment of the IT Security Act 2.0 the standard is also required for companies with a special public interest in Germany. To date, only critical infrastructure operators and public authorities have been audited for implementation of and compliance with the standard. In general, all companies in Germany can follow this standard and be certified and re-certified in a reoccurring period of time (e.g., three years for the ISO/IEC standard).[49, 50, 9] Airports are included in the definition of a critical infrastructure only above an annual turnover of over 20 million passengers.[4] Hence, in Germany only the four largest airports are counted as critical

[1]The translation of the German term $IT\text{-}Grundschutz$ is used in this thesis based on ENISA.[54]

infrastructures. Safety critical operations are participated in every airport and are also increasingly connected to the cyber space with little focus on cyber security.[56] Willemsen and Cadee (2018) describe such potential attack vectors where physical security could be eliminated through cyber related exploits. They suggest an airport-specific platform specific cyber security risks management.[56]

For the aviation industry, the EU has established the European Union Aviation Safety Agency (EASA) in 2003 with focus on flight safety and safety regulations within the aviation supply chain which.[57] Aviation safety regulations force OEMs of aircraft types to obtain a type certificate for assuring their airworthiness safety.[6] This establishes traceability of each component to its producer(s) but also slows down the adaption process of the supply chain to acute cyber security risks.[6] Airworthiness (safety)[2] is defined by the EASA as "[...] the fitness of an aircraft for flight in all conditions for which it has been designed, and to which it may therefore be exposed. This means that during the whole lifecycle of the aircraft, for all types of operations and in all environments, the structure of the aircraft must remain unchanged."[58] Hence, cyber security impacts the airworthiness safety of an aircraft as aircraft systems depend increasingly on software and hardware.[14]

With increasing cyber security focus, the EASA introduced the first regulation in Europe demanding for cyber security in the aviation industry and in particular in its supply chain [11]. The new implementing regulation (EU) 2023/203 of October 27, 2022 has a transformation phase of three years. Its annex, referred to as Part-IS, includes first cyber security requirements for the aviation industry and authorities to consider [59]. From 2025 to 2026 on, all organisations and authorities within the industry have to comply with the act. It provides requirements of identifying and managing information security risks which could influence ICT and data of the civil aviation industry.[11] Ukwandu et al. (2022) analysed current cyber attack trends in the aviation industry.[14] Main threats emerge from APTs cooperating with state actors to perceive intellectual property and to "monitor, infiltrate, and subvert other nations' capabilities"[14]. Additionally, ENISA proposes a taxonomy of supply chain attacks which is categorised in attack vectors and attacked assets of the suppliers and customers.[5] Table 1 shows the four categorisations. Martínez and Durán (2021) are consulted to show the significance of these attack techniques. They describes that 85% up to 97% of the code used in the supply chain origins from repositories of third-party software and open source code frameworks.[2] Having the described attack vectors and assets in mind, the fact that an aircraft type certificate does not allow for major changes in the supplier base in case a component turns insecure, increases the impact potential of possible attack vectors. Moreover, then various if not all produced aircrafts of that type turn vulnerable.

[2]Safety is added to "Airworthiness" in this work to clearly distinct between safety and security.

Table 1. *ENISA Taxonomy of Supply Chain Attacks [5, p. 7, Table 1]*

Suppliers		Customers	
Attack Techniques to Compromise the Supply Chain	**Suppliers' Assets Targeted by Supply Chain Attack**	**Attack Techniques to Compromise the Customer**	**Customers' Assets Targeted by Supply Chain Attack**
Malware Infection	Pre-Existing Software	Trusted Relationship	Data
Social Engineering	Software Libraries	Drive-by Compromise	Personal Data
Brute-Force Attack	Code	Phishing	Intellectual Property
Exploiting Software Vulnerability	Configurations	Malware Infection	Software
	Data	Physical Attack or Modification	Processes
Exploiting Configuration Vulnerability	Processes		Bandwidth
	Hardware	Counterfeiting	Financial
Open-Source Intelligence (OSINT)	People		People
	Supplier		

In the USA, the DoD published a maturity standard in 2020 which should strengthen the cyber security hygiene against the loss of Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) of its supply chain.[60] The DoD has struggled since 2013 to implement an accepted standard within its supply chain focusing cyber security. The DoD did not want to discourage its suppliers and introduced as little bureaucracy as possible in the integrating process of the CMMC into its contracting. The DoD assumed certain basic security practices and reduced the initial supplier requirements by 30% compared to what authorities should comply with. They further it avoided external auditing of compliance to reduce the costs for its DIB.[61] Cyber security maturity in the supply chain did not increase as hoped and after the hack of the U.S. Office for Personnel Management (OPM) in 2015, the NIST SP 800-171 was adopted in 2016, expanding the controls to include those that had been assumed before.[61, 62] The situation did not improve and resulted in the development of the Cyber Security Maturity Model Certification (CMMC), which not only expanded the controls, but for the first time included external certified auditors, called third party assessment organisations (C3PAO).[12] The frustration in the DIB regarding the costs was enormous, especially for SMBs.[61] On November 4, 2021, the second CMMC version (CMMCv2) was released and eased the external auditing process by C3PAOs for suppliers.[63] Additionally, it also reduced the number of required practices to implement. Henceforth, the CMMCv2 is mirroring the NIST SP 800-171 to its second maturity level and NIST SP 800-172 on its third maturity level. Both maturity niveaus are accessible in the NIST standards:[10, 64].

The history of the CMMC exemplifies that the implementation of a supply chain standard is constrained even for authorities with military background. The DoD's insistence led to over-regulation that had to be eased eventually. Hence, the first CMMC version (CMMCv1) requests more extensive cyber security practices than the second version. To visualise an exemplary cyber security maturity certification, the CMMCv1 and CMMCv2 are shortly introduced. Figure 2 shows the different maturity niveaus and the specific number of cyber security practices for each version of the CMMC. The maturity levels of CMMCv1 consists of an ISMS on maturity level 3 and maturity niveau 5 is reached by implementing

171 practices. The highest maturity level of CMMCv2 ends with less than 120 practices. Additionally, the CMMCv1 is structured in 17 domains which contain cyber security practices and processes shown in Figure 3. Figure 3 visualises further the eliminated domains for the CMMCv2.

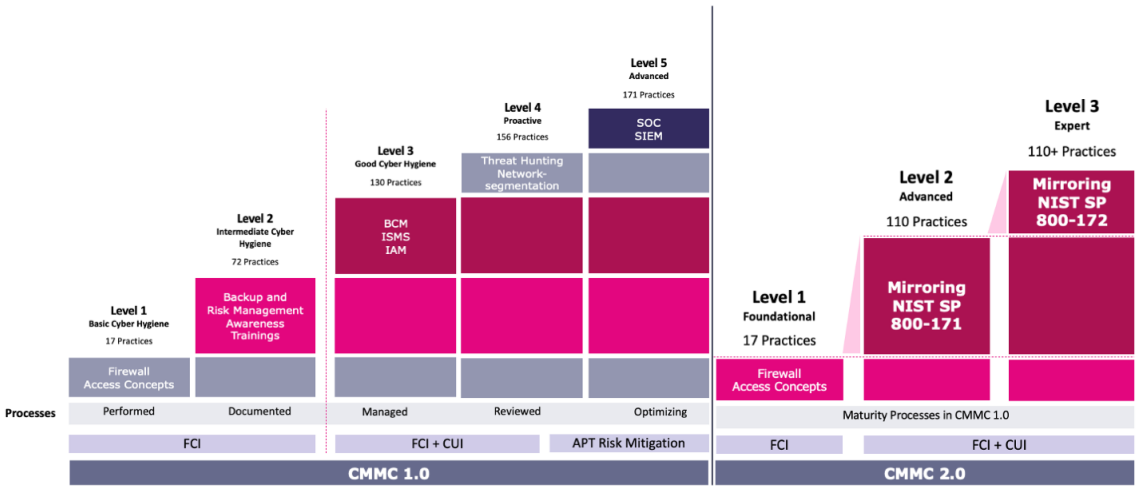


Figure 2. *Niveaus of the Cyber Security Maturity Certification Model: CMMCv1 and CMMCv2*

The structure of the CMMCv1 is based on domains that are categorised by subject. This differs from the approach of the IT Baseline Protection Manual. Here, the requirements are not sorted by thematic domains but by target objects. The various building blocks of the IT Baseline Protection Manual are split in two groups of process and system building blocks.[49] Thus, not only different levels of granularity are evident for different certification standards, but also different approaches in the categorisation of cyber security practices, which exemplary support the research findings of [38, 39, 19].

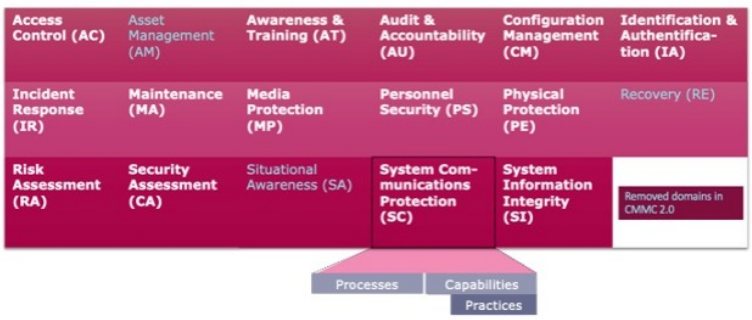


Figure 3. *Domains of the Cyber Security Maturity Certification Model (CMMCv1)*

2.2 Graph-Theoretic Construct Metagraph

Graph structures are commonly used to represent systems that contain multiple entities. A graphical construct represents a system by using a set of *nodes* or *vertices* which are connected through a set of edges or arcs (the notion *edge* will be subsequently used). However, existing graph structures cannot adequately represent the relationships between sets of entities what induced Basu and Blanning (1994) to introduce a new graph structure, the metagraph in the middle of the 90s.[65]

Essentially, a graph structure offers two advantages: First, it provides the possibility of visualising complex systems, and second, it has formal properties that allow calculations on structural behavior of the system, e.g., connectivity, cyclicity, and dependency. [15, 65] These properties have been analysed for different graph-theoretic constructs. Based on an example which was brought up by Basu and Blanning (1994), the different graph constructs are introduced, in order to discuss the metagraph's differences and advantages to previous graph structures [65, 15]. After a presentation of the formal properties, the previous applications of the metagraph over the last 20 years are summarized.

2.2.1 Benefits and Differentiation to Existing Graph Structures

The metagraph is able to represent "directed relationships between sets of elements"[65, p. 14] in a non-sequential way. To demonstrates the benefit of the metagraph, alternative graph structures are introduced: Starting with the traditional simple graphs and directed graphs moving towards "more recent structures"[15, p. 4] as the hygraph and higraph. The focus lies on graph structures which are able to analyse and visualise. Thus, graph structures such as entity-relationship or data flow diagrams will be excluded as they only hold for graphical representation.[65] The example based on Basu and Blanning (2007) [15] will consist of a company developing an antivirus software with the following variables categorised into input, intermediate, and output elements:

Input Variables:

- *Pri* = the sales price of an antivirus software licence
- *Vol* = the sales volume of the antivirus software licence
- *Wage* = the prevailing wage rate of the software developers

Intermediate Variables:

- *Rev* = the realized revenue, depending on price (*Pri*) and volume (*Vol*) of the sold antivirus software licences
- *Exp* = the expense, which depends on the volume sold (*Vol*) and the wage rate (*Wage*)

Output Variables:

- *Prof* = the realized profit through the sale of the antivirus software licences
- *Notes* = payable notes as a result of borrowings to cover expenses

The example shows interconnectivity between these three categories of variables as it is assumed that

- *Pri* and *Vol* define *Rev*,
- *Vol* and *Wage* define *Exp*,
- *Rev* and *Exp* define *Prof* and *Notes*,
- *Exp* defines *Notes*.

Those relationships show that *Notes* is determined through *Rev* and *Exp* or only through *Exp*. Subsequently, *Prof* is also output along with *Notes* from *Exp* and *Rev*. Hence, the dependencies of the different entities in the system are intervened with each other and lead to a limited amount of redundancy in calculation procedures.[15, pp.4]

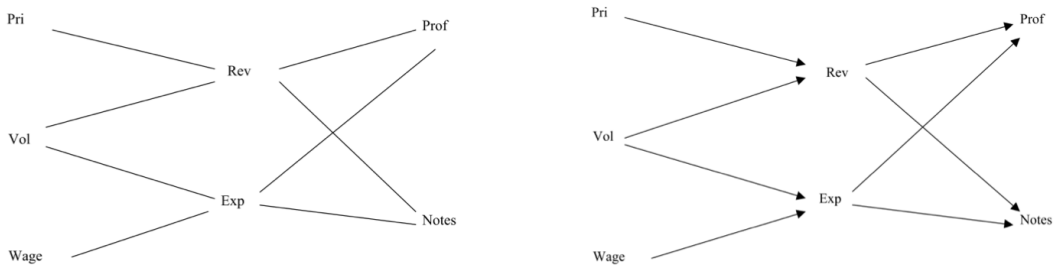


Figure 4. *Simple Graph (left) and Directed Graph (right)[15, pp. 5]*

Based on Berge (1985), a simple graph and a directed graph shown in Figure 4 visualise the example [66]. Another exemplary simple or directed graph is a bipartite graph which describes two disjoint sets of elements connected through edges with each other and holds different propositions on how the elements in the sets are connected through edges (e.g., being independent or biclique).[67] The graphs in Figure 4 consist of seven nodes which are connected through edges with each other representing their interconnectivity.[66, 15] A pair of two variables is directly connected through an edge (as e.g., *Pri* and *Rev*) which

symbolises an unordered pair of nodes. Further, the simple graph also shows indirect dependencies which are called paths as e.g., *Pri* and *Vol* define *Rev* which determines *Prof*. As the simple graph does not visualise the direction of dependencies, *Pri* is also indirectly interconnected with *Vol*. Thus, the indirect determination and co-input cannot be differentiated through a simple graph. The directed graph overcomes this problem by visualising the direction of dependencies or determination through ordered pairs of nodes which are presented through arrows. Thus, a differentiation between *Pri-Vol* and *Pri-Prof* is possible. But the directed graph holds another problem as it is not clear if *Pri* alone is able to determine *Rev* or if *Vol* and *Pri* are both needed. This dependency is possible to visualise with an AND/OR graph. As this graph structure is getting very complex and complicated for large sets of data it will not further be analysed.[15, 66]

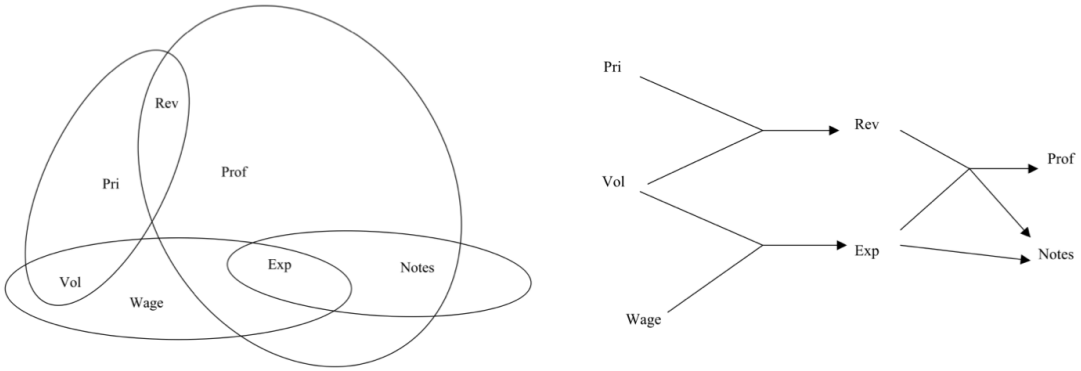


Figure 5. *Hypergraph (left) and Directed Hypergraph (right)[15, pp. 6]*

Berge came up with another approach, the so-called hypergraph in 1989 which solves partly the problem of interdependencies of multiple variables. The hypergraph allows to connect multiple nodes into a shared relationship.[68] Thus, the *Vol*, *Pri* and *Rev* are visualised in one relationship. The disadvantage is the missing determination of node direction which the simple graph had as well. This is solved by Ramaswami, Sarkar and Chen (1997) through the use of a directed hypgergraph which is the combination of a hypergraph and a directed graph [69]. Both graphs are shown in Figure 5. The directed hypergraph consists of edges which have a tail containing the input nodes and a head containing the output nodes. Exemplary *Pri*, *Vol* represent the tail and *Rev* the head of an edge. Thus, it is possible to define an interconnectivity between *Pri*, *Vol* with *Prof*.[15] Except for the different nomenclature of invertices and outvertices, and different fields of application [15] the only difference between metagraphs and hypergraphs is that a metagraph involves disordered edges for its metapaths, while hypergraphs initially assume ordered edges. However, these ordered hypergraphs can be converted to disordered edges according to Ward et al [70]. As for the subsequent thesis unordered pairs of edges are necessary, the metagraph will be preferred over the hypergraph.

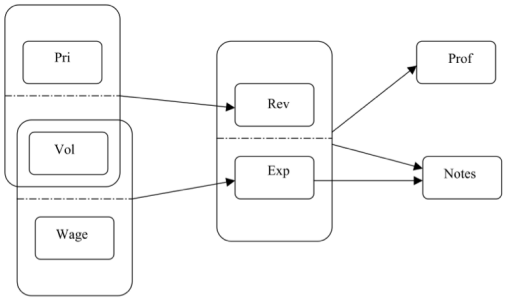


Figure 6. *Higraph [15, p. 8]*

The last graph structure which makes a further step towards the metagraph, is the hierarchical graph, the so-called higraph.[15] Harel (1988) describes the components of a higraph as blobs which include elements and further subblobs (see Figure 6). It has the benefit of having edges ending in subblobs which causes flexibility on the one hand but on the other an increased analytical complexity to analyse.[71] Combining the analytical potential of a directed hypergraph with the generalised graph structure of a higraph makes the metagraph a graph-theoretic structure which holds visualisation and analytical properties.[15, 65] Having the flexibility but less analytical complexity of a higraph, the metagraph is finally introduced and shown in Figure 7. [15]

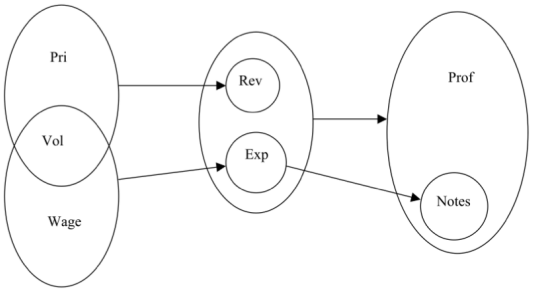


Figure 7. *Metagraph[15, p. 9]*

The metagraph consists of ordered pairs of sets of elements which are connected through edges. Additionally, the metagraph can be transformed to a conditional metagraph for which the edges hold attributes and thus, provide qualitative and quantitative analysis.[65] The graph structure is able to represent the differences between *Rev* and *Exp* determining *Prof* and *Notes* as well as only *Exp* defining *Notes* in two edges. Thus, the metagraph visualises the interconnectivity assumptions which were defined for the example. Based on the adjacency matrix it is possible to analyse the system of sets of elements by using addition and multiplication operators to obtain the closure matrix. The closure matrix builds the foundation for the connectivity, transformation, and attributed properties of a metagraph which are explained in the following Subsection 2.2.2.

2.2.2 Formal Properties

The **algebraic structure of the metagraph** consists of matrices which are the foundation for the subsequent algebraic calculations [15]. The following definitions 1-3 - 14 of the formal representation of a metagraph are cited from Basu and Banning (2007). In order to enable comprehensibility or in case a deeper insight into the referenced documents is desired, the same variables are used as in [15]. Furthermore, the example from the previous section is used to illustrate the formal representation of the metagraph.

> DEFINITION 1 The $generating\ set$ of a metagraph is the set of elements $X = \{x_1, x_2, \ldots, x_n\}$, which represent variables of interest, and which occur in the edges of the metagraph.[15, p. 15, Definition 2.1]

> DEFINITION 2 An edge e in a metagraph is a pair $e = \langle V_e, W_e \rangle \in E$ (where E is the set of edges) consisting of an invertex $V_e \subset X$ and an outvertex $W_e \subset X$, each of which may contain any number of elements. The different elements in the invertex (outvertex) are coinputs (cooutputs) of each other.[15, p. 15, Definition 2.2]

> DEFINITION 3 A metagraph $S = \langle X, E \rangle$ is then a graphical construct specified by its generating set X and a set of edges E defined on the generating set.[15, p. 15, Definition 2.3]

The metagraph of the aforementioned example is defined as $S_{ex} = \langle X_{ex}, E_{ex} \rangle$ with a node set of

$$X_{ex} = \{Pri, Vol, Wage, Rev, Exp, Prof, Notes\}$$

and the edges as an edge set of

$$E_{ex} = \{\langle e_1 = \{Pri, Vol\}, \{Rev\}\rangle, \langle e_2 = \{Vol, Wage\}, \{Exp\}\rangle,$$
$$\langle e_3 = \{Exp\}, \{Notes\}\rangle, \langle e_4 = \{Rev, Exp\}, \{Prof, Notes\}\rangle\}.$$

The tools for algebraic constructs and operations on the metagraph are the adjacency and incidence matrices. Both represent fully the metagraph structure and are also used in traditional graph structures. The adjacency matrix is a square matrix which includes for each element in the generating set of the metagraph a column and a row. The matrix is filled with sets of triples in each cell, defining a metagraph edge for the two nodes (column, row)

showing their co-inputs, co-outputs and the edge itself. The exemplary adjacency matrix of the aforementioned example (Figure 7) is shown in Table 2. Using defined algebra for adjacency matrices allows us to calculate connectivity trough the metagraph. The addition of two adjacency matrices with the same generating set of two metagraphs symbolises the union of two metagraphs. A multiplication of two adjacency matrices of two metagraphs with the same generating set allows a representation of paths containing two edges, the first one from the first adjacency matrix and the second edge from the second adjacency matrix. Hence, the multiplication of an adjacency matrix by its nth power (A^n) consists of simple paths ($h(x_i, x_j)$ with length n) connecting the nodes x_i and x_j with each other.

Table 2. *Exemplary Adjacency Matrix of the Metagraph*

	Rev	Exp	Prof	Notes
Pri	$\langle\{Vol\}, \varnothing, e_1\rangle$	$\varnothing$	$\varnothing$	$\varnothing$
Vol	$\langle\{Pri\}, \varnothing, e_1\rangle$	$\langle\{Wage\}, \varnothing, e_2\rangle$	$\varnothing$	$\varnothing$
Wage	$\varnothing$	$\langle\{Vol\}, \varnothing, e_2\rangle$	$\varnothing$	$\varnothing$
Rev	$\varnothing$	$\varnothing$	$\langle\{Exp\}, \{Notes\}, e_4\rangle$	$\langle\{Exp\}, \{Prof\}, e_4\rangle$
Exp	$\varnothing$	$\varnothing$	$\langle\varnothing, \varnothing, e_3\rangle$, $\langle\{Rev\}, \{Notes\}, e_4\rangle$	$\langle\varnothing, \varnothing, e_3\rangle$, $\langle\{Rev\}, \{Prof\}, e_4\rangle$
Prof	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$
Notes	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$

The incidence matrix shown in Table 3 consists of a column for each edge and a row for each node of the generating set of the metagraph. This matrix shows a node as an invertex of the corresponding edge as a -1 and an outvertex as a $+1$. Cells for nodes not being connected to the corresponding edge are filled with $\varnothing$.

Table 3. *Exemplary Incidence Matrix of the Metagraph*

	e_1	e_2	e_3	e_4
Pri	-1	$\varnothing$	$\varnothing$	$\varnothing$
Vol	-1	-1	$\varnothing$	$\varnothing$
Wage	$\varnothing$	-1	$\varnothing$	$\varnothing$
Rev	+1	$\varnothing$	$\varnothing$	-1
Exp	$\varnothing$	+1	-1	-1
Prof	$\varnothing$	$\varnothing$	$\varnothing$	+1
Notes	$\varnothing$	$\varnothing$	+1	+1

The **connectivity properties** of the metagraph consist of the metapath definition which differentiates from simple and directed graphs. The path of a directed graph connects source nodes to target nodes in a sequence of edges. This definition does not hold for metapaths as they differ from simple paths through three characteristics. The *metapath* definition from Basu and Blanning (2007) is the following:

> DEFINITION 4 Given a *metagraph* $S = \langle X, E \rangle$, a $metapath$ $M(B, C)$ from a source $B \subset X$ to a target $C \subset X$ is a set of edges $E' \subseteq E$ such that
>
> 1. each $e' \in E'$ is on a simple path from some element in B to some element in C,
> 2. $[\bigcup_{e'} V_{e'} \setminus \bigcup_{e'} W_{e'}] \subseteq B$,
> 3. $C \subseteq \bigcup_{e'} W_{e'}$.[15, p. 16, Definition 2.5]

To explain the distinction between metapaths and simple paths based on an example, the definition of a *simple path* is briefly introduced:

> DEFINITION 5 A *simple path* $h(x, y)$ from an element x to an element y is a sequence of edges $\langle e_1, e_2, ..., e_n \rangle$ such that
>
> 1. $x \in invertex(e_1)$,
> 2. $y \in outvertex(e_n)$, and
> 3. for all e_i, $i = 1, ..., n-1$, $outvertex(e_i) \cap invertex(e_{i+1}) \neq \varnothing$.
>
> [15, p. 15, Definition 2.4]

An exemplary metapath $M_{ex}(B_{ex}, C_{ex})$ of S_{ex} between the sets of elements $B_{ex} = \{Pri, Vol, Wage\}$ and $C_{ex} = \{Prof, Notes\}$ has the following metagraph edges:

$$M_{ex}(B_{ex}, C_{ex}) = \{\langle\{Pri, Vol\}, \{Rev\}\rangle, \langle\{Vol, Wage\}, \{Exp\}\rangle, \\ \langle\{Rev, Exp\}\{Prof, Notes\}\rangle\}.$$

The metapath consists of two edges ($\langle\{Pri, Vol\}, \{Rev\}\rangle$ and $\langle\{Vol, Wage\}, \{Exp\}\rangle$) which are not connected through a sequence. Concluding from Definition 5, they are not representable in a simple or directed path.

Hence, a metapath connects sets of elements (which can also include singleton sets) rather single elements in case of a simple or directed path. Further, it consists of a set of edges rather a sequence of edges and allows to analyse and present interconnectivity in complex systems which can appear parallel. The third difference, is that the source set of

elements includes all input which is needed. There is no co-input for a metapath (see (2) of Definition 4). However, co-outputs can exist for a metapath as the target set of elements is only a subset of the metapath outvertex (see (3) of Definition 4).[15] Further, the metapath dominance defines metapaths which exclude superfluous input elements and edges. Thus, having a dominant metapath origins from an edge- and input-dominant metapath. Only when both properties hold, the metapath is dominant and further non-redundant.

> DEFINITION 6 $Edge\text{-}dominance$ is given for a metapath $M(B, C)$ between two sets of elements B and C in metagraph $S = \langle X, E \rangle$ when no proper subset of $M(B, C)$ is also a metapath from B to C.[15, p. 27, Definition 3.1]

Edge-dominance thus ensures that only necessary edges are included. Input-dominance assures that only the necessary inputs appear in a metapath.

> DEFINITION 7 $Input\text{-}dominance$ is given for a metapath $M(B, C)$ between two sets of elements B and C in metagraph $S = \langle X, E \rangle$ when there is no metapath $M'(B', C)$ such that $B' \subset B$.[15, p. 27, Definition 3.2]

Dominance of a metapath $M(B, C)$ is given when it is edge- and input-dominant [15, p. 27, Definition 3.3]. The exemplary metapath $M_{ex}(B_{ex}, C_{ex})$ is both input- and edge-dominant and thus, a dominant metapath. Ward et al. (in print) analyse recently the differences of a hypergraph and a metagraph in finding input-dominant hyperpaths and metapaths. They proof that for both types of graph structures the input-dominant hyperpaths or metapaths are NP-hard even for acyclic hypergraphs and metagraphs. However, metapath calculations without input-dominance are linear solveable.[70] Further, the dominant metapath is also *non-redundant*.

> DEFINITION 8 $Non\text{-}Redundancy$ is given for an edge e in a metapath $M(B, C)$ between two sets of elements B and C in metagraph $S = \langle X, E \rangle$ when there is some $Y \subset C$ such that for every metapath M' from B to Y there is a $e \in M'(B, Y)$.[15, p. 28, Definition 3.4]

Concluding from Definition 6 and 8 a metapath with all of its edges being non-redundant is edge-dominant: $M(B, C)_{Non-Redundant} \iff M(B, C)_{Edge-Dominant}$.[15, p. 29, Theorem 3.1]

The last two terms which are related to the connectivity of the metagraph's sets of elements are the *bridge* and the *cutset*.

DEFINITION 9 A set of edges E' is a $cutset$ between two sets of elements B and C of a metapath $M(B, C)$ in a metagraph $S = \langle X, E \rangle$ such that there is no metapath from B to C in $S' = \langle X, E \setminus E' \rangle$ with one constraints:

1. There is also no proper subset of E' being a cutset between B and C.[15, p. 29, Definition 3.5]

DEFINITION 10 A singleton cutset between two sets of elements B and C is a $bridge$.[15, p. 29, Definition 3.6]

Another view on the metagraph can be generated through the use of **attributed metagraph properties**, the conditional metagraph. In this case, the edges are associated with attributes which can have different forms (qualitative, quantitative and boolean types). Based on the definition which attributes should hold, the view (so-called context) is generated on which than similar to the projection the underlying metagraph's metapaths are matched to the existing edges and sets of elements in the context.[15] This thesis uses the qualitative type of attribute. Subsequently this type of attribute is explained. A qualitative attribute of the metagraph is attached to each metagraph edge. As these attributes are non-numerical, they can be used for algebraic analysis of the metagraph structure rather for arithmetic operations. They allow to restrict the selection of metapaths. Unlike normal graphs, where attributes can also be used, the metagraph allows attributes to be represented in two ways. On the one hand there is the graphically visualisation of the qualitative attributes on the edges which enables a more informative representation of the attributes and corresponding edges of the metagraph. On the other hand, the algebraic analysis uses the mapping of the qualitative attributes as a sub types of elements of the generating set on the invertex of the edge. The benefit of this representation is the integration of the qualitative attributes into the adjacency matrix. Thus, the qualitative attributes can be analysed as any other element in the generating set X. For the two different representations holds the same semantic equivalence, which causes no significant changes of the basic metagraph's algebraic constructs and operations when adding qualitative attributes. In order to lead over to the conditional metagraph, a certain form of qualitative attributes is presented. The so-called *proposition* is a qualitative attribute with the property that can either be satisfied or not. If this property is part of an edge's invertex it must be satisfied to be deployed in the metagraph. Propositions can be added to more than one edge and an edge can have zero or up to a finit number of properties. The generating set of a conditional metagraph can

contain elements of different types of variables which also include the propositions. The *conditional metagraph* is formally defined as follows by Basu and Blanning (2007):

> DEFINITION 11 A $conditional\ metagraph$ is a metagraph $S = \langle X_p \cup X_v, E\rangle$, in which X_p is a set of propositions and X_v is a set of variables, and:
>
> 1. $\forall e' \in E, V_{e'} \cup W_{e'} \neq \varnothing$;
> 2. $X = X_v \cup X_p$ with $X_v \cap X_p = \varnothing$ such that $\forall p \in X_p,\ \forall e' \in E$, if $p \in W_{e'}$, then $W_{e'} = \{p\}$.[15, p. 55, Definition 5.1]

Thus, a simple metagraph introduced in the beginning of this chapter is a conditional metagraph without any propositions, $X_p = \varnothing$.

Further, a conditional metagraph must hold three constraints: First, the generating set must be split in a set of variables and a set of propositions. These two sets must be disjoint. Second, the union of invertex and outvertex has to be non-empty. Third, if an outvertex of an edge includes a proposition, no other element is allowed in the outvertex. Based on these three constraints, the conditional metagraph gives the possibility to build the aforementioned *context*.

> DEFINITION 12 Given a conditional metagraph $S = \langle X_v \cup X_p, E\rangle$, a set of propositions $P \subseteq X_p$ that are known to be true and a set of propositions $Q \subseteq X_p$ that are known to be false, we define a $context\ K(P, Q, S)$ as a conditional metagraph derived from S as follows:
>
> 1. For any edge $e' \in E$ containing a proposition $p \in P$ simplify the edge by deleting p; if the resulting edge has a null in- or out-vertex, delete the edge;
> 2. For any edge $e' \in E$ containing a proposition $q \in Q$ in either vertex, delete the edge (only the edge and q are deleted, not the other elements in the edge's vertices).[15, p. 56, Definition 5.2]

A context simplifies a conditional metagraph by dropping edges which are not valid based on a set of propositions P which are satisfied and a set of propositions Q which are not satisfied. Undetermined propositions as $p \in X_p \setminus (P \cup Q)$ are kept in the context for further algebraic analysis. Further, the first enumeration of the definition 12 is needed to delete edges, which contain not only satisfied propositions $q \in Q$ but also satisfied propositions $p \in P$. In order to investigate connectivity properties of the edges holding satisfied and undetermined attributes, a *conditional metapath* is introduced:

DEFINITION 13 Given a conditional metagraph $S = \langle X_v \cup X_p, E \rangle$ a source $B \subseteq X_v$ and a target $C \subseteq X_v$, a $conditional\ metapath$ is a set of edges $CM(B, C) = \{l'_l, l = 1, ..., L\}$, forming a *conditional metapath* from $B \cup X_p$ to C. The set of relevant propositions is defined by [15, pp. 57, Definition 5.3] as

$$\alpha = \left(\bigcup_{l=1}^{L} V'_l \right) \cap X_p.$$

This may be partitioned into two subsets, the set of input propositions

$$\beta = \left(\bigcup_{l=1}^{L} V'_l \setminus \bigcup_{l=1}^{L} W'_l \right) \cap X_p$$

and the set of intermediate propositions is

$$\gamma = \left(\bigcup_{l=1}^{L} V'_l \right) \cap \left(\bigcup_{l=1}^{L} W'_l \right) \cap X_p.$$

The conditional metapath uses any needed proposition being part of edges which connect two sets of elements. Thus, all propositions which have to be satisfied to connect two sets of elements are part of the metapath between these sets. Properties can appear in the invertex of at least one edge and can also be part of the outvertex of at least one edge. In case properties appear only in the invertices, they are part of the input properties. Being as well part of outvertices, a proposition is an intermediate proposition which is dependent on other elements' values and thus cannot be known before execution of the conditional metapath. [15]

The **metagraph transformation** gives the possibility to explore subsets of the metagraph through *projection*. Thus, only the sets of elements of the subsets are used in the projection and the metapaths between these sets of elements equal the underlying metagraph's metapaths.[15] This can increase the visualisation capability of the metagraph as views for specific users of the metagraph can be generated taking different perspectives of the metagraph into focus. Projections hold for conditional metagraphs if a dominant conditional metapath exists.[15]

DEFINITION 14 Given a metagraph $S = \langle X, E \rangle$, and $X' \subseteq X$, a metagraph $S' = \langle X', E' \rangle$ is a *projection* of S over X' existing if:

1. For any edge $e' = \langle V', W' \rangle \in E'$ and for any $x' \in W'$ there is a dominant metapath $M(V', \{x'\})$ in S, and

2. For every $x' \in X'$, if there is any dominant metapath $M(V', \{x'\})$ in S with $V' \subseteq X'$, then there is an edge $\langle V', W' \rangle \in E'$ such that $V = V'$ and $x' \in W'$.
3. No two edges in E' have the same invertex. [15, p. 34, Definition 4.1]

The last paragraph of the formal properties of the metagraph includes the investigation of **sub-metagraphs and three properties**. The conditional metagraph can hold three properties: independency, full connectivity, and non-redundancy.[15] Full connectivity and redundancy describe different capabilities of the conditional metagraph to connect specific input elements with specific output elements based on different interpretations I (or possible sets holding true values) of satisfied propositions' logical expressions. An interpretation shows the different forms of satisfied. Full connectivity allows to connect two sets of elements based on every interpretation I. Connectivity only connects two sets of elements based on some interpretations I. Redundancy allows to connect two sets of elements through more than one option or non-redundancy only at most one option. Thus, full connectivity and non-redundancy of a conditional metagraph are given, when for every interpretation I only one edge-dominant metapath exists.[15, pp. 62] Also *cycles* are possible to be represented in a metagraph and influence the connectivity. However, as long as they appear through edges cyclically connecting elements rather than propositions, it is possible to implement them in a metagraph. Further, the *inverse* of the metagraph can be analysed which swaps the edges and sets of elements. [15] Additionally, a sub-metagraph $Lille$ embedded in a metagraph S holds the property of independence if it connects to S only through its input and output elements rather than through its intermediate elements. [15]

2.2.3 Fields of Application

Metagraphs have been already implemented in various fields which are shortly introduced. Basu, Blanning, and Shtub (1997) introduced metagraphs as possibility to model hierarchies and help in chosing right models in decision support systems (DSS) as those often contain large model bases [72]. Through the use of views of the model base, the interaction with a DSS is simplified and increases efficiency in individual decision making as well as in collective ones (via multiple views). [72] Further, assumptions in decision modeling were supported by metagraph views. The metagraph is able to help model management in cases of model evaluation and selection as well as project or workflow management. [73, 74] In 2003, Basu and Blanning introduced the metagraph to workflow decomposition and synthesis because the metagraph's connectivity properties (i.e., full connectivity, redundancy, and independency) explain structural behavior.[75, 76] Additionally, the metagraph

is applied to resource allocation being impacted by business process redesign and workflow system analysis from perspective of the transaction management.[76]

In 2007, Basu and Blanning published a book and briefly summarized their fields of application to date how they applied the edges: For the implementation into the area of data bases, they used the invertex of an edge to demonstrate a key attribute and the outvertex to show the content elements. In the area of model bases, they would use the model inputs as invertices and model outputs as edges' outvertices. Implementing metagraphs in rule bases, would attach the antecedent variables to the invertices of its edges and to its outvertices the consequent variables. Last but not least, the workflow systems are represented through metagraphs with edges containing "information flows entering a workstation"[15, p. 11ff.] as invertices and "information flows emanating from workstations as outvertices"[15, p. 11ff.]. [15]

Finally, other introduced areas of application for the metagraph's decomposition and synthesis of processes are organisations which are linked to their business partners via electronical connection, or having employees which are able to work regardless of their geographical location. The third application is an organisation which is structured in constant project work. Hence, it includes teams which work temporarily on problem solving tasks.[75] On the one hand, these are approaches towards an inter-organisational use of the metagraph structure. A supply chain has not yet been applied to the metagraph structure. On the other hand, there are approaches to apply the metagraph construct as an information security method onto computer network models. These approaches apply different rules on a graph structure connecting operating systems, sets of software, and local area networks.[16] Further research applies the metagraph construct in 2018 on IoT networks as a solution to execute compatibility checks of IoT configurations with organisations' policies [77]. Continuing research practises on specific network programming paradigm, as e.g., the Formally-Verifiable Policy-Defined Networking which includes a verifiability mechanism that can be included in the metagraph structure [78].

Concluding, the metagraph structure has been already applied to information security research questions but limited to configuration policies of organisational networks. Hence, the metagraph structure has not been implemented on a supply chain with an inter-organisational perspective on cyber security aspects.

3. Research Design

The research aim of this thesis is to apply the graph-theoretic construct metagraph with cyber securtiy attributes to the aviation supply chain. The research objective of the methodology is to explain and evaluate the graph-theoretic construct metagraph for applicability in the aviation industry's supply chain.

This chapter introduces the research methodology decision using Saunders' Research Onion [79] in the Section 3.1. Subsequently, the systematic construction of the research method is described, which includes procedures for designing and testing the metagraph's application to the aviation supply chain.

3.1 Methodological Justification

According to Saunders (2007), the research method can be justified by answering six questions. [79] Figuratively, one speaks of an onion, whose core (research techniques and procedures, see Section 3.2) is approached through the decision for the research philosophy, the research approach, the research strategy, used data types, and the time horizon.

The question of how a metagraph can be applied to the aviation industry supply chain is grounded on requirements formulated by the aviation industry experts and thus implements an interpretive philosophy approach. In addition, the metagraph application to the aviation supply chain depends on the author's conceptual contribution, since the construct of the metagraph has not yet been applied to supply chains. However, the author's contribution is structured and framed by systematic procedures of the research methodology. Thus, the research methodology should be replicated by any researcher which eliminates the choice for a pragmatist's philosophy, see [79]. Further, this thesis uses the deductive research approach by grounding the research on already existing theory [80] of the graph-theoretic construct metagraph (see [15]).

An experiment, a case study, or the design science research present appropriate options for the research strategy of this thesis[79, 81, 82]. Three requirements justify the chosen research strategy: Firstly, the research strategy should examine a contemporary event [79] as the metagraph should be applicable to current aviation supply chains. Secondly,

the research strategy does not need to control the behavior of the event, as the supply chain should not be changed by the metagraph [82, p. 9]. Third, the research strategy should focus on in-depth investigation of one event rather investigating various events [83]. The second requirement eliminates the experiment as research strategy, as an experiment requires control over the behavior of the event. The design science research methodology provides guidance on how to design a problem solution in a "systematic way"[81, p. 85]. Further, it focuses on the design process as an object of study. This could be applicable for the design process of the metagraph construct. Both, design science research and a case study describe an iterative process for the design of the research outcome. [84, 81] However, this thesis addresses the question of how a metagraph construct is mapped to a specific target environment. The interaction between the graph-theoretic construct and the reality of an aviation supply chain is the central focus of the research question. Simone (2009) and Stake (2005) define a case study as an "in-depth exploration"[85, p. 21] into a system in a real life context, emphasizing the case itself [86, p. 443]. A case study is therefore the most appropriate research strategy, since the metagraph is only applied to supply chains in the aviation industry and no generalisation for other industries is in scope of this thesis. Further, a case study research strategy fits to the nature of the research questions, which have a descriptive form [82]. However, common concerns of case studies are caused by a prevailing "methodological limbo"[83] as the case study struggles with the lack of rigorous systematic procedures for its implementations.[82] Thomas (2011) and Yin (2014, 2018) have addressed the issue of a systematic design process [83, 82] which is introduced in Section 3.2.

The fourth layer of Saunders' Onion decides on the data type which is used by the research methodology [79]. In order to set up the case of the aviation supply chain, qualitative data of the experts' interviews is utilised. Finally, a cross-sectional time horizon is applied as the supply chain is observed at one certain point in time. The core of the onion which describes the procedures and techniques [79] of the case study is described in Subsection 3.2.6.

3.2 Case Study Research Methodology

Thomas and Yin address systematic procedures and design principles for the design of a case study categorised in classification layers. This typology is applied by the following subsections to construct the case study. Yin describes the systematic procedure of the construction of a case study as a linear but iterative process [84, p. 70]. Thomas' typology of a case study design is shown in Figure 8.

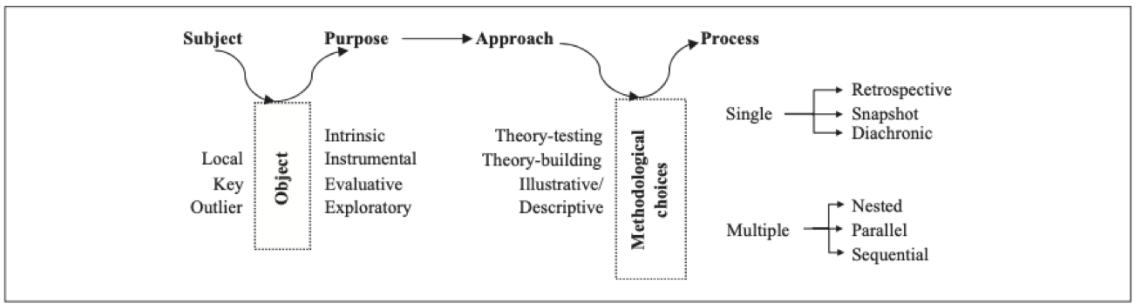


Figure 8. *Typology of a Case Study ([83, Fig.1, p. 518])*

3.2.1 Subject

Thomas differentiates between the subject and object of the case study [83]. The subject defines the example which gives the object its sphere to interact in and origins from one of three possible selection options. It can give insight into local knowledge which is accessible through in-depth knowledge of the inquirers and their ability to poke the knowledge for a grounded analysis and discussion. The other subject types to chose from are a "*key-ness* or *outliner-ness* of the case"[83, p. 514]. Thus the object can be analysed by interacting with a deviant case or a typical example case. Both cases "exemplify the analytical object of the inquirer"[83, p. 514]. The subject is the aviation supply chain. Considering the supply chain as a SoS [7] it exceeds an exemplary case in comprehensibility. Hence, an exemplary segment of the aviation industry supply chain is chosen as subject representing a key case. The key case should be able to adapt to various segments of the supply chain and present the perspective of an aircraft manufacturer. The chosen segment of the supply chain comprises the component of the landing gear in a depth of three tiers and a wide of three subcomponents (see Figure 11 in Chapter 4). The key case consists further of cyber security maturity niveaus of the suppliers which are added in form of the introduced certification standards (CMMCv1, NIST SP 800-171, IT Baseline Protection Manual, and ISO 27001) in Subsection 2.1.1. These certification standards represent a majority of international accepted certification standards as they differ in maturity niveaus and granularity. Exemplary, three CMMCv1 Practices were selected for the key case to represent the interaction within the certification standards. Reason for the focus on three CMMCv1 Practices is the high granularity of the IT Baseline Protection Manual which would damage the comprehensibility of the conditional metagraph propositions. An exception is made for the verification chapter to test the scalability of the metagraph model.

3.2.2 Object

The object of the case study is the theoretic or analytical frame through which the subject is explained and viewed [83]. The object of this case study is the graph-theoretic construct of a conditional metagraph, which emerges through the progress of the case study's inquirer. The object is "the heart of the study"[83, p. 514], which is analysed and studied through the application of the subject. A specific graph-theoretic construct of the metagraph (further referred to as model) is developed by the inquirer through the process of exemplifying the landing gear supply chain. However, the developed conditional metagraph model of the aviation supply chain is only possible to verify and validate when the purpose of the structure is set clearly [87]. It has to be differentiated between the purpose of the conditional metagraph model and the purpose of the case study as part of the typology of a case study design. The purpose of the conditional metagraph model is to answer the three defined research questions: Whether and how the applicability of the conditional metagraph to the aviation supply chain and the integration of cyber security certifications are feasible and if the construct of the conditional metagraph holds the potential to improve the cyber security maturity of the aviation supply chain.

3.2.3 Purpose

Thomas (2011) introduces the purpose as the reason why the case study is conducted and can be categorised into four terms: The intrinsic and instrumental views used by Stake (2005) are supplemented by evaluative or exploratory/heuristic kinds of case studies mentioned by Merriam (1988) and Bassey (1999)[88, 89, 86, 83]. It is essential to establish the connection to the object in order to determine the purpose of the case study: The necessary understanding in this case study is the mapping of supply chain and cyber security characteristics onto the graph-theoretic metagraph construct. An evaluative approach mentioned by Thomas (2011) would fit best for this case study (see [83]). However, the purpose for conducting the case study exceeds a simple evaluation of whether the metagraph can be applied to the supply chain of a landing gear component and its cyber security properties. Rather, it will also include the description of how the application looks like. This is possible by extendeding Yin's purpose categorisation [83, 82]. Hence, the reliability and replication of the execution of the case study are ensured. The purpose of the case study is closely related to the research objective, which is the description and evaluation of the conditional metagraph model for its applicability onto the aviation supply chain with cyber security properties.

3.2.4 Approach

The approach of the case study focuses on the impact which theory gives in the design process of the case study. Thomas (2011) argues that the object of a study can either have illustrative or theoretic character.[83] Since the object of the case study is a graph-theoretic construct which is based on academic research, this case study is grounded on previously existing theory [80, 79]. Thus, the theory is determined as an outset of the case study which is tested for its applicability in supply chains (theory testing) [83]. The case study can further highlight the theory's benefits and challenges in context of aviation supply chains.

3.2.5 Process

The last classificatory layer of Thomas' typology is the decision about the operational process of the case study. The decision lies between single and multiple case study execution(s) and the temporal boundary. [83] This thesis distinguishes between the subject, which is the exemplary supply chain of the landing gear component, and scenarios to evaluate the conditional metagraph model. These scenarios show different perspectives of the exemplary supply chain of the landing gear and thus can be seen as multiple case studies which are executed sequential as the scenarios show different snapshots of the supply chain management of the landing gear (see [83]). The scenarios are build on the requested properties listed in Section 1.1 and support in the evaluation process whether the conditional metagraph structure contributes to an enhanced cyber security maturity in the aviation supply chain.

3.2.6 Methods

The methods used in the case study are separately described and subdivided into the data collection (including the data access), data sampling and data analysis. The decision for these three steps impacts the overall validity and reliability of the case study [82]. Thus, concepts for data reliability and validity by Yin (2018) are addressed additionally in Subsections 6.1.1 and 6.1.1[82]. This case study is based on the following methods: A literature review, semi-structured expert interviews, and scenario designing.

To provide the necessary scientific depth to the research areas, the literature review is divided into a pure academic and a multivocal literature review. First, an academic literature review of cyber security in supply chains and the graph-theoretic metagraph construct summarises the scientific discourse in journal articles and conference papers of the IEEE

Xplore and Scopus databases. Subsequently, a multivocal literature review is done based on official organisational and governmental sources as they provide the necessary overview of cyber security regulations and certifications. To keep the literature review systematic and to reduce the bias of the inquirer's opinion, the flow diagram in Figure 9 (oriented on the Prisma Statement [90]) introduces the procedure of data collection and data sampling performed by the inquirer at the begin of 2022 and checked for up-to-dateness at the begin of 2023.

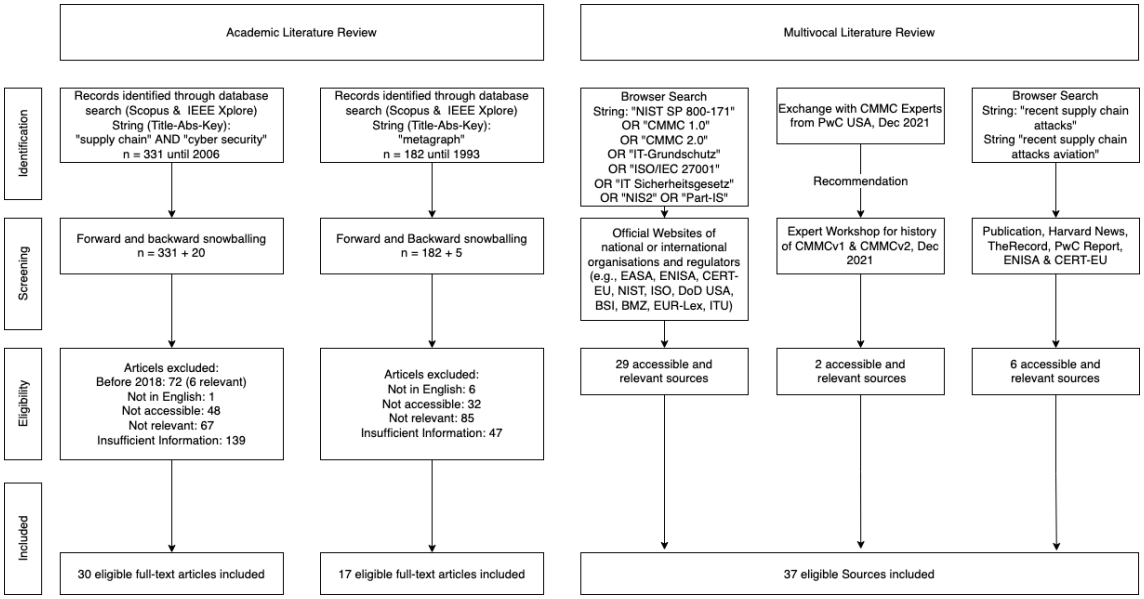


Figure 9. *Research Method: Flow Diagram of the Literature Review*

As the search success of both databases was congruent, forward and backward snowballing was done after the first search to identify additional literature. Additionally, the sampling of the literature review which is the selection process of the outcome of the search strings, was systematically structured. It was focused on timeliness and reputation of the conference papers and journals. However, timeliness should be considered in the context of the pandemic which could have caused publication delays or topic shifts starting in 2021. Hence, this justifies the consideration of six papers published before 2018. Further, except for two papers, studies were used which were available in public libraries and over universities' VPN access to databases. An exception for the timeliness of the graph-theoretic metagraph literature is made as all literature comprising the metagraph construct up to the initial literature by Basu and Banning [91] from 1992 (collected as part of the snowballing) were included to thoroughly analyse the research directions and fields of application of the metagraph construct. The data analysis of the literature review was conducted through manual content analysis.

The second research method is the performance of in-depth interviews. The data collection consist of the execution of semi-structured interviews as these are a commonly used method for the collection of qualitative data [92]. The sampling of data is important for the reliability of the research study [82]. The selection of interview partners was done based on the requirements shown in Table 4. No consideration was given to characteristics such as gender, age, and origin as these are irrelevant to the outcome of the study. Experts working in the field of security and safety related to the aviation supply chain, aviation certification, and aviation regulation were chosen. The first contact to experts was initiated through business contacts at the work place of the inquirer, through an aviation security course of the Tallinn University of Technology, and conferences [93, 94].

Table 4. *Research Method: Requirements for the Industry Experts*

Category	**Requirement**
Expertise	(General Aviation or Landing Gear) and (Security or Safety) and (Industry or Authority)
Years of Work Experience	10 years in the Aviation Industry
Place of Work	Europe
Gender	Indifferent
Origin	Indifferent
Age	Indifferent

The inquirer presented the idea of this thesis at BSides Tallinn 2022 [93] which enabled the contacting of experts, who provided valuable contribution for the development of the scenarios and partly became interviewees. Snowball sampling was used to obtain further connections from the first interview partners. In total six experts were interviewed. Their characteristics are shown in Table 5.

Table 5. *Research Method: Specifications of the Interviews*

Contact	**Years of Work Experience**	**Field of Expertise**	**Date**	**Time**
Conference	>10	Safety Assessment of the Aviation Supply Chain	23.11.2022	01:37:16
University	>10	Safety and Security Audit for a European Authority for Aviation Safety	16.12.2022	01:11:39
Workplace	>10	Security Design of an Aircraft Manufacturer	16.12.2022	01:15:52
Snowballing	>10	Safety Regulation Compliance of a Landing Gear OEM	09.12.2022	00:57:59
Snowballing	>10	Landing Gear Audit for a European Authority for Aviation Safety	14.12.2022	01:21:34
Conference	>10	Security Assessment of the Aviation Supply Chain	17.12.2022	00:59:13

The experts' workplaces are based in Germany, France, Bulgaria, and Estonia. The country allocation to the characteristics of the interviewees could have disclosed their identities. The semi-structured in-depth interviews had a set time of an one hour and were conducted

remotely via Microsoft Teams, where they were recorded and transcribed in separate documents. The inquirer took additional notes. Subsequently, the data was manually analysed and grouped by scenario comments, comments to the aviation supply chain, and additional comments. The foundation of the semi-structured interviews lies in an interview guide which is available in Appendix A1. The interview guide was created based on the literature review, the exchange with experts on the conferences, and the scenario designing [93, 94].

The third methodological tool of the case study is the use of scenarios to bridge the gap between interviewees and the metagraph model [87]. Since scenarios are mainly used with qualitative data, their use in this case study is feasible. Jarke, Bui and Carroll (1998) define a scenario as a set of events which can take place. A scenario encourages to engage with incidents and possible courses of action, risks, and opportunities. Since the developer can use scenarios to understand the users' needs and to verify the system for its behaviour, scenarios improve the communication between the user and the developer.[87] Consequently, scenarios create comprehensibility by bridging the gap between a purely graph-theoretic model and possible deployment options of the model. The metagraph model can be evaluated for its applicability in the aviation supply chain without the need for the interviewees to understand the graph-theoretic foundation of the metagraph construct. The creation of the scenarios is based on the literature review and on the gained knowledge about the needs of the aviation industry by interacting with the industry experts at the conferences [93, 94].

3.2.7 Procedure

The overall case study setup is shown in Figure 10[1]. The case study subject is based on requirements defined by the interviewed industry experts, as a literature review on the aviation supply chain did not lead to a similar depth of knowledge and understanding of the aviation supply chain characteristics as the extraction of the interviews. Hence, the interviewees' insights build the foundation for the characteristics of the aviation supply chain and the exemplary design of the landing gear segment (key case). Additionally, the key case is based on the supplier link analysis of the website Airframer [95]. The website Airframer is not unlimited free to use, request for unlimited access had been submitted but in the final state rejected. Thus, the author used only publicly available data of this website and ability for reproduction holds also for researchers with missing unlimited access.

Based on the exemplary landing gear supply chain and the graph-theoretic literature review,

[1] Icons obtained from https://thenounproject.com

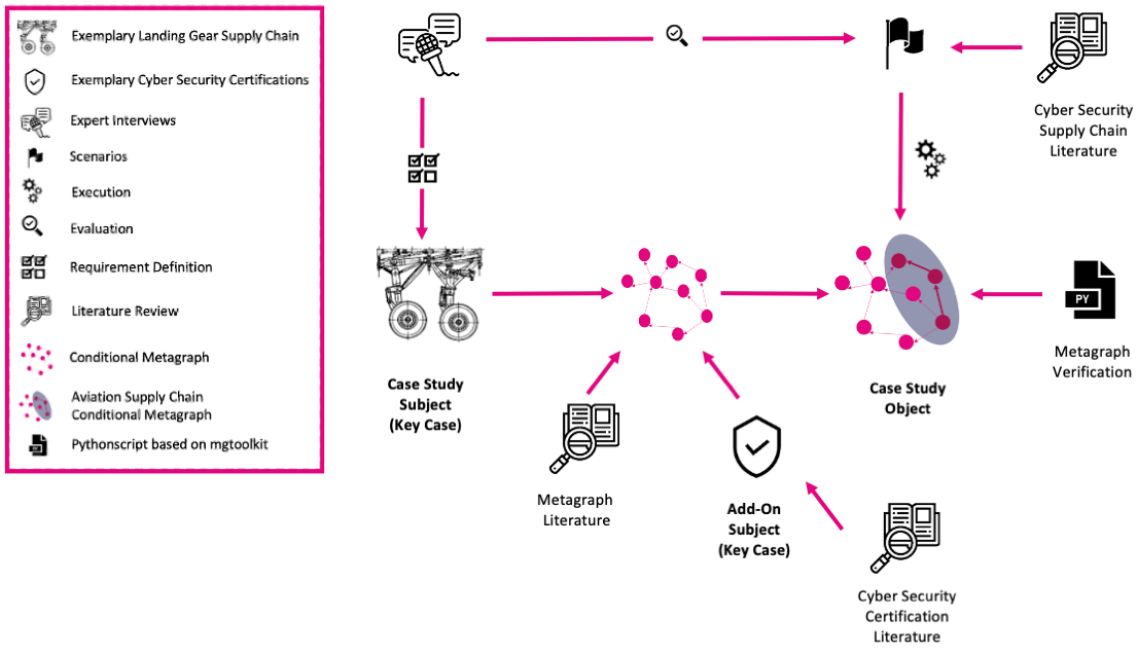


Figure 10. *Overview of the Used Methods in the Case Study*

the conditional metagraph model is build. Additionally, the multivocal literature review on cyber security certifications lays the basis for adding the four certification standards onto the conditional metagraph model. The harmonisation of the four standards (BSI IT Baseline Protection Manual, the CMMC, the ISO 27001, the NIST SP 800-171) and the cyber security practices was done through two mappings: The Infodas published an excel file containing a mapping in 2021 called the "CMMC Awesomeness v2021.2"[96] where the ISO 27001 and the NIST SP 800-171 were mapped onto the CMMCv1. The BSI has mapped the IT Baseline Protection Manual in accordance with the ISO 27001:2013.[2] As the BSI mapping is rather current with referencing the fourth edition from 2021 it was used despite the reference to the older ISO 27001 version.[97] The mapping of Infodas is based on the first version of the CMMC. As the scope of the CMMCv1 comprises more practices, the focus lies on the initial CMMC version. In addition to the referenced links the mapping documents are handed in with the thesis to ensure traceability. The file *MappingCertificationsAC* consists of a mapping of the CMMCv1 Access Control (AC) Domain with the four alternatives conducted by the inquirer.

Similarly to the subject of the case study, the conditional metagraph model went through several iterative adaptation processes. In case, the researcher had to determine assumptions (further referred to as patterns) in the design process of the conditional metagraph model, these are introduced in Section 4.2 for reliability purposes. The metagraph model was iteratively adapted based on changes of the supply chain example and revalidated in case

[2]The current version of ISO 27001 in English was published in October 2022. At that time, this section had already been written.

the scenarios were changed. Subsequently, the created case study object is evaluated by the interviewees based on five scenarios. The scenarios are created based on the literature review on cyber security in supply chains and requests of experts from the conferences.

The validation process consists of the comparison of the model's result with the real world and thus, with the experts' opinions as shown in Figure 10. Validation of the metagraph model with the real world is made possible by the interviews with the experts. Their input based on their experience within the aviation industry represent the "real world". With the help of scenarios and the exemplary landing gear supply chain, bridges are built to evaluate the proximity and relevance of the metagraph model to reality. The interviewed experts validated the key case on its relevance and applicability to the aviation supply chain.

The case study object is further verified through a pythonscript. The verification process of the metagraph model influences the quality of the case study as it is checking for the logical correctness of the graph-theoretic model [98]. It describes the correctness of the mathematical setup of the metagraph model. The verification process compares the metagraph model with the exemplary landing gear supply chain, the characteristics of the aviation supply chain, and the graph-theoretic literature. The verification is done through the use of a pythonscript with a general good programming practice [98]. Through its use it is possible to automate and generalise the conversion steps and to set break points for reviewing the intermediate results. The outcome is verified with the conceptual outcome of the exemplary landing gear supply chain and thus, checked for inconsistencies in the conversion process to a metagraph model.[98] Still this approach holds the risk of self assessment as model and pythonscript are set up by the same inquirer. However, this approach gives the opportunity to mitigate the overfitting of the exemplary landing gear key case. Thus, using a pythonscript helps in understanding whether the metagraph structure is implemented correctly as the case object and is based on the python library *mgtoolkit* by Dinesha Ranathunga [99]. The pythonscript is divided into three parts: A setup part of the conditional metagraph model, a scenario execution part (including a sensitivity analysis), and a scalability analysis (see Subsection 4.2.4) [100]. While this thesis was written an upgrade to python 3 of the mgtoolkit library was performed by Eric Parsonage [101]. Accordingly an upgrade of the pythonscript from 2.7 to 3 was carried out by the inquirer [100]. In case of any questions, the inquirer could contact both library authors.

3.3 Ethical Consideration

Reliability of the study is also closely related to the access of the data of the interviewees [102]. The context of cyber security maturity in supply chains holds the risk of unintentional disclosure of vulnerabilities that a malicious third party could exploit. Thus, the

transcribed interviews are not publicly available and only disclosed in the confidential Appendix A2. Furthermore, the companies are only mentioned according to their function in the supply chain and not identified by name. The names of the interview partners are also anonymised and not assigned to the company in which they acquired their expertise. In addition, a non-disclosure agreement was concluded with one interview partner upon request. This ensures that the information provided in the interviews fully reflects the opinion of the interviewed experts. No restrictions were made in the interest of confidentiality when defining the requirements for the exemplary structure of the landing gear supply chain and when evaluating the scenarios.

Reliability is not only subject to the confidentiality agreements with the interview partners. Additionally, the setup of the exemplary landing gear supply chain consists of existing suppliers based on the supplier link analysis of the website Airframer [95]. The metagraph model is used to demonstrate the implementation of cyber security practices through scenarios which represent exemplary suppliers with missing cyber security practices. These attributes of the suppliers are not related to the precedent suppliers. Nevertheless, in order to not portray any company negatively, the supply chain is presented anonymously as case study subject. Hence, only the censored supply chain of the landing gear is used in Chapter 4. The uncensored key case is attached in Appendix A3 which is unavailable to the public but allows traceability and reproducibility via disclosure through direct contact with the inquirer.

4. Metagraph Application

The thesis' case study results stem from a literature review and six conducted expert interviews and consists of four outcomes. The first Subsection 4.1.1 introduces characteristics of the supply chain which have to hold for the aviation industry. Second, the exemplary aviation supply chain of a landing gear component is described in Subsection 4.1.2. The third part (Section 4.2) describes how to apply a conditional metagraph onto the characteristics of the aviation supply chain and how to integrate cyber security certification standards. The section ends with the conditional metagraph model applied to the landing gear supply chain. The scenarios used to evaluate the application of the conditional metagraph to the landing gear supply chain are described in Chapter 5. Their layout as snapshots of the case study is introduced as last Section 4.3 of this chapter.

Since the examination of the supply chain starts with the aircraft manufacturer, business to business (B2B) supply chains are considered. Thus, the terms buyer and supplier or producer are used throughout the rest of the thesis. Further, the term airframe manufacturer is often used as a synonym for the term aircraft manufacturer (OEM) since the aircraft OEM mostly also designs the airframe.[103] As the key case of the landing gear is not part of the airframe but only the aircraft, the use of the term aircraft OEM is preferred in this thesis. The terms component and subcomponent are used as placeholders for parts (including services, e.g., the assembling process) of an aircraft type. Important here is that the subcomponent is part of the component. A more detailed definition with reference to the key case is introduced in Subsection 4.1.2.

4.1 Case Study Subject: The Aviation Supply Chain

The setup of the subject of case study consists of two parts. The first part describes the characteristics of the aviation supply chain. These characteristics form the basis for the second part, the design of an exemplary landing gear supply chain. Subsequently, they reoccur in the setup of the conditional metagraph model as the model must be capable to transpose the expressions of the characteristics into a graph structure.

4.1.1 Characteristics of the Aviation Supply Chain

The characteristics of the aviation supply chain are in the following used to set up the key case of the case study subject. Additionally, they build the foundation for the structure and the use of algebraic calculations in the case study object, the metagraph structure.

The expert interviews revealed six characteristics of the aviation supply chain: The setup of competing suppliers on each tier level, the characteristics of sourced components, dependencies of suppliers on the same tier level, the scope and type of information exchange between buyer and supplier, between suppliers of the same tier level, and the exact assignment of a component to its producer(s).[103, 104, 105, 106, 107, 108] These characteristics are subsequently enumerated:

1. **Structure of Competing Suppliers:**
   The number of competing suppliers rises with the increasing tier level as pointed out by Expert B and Expert C. A few suppliers are close to the aircraft manufacturer taking a lot of responsibility as OEMs of the aircraft components.[104, 106] Further, suppliers can produce multiple components which can also lead to suppliers producing subcomponents of their own components. Additionally, a component can be produced by different suppliers.[109, 108] Based on Expert B, suppliers practice at least a double sourcing strategy in the aviation industry. Thus, there won't appear a supplier as the sole source of a (sub-)component in the supply chain [105].[104]
2. **Assignment of a Component to its Producer(s):**
   Traceability of components and their suppliers of each produced aircraft is anchored in the strict safety regulations of the aviation industry [57]. Each buyer is responsible for the credibility and recording of their direct suppliers. Thus, it is feasible to trace, e.g., the valve of a landing gear component by cascading through the supply chain.[105, 108]
3. **Characteristics of Sourced Components:**
   (a) **Interconnectivity of Sourced Components**
   The components manufactured in the supply chain can have three different stages of modularity or forms of interconnectivity with other components on the same tier level. [104, 107] The same tier level for interconnectivity is assumed at this point to keep the key case comprehensible.
   - **Low modularity/strong interconnectivity:** The component is highly interconnected with other components in a non-standardised manner. The construction of the component depends on the design of other suppliers' components and is rather individualised. This relation can be unilateral or bilateral.[106]

- **Medium modularity/medium interconnectivity:** The component has different variants depending on other suppliers' components. Depending on the cooperating supplier, adjustments are made in the own component. Hence, different variants of the own component are provided in a standardised manner pending on the deployment of another component. Expert C mentions exemplary the aircraft engines for which this characteristic holds. This relation can be again unilateral or bilateral.[106]
- **Strong modularity/low interconnectivity:** Suppliers produce modular components which are based on standardised interfaces. The selection of other components does not affect the design of the own component.[107, 105]

(b) **Cyber Security Related Criticality of the Sourced Components (CC)**
The components can have different criticality levels for cyber security which can affect the safety of an aircraft.[104] The author introduces two perspectives: The focus on the lifecycle of a component and the perspective on the component's properties. First, Expert B mentions three phases which have to be differentiated when the component's lifecycle is considered in focus of cyber security: The design phase, the production phase and the final component itself. In all phases cyber related attacks can influence the security properties (confidentiality, integrity, and availability) of the component even though the component can completely consist of non-hardware and non-software parts. In the design phase the confidentiality of the design of the component can be compromised, e.g., for espionage. A cyber security attack in the production phase could influence the integrity and availability of a component as its production is increasingly automated. Thus, the structure of the material can be weakened and can have a safety critical impact onto the aircraft functionality.[104] Last, the final component can provide vulnerabilities to attack if the component consists of hardware and software parts. The design phase can be secured through the categorisation of information exchange between buyer and supplier as mentioned subsequently (see 5. Types of Information Exchange (IE) Between Buyer and Supplier). According to Expert B, the potential change of integrity affecting the safety of the aircraft is mitigated by quality checks being - especially in the aviation industry - already part of the production phase.[104] The second perspective on different criticality levels of components is focusing on the final component which includes hardware and software parts. Expert E introduces the categorisation of cyber attacks' entry points (see also [57, 107]) [107]:

- **CC0 Non-Critical Characteristics:** Usage of components that do not contain software and hardware or components that have software and

hardware included but do not consist of the following features,

- **CC1 Critical Characteristic 1:** Usage of Commercial-off-the-shelf (COTS) software and hardware,
- **CC2 Critical Characteristic 2:** Access by unauthorized people to the software and hardware of a component, e.g., the access to the infotainment system by passengers,
- **CC3 Critical Characteristic 3:** Connection towards non-governmental networks, e.g., the Internet. [57]

In case a component is part of one of these three categories, the security has to be checked and a risk assessment performed. Depending on the impact of the component towards safety (restricted functioning of the landing gear control unit), operation delays (replacement of a non-functioning coffee machine) or dissatisfied customers (non-functional infotainment) mitigating measurements based on a risk assessment must be implemented by the aircraft manufacturer [107].

4. **Interaction of Suppliers of the Same Tier Level:**
   Suppliers who are providing components can have different levels of interaction with each other as the components' characteristics and interfaces could be coordinated with each other [106]. Three types of interaction are possible:
   - **Cooperation:** The suppliers are cooperating with each other. The component is designed, produced, and sold by the resource sharing of two or more suppliers. Hence, these suppliers act as a joint venture. In case the joint venture becomes an own legal entity, the cooperation is seen as one additional supplier.[105]
   - **Dependency:** Depending on another supplier, adjustments have to be made in the own component. Different variants dependent on the other supplier are standardised available (accompanied by the medium modularity of components).[106]
   - **Independency:** There is no need to exchange information with other suppliers or the buyer as the component has a high modularity [106].
   - **Competition:** Suppliers are competing for the same component(s) with each other [106].
5. **Types of Information Exchange (IE) Between Buyer and Supplier:**
   The information exchange between supplier and buyer can vary regarding the type and scope of critical information which is exchanged. Based on Expert B and E, the information exchange is categorised into two groups: The black box component purchase or the subcontracting of the production of designed components by the buyer. Depending on these two categories, the criticality of exchanged information differs and thus, the risk of information leakage through the supply chain is impacted differently.[104, 107]

- **IE0 No Information Exchange:** Buyer and supplier do not exchange information as, e.g., a standardised single component is purchased.
- **IE1 Uncritical Information Exchange:** The black box component is in its design part of the supplier's intellectual property. Thus, the transferred information between buyer and supplier consists of input and output parameters and requirements of the component.
- **IE2 Critical Information Exchange:** The design of the component is created by the buyer and the outsourcing of its production is forwarded to the supplier. Hence, the information exchange contains information about the design of the component. Expert B and E classify this information as critical with increasing need for protection.[104, 107]

6. **Scope of Information Exchange between Suppliers of the same Tier Level:** Different factors impact the information exchange between suppliers of the same tier level. On the one hand, the buyer is playing the card of concealing knowledge about additional co-competitors in order to suppress prices. On the other hand, the requirements for components originate from the buyer and thus, the information exchange between non-cooperating suppliers is controlled by the buyer. In case of a cooperation of suppliers, it is assumed that they have one coordinated communication channel with the buyer.[107, 104]

4.1.2 Key Case: The Landing Gear Supply Chain

The landing gear supply chain represents the key case of the case study's subject. As Thomas (2011) pointed out, the key case presents an exemplary part of the subject [83]. Whether the landing gear constitutes a suitable key case is determined by falling back on the aforementioned characteristics of the aviation supply chain. [104, 95] A landing gear component consists on average of 60 subcomponents [104]. To ensure the manageability of the case study, the design of the key case does not focus on the detailed representation of all components and the complete mapping of all supplier options. Rather the considered segment of the landing gear supply chain focuses on three subcomponents of a specific aircraft type's landing gear component and three supplier tiers. Based on Expert D, the setup of the chosen landing gear segment consists of components comprising all characteristics mentioned in Subsection 4.1.1 [105]. The (sub-)components that appear in the three tiers of the key case are shown in Figure 11 [1]).

The supplier which provides the landing gear is referred to as the *OEM of the landing gear* and is located on tier 1. The landing gear components of the key case include the

[1] Icons obtained from https://thenounproject.com

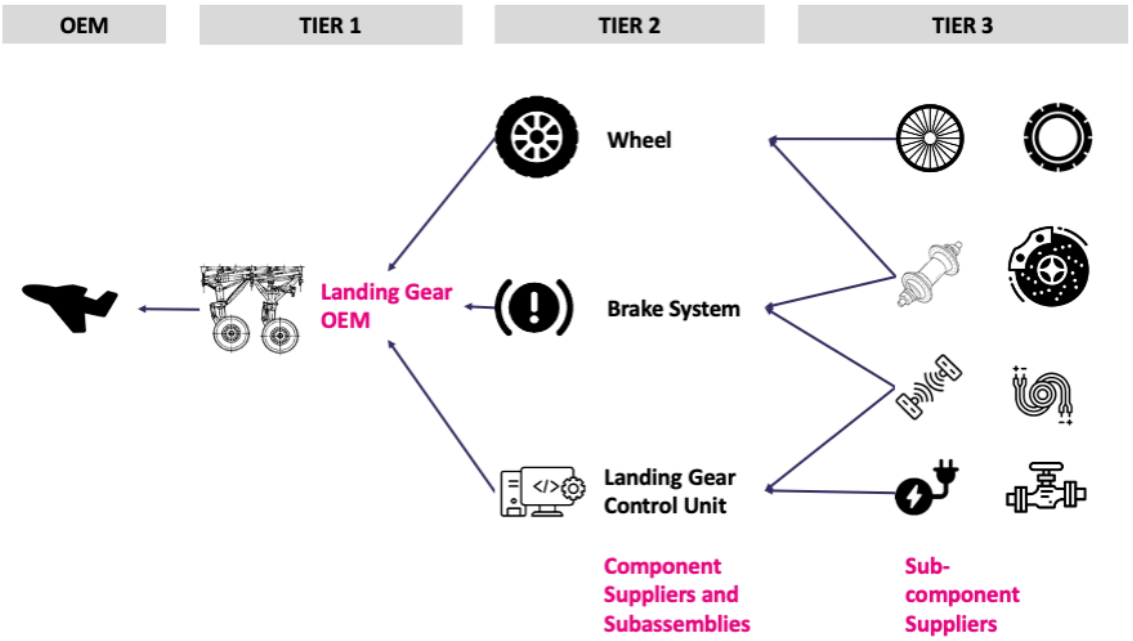


Figure 11. *Considered Segment of the Landing Gear Supply Chain*

braking system (a brake-by-wire system or a hydraulic brake system), the wheel, and the landing gear control unit. For the upcoming chapters the term *component* is used for tier 2 parts of the landing gear and the term *subcomponent* is used for tier 3 parts of the landing gear. The brake-by-wire component consists of five subcomponents on tier 3: Sensors, actuators, control algorithms, power supply, and the wiring. The wheel component includes subcomponents as the tyre, tyre inflation system, the brake caliper, the wheel bearings, the wheel hub, and the wheel itself. The third component is the landing gear control unit which consists of sensors, actuators, control algorithm & interface, power supply, and the wiring. The setup of the component structure shows that subcomponents can be impacted by other subcomponents being part of the same component (e.g., the tyre inflation system and the tyre) as well as by subcomponents from other components (e.g., the brake caliper of the wheel and the sensors from the braking system). Additionally, the same subcomponent type can appear in different components and thus, the same supplier on tier 3 level can provide a subcomponent to different suppliers on tier 2 level (e.g., the power supply or the wiring).

Table 6 shows the numbered components and their censored suppliers from 1 to 31. The numbering of the components includes the tier level (100 ff. for tier 1, 200 ff. for tier 2, and 300 ff. for tier 3). Mapping the suppliers to a tier level is not possible because a supplier can appear in different tiers. The references and structure of the landing gear components and suppliers origin from an exemplary aircraft type (see [95]) which is adapted by insights of the six interviewees.

Table 6. *Considered Censored Suppliers of the Landing Gear Supply Chain*

Tier n	Component	Modularity	Suppliers	Dependency	CC	IE	Tier n+1 Component
1000	aircraft	Low	0	-	0,1,2,3	-	101
101	Landing Gear	Low	1	-	0,1,2,3	IE1	211,212,213
			2	-	0,1,2,3	IE1	221,222,223,224
211	Brake-by-Wire	Low	6	-	0,1,2,3	IE2	301,302,303,304,305
	(Option 1)		7	-	0,1,2,3	IE2	301,302,303,304,305
221	Hydraulic Brake	Low	6	-	0,1,2,3	IE1	301,302,303,304,305
	(Option 2)		7	-	0,1,2,3	IE1	301,302,303,304,305
			8	-	0,1,2,3	IE1	301,302,303,304,305
212	Wheel (Option 1)	Low	1 (inhouse)	-	0,3	IE0	306,307,308,309,310,311
			6	-	0,3	IE2	306,307,308,309,310,311
222	Wheel (Option 2)	Low	6	-	0,3	IE1	306,307,308,309,310,311
			1	-	0,3	IE1	306,307,308,309,310,311
			8	-	0,3	IE1	306,307,308,309,310,311
213	Control Unit	Low	3	-	0,1,2,3	IE2	302,304,305,312,313
	(Option 1)		4	-	0,1,2,3	IE2	302,304,305,312,313
			5	-	0,1,2,3	IE2	302,304,305,312,313
223	Control Unit	Low	3	-	0,1,2,3	IE1	302,304,305,312,313
	(Option 2)		4	-	0,1,2,3	IE1	302,304,305,312,313
			5	-	0,1,2,3	IE1	302,304,305,312,313
224	Subassembly	High	9	-	0	IE2	-
	Landing Gear		10	-	0	IE2	-
			11	-	0	IE2	-
301	Sensors I	Medium	16,17	309	3,1	IE2	...
			24,25	309	3,1	IE1	...
			26	-	3,1	IE2	...
302	Actuators	High	18	-	0	IE1	...
		High	19	-	0	IE1	...
303	Control Algorithm	Medium	20	301	1,3	IE2	...
			21	301	1,3	IE1	...
304	Power Supply	High	14	-	0	IE1	...
			15	-	0	IE0	...
305	Wiring	High	14	-	0	IE1	...
			15	-	0	IE0	...
306	Wheel	Medium	28,29	310,311	0	IE1	...
		Medium	30,31	310,311	0	IE2	...
307	Tyre	Medium	23	-	0	IE1	...
			27	308	0	IE1	...
			22	-	0	IE1	...
308	Tyre Inflation	Medium	23	-	3	IE1	...
	System		27	307	0	IE1	...
309	Brake Caliper	Medium	16, 17	301	3,1	IE2	...
		Medium	24,25	301	3,1	IE1	...
310	Wheel Bearings	Medium	28,29	306,311	0	IE1	...
		Medium	30,31	306,311	0	IE2	...
311	Wheel Hub	Medium	28,29	306,310	0	IE1	...
			30,31	306,310	0	IE2	...
312	Sensors II	High	13	-	3	IE2	...
			16	-	3	IE1	...
			12	-	3	IE1	...
313	Control Algorithm	Medium	20	312	1,2	IE2	...
	& Interface		21	312	1,2	IE1	...

CC - *Critical Characteristic: 0 Non-critical, 1 COTS Usage, 2 Critical Access, 3 Critical Connection*
IE - *Information Exchange: 0 None, 1 Black Box Approach, 2 Critical Information Exchange*

The landing gear is a main part of the aircraft [110] and includes the specified information exchange relationships between suppliers and buyers, the cyber secure critical component characteristics, and the components modularity by starting at the perspective of the aircraft OEM and moving towards increasing tier levels. Based on Expert B the information exchange between the aircraft manufacturer and the landing gear OEMs counts to an uncritical information exchange, i.e., the black box apporach (IE1) as the suppliers in tier 1 have full responsibility for the design, production, assembly, and maintenance of

the landing gear. Additionally, the design of the landing gear must be closely matched to the design of the aircraft as it depends, e.g., on the weight distribution of the overall aircraft. Thus, the landing gear is an individualised product which is in close alignment of the requirements of the aircraft manufacturer (high interconnectivity with other main parts of the aircraft).[105, 104] Supplier 1 and supplier 2 are possible vendors for the aircraft manufacturer to purchase the landing gear from. The landing gear component contains all critical characteristics (CC) inherited through its subcomponents. Both suppliers differ in the supply of their subcomponents. Supplier 2 needs one additional subcomponent when comparing the *Tier n+1 Component* with supplier 1. This is the subassembler which is used by supplier 2 (component 224). Thus, the landing gear is assembled by a different company based on the critical design exchange with supplier 2 (IE2). The subassembly is used in this key case as an example for all services performed on the landing gear components in purchasing as well as in operations (e.g., maintenance). In the following the term component or subcomponent is also used for services for the assembly or maintenance of the landing gear components.

With increasing tier level, the suppliers of (sub-)components increase in number with increasing modularity of the supplied (sub-)components. The components on tier 2 level still feature a low modularity as those are specialised for the customised landing gear. For example, the braking systems (components 211 and 221) differ between supplier 1 (brake-by-wire system) and 2 (hydraulic braking system). Further, the wheel (component 212) can be produced inhouse by supplier 1 or by supplier 7 who is also producing the hydraulic braking system (component 221). Thus, suppliers can appear at different tier levels and for various components and can even become own and others supplier on lower tier levels. However, it is important to mention that a supplier that is part of a corporate group which consists of several subsidiaries is seen as an individual supplier if there is a contractual exchange with other subsidiaries. This approach is inspired by the EASA safety audit [105].

On the third tier the subcomponents have a high or medium modularity. A medium modularity symbolises that the supplier of the subcomponent has to adjust the component's interfaces based on other subcomponents. Hence, the column "Dependency" directly connects to the relevant subcomponent(s) and can occur across components (see example from above of sensor I (301) and the brake caliper (309)) but restricted to the same tier level (as mentioned in Subsection 4.1.1). Further, this dependency can appear bilateral as well as unilateral. In case of the control algorithm (303) and the sensors (301) of the brake component, the sensors do not depend on the control algorithm but the control algorithm on the sensors. A high modularity as exemplary shown for the wiring (305) describes a product which has standardised interfaces known in the industry. Hence, the

buyer does not have to organise parameter exchange between the suppliers as there exists no interconnectivity between suppliers. Additional, no information exchange between the supplier and the buyer is possible as the product could be purchased without exchanging information via an anonymous platform. However, the interaction with the supplier for quantity discounts or to maintain the supplier relationship counts into the non-critical information exchange (IE1). Finally, components can be provided through a cooperation of suppliers causing a direct information exchange between the suppliers and a common interface towards the purchasing buyer. Exemplary, the brake caliper (309) is produced in a cooperation of supplier 16 and 17 or 20 and 21. Expert B points out that landing gear OEMs purchase their components mostly from non-cooperating suppliers [104]. Thus, the tier 2 level provides only suppliers which are competing. However, to include alternative purchase options which are used in the industry and keep the key case applicable, supplier cooperation is included on tier 3.[105]

4.2 Case Study Object: The Metagraph Model

The graph-theoretic construct of the metagraph was introduced in Chapter 2. The metagraph model is mapped onto the characteristics of the aviation supply chain in a first introduction of the basic algebraic constructs and operations of a simple metagraph. Secondly, the simple metagraph transforms into a conditional metagraph by including the propositions which are adapted from the characteristics of the aviation supply chain (i.e., CC and IE).

4.2.1 Adaption of the Aviation Supply Chain Characteristics

Two questions have to be answered when the graph-theoretic construct of a conditional metagraph is applied onto the aviation supply chain:

1. Why should the metagraph be used to represent and analyse supply chains and not other graph structures presented in the graph theory literature (see Section 2.2)?
2. How can the aviation supply chain be represented by a conditional metagraph?

Fundamentally, a supply chain is suitable for graphical representation as companies in a supply chain are interacting with each other through various business connections which can be represented as directed edges pointing from the buyer to the supplier (having the perspective of the desire for a business performance of a supplier) or vice versa from the supplier to the buyer (having the perspective of distributing a service or a good). Further, goods and services being part of the supply chain can be mapped as a graphical structure

cascading from subcomponents towards the final product which symbolises one end of the supply chain. These two approaches can be combined in a bipartite graph connecting two disjoint sets, the set of suppliers X_S and the set a components X_C. The bipartite graph is not necessarily balanced as the sets can have different cardinality.[67] The edges between the two sets are directed and connect suppliers to their produced components and not the other way around which is necessary for the properties of the metapath [15]. Thus, different suppliers can provide the same component (see c_1) and various components can be produced by one supplier (see s_1) (see Characteristics of the Aviation Supply Chain 1. & 2. in Subsection 4.1.1). Further, purchased subcomponents (e.g., c_6) are connected to the suppliers (e.g., s_1) as input for their components' production (here c_1 and c_2). The bipartite graph is shown in Figure 12 and split into two projections ($X_{ComponentOfS_{1-5}} \subseteq X_C$ on the left side; $X_{SubcomponentOfS_{1-5}} \subseteq X_C$ on the right side) with $\{s_1, \ldots, s_5\} \subseteq X_S$ and $\{c_1, \ldots, c_5\} \subseteq X_C$ to simplify the graph for the reader.

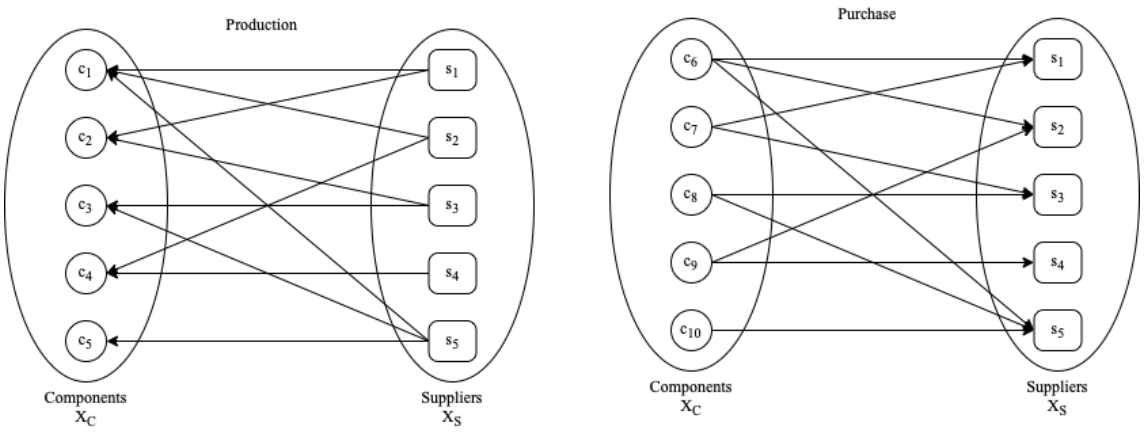


Figure 12. *Two Projections of the Bipartite Graph of the Landing Gear Supply Chain*

The classification of the supply chain into two sets is not yet enough visualisation of the landing gear supply chain as subcomponents can be part of a component. This hierarchical setup is not implementable through a bipartite graph. Instead, the metagraph gives the possibility to build subcomponents in sets of nodes and allows a hierarchical presentation (using the potential of higraphs) [15]. Further, it also allows the implementation of dependencies through sets of elements. The landing gear supply chain is a SoS [7] and consists of activities which take place simultaneously (e.g., the production of two subcomponents without cooperation of the suppliers) which can be modeled in metapaths as these do not depend on a sequence and order of paths (excluding simple, directed, and hypergraphs). Components 313 and 301 are manufactured independently of each other and it does not matter which component is finished first and in which order. However, it is relevant that the subcomponents are manufactured before the components. This is achieved by the use of direct graphs and the expression of start sets and end sets of the metapaths. Additionally, the metapath allows to generate paths without the need to include all edges'

outvertices which is mandatory for implementing a supply chain where suppliers provide components which are not part of the targeted final OEM component (for the key case the landing gear). Finally, the invertices of conditional metagraph edges can hold propositions which are considered in algebraic calculations of the metagraph and allow to filter for suppliers or components which hold certain attributes.[15] Hence, the first question is answered as to why the metagraph is preferred over other introduced graph structures.

To respond to the second question, the characteristics specific to the aviation supply chain allow the use of the metagraph in a way which represents a supply chain in the aviation industry close to the reality. Since the safety standards [57] of the aviation industry mentioned in Subsection 4.1.1(see Assignment of a Component to its Producer(s)(2)) caused the establishing of an industry wide traceability of components for aviation products, the setup of the metagraph is based on the assumption that components are directly traced back to their suppliers. The aviation supply chain is implementable as a directed and cyclic conditional metagraph.

The direction of the metagraph is determined through two constraints of the metagraph. Directed edges initially start at the last supplier and cascade towards the aircraft manufacturer for two reasons. First, the edges' invertices hold the propositions [15]. Since suppliers are influencing the distinction of the characteristics (i.e., What kind of information exchange is offered by the supplier? With which components is the product developed so that different secure critical characteristics can be caused? Which cyber security practices has the supplier in place?) the proposition lies within the boundary of the suppliers. Thus, the directed edge starts with the suppliers and ends with their products. The direction decision is supported by the properties of a (conditional) metapath [15]. As the target is only a subset (or equal) to the outvertices of all edges in the metapath, suppliers can produce also non-relevant components for the considered target component (e.g., the landing gear).[15, p. 16, Definition 2.5] Thus, both properties of the bipartite graph (see Figure 12) hold.

The aviation supply chain characteristics can be split into implementations through a subset pattern, an edge pattern, and through the use of propositions:

Application of the Metagraph-Theoretical Construct: Subsets and Edge Pattern

Characteristic 1:	Structure of competing suppliers
Characteristic 3a:	Interconnectivity of sourced components
Characteristic 4:	Interaction of suppliers of the same tier level
Characteristic 6:	Scope of information exchange between suppliers of the same tier level

Application of the Metagraph-Theoretical Construct: Propositions

Characteristic 3b: Cyber security related criticality of the sourced components (four options)

Characteristic 5: Type of information exchange between buyer and supplier (three options)

Overall, the number of competing suppliers (based on the **structure of competing suppliers (1)**) has no influence on the algebraic calculations of the metagraph structure. However, the increase of suppliers on higher tier levels for subcomponents should be visually represented by the conditional metagraph structure in Subsection 4.2.3. The **pattern behind subsets and edges** is visualised in Figure 13. Fundamentally, the interpretation of an edge depends crucially on the invertex. An edge e_0 with an invertex of v_0 and v_1 symbolises $v_0 \wedge v_1$ since all elements of the invertex have to be included for algebraic calculations, see Figure 13a)[15]. Different sizes of subsets can be nested within each other. Smaller subsets would merge with extensive ones if the smaller ones are no longer addressed. Two edges (e_1, e_2) from two different suppliers v_0 and v_1 with the same outvertex w present a logical exclusive OR. Hence, the Figure 13b) represents $v_0 \oplus v_1$. The last Figure 13c) describes a logical OR which combines the two approaches before: $v_0 \vee v_1$.

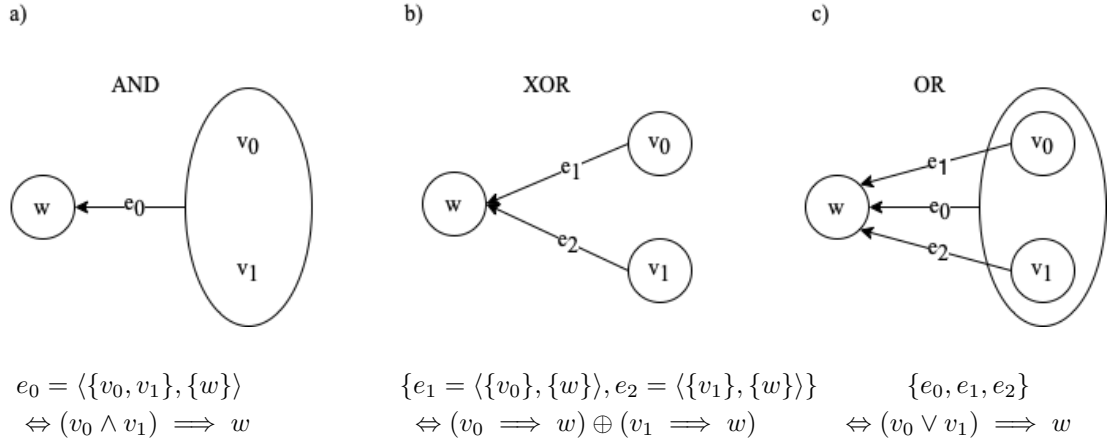


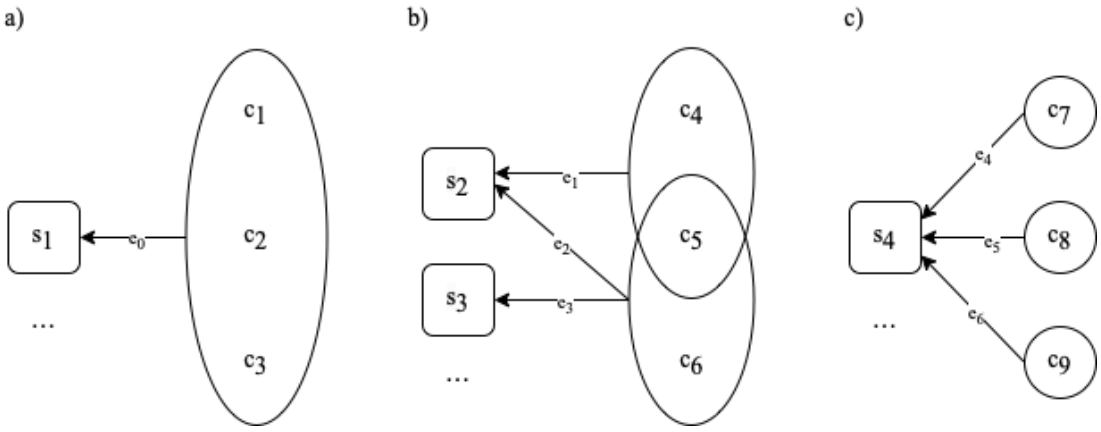
Figure 13. *Metagraph-theoretic Implementation: Logical AND, Logical Exclusive OR & Logical OR*

Given a metagraph of the aviation supply chain $S_A = \langle X_S \cup X_C, E_A\rangle$ with two disjoint sets, where $X_S = \{s_1, s_2, \ldots, s_n\}$ is the set of suppliers and $X_C = \{c_1, c_2, \ldots, c_n\}$ is the set of components. The set of edges E_A consists of edges $e_A = \langle V_{e_A}, W_{e_A}\rangle$ where the invertex $V_{e_A} \subset (X_S \cup X_C)$ and the outvertex $W_{e_A} \subset (X_S \cup X_C)$ have the following constraints:

1. $e_A = \langle V_{e_A}, W_{e_A} \rangle$ with $V_{e_A} \subseteq X_S$ and $W_{e_A} \subseteq X_C \in E_{A1}$
2. $e_A = \langle V_{e_A}, W_{e_A} \rangle$ with $V_{e_A} \subseteq X_C$ and $W_{e_A} \subseteq X_S \in E_{A2}$
3. $e_A = \langle V_{e_A}, W_{e_A} \rangle = \varnothing$ with $V_{e_A} \subseteq X_C$ and $W_{e_A} \subseteq X_C$
4. $e_A = \langle V_{e_A}, W_{e_A} \rangle = \varnothing$ with $V_{e_A} \subseteq X_S$ and $W_{e_A} \subseteq X_S$

The first constraint describes the connecting edges between suppliers and their produced (sub-)components. The second constraint describes edges connecting the purchased (sub-) components to the buyer. Further, it is not allowed to include edges in the metagraph which consist of elements of the same set X_S or X_C in the invertex as well as in the outvertex (see 3. and 4.). The connection of two subsets of components is not feasible as the perspective of edges is the production (1.) or the purchase (2.). Components cannot produce or purchase themselves. Hence, edges from constraint 3. are not applicable to supply chains in general. Edges (see constraint 4) connecting subsets of suppliers can be argued on as suppliers could communicate with each other. However, aviation characteristic 6 describes that the information exchange between suppliers is prevented by the buyer in order to keep competition ongoing. If necessary, communication takes place via the buyer.[107] Cooperating suppliers are implemented in a different way (see aviation characteristic 4).

The **interconnectivity of sourced components (3a)** can be presented through the use of the introduced pattern and the the metagraph edge introduced in the S_A Definition, constraint 2. The edge invertex consists of the set of subcomponents ($\subseteq X_C$) and the outvertex of the supplier set as buyers ($\subseteq X_S$). Figure 14 shows the three types of subcomponents' interconnectivity. The left visualisation, Figure 14a) describes subcomponents with a low modularity. Thus, the subcomponents are interconnected with each other or specially designed for a certain component. Hence, each of them is mandatory for the purchase of supplier s_1: $(c_1 \wedge c_2 \wedge c_3) \implies s_1$. The middle Figure 14b) describes a medium modularity of the subcomponent c_5. The subcomponent is part of different interconnected subcomponents for two reasons: The two subsets of subcomponents can be substitutes for the buyer s_2 as they consist of different alternative subcomponents: $(c_4 \oplus c_6) \wedge c_5 \implies s_2$, where c_5 is a mandatory subcomponent. Alternatively, the two subsets of subcomponents can be purchased by different buyers and would not compete with each other: $(c_4 \wedge s_2) \vee (c_6 \wedge s_3) \implies c_5$, where c_5 would appear in all three options. Figure 14c) shows subcomponents which are not connected through a subset. Thus, they have a high modularity. However, mostly multiple subcomponents are necessary for the production process of one component. Hence, modular subcomponents can end up in a logical AND subset (see Figure 13) through a bundled purchase of the buyer s_4 which would make it look like Figure 14a). As shown in Figure 14c), the components c_7, c_8, c_9 are connected through three separate edges with the same outvertex (supplier s_4). Hence, they are substitutes in the purchasing decision of s_4 and competing with each other: $(c_7 \oplus c_8 \oplus c_9) \implies s_4$.



Rectangle: *Element of the Supplier Set* X_S; Circle: *Element of the Component Set* X_C;
Oval: *Subset of Sets* $X_C \oplus X_S$

Figure 14. *Metagraph-theoretic Implementation: Interconnectivity of Sourced Components (3a)*

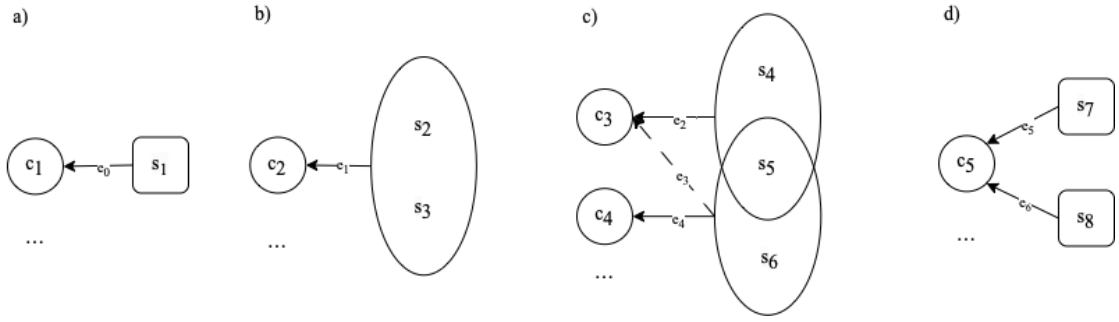
a) $e_0 = \langle\{c_1, c_2, c_3\}, \{s_1\}\rangle \Leftrightarrow (c_1 \wedge c_2 \wedge c_3) \implies s_1$

b) $\{e_1 = \langle\{c_4, c_5\}, \{s_2\}\rangle, e_2 = \langle\{c_5, c_6\}, \{s_2\}\rangle, e_3 = \langle\{c_5, c_6\}, \{s_3\}\rangle\}$
$\Leftrightarrow (((c_4 \wedge c_5) \oplus (c_5 \wedge c_6)) \implies s_2) \vee ((c_5 \wedge c_6) \implies s_3))$

c) $\{e_4 = \langle\{c_7\}, \{s_4\}\rangle, e_5 = \langle\{c_8\}, \{s_4\}\rangle, e_6 = \langle\{c_9\}, \{s_4\}\rangle\}$
$\Leftrightarrow (c_7 \implies s_4) \oplus (c_8 \implies s_4) \oplus (c_9 \implies s_4)$

The aviation characteristic **interaction of suppliers with the same tier level (4)** is based on the metagraph edges from the S_A Definition, constraint 1. In Figure 15, an invertex of an edge consists of a subset of suppliers ($\subseteq X_S$) and the outvertex of a subset of components ($\subseteq X_C$). Thus, the edges e_0, e_1, e_2, e_3, e_4 symbolise the production of components by suppliers and attributes the properties of the suppliers which are introduced below. Suppliers in the aviation supply chain can have three different stages of cooperation with other suppliers (common are cooperations of two suppliers and those are implemented in the key case but cooperations are not restricted in size) which is shown in Figure 15. Figure 15b) describes cooperating suppliers in a *logical AND* setting: $(s_2 \wedge s_3) \implies c_2$. Both suppliers share their resources for the production of c_2. Thus, they have one common interface with a buyer (one edge, here e_1 and hence, one common information exchange). Since they produce one common product, they have one criticality expression of the component c_2. For organisational properties where both suppliers can have different maturity levels, the inferior attribute is chosen above the superior one, based on the conservative assumption that the weakest link in a supply chain should be known [103]. The first Figure 15a) describes the strongest way of supplier cooperation which ends in a separate join venture organisation. As both cooperating suppliers establish a legally independent unit it is treated as own supplier s_1. The third Figure 15c) describes a supplier s_5 which has two cooperations with s_4 and s_6 ongoing. Edges e_2 and e_4 describe two supplier cooperations

producing different components. Thus, $((s_4 \wedge c_3) \vee (s_6 \wedge c_4)) \wedge s_5$ has to hold. Additionally, two cooperations could produce the same component (see e_2 and e_3). This situation is questionable as suppliers (e.g., s_5) would compete against themselves. Thus, it is not implemented in the key case (see Table 6 but not restricted as those cases could appear). This thesis is not a legal work on antitrust and competition law and thus, this issue will not be pursued further. The fourth Figure 15d) introduces two competing suppliers for the same component c_5: $(s_7 \oplus s_8) \implies c_5$. They can differ from each other through their attributes which can influence the decision on which supplier to chose. How these attributes are included is explained below.



Rectangle: *Element of the Supplier Set* X_S; Circle: *Element of the Component Set* X_C;
Oval: *Subset of Sets* $X_C \oplus X_S$

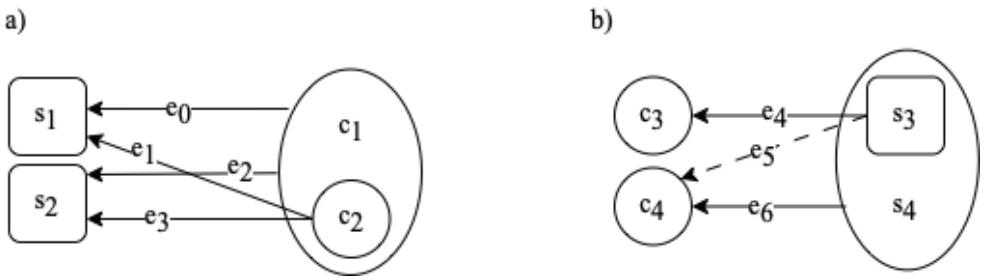
Figure 15. *Metagraph-theoretic Implementation: Interaction of Suppliers with the Same Tier Level (4)*

a) $e_0 = \langle s_1, c_1 \rangle \Leftrightarrow s_1 \implies c_1$
b) $e_1 = \langle \{s_2, s_3\}, c_2 \rangle \Leftrightarrow s_2 \wedge s_3 \implies c_2$
c) $e_2 = \langle \{s_4, s_5\}, c_3 \rangle, e_3 = \langle \{s_5, s_6\}, c_3 \rangle, e_4 = \langle \{s_5, s_6\}, c_4 \rangle$
$\Leftrightarrow ((s_4 \oplus s_6) \wedge s_5 \implies c_3) \vee ((s_5 \wedge s_6) \implies c_4)$
d) $e_5 = \langle s_7, c_5 \rangle, e_6 = \langle s_8, c_5 \rangle \Leftrightarrow (s_7 \implies c_5) \oplus (s_8 \implies c_5)$

Additionally, the dependency of the interconnectivity of multiple components can be **unilateral and bilateral**. Figure 14 introduced the bilateral interconnectivity of (sub-) components. Figure 16a) introduces the unilateral dependency of the subcomponent c_1 towards c_2 as it is exemplary included in the key case for the sensors (312 as c_2) and the control algorithm (313 as c_1). The subcomponent c_2 is not dependent on c_1. Hence, c_2 has an own purchasing edge while c_1 is only able to be purchased in combination with c_2:

$$\{e_0, e_1, e_3, e_3\} \Leftrightarrow (c_1 \wedge c_2) \oplus (c_2 \neg c_1) \implies (s_1 \vee s_2)$$

Figure 16b) introduces the unilateral approach for suppliers and describes different stages of interaction between suppliers of the same tier level. As suppliers cooperate in production of one component (here c_4) they can produce independently from each other additional



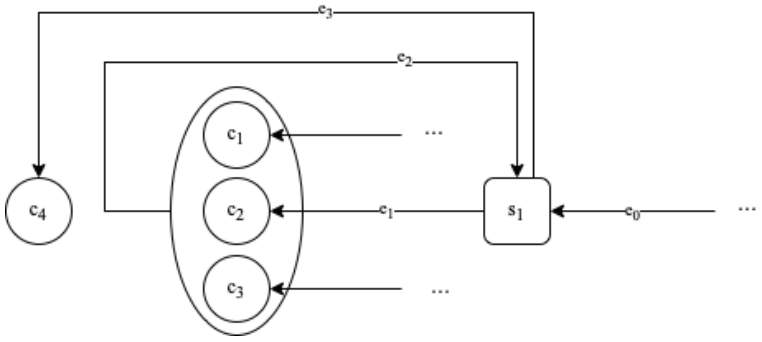
Rectangle: *Element of the Supplier Set* X_S; Circle: *Element of the Component Set* X_C; Oval: *Subset of Sets* $X_C \oplus X_S$

Figure 16. *Metagraph-theoretic Implementation: Unilateral Elements of 3a and 4*

products. Thus, supplier s_3 produces the component c_3 non-cooperatively. In case a production of component c_4 is conducted in cooperation the investment of producing the component alone (see edge e_5) is not rationally justifiable for the aviation supply chain and hence, not included in the key case. However, since this situation is not necessarily impossible, an edge $e_5 = \langle s_3, c_4 \rangle$ is not explicitly forbidden:

$$\{e_4, e_5, e_6\} \Leftrightarrow ((s_3 \wedge s_4) \oplus (s_3 \neg s_4) \implies c_4) \vee (s_3 \implies c_3).$$

The last feature of the aviation supply chain metagraph is the cycle of self-producing suppliers (see aviation characteristic 1). The self supplied component has to be implemented as an external component of the specific supplier as the supplier could sell it as well to other buyers or could also supply it from another supplier in case of emergencies at the own production site. Exemplary, Figure 17 visualises a supplier s_1 who is producing an own subcomponent c_2. Hence, the cycle $\ni \{e_1, e_2\}$ is generated. This cycle could hold two problems of metapath calculation: On the one hand, it could be caught in a loop which iterates infinite. On the other hand, the whole subset $\{c_1, c_2, c_3\}$ could be ignored by a metapath cascading directly via the edges $\{e_0, e_3\}$ to the target set (here exemplary c_4).



Rectangle: *Element of the Supplier Set* X_S; Circle: *Element of the Component Set* X_C; Oval: *Subset of Sets* $X_C \oplus X_S$

Figure 17. *Metagraph-theoretic Implementation: Cycle of Self-Producing Supplier*

To solve both issues the propositions of the conditional metagraph can help (see below). For each (sub-)component an attribute with the number of the following component is attached to the purchasing edge (here e_0). Thus, it would be known that c_2 must be navigated to c_4. Since the cycle contains elements rather than proposition, the cycle can be satisfied with the use of iterations.[15] Another examplary cycle would be a cooperating supplier pair which is purchasing components from each other. The propositions of the conditional metagraph would also solve the cyclic issues mentioned above in this case.

For the attentive reader, the question arises as to where the two remaining characteristics (**cyber security related criticality of the components (3b) and information exchange of suppliers (5)**) of the aviation supply chain apply in the metagraph structure. These properties are not deployable in a simple metagraph. Subsequently, the conditional metagraph is applied to the aviation supply chain. The properties of the simple metagraph mentioned above also hold for the conditional metagraph.

Given a conditional metagraph of the aviation supply chain $S_{AC} = \langle X_p \cup X_v, E_{AC} \rangle$ with two disjoint sets, where $X_v = \langle X_S \cup X_C \rangle$ is a set of variables consisting of two disjoint sets: $X_S = \{s_1, s_2, \ldots, s_n\}$ as a set of suppliers and $X_C = \{c_1, c_2, \ldots, c_n\}$ as a set of (sub-)components. X_p is a set of propositions consisting of four disjoint sets $X_p = \langle X_{pi} \cup X_{pk} \cup X_{pt} \cup X_{pm} \rangle$:

$X_{pi} = \{i_1, i_2, \ldots, i_n\}$, X_{pi} : Set of information exchange attributes
$X_{pk} = \{k_1, k_2, \ldots, k_n\}$, X_{pk} : Set of component's cyber security criticality attributes
$X_{pt} = \{t_1, t_2, \ldots, t_n\}$, X_{pt} : Set of target component attributes
$X_{pm} = \{m_1, m_2, \ldots, m_n\}$, X_{pm} : Set of cyber security maturity niveaus
with $V_{AC} \subseteq X_S$ and $W_{AC} \subseteq X_C \forall i, k, m \in X_{pi} \cup X_{pk} \cup X_{pm}$
and $V_{AC} \subseteq X_C$ and $W_{AC} \subseteq X_S \forall t \in X_{pt}$

Each set of propositions is assigned to one of the constraints from the S_A Definition. Attributes in the proposition sets are not restricted in their repetition. Further, $\forall e_{AC} \in E$ with $V_{e_{AC}}$ as invertex and $W_{e_{AC}}$ as outvertex has to hold $V_{e_{AC}} \cup W_{e_{AC}} \neq \varnothing$. As we do not have attributes on the variables themselves, the second requirement of the metagraph definition of [15, p. 55, Definition 5.1] is obsolete. As there exist two subsets of edges

Additionally, the metapath $M_{AC}(B_{AC}, C_{AC})$ of the conditional metagraph of the aviation supply chain is a set of edges $E'_{AC} \subseteq E_{AC}$ and has a source set $B_{AC} \subset X_v$ and a target set $C_{AC} \subset X_v$ with the following constraints:

1. each $e'_{AC} \in E'_{AC}$ is on a simple path from some element in B_{AC} to some element in C_{AC},
2. $[\bigcup_{e'_{AC}} V_{e'_{AC}} \setminus \bigcup_{e'_{AC}} W_{e'_{AC}}] \subseteq B_{AC}$,
3. $C_{AC} \subseteq \bigcup_{e'_{AC}} W_{e'_{AC}}$. [15, p. 16, Definition 2.5]

Further, the metapath is constructed through the use of $B_{AC} \cup X_p$ to reach C. The relevant set of propositions is defined by differentiating between input propositions and intermediate propositions. As the graph only holds propositions in the invertices of the edges of $M_{AC} = \{g'_g, g = 1, \ldots, G\}$, the intermediate propositions can be excluded at this point and the input propositions are the following [15, pp. 57, Definition 5.3]:

$$\alpha_{AC} = \left(\bigcup_{g=1}^{G} V'_g \right) \cap X_p.$$

One special rule applies for the set of propositions of X_{pk} as the choice of a subcomponent can influence the secure critical property of the component produced. Exemplary, the tyre inflation system 308 can be produced with a critical connection to the airport systems by supplier 18 and without any critical subcomponent by supplier 19, see Table 6 [104]. Hence, the proposition is only known in runtime depending on the edges being included in a metapath. This would be no issue in case the proposition would be part of the outvertex as propositions are allowed to be a subset of the outvertices W_{AC}. However, this would also mean that the outvertex of an edge would be in that case solely a proposition.[15, p. 55, Definition 5.1] Since the subset of suppliers in the outvertex is an essential part of the metagraph, this property of the metagraph cannot be used. Thus, the proposition $\in X_{pk}$ is part of the set of invertices V_{AC} of the subset E_{A1} and supported by a function which is generated after calculating the metapaths. This function adds and attaches the critical properties of the different subcomponents for each necessary path (the change of criticality is mostly an exception) to allow tracability of the tier level on which a special criticality was included for a specific component. As the conditional metagraph is built based on logical operations shown in Figure 13, the metapath has to be filtered for *edge-dominant* metapaths after including the checks of attributes of X_{pk} and X_{pt}. Elements $t \in X_{pt}$ are the only attributes which are allowed on the edges of the subset E_{A2} and contribute to the correct mapping of (sub-)components which also include self-supplying suppliers.

Finally, the context of a conditional metagraph of the aviation supply chain is introduced as it is relevant for the implementation of the scenarios. The context is built on two sets of propositions which are labeled *true* and *false*. In the aviation cyber security context it is differentiated between propositions sets which are accepted and ones which are not as

thresholds have to hold for certain security and safety standards. Thus, the terms true and false do not fit here and won't be used in this environment. The sets of propositions which were already mentioned in S_{AC} Definition can be part of either accepted or not accepted propositions shown in the following definition:

Given a conditional metagraph of the aviation supply chain $S_{AC} = \langle X_v \cup X_p, E_{AC} \rangle$, we can define a *context* $K(P_{AC}, Q_{AC}, S_{AC})$ by having two sets of propositions

$P_{AC} \subseteq (X_{pi} \cup X_{pk} \cup X_{pm})$ that includes the *accepted* attributes
$Q_{AC} \subseteq (X_{pi} \cup X_{pk} \cup X_{pm})$ that includes the *non-accepted* attributes

and for any edge $e'_{AC} \in E_{AC}$ the following rules apply:

- if $e'_{AC} \in E_{AC}$ contains any $p \in P$ the edge is edge is simplyfied by deleting p and in case the edge results in a null vertex the whole edge is deleted;
- if $e'_{AC} \in E_{AC}$ contains any $q \in Q$ in either vertex, delete q and the edge which excludes the deletion of other elements in the vertices of the edge and includes also further propositions on the edge (which deleted as well).

The rules show that only edges are deleted which include subsets of P and Q. Edges which include neither $p \in P$ nor $q \in Q$ will stay part of the context. This is beneficial for the setup of the two subsets E_{A1} and E_{A2} of the edge set E_{AC}. Since all attributes are on edges which are in subset E_{A1}, the edges of E_{A2} stay untouched independent of the chosen P and Q. This can cause an overhead in the calculation of the metapaths as not required edges of E_{A2} also stay untouched.

The use of *projections* generates views on top of the graph similar to the definition of contexts but instead of filtering for attributes on the edges, the projection focuses on selected nodes (suppliers X_S or components X_C). By selecting only elements $\in X_C$ the supply chain is visualised for the user without the need to disclose suppliers in the supply chain as long as there is a dominant metapath between the components existing (see Definition 14[15]). However, the calculation of projections is proven difficult as dominant metapaths consist of input-dominant metapaths [15, p. 27, Definition 3.3]. As input-dominant metapaths are NP-hard [70], the execution of projections has to be further researched.

Concluding, the conditional metagraph implements all aviation characteristics from Subsection 4.1.1. The second question is answered as to how the aviation supply chain is represented by the graph-theoretic construct of the conditional metagraph.

4.2.2 Integration of Cyber Security Maturity Niveaus of the Suppliers

This chapter focuses on the integration of the cyber security maturity of suppliers onto the conditional metagraph of the aviation landing gear supply chain. Before introducing the mapping of the suppliers to their cyber security maturity niveaus (in Table 8), the representation of the cyber security maturity is shortly explained which has five options:

1. CMMCv1 Practices: Cyber Security Maturity Model Certification [12]
2. NIST SP 800-171: Protection of Controlled Unclassified Information in Non-Federal Systems and Organisations [10]
3. ISO 27001: Reference Set of Generic Information Security Controls Including Implementation Guidance [9]
4. IT Baseline Protection Manual: Basic Protection in Information Security [13]
5. Cyber Security Practices, Orientated on the CMMCv1 Practices [12]

The suppliers' cyber security maturity levels are randomly distributed and can become apparent through one (or more in case they own certifications of more than one mentioned standard) of the introduced presentations of cyber security maturity niveaus. This should demonstrate the global dispersion of suppliers and that they are therefore subject to comply with different standards. The standards are exemplary chosen for the key case and based on the certification standards introduced in Chapter 2. However, they can be expanded to include additional standards. Additionally, *cyber security practices*[2] relate to different practices of standards without the need of an extensive, time, and cost consuming certification process. This allows SMBs to comply to the mandatory cyber security practices and to be part of the cyber security mature supply chain of the landing gear without having a cyber security budget that has to keep up with that of larger companies. The introduced certification standards are only useful for a cyber maturity assessment if they can be compared with each other. A mapping of the four standards plus the practices is possible as they overlap with each other. But the mapping comes with two drawbacks: First, the standards can intersect on different granularity levels with each other (see IT Baseline Protection Manual and the CMMCv1)[96]. Secondly, the certification standards can encompass different scopes of coverage. The CMMCv1 is the certification standard that achieves the highest level of maturity. Therefore, its maturity levels ($L1, L2, L3$) are used as reference maturity levels which are integrated in the supply chain key case S_{AC} in form of three CMMCv1 Domain Access Control (AC) Practices. Table 7 shows the mapping of the different certificates and practices for the three practices ($L1AC1001$, $L2AC3017$ and $L3AC4023$) of the AC domain.

[2]The assessment of the cyber security practices could be conducted by the buyer or an additional third-party auditor.

Table 7. *Exemplary Mapping of CMMCv1, NIST SP 800-171, BSI IT Basic Protection and practices for three CMMCv1 Domain Access Control Practices*

CMMCv1Level	CMMCv1Domain	CMMCv1Practice	NISTSP800-171	ISO27001	BSI-BS[a]	BSI-BS-A[b]	Practice
L1	L1AC	L1AC1001	Rev 2 3.1.1	6.2.1	INF.9	INF.9.A2 Safety guideline for mobile workplaces	Technical Configurations - Limit access to authorized users
L1	L1AC	L1AC1001	Rev 2 3.1.1	6.2.1	INF.9	INF.9.A8 Safety guideline for mobile workplaces	Technical Configurations - Limit access to authorized users
L1	L1AC	L1AC1001	Rev 2 3.1.1	6.2.1	SYS.3.1	SYS.3.1.A1 Regulations on the mobile use of laptops	Technical Configurations - Limit access to authorized users
L1	L1AC	L1AC1001	Rev 2 3.1.1	6.2.1	SYS.3.1	SYS.3.1.A14 Appropriate storage of laptops	Technical Configurations - Limit access to authorized users
L1	L1AC	L1AC1001	Rev 2 3.1.1	6.2.1	SYS.3.2	SYS.3.2.1.A10 Guideline for employees on the use of mobile devices	Technical Configurations - Limit access to authorized users
L1	L1AC	L1AC1001	Rev 2 3.1.1	6.2.1	SYS.3.2	SYS.3.2.2.A1 Establishment of a mobile device management policy	Technical Configurations - Limit access to authorized users
L1	L1AC	L1AC1001	Rev 2 3.1.1	6.2.1	SYS.3.2	SYS.3.2.2.A2 Determination of permitted mobile devices	Technical Configurations - Limit access to authorized users
L1	L1AC	L1AC1001	Rev 2 3.1.1	6.2.1	SYS.3.2	SYS.3.2.3 iOS (for Enterprise)	Technical Configurations - Limit access to authorized users
L1	L1AC	L1AC1001	Rev 2 3.1.1	6.2.1	SYS.3.2	SYS.3.2.4 Android	Technical Configurations - Limit access to authorized users
L1	L1AC	L1AC1001	Rev 2 3.1.1	6.2.1	SYS.3.3	SYS.3.3 Mobile Phones	Technical Configurations - Limit access to authorized users
L1	L1AC	L1AC1001	Rev 2 3.1.1	6.2.1	IND.1	IND.1.A9 Restrictive use of removable storage devices and mobile devices in ICS environments	Technical Configurations - Limit access to authorized users
L1	L1AC	L1AC1001	Rev 2 3.1.1	6.2.2	OPS.1.2	OPS.1.2.4.A1 Rules for teleworking	Technical Configurations - Limit access to authorized users
L2	L2AC	L2AC3017	Rev 2 3.1.4	6.1.2	ORP.1	ORP.1.A4 Separation of functions between incompatible tasks	Technical Configurations - Separation of Duties
L2	L2AC	L2AC3017	Rev 2 3.1.4	6.1.2	ORP.4	ORP.4.A4 Allocation of tasks and separation of functions	Technical Configurations - Separation of Duties
L3	L3AC	L3AC4023					Configuration or Software Solution

[a]BSI-BS = IT Baseline Protection Manual Module (German: Baustein)
[b]BSI-BS-A = IT Baseline Protection Manual Requirement (German: Baustein Anforderung)

The four certification standards are built on the same principle: A higher maturity level builds on the lower ones. This implies that the highest maturity level is only achieved if all maturity levels below are met. Hence, the properties of the standards are extracted in the following enumeration:

1. CMMCv1 Practices
   - $L1 \implies L1AC1001$
   - $L2 \implies L1AC1001 \wedge L2AC3017$
   - $L3 \implies L1AC1001 \wedge L2AC3017 \wedge L3AC4023$
   - Hence, $L3 \implies ((L1 \wedge L2 \wedge L3) \Leftrightarrow (L1AC1001 \wedge L2AC3017 \wedge L3AC4023))$
2. NIST SP 800-171
   - $L1 \implies Rev23.1.1$
   - $L2 \implies Rev23.1.1 \wedge Rev23.1.4$
   - $L3$ cannot be met as there is no NIST SP 800-171 practice encompassing the requirements of this CMMCv1 maturity level.
3. ISO 27001
   - $L1 \implies 6.2.1 \wedge 6.2.2$
   - $L2 \implies 6.2.1 \wedge 6.2.2 \wedge 6.1.2$
   - $L3$ cannot be met as there is no ISO 27001 practice encompassing the requirements of this CMMCv1 maturity level.
4. IT Baseline Protection Manual
   - $INF.9 \implies INF.9.A2 \wedge INF.9.A8$
   - $SYS.3.1 \implies SYS.3.1.A1 \wedge SYS.3.1.A14$
   - $SYS.3.2 \implies SYS.3.2.1.A10 \wedge SYS.3.2.2.A1 \wedge SYS.3.2.2.A2 \wedge SYS.3.2.3 \wedge SYS.3.2.4$
   - $IND.1 \implies IND.1.A9$
   - $OPS.1.2 \implies OPS.1.2.4.A1$
   - $ORP.1 \implies OPR.1.A4$
   - $ORP.4 \implies OPR.4.A4$
   - $L1 \implies INF.9 \wedge SYS.3.1 \wedge SYS.3.2 \wedge SYS.3.3 \wedge IND.1 \wedge OPS.1.2$
   - $L2 \implies INF.9 \wedge SYS.3.1 \wedge SYS.3.2 \wedge SYS.3.3 \wedge IND.1 \wedge OPS.1.2 \wedge ORP.1 \wedge ORP.4$
   - $L3$ cannot be met as there is no BSI-BS practice encompassing the requirements of this CMMCv1 maturity level.
5. Cyber Security Practice
   - $L1 \implies$ Technical Configurations - Limit access to authorized users [$csp1$]
   - $L2 \implies$ Technical Configuration - Separation of Duties [$csp2$] $\wedge csp1$
   - $L3 \implies$ Configuration or Software Solution [$csp3$] $\wedge csp2 \wedge csp1$
   - Hence, $L3 \implies csp1 \wedge csp2 \wedge csp3$

The cyber security maturity niveaus of $L1$, $L2$, and $L3$ are the ones described in Chapter 2: Basic cyber hygiene, intermediate cyber hygiene, and good cyber hygiene. The considered CMMCv1 Domain (AC) has no practices in maturity niveaus of $L4$ (proactive) and $L5$ (advanced). Since the remaining standards do not have them either, the absence does not pose a problem. Additionally, the maturity niveau $L0$ is added for suppliers who have no cyber security maturity at all and nL for suppliers which have their degree of maturity not disclosed. The enumeration of the certification standards' properties visualises that only CMMCv1 Practices (1.) and the cyber security practices (5.) have representative cyber security maturity niveaus of $L3$. The other three certification standards have equivalent practices to the niveau of $L2$. Table 8 shows the cyber security maturity niveaus of the key case suppliers 1-31. Additionally, the reference CMMCv1 maturity level is mapped in the right column. A comparison is therefore possible.

Table 8. *Cyber Security Maturity Niveaus of the Considered Landing Gear Suppliers*

No Supplier	Co Produced	CC	IE	Cyber Sec Maturity	CMMCv1Level
0	1000	0,1,2,3	IE0	Start Point of the Landing Gear Supply Chain (not in Scope)	
1	101	0,1,2,3	IE1	6.2.1, 6.2.2, 6.1.2	L2
	212	0,3	IE0	6.2.1, 6.2.2, 6.1.2	L2
	222	0,3	IE1	6.2.1, 6.2.2, 6.1.2	L2
2	101	0,1,2,3	IE1	L1AC1001, L2AC3017, L3AC4023	L3
3	213	0,1,2,3	IE2	L1AC1001, L2AC3017, L3AC4023	L3
	223	0,1,2,3	IE1	L1AC1001, L2AC3017, L3AC4023	L3
4	213	0,1,2,3	IE2	INF.9,SYS.3.1,SYS.3.2,IND.1,OPS.1.2,ORP.1,ORP.4	L2
	223	0,1,2,3	IE1	INF.9,SYS.3.1,SYS.3.2,IND.1,OPS.1.2,ORP.1,ORP.4	L2
5	213	0,1,2,3	IE2	SYS.3.1, SYS.3.2, OPR.1	L0
	223	0,1,2,3	IE1	SYS.3.1,SYS.3.2, OPR.1	L0
6	211	0,1,2,3	IE2	L1AC1001,L2AC3017,L3AC4023	L3
	212	0,3	IE2	L1AC1001,L2AC3017,L3AC4023	L3
	221	0,1,2,3	IE1	L1AC1001,L2AC3017,L3AC4023	L3
	222	0,3	IE1	L1AC1001,L2AC3017,L3AC4023	L3
7	211	0,1,2,3	IE2	INF.9,SYS.3.1,SYS.3.2,IND.1,OPS.1.2,ORP.1,ORP.4	L2
	221	0,1,2,3	IE1	INF.9,SYS.3.1,SYS.3.2,IND.1,OPS.1.2,ORP.1,ORP.4	L2
8	221	0,1,2,3	IE1	6.1.2	L0
	222	0,3	IE1	6.1.2	L0
9	224	0	IE2	L1AC1001,L2AC3017,L3AC4023	L3
10	224	0	IE2	Rev 2 3.1.1, Rev 2 3.1.4	L2
11	224	0	IE2	6.2.1, 6.2.2	L1
12	312	3	IE1	Rev 2 3.1.1	L1
13	312	3	IE2	L1AC1001,L2AC3017	L2
14	304	0	IE1	6.2.1, 6.2.2, 6.1.2	L2
	305	0	IE1	6.2.1, 6.2.2, 6.1.2	L2
15	304	0	IE0	nL	nL
	305	0	IE0	nL	nL
16	312	3	IE1	L1AC1001,L2AC3017,L3AC4023	L3
	301,309	1,3	IE2	L1AC1001,L2AC3017,L3AC4023	L3 (L2 - 17)
17	301,309	1,3	IE2	Rev 2 3.1.1, Rev 2 3.1.4	L2
18	302	0	IE1	L1AC1001	L1
19	302	0	IE2	6.2.1, 6.2.2, 6.1.2	L2
20	313	1,2	IE2	L1AC1001,L2AC3017,L3AC4023	L3
	303	1,3	IE2	L1AC1001,L2AC3017,L3AC4023	L3

Table 8. *Cyber Security Maturity Niveaus of the Considered Landing Gear Suppliers*

No Supplier	Co Produced	CC	IE	Cyber Sec Maturity	CMMCv1Level
21	313	1,2	IE1	6.2.1,6.2.2,6.1.2	L2
	303	1,3	IE1	6.2.1,6.2.2,6.1.2	L2
22	307	0	IE1	6.2.1	L0
23	307	0	IE1	INF.9,SYS.3.1,SYS.3.2,IND.1,OPS.1.2,ORP.1,ORP.4	L2
	308	3	IE1	INF.9,SYS.3.1,SYS.3.2,IND.1,OPS.1.2,ORP.1,ORP.4	L2
24	301,303	1,3	IE1	csp1,csp2,csp3	L3
25	301,303	1,3	IE1	csp1,csp2,csp3	L3
26	301	1,3	IE2	6.2.1,6.2.2	L1
27	307, 308	0	IE1	L1AC1001	L1
28	306,310,311	0	IE1	L1AC1001,L2AC3017	L2 (L1 - 29)
29	306,310,311	0	IE1	6.2.1, 6.2.2	L1
30	306,310,311	0	IE2	L1AC1001,L2AC3017,L3AC4023	L3 (L2 - 31)
31	306,310,311	0	IE2	L1AC1001,L2AC3017	L2

CC - *Critical Characteristic: 0 Non-critical, 1 COTS Usage, 2 Critical Access, 3 Critical Connection*
IE - *Information Exchange: 0 None, 1 Black Box Approach, 2 Critical Information Exchange*
CMMCv1Level - *Cyber Security Maturity: L0 none, L1 Basic, L2 Intermediate, L3 Good, nL non-disclosed*

In Chapter 4 the cyber security maturity niveaus are introduced as a subset X_{pm} of the proposition set X_p of the conditional metagraph S_{AC} with the constraint that they can only be mapped on edges of the subset E_{A1}. Using the reference certification maturity niveaus of the CMMCv1, the set of X_{pm} consists of the following elements:

$$\begin{aligned} X_{pm} = \; & \{L0, L1, L2, L3, nL, nnL, nL0, nL1, nL2, nL3\} \text{ with} \\ & (L3 \wedge L2 \wedge L1 \neg(L0 \wedge nL)) \\ \oplus \; & (nL3 \wedge L2 \wedge L1 \neg(L0 \wedge nL)) \\ \oplus \; & (nL3 \wedge nL2 \wedge L1 \neg(L0 \wedge nL)) \\ \oplus \; & (nL3 \wedge nL2 \wedge nL1 \wedge L0 \neg nL) \\ \oplus \; & (nL3 \wedge nL2 \wedge nL1 \wedge nL0 \wedge nL) \end{aligned}$$

The supplementation of negations in X_{pm} is important for generating contexts. To illustrate the filter for each element, Table 9 introduces the input of each elements' P and Q.

Table 9. *Metagraph-theoretic Implementation: Context P and Q for the Cyber Security Maturity Niveaus*

PnL	nL	nL0	nL1	nL2	nL3
PL0	nnL	L0	nL1	nL2	nL3
PL1	nnL	nL0	L1	nL2	nL3
PL2	nnL	nL0	L1	L2	nL3
PL3	nnL	nL0	L1	L2	L3

QnL	QL0	QL1	QL2	QL3
nL	nL0	nL1	nL2	nL3
nnL	L0	nL1	nL2	nL3
nnL	nL0	L1	nL2	nL3
nnL	nL0	L2	L2	nL3
nnL	nL0	L3	L3	L3

CMMCv1Level - *Cyber Security Maturity: L0 none, L1 Basic, L2 Intermediate, L3 Good, nL non-disclosed, n . . . Negation of the aforementioned*

4.2.3 Conditional Metagraph Model of the Landing Gear

The variable set of the conditional metagraph of the landing gear supply chain consists of the suppliers and their (sub-)components of the landing gear component of an aircraft manufacturer. The suppliers in the generating set are numbered as shown in Table 6. The variable set consists of numbers in range of 0 up to 1000 split into different categories:

$0-100$	Suppliers
1000	Component Tier 0 (aircraft type)
$101-199$	Components Tier 1
$201-299$	Components Tier 2
$300-399$	Components Tier 3
$901-999$	Support Nodes for Components of Tier 1

This categorisation at early stage is necessary as possible sub-metagraphs can be included which need a buffer for the numbering of components and suppliers on various tier levels. Further, also the propositions are named beforehand. As the context of a conditional metagraph (see Definition 11) includes also undetermined propositions as $p \in X_p \setminus (P \cup Q)$. As the aim is to generate contexts with a particularly secure supply base, it is necessary to address undetermined propositions. In order to address non-expression, negative attributes ($\neg p$) are integrated into the four disjoint sets in addition to the expressed p attributes:

1. $X_{pi} = \{IE0, IE1, IE2, nIE0, nIE1, nIE2\}$
   with $(IE0 \oplus nIE0) \oplus (IE1 \oplus nIE2) \oplus (IE2 \oplus nIE2)$
2. $X_{pk} = \{CC0, CC1, CC2, CC3, nCC0, nCC1, nCC2, nCC3\}$
   with $(CC0 \oplus nCCO) \vee (CC1 \oplus nCC1) \vee (CC2 \oplus nCC2) \vee (CC3 \oplus nCC3)$
3. $X_{pt} = \{t101, t102, \ldots, t399, t1000\}$
4. and $\bigcup_{i=1}^{I} m_i \oplus \neg m_i \subseteq X_{pm}$, I depends on user input (see below)

The elements of the proposition categories have different correlations with each other. Ordinal characteristics count for elements of the sets X_{pi} and X_{pm} (the rank of nL is decided based on the user input, see below). In set X_{pk} only the distinction between $CC0$ and $(CC1, CC2, CC3)$ is ordinal, as $CC0$ is less critical than the rest. The ranking of $(CC1, CC2, CC3)$ is not possible, thus they have nominal property, and can appear simultaneously on the same edge. Similar correlation is attributed to the elements of X_{pt} as they visualise different components.

The setup of the metagraph of the landing gear assumes a decentral information collection (through excel sheets/csv files) from different suppliers which only deliver the information

they know, which is: The suppliers' own cyber security maturity niveau (X_{pm}: certification practices or cyber security practices), the associated expire date of the certification (na for the practices), their direct suppliers with their components and respectively the cyber criticality of the purchased subcomponents (X_{pk}), and the information exchange type (X_{pi}). Figure 18[3] visualises the building process of the conditional metagraph for the landing gear.

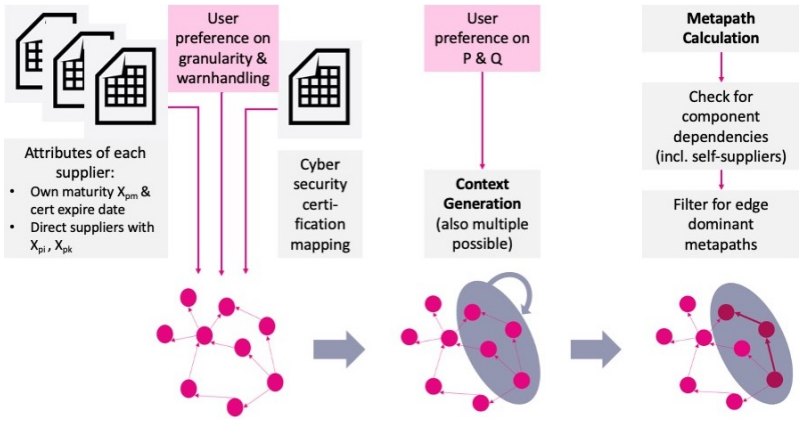


Figure 18. *Building Process of the Conditional Metagraph*

Before generating the conditional metagraph S_{AC}, the user has to configure three inputs:

1. The *reference code* of the cyber security maturity: The reference code is the certification standard or practice on which the edge elements of X_{pm} should be designed on. In this case, the reference code is the *CMMCv1Level*.
2. The warnhandling for *incompleteness*: The user can choose between
   - The supplier with missing cyber security matuirty niveau (nL) is excluded.
   - The supplier with missing cyber security matuirty niveau (nL) is included but with a warning.
   - The supplier with missing cyber security matuirty niveau (nL) is included without a warning. This option is chosen in this example.
3. The warnhandling of the certifications' expiration dates: Configuration of a certain date as treshold (warning when expiration before that date) (see pythonscript [100], not included in this example)

Based on the input of the suppliers information, the certification mapping Table 7, and the user input S_{AC} can be generated: The set of nodes, set of components, set of propositions, and thus, also the set of edges is generated. The foundation for further calculation is laid. Contexts are produced on top of S_{AC} based on further user input (P and Q). Contexts can

[3] Icons obtained from https://thenounproject.com

filter for certain component properties, information exchange types, or maturity niveaus. Hence, through a combination of the three filtering options, the securest path from the start edge 999 to the final component (the landing gear 101) is identified by using the metapath. The metapath can be used with an additional function of checking that every component ends in a metapath with its subcomponents (in case a supplier produces different products and for every component different subcomponents, e.g., supplier 8). Finally, after filtering the metapaths for logical correct paths, the edge-dominant paths are chosen above the non edge-dominant ones, to ensure that only one supply chain path is included and not partial supply chain paths (single edges) are added to full functioning supply chain paths. Based on the assumptions from Subsection 4.1.1 (in particular the Table 6) and Section 4.2 the conditional metagraph of the landing gear is shown in Figure 19.

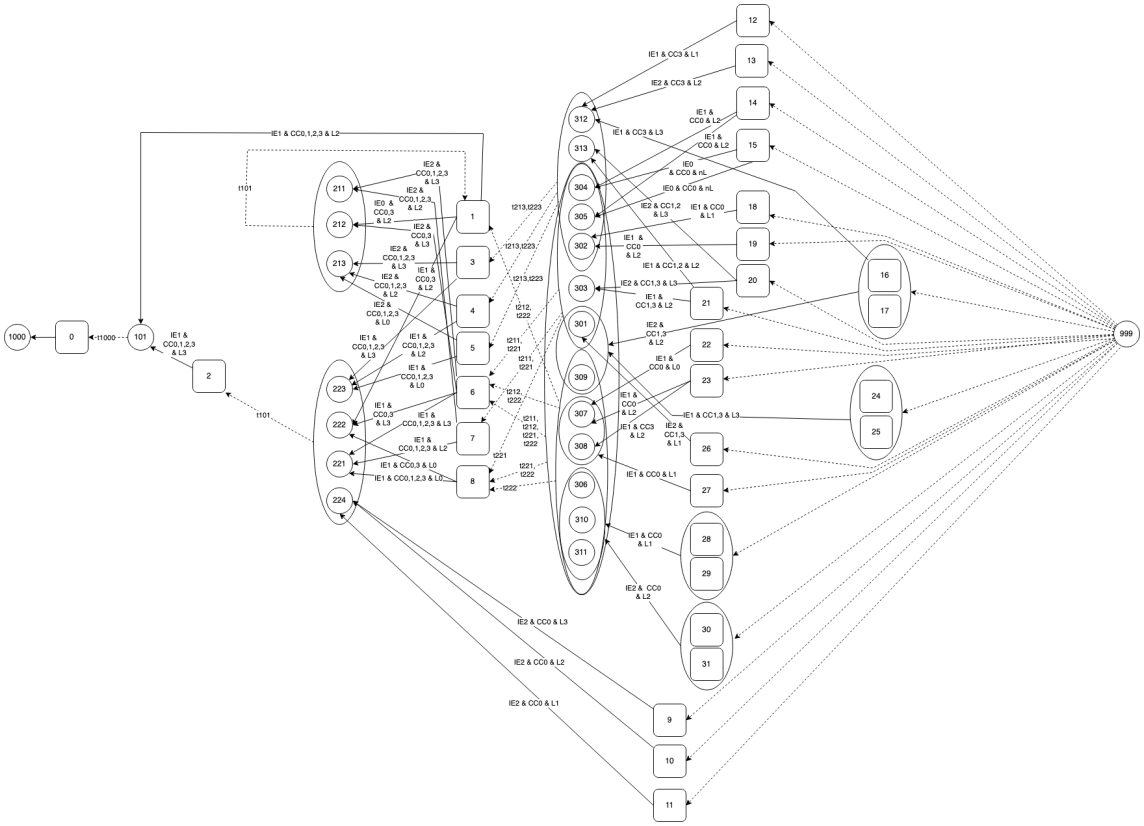


Figure 19. *Conditional Metagraph of the Censored Segment of the Landing Gear Supply Chain*

This Figure only shows the attributes without the negations for comprehensibility reasons. It is referred to the Table 9, in order to see which further attributes are needed to be added. Furthermore, the version control of a conditional metagraph and its contexts is possible by copying whole metagraphs or contexts. Additionally, contexts are detached from the base which can be a conditional metagraph or another contexts. Thus, if changes are done in the conditional metagraph, they won't impact the contexts above. Thus, an update of the graph structure can end tedious, if the user does not work with version control. Otherwise, the contexts are generated based on the new conditional metagraph version and a new context

version is established. The last point to mention is an incomplete ending of a supply chain. This characteristic can be caught through the integration of an additional element on edges of E_{A2}, precisely the edges between invertex 999 and the last layer of suppliers which then could trigger an incompleteness warning for the user of the metagraph structure.

4.2.4 Verification

The conditional metagraph of the landing gear supply chain is verified through the automation of the graph setup. Hence, it allows to change the input parameters (number of suppliers, attributes of suppliers, produced and purchased components, and attributes of the components). A pythonscript based on the library of Ranathunga and Parsonage[99, 101, 100] automates the process of establishing the generating set, the propositions, and the edges of the conditional metagraph. If the patterns and rules mentioned above hold for the output of the pythonscript, the graph structure is verified.

Overall, the conditional metagraph setup and its scenarios can be traced and reproduced through the use of the mentioned pythonscript[100]. Additionally, the verification of the conditional metagraph includes a sensitivity analysis and a scalability analysis.

The sensitivity analysis is visualised by scenario 4. Through the change of attributes of an edge, a reassessment of the most secure metapaths must be initiated. The change of CC or IE attributes would cause scenario 2 to replay its steps. Sensitivity is also shown in case a new node (supplier) or a complete sub-metagraph (a whole part of a sub-supply chain) is included, as the new node(s) are taken into consideration for calculating the securest path based on scenario 1, 2, and 3. Again, the version controlling has to be mentioned. Changes only affect the targeted conditional metagraph or view, e.g., context or projection.

The scalability analysis comes in two forms: First, the number of suppliers, components, and their connections is increased. Secondly, the number of propositions on the edges is increased. Both forms have their scaling limits, which are visible in the pythonscript [100]. Further, two characteristics of the metagraph cause drawbacks. Input-dominant metapaths are NP-hard [70]. However, the design of the conditional metagraph with one starting point in 999 requires only edge-dominant metapaths which are solveable in linear time [70]. Secondly, the generation of contexts does not delete suppliers which are not feasible for the context, e.g., the qualified supplier panel, which adds an overhead to the the calculation of metapaths. To handle the drawback, a function is developed which deletes nodes when they are excluded for contexts or in case they do not present vertices in edges $e \in E_{A1}$ of the conditional metagraph.

4.3 Case Study Snapshots: The Scenarios

The scenarios are based on snapshots which are taking place at different phases in the landing gear development which have also an effect on the supply chain management. Expert B clarifies that the aviation supplier management can be divided into the design and the production phase [104]. In the design phase of the aircraft or landing gear component the direct suppliers are chosen based on different economic parameters and then checked for qualification (compliance with regulated safety procedures) to become part of the *qualified supplier panel*. This panel exists for each aircraft and landing gear OEM. Additionally, the aircraft manufacturer has to require the airworthiness certificate of major aircraft components which also applies to the landing gear component. In the final state the aircraft type has to be certified with an airworthiness certificate. This certificate maps direct suppliers to their produced components [103]. Since these certification processes are time consuming and costly, once a certification has been issued, changes in the panel are made extremely rarely and reluctantly. It is more common to discuss or even support a direct suppliers than to part with them. These panels enable double sourcing. Hence, in the production phase they have a minimum of two qualified suppliers to purchase a component from. [104] The inquirer has taken the following snapshots as important points for the necessity to include cyber security in decision making for supplier relationships:

- **Initial Setup of the Qualified Supplier Panel:**
  Scenario 1, scenario 2, and scenario 3 represent metagraph deployment options for the decision support which supplier should enter the panel based on cyber security maturity.
- **Established Qualified and Cyber Secure Supplier Panel:**
  The decision on how to proceed with cyber security related changes in a qualified supplier panel since double sourcing still allows different purchasing options in the panel. Reassessment of the purchase option if supplier's security is increased, weakened, or because of supplier failure (scenario 4). Scenario 5 analyses the supply chain for a potential security breach.

The scenarios are implemented in Chapter 5.

5. Metagraph Scenarios

This chapter explains, implements, and discusses the scenarios of the conditional aviation metagraph S_{AC} which are used to validate the metagraph application onto the aviation supply chain by the experts. The scenarios use the graph-theoretic definitions, the introduced segment of the landing gear supply chain, the cyber security maturity mapping of the suppliers (in particular Table 9), and the final conditional metagraph and its properties from Subsection 4.2.3. Further, the scenarios build on top of each other and assume a cyber secure perfect world in which no other parameters rather than cyber secure ones have to be considered. To illustrate the potential of the metagraph, this is feasible. However, more restrictions can be added on the metagraph construct. Additionally, the same configuration for the reference certification and the handling of missing information with regard to cyber security maturity are used in this chapter as in Subsection 4.2.3. Thus, supplier 15 is included as an option for the qualified supplier panel even though the cyber security maturity level is yet unknown. Further, the reference certification is the *CMMCv1Levels*.

5.1 Scenario 1: Exclusion of Suppliers Not Considering Cyber Security

Different cyber security certificates (exemplary: CMMCv1, ISO 27001, NIST SP 800-171, BSI IT Basic Protection) and practices of suppliers are mapped to be comparable integrated into the conditional metagraph model. The aim of this scenario is to establish a supplier panel based on the requirement that every supplier needs to have at least a basic cyber hygiene. Therefore, suppliers known not to have implemented cyber security practices or maturity levels are dropped. This scenario relates to the introduction of Part-IS.[11]

5.1.1 Scenario 1: Implementation

The aim of this scenario is to define and implement a threshold for the qualified supplier panel of the landing gear component which is still in the design phase. Thus, the qualified supplier panel is still under construction. The starting point of this scenario consists of 31 suppliers which are filtered for cyber security practices. This includes that a certification or assessable practices are in place.

Hence, a context K_{S1} can be generated on top of S_{AC}. Based on S_{AC}, we define $K_{S1}(P_{S1}, Q_{S1}, S_{AC})$ with two sets of propositions

$P_{S1} = \{nL0\}$ as accepted attribute, which implies that $nL, L1, L2, L3$ are accepted.
$Q_{S1} = \{L0\}$ as non-accepted attribute.

By defining these context attributes, the not accepted attribute $nL0$ as well as the accepted attribute $L0$ will disappear in K_{S1}. The definition of the context includes the deletion of the filtered attribute for simplification. As long as the edge is not empty, the edge with the accepted attribute $L0$ is included in the context. Figure 20 shows the suppliers with a missing cyber security maturity niveau highlighted in color.

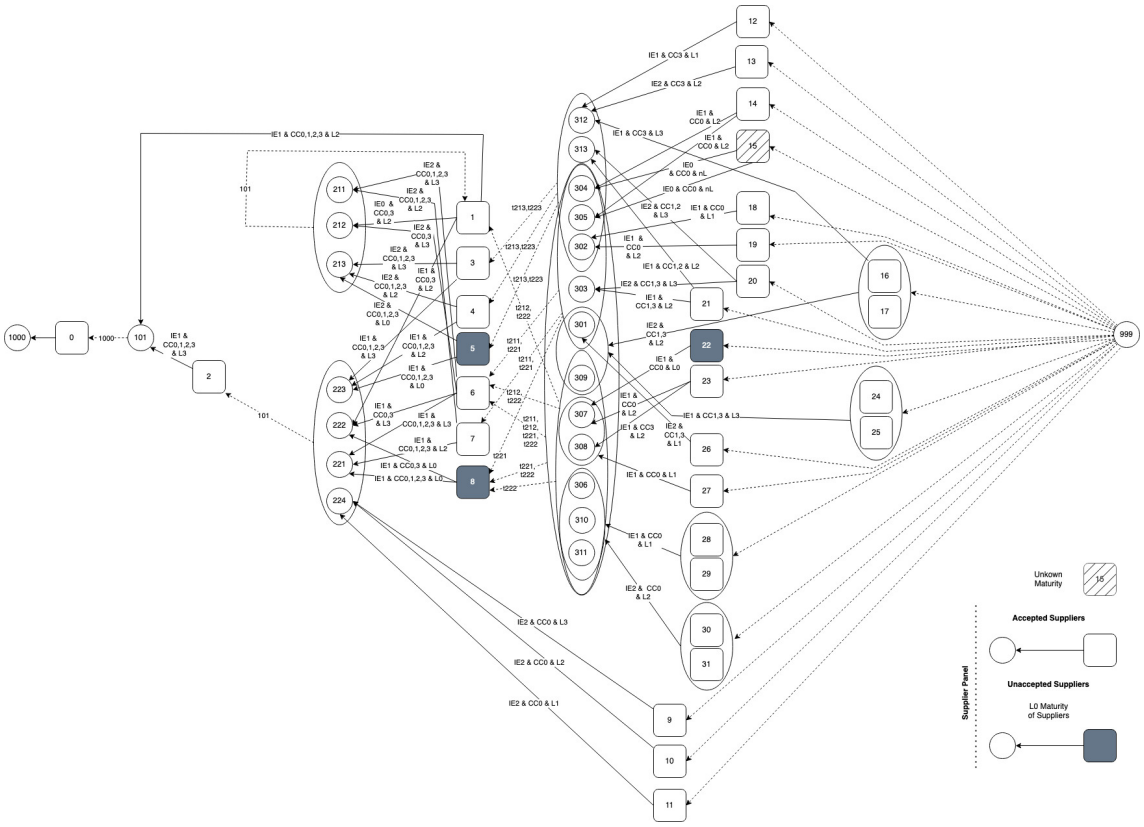


Figure 20. *Scenario 1: Suppliers with a missing Cyber Security Maturity Niveau (L0) in* S_{AC}

Hence, K_{S1} is equal to S_{AC} with exception of the missing edges $\{e_1, e_2, e_3, e_4, e_5\}$:

$e_1 = \langle\{5\}, \{213\}, [IE2, CC0, CC1, CC2, CC3, L0]\rangle$,[1]
$e_2 = \langle\{5\}, \{223\}, [IE1, CC0, CC1, CC2, CC3, L0]\rangle$,
$e_3 = \langle\{8\}, \{222\}, [IE1, CC0, CC3, L0]\rangle$,

[1]The propositions on the edges include also the negative versions of the other expressions (e.g., for e_1: $nL1, nL2, nL3, nnL, nIE1$), which are described in Table 9. For simplification reasons those are traced through Table 9 but not included in the explanation of the edges.

$$e_4 = \langle\{8\}, \{221\}, [IE1, CC0, CC1, CC2, CC3, L0]\rangle,$$
$$e_5 = \langle\{22\}, \{307\}, [IE1, CC0, L0]\rangle.$$

The edges $\{e_1, e_2, e_3, e_4, e_5\}$ are deleted because $L0$ is a proposition of them. The elimination also includes the edges' propositions. The nodes of the suppliers and components are not deleted as vertices of the edges are not removed. Thus, the link of the suppliers $\{5, 8, 22\}$ towards the landing gear component is removed and they won't be able to participate in the supply chain of the landing gear. In case they'll upgrade their cyber security maturity while the design process of the supplier panel is still ongoing, they can be reactivated by adding a renewed edge between the suppliers and their produced components. Scenario 1 is verifiable and reproducible based on a pythonscript [100].

5.1.2 Scenario 1: Discussion

Scenario 1 describes the first phase of the setup of a qualified supplier panel by dropping all suppliers with missing cyber security maturity niveaus requiring that the different certification standards and practices have been mapped, harmonised, and outputted to a preferred standard.

The overall mapping of standards is seen as beneficial since the Part-IS regulation orientates on already established and renown cyber security certification standards (e.g., NIST and ISO/IEC)[105]. Hence, the gap analysis is less complex which has two benefits: The organisation who already complies to one of those standards has a less time-consuming and cost-intensive transformation to the Part-IS compliance ahead. Secondly, the buyer can use this knowledge to prefer a supplier over another who has less investments for the transformation to take and has already a certain cyber security hygiene implemented. Expert B notes that the aviation industry could increase its cyber security requirements at one point to a level where generic cyber security certification standards would no longer be considered helpful by referring to the example of the standard EN9100 (global quality standard [111]) which is no longer sufficient for the aviation industry. However, as a starting point the mapping would be useful.[104]

Furthermore, the inclusion of suppliers with cyber security maturity is seen more appealing because of the Part-IS transformation ahead. Until now, Expert B and A did not recognise cyber security practices being included in the decision for suppliers.[104, 108] Expert C states that filtering for suppliers with certain cyber security maturity niveaus is only possible if the regulator exerts regulatory pressure onto suppliers and the aircraft OEM [106]. However, Expert D appeases the definite decision of dropping suppliers by their missing maturity niveaus. The suppliers would need to have the possibility to fulfill the

requirements and could comply belated as well. Hence, the scenario is manoeuvring - similar as the regulator - between over-regulation and too loose implementation. Being to strict with suppliers could lead them abandoning the business or being driven into insolvency. Being to loose could enable serious supply chain attacks through these suppliers.[105, 106] Hence, the cyber security practices are implemented to give these suppliers, e.g., SMBs, the chance to be admitted for a qualified cyber secure supplier panel. The implementation restriction with the cyber security practices lies within the definition of a standardised set of cyber security practice terms and the definition of the scope of each cyber security practice. Hence, even tough the extensive certification auditing is omitted, the setup of the cyber security practices encompasses an (globally enganged) authority which sets standard terms and content of each practice. Expert E, D, and F mention contractual agreements in which cyber security practices are already defined for suppliers. Those requirements could be used for the definition of cyber security practices as they target the cyber security of the purchased component as well as infrastructural and environmental aspects for a cyber secure production (e.g., authorised access of design drawings). In addition, these requirements can be verified through random visits by the buyer to the supplier's premises.[107, 105, 103] Expert B confirms that in case the decision lies between a supplier with and without a cyber security maturity, the supplier with a cyber security maturity niveau would be preferred over the other [104]. Further, linking the research of Wong et al. (2022) on SMBs, the practices should focus on employee cyber security hygiene as the backbone of SMBs lies within their human workforce [44].

Additionally, this scenario also includes one example of incompleteness of the properties of a maturity niveau of a supplier. From an overall perspective, missing information should not occur in the aviation industry. However, in the case of cyber security, it is not yet understood enough for missing aspects to be considered relevant.[103] In this example, the incompleteness of cyber security aspects is allowed (see Subsection 4.2.3 for other options) and confirmed as a common phenomena in the aviation supply chain as the Part-IS is not yet entered into force.[105, 107, 104, 108, 106, 103] From perspective of the aircraft OEM, the contract is only signed with the direct supplier. The knowledge of cyber security practices and scope of influence of the buyer only extends to the area in which contracts are formed. The contractual agreements on cyber security practices mentioned by experts E and F support this statement.[107, 103] However, the direct supplier can be contractually obliged to impose these cyber security practices as well onto its direct suppliers. But since the indirect suppliers are unknown to the buyer, potential audits cannot be carried out by the buyer. Hence, the suppliers' inheritance of the cyber security practices proceed on a basis of trust. Additionally, Expert F describes that suppliers could claim they have integrated cyber security practices but because of proprietary and confidentiality reasons, they won't disclose them [103]. Expert B describes the contractual obligation of suppliers

to inform the buyer in case an indirect supplier changes because of various reasons (see scenario 4). Hence, the decision ownership lies within the supplier but the buyer needs to be updated about the change. This counts for buyers being on tier levels of aircraft OEMs and aircraft component OEMs.[104] On a component perspective, the buyer can execute security tests on the final purchased product and implement security controls which isolate a potential insecure component and reduce the impact on the overall airworthiness safety of the system [105, 104, 107].

5.2 Scenario 2: Cyber Security Maturity Based on Information Exchange and Component Production

The second scenario filters the suppliers for certain cyber security maturity niveaus on specific information exchange types and criticality levels of components using exemplary the introduced cyber security critical component types by EASA [112]). A specific type of information sharing between buyer and supplier requires a certain level of cyber security maturity. Manufacturing a specific component (e.g., software) necessitates a certain level of cyber security maturity of the supplier. On these requirements, possible supply chain paths can be determined.

5.2.1 Scenario 2: Implementation

The starting point of this scenario is the endpoint of scenario 1. Thus, the landing gear is still in its design phase and the qualified supplier panel in its establishment. There are two OEMs (1 or 2) alternatives for producing the landing gear. Both will be part of the qualified supplier panel as the qualified supplier panel is based on double sourcing. However, a choice must be made as to which supplier will be responsible for production and which will serve as backup.

This choice depends in this scenario on the cyber security maturity of the suppliers in conjunction with the information exchange and component criticality degrees. Exemplary, the propositions of IE and CC are demanding for certain cyber security maturity niveaus. The critical exchange of information (IE) could attract attackers to intercept the communication channels (e.g., see example of Airbus [3] from Chapter 1). This threat can be counteracted with increased cyber security maturity levels. Hence, employees recognise spear phishing attempts with higher probability (e.g., even if they are designed in a communication format of known suppliers). In case of the component property (CC), special security requirements have to be met, e.g., in the design process of the components (proper check of the COTS software ($CC1$), proper design of the component to inter-

cept unauthorized users ($CC2$), or adding zero trust mechanisms for critical connections ($CC3$)). These process requirements are covered by the CMMCv1 in higher maturity niveaus.

A mapping in Table 10 shows the minimum required cyber security maturity levels for each property of supplier relation (respectively the attribute of the edge).

Table 10. *Scenario 2: Mapping of IE and CC Attributes to the Cyber Security Maturity Niveaus*

$X_{pk} \cup X_{pi}$	$P \subseteq X_{pm}$				$Q \subseteq X_{pm}$	
CC0	nL	L1	L2	L3	L0	
CC1	nL		L2	L3	L0	L1
CC2	nL		L2	L3	L0	L1
CC3	nL		L2	L3	L0	L1
IE0	nL	L1	L2	L3	L0	
IE1	nL	L1	L2	L3	L0	
IE2	nL		L2	L3	L0	L1

CC - *Critical Characteristic: 0 Non-critical, 1 COTS Usage, 2 Critical Access, 3 Critical Connection*
IE - *Information Exchange: 0 None, 1 Black Box Approach, 2 Critical Information Exchange*
CMMCv1Level - *Cyber Security Maturity: L0 none, L1 Basic, L2 Intermediate, L3 Good, nL non-disclosed*

Given the context K_{S1} of the previous scenario, we define two contexts on top of it which as well each have a context on top of them:

1. K_{CC} with $P = \{CC1, CC2, CC3\}$ and $Q = \{nCC1, nCC2, nCC3\}$
   with $K_{CC_{L3L2}}$ with $P = \{nL, L2, L3\}$ and $Q = \{nL2, L1\}$
2. K_{IE} with $P = \{IE2\}$ and $Q = \{nIE2\}$
   with $K_{IE_{L3L2}}$ with $P = \{nL, L2, L3\}$ and $Q = \{nL2, L1\}$

Subsequently, compliant suppliers to all P of the four contexts are discovered by checking suppliers in the invertices of all $e \in E_{K_{nS2}}$ of $K_{nS2} = K_{S1} \setminus (K_{CC_{L3L2}} \cup K_{K_I E_{L3L2}})$.

The approach above depicts a version that successively filters out the non-sufficient suppliers. Alternatively, one can form a context that expresses the insufficient suppliers as P and then subtracts this context from the original one. This approach is introduced by using context K_{S1} as the foundation of the following contexts:

K_{L1} with $P = \{L1\}$ and $Q = \{nL1\}$ with two contexts on top:
1. $K_{L1_{IE}}$ with $P = \{IE2\}$ and $Q = \{nIE2\}$
2. $K_{L1_{CC}}$ with $P = \{CC1, CC2, CC3\}$ and $Q = \{nCC1, nCC2, nCC3\}$

From the two context every $e \in E_{AC_{L1IE}}$ and every $e \in E_{AC_{L1CC}}$ is extracted which include the suppliers in their vertices. Hence, a new edge set $E_{AC_{S2}} = E_{AC_{S2}} \setminus (E_{AC_{L1IE}} \cup E_{AC_{L1CC}})$ establishes K_{S2} with the given set of components, suppliers, and propositions from K_{S1}.

The Figure 21 shows the suppliers which are producing components with cyber security criticality and/or using a critical information exchange without having the necessary cyber security matuirty niveaus of $L2$ or $L3$ highlighted in color.

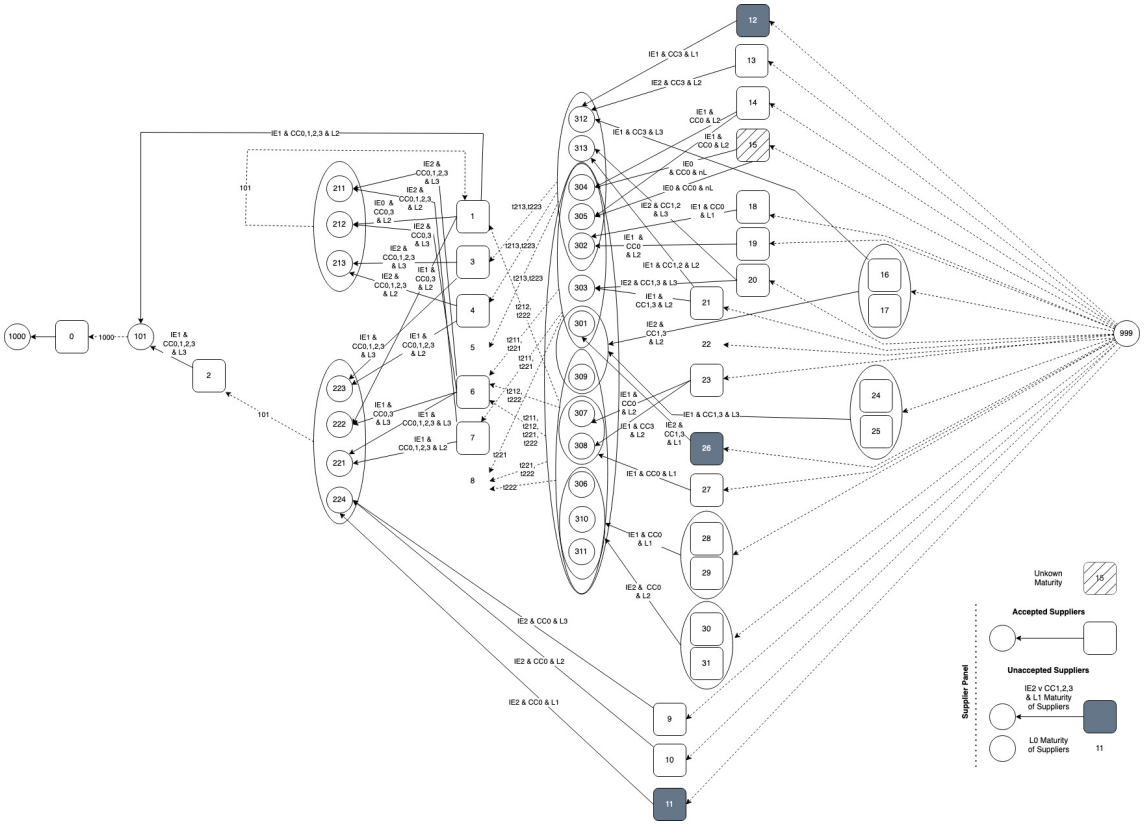


Figure 21. *Scenario 2: Suppliers with Cyber Security Maturity Niveau Not Complying with Table 10*

Thus, the context K_{S2} is similar to K_{S1} with exception of the following missing edges $\{e_6, e_7, e_8\}$:

$$e_6 = \langle \{12\}, \{312\}, [IE1, CC3, L1] \rangle,$$
$$e_7 = \langle \{26\}, \{301\}, [IE2, CC1, CC3, L1] \rangle,$$
$$e_8 = \langle \{11\}, \{224\}, [IE2, CC0, L1] \rangle.$$

Scenario 2 is verifiable and reproducible based on a pythonscript [100].

5.2.2 Scenario 2: Discussion

When signing contracts, the information to be exchanged is already described in great detail and specifications of the component and requirements are disclosed [103, 106]. Thus, the types of information exchange and component properties are already known and can be integrated into the design of the qualified supplier panel.

The interviewed experts differ in their opinion on what part of component is relevant for a higher cyber security maturity niveau. Some focus on criticality of certain software or hardware related aspects of components [105, 103] while others priorities the safety critical components, as a lack of cyber security reflects a weakness of the entire organisation [104, 107]. Expert F states that the weakest link should be considered and is often the one being the least secured. Exemplary, a purely structural component could turn into the weakest link through missing security controls for its design data (see Expert B and the design and production process which could be manipulated [104])[103]. Expert B adds that the criticality of components should not differ between software and hardware but rather within the impact on flight safety. Hence, the tyre should be classified more safety and cyber security critical than a seat technology which can include software (e.g., an airbag systems integrated in seats of front rows) but won't affect the airworthiness safety of the aircraft.[108, 104] Expert E mentions the implementation of a functional hazard analysis as a foundation to understand how critical the malfunctioning of a component impacts the flight safety. Subsequently, the lines of defense are decided (first of all independent of software and hardware).[107] All in all, the integration of a component dependent security assessment is validated as beneficial from all interview partners [105, 106, 108, 103, 107]. One expert was pointing out that it is necessary to combine certain components (since integration is also increasing) to have a homogeneous security barrier in the aircraft. Otherwise, the potential for established vulnerabilities increases because of different levels of security controls.[107]

Similar to the component properties, the information exchange is confirmed as cyber security critical by all interview partners [105, 106, 108, 103, 107]. Fundamentally, Expert F lists four types of information exchange between suppliers in the aviation supply chain:[103]

1. Exchange between entities based on agreements
2. Access to design data between entities, especially during product development
3. Membership at Aviation Exchange Platforms
4. Official reports from, e.g., EASA

The first two information exchanges are used in the scenario as they are relevant for the supply chain setup (production and purchase connections). The classification and criticality assessment of the transmitted information differs between the experts. Expert D states that many suppliers would prefer the information exchange of type 1 (the blackbox appraoch) over the type of design disclosure as the design often counts as their "bread and butter"[105] (exception is made for authorities). While Expert D assesses the criticality of the information exchange depending on the relationship between buyer and supplier, Expert B categorises the exchange of an interface information (type 1 as, i.e., the black box) already as very critical.[105, 104] Hence, the criticality of information exchange can depend on much more. Expert E, B, and A describe different types of technical information exchange. In case of a type 2 information exchange, collaboration platforms are provided on which design drawings are shared. Alternatively, the supplier gets restricted access in the buyer's systems to access the mandatory design drawings.[107, 108, 104] On the other side of the spectrum, also communication via email is still possible [108]. Hence, the variety of technical communication options reinforces the complexity of criticality categorisation of information exchange.

The third information exchange is considered as important to enhance the cyber security in each organisation (supporting the approach of C-SCRM [28]) by all interview partners. Currently, there are exchange networks in the aviation industry established which include suppliers on international and European level addressing cyber security incidents and latest news. Expert F and D mention the European Centre for Cybersecurity in Aviation (ECCSA) as cooperative partnership of the aviation community to provide collective support.[103, 105] Additionally, also the Aviation Information Sharing and Analysis Center (A-ISAC) fulfills the purpose to exchange information about emerging cyber security risks.[103] This communication and the fourth type are not represented in the conditional metagraph as they do not count into a supply chain's operability. However, the fourth type of official report exchange is interesting in the field of maintenance, repair, and operations (MRO). Here, the handling of certifications could turn into an interesting target point as the transmission of component certifications is done via email. As digital signatures are enough to verify the origin of the certificates, the integrity of these should not only be considered from cyber security maturity perspective.[108]

5.3 Scenario 3: Identification of a Cyber Secure Supply Chain Path

Based on scenario 1 and scenario 2 the qualified supplier panel is established and with it comes the search for the most secure supply chain path inside the supplier panel. Thus, the panel is split into the operating suppliers and the backup suppliers which hold less cyber secure properties. This scenario assumes the need for the highest cyber security maturity

niveau of the operating suppliers for two reasons: Compromised suppliers of the aviation industry could have an impact on the tertiary propagation zone which includes negative effects on the safety of societies [17, 35] and secondly, the adaption of cyber security requirements to the level of the developed airworthiness safety in the last decades within the aviation industry [6].

5.3.1 Scenario 3: Implementation

Before we can start into the remaining scenarios, the qualified supplier panel has to be established. Thus, the choice of the most secure supply chain path for the landing gear component has to be determined. This is done through the use of the metapath which is calculated through the adjacency matrix. Based on the context K_{S2} of scenario 2, we can calculate all possible metapaths. With the help of an additional written function (see cycle implementation in Section 4.2) the edge-dominant metapath is calculated. The difference between an edge-dominant and a normal metapath is visible for supplier 8, which has been already disqualified for the panel as the supplier has no cyber security maturity (see scenario 1). Since the context only deletes edges and not the nodes in the edges vertices, the supplier is still appearing in the context. Thus, the calculation for metapaths would consider options containing supplier 8 which can be accessed through the edges:

$$\langle\{309, 307, 308, 306, 310, 311\}, \{8\}, [t222]\rangle,$$
$$\langle\{301, 302, 303, 304, 305, \}, \{8\}, [t221]\rangle,$$
$$\langle\{301, 302, 303, 304, 305, 309, 307, 308, 306, 310, 311\}, \{8\}, [t221, t222]\rangle.$$

By calculating edge-dominant metapaths, those options would drop out of consideration as there exist metapaths which reach the target destination without those edges. Additionally, after finishing the design phase and suppliers as 8 who did not upgrade their cyber security maturity niveau, are removed completely. This approach gives us supply chain paths which hold suppliers with maturity levels of $L1$,$L2$, and $L3$. Those could be sorted in descending order by the number of highest maturity niveaus to lower ones. The supply chain path with the highest number of maturity niveaus could determine the operating suppliers of the qualified supplier panel. The backup suppliers would be ones not included in the highest ranked metapath. This approach is shown in the pythonscript [100].

Another approach is possible and shortly introduced as it is visually more representative: There will be two contexts generated: K_{L3} for suppliers with cyber security maturity niveau $L3$ and K_{L2} for suppliers with $L2$ maturity. Then, the sets of edges ($E_{AC_{K_{L3}}}$, $E_{AC_{K_{L2}}}$, and $E_{AC_{K_{S2}}}$) can be used to extract the components out of their outvertices. In the following,

the sets of edges and the sets of components ($X_{EC_{K_{L3}}}$, $X_{EC_{K_{L2}}}$, and $X_{EC_{K_{S2}}}$[2]) and are extracted from contexts K_{L3},K_{L2}, and K_{S2} and compared:

1. $X_{EC_{K_{L3}}} = X_{EC_{K_{S2}}} \implies$ metapath calculation can be done in K_{L3}
2. $X_{EC_{K_{L3}}} \subset X_{EC_{K_{S2}}} \implies X_{L3L2} = (X_{EC_{K_{L2}}} \setminus X_{EC_{K_{L3}}}) \cup X_{EC_{K_{L3}}}$
3. $X_{L3L2} = X_{EC_{K_{S2}}} \implies$ metapath calculation in K_{L2} from 999 to each $c \in (X_{EC_{K_{L2}}} \setminus X_{EC_{K_{L3}}})$ and adding each edge of the metapath to K_3 if not already existing
4. $X_{L3L2} \subset X_{EC_{K_{S2}}} \implies X_{L3L2L1nL} = (X_{EC_{K_{S2}}} \setminus (X_{EC_{K_{L3}}} X_{EC_{K_{L2}}})) \cup (X_{EC_{K_{L3}}} \cup X_{EC_{K_{L2}}})$
5. with $X_{L3L2L1nL}$ metapath calculation in K_{S2} from 999 to each $c \in (X_{EC_{K_{S2}}} \setminus (X_{EC_{K_{L3}}} X_{EC_{K_{L2}}}))$ and adding each edge of the metapath to K_3 if not already existing
6. Final metapath calculation in K_{L3} with target node 101 and start node 999.

The approach is shown in Figure 22 - 24. Figure 22 hihglights context K_{L3}. K_{L2} is marked in Figure 23. The final metapath is highlighted through thicker edges in Figure 24. Scenario 3 is verifiable and reproducible based on the pythonscript [100].

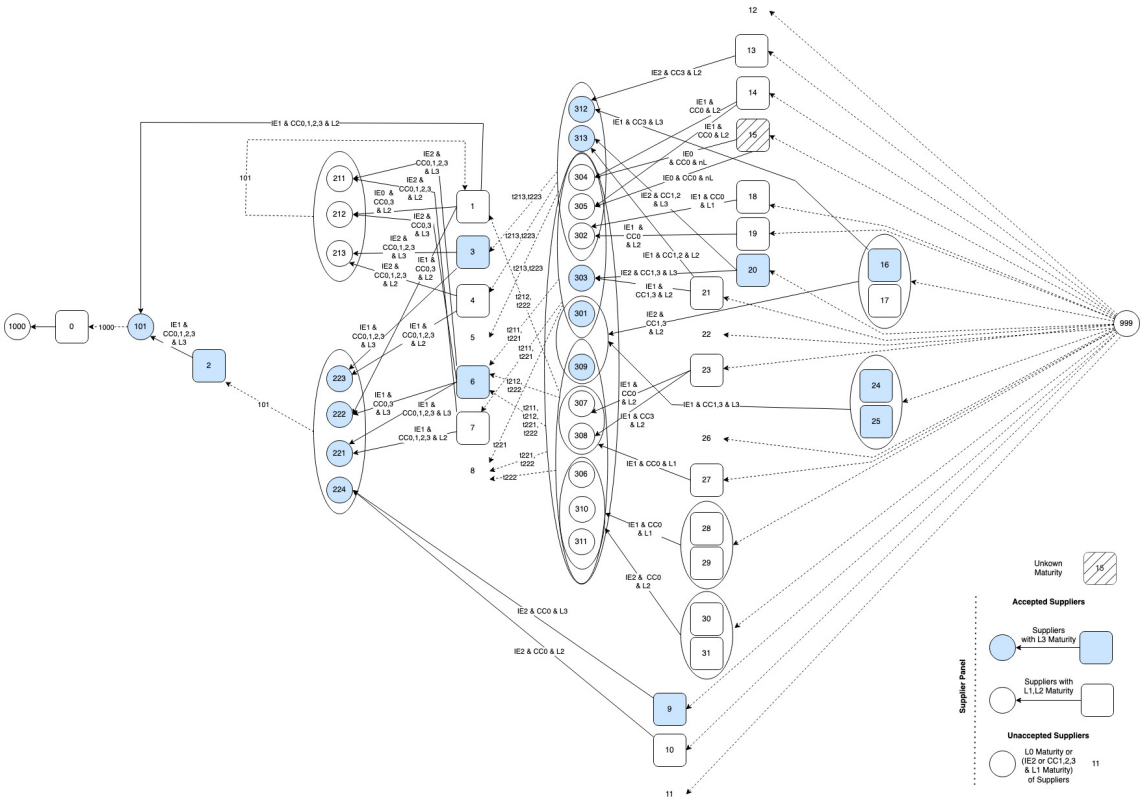


Figure 22. *Scenario 3: Context K_{L3} Highlighted (Base K_{S2})*

[2]These sets of components X_{EC} are not equal to X_C.

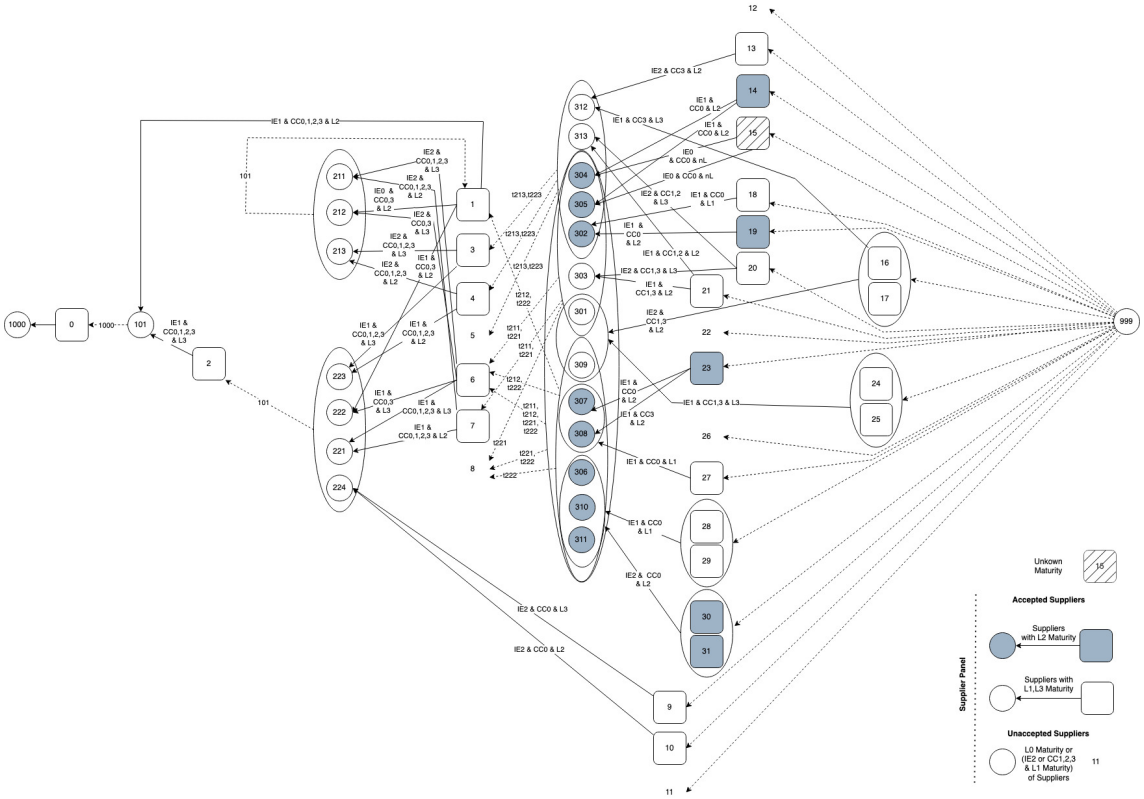


Figure 23. *Scenario 3: Context K_{L2} Highlighted (Base K_{S2})*

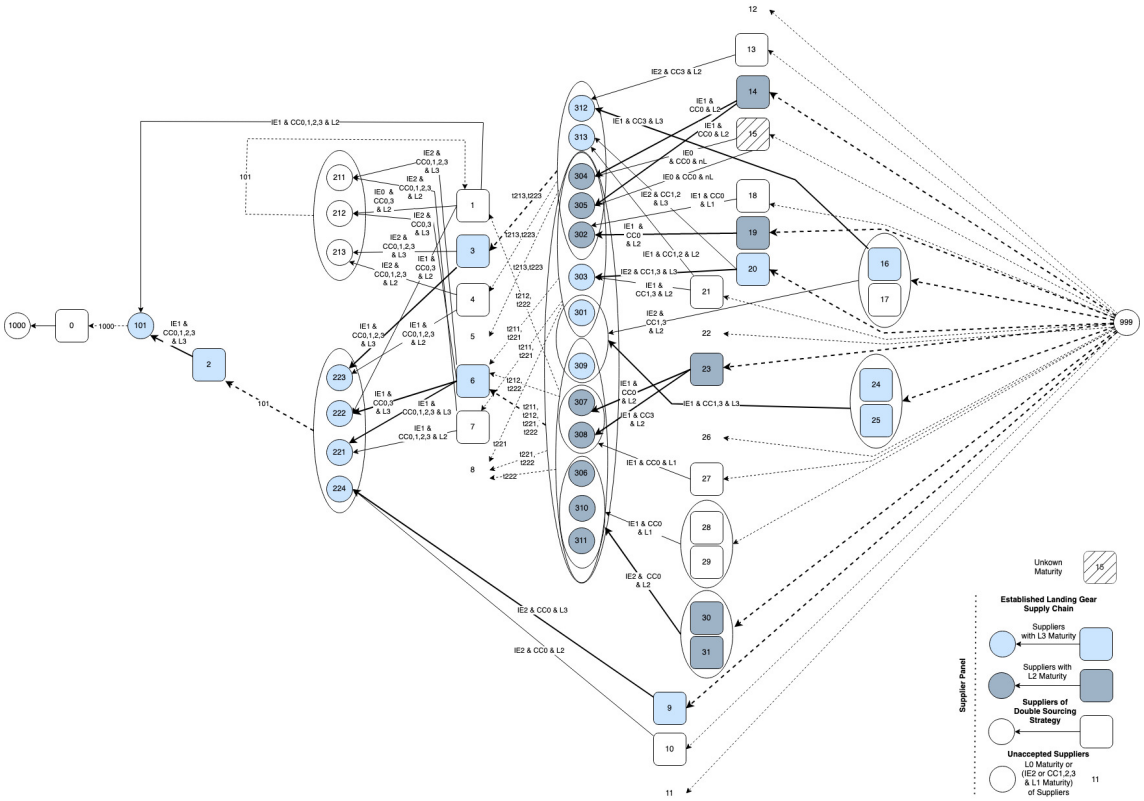


Figure 24. *Scenario 3: Context K_{L3} with the Final Metapath Highlighted (Base K_{S2})*

5.3.2 Scenario 3: Discussion

This scenario calculates the qualified supplier panel based on two most secure supply chain alternatives. The overall question, which has to be answered here, is whether it is feasible to have an active operating supply chain with one supplier for each component and backup suppliers in case of failures. The alternative would be that the purchase from two or more competitors appears random for each production of the component.

First of all, the qualified supplier panel is definite. Once established, the components of the admitted suppliers are added into the Illustrated Parts Catalogue (IPC) or Component Maintenance Manual (CMM) and hence, become part of the type certification of the aircraft.[108] Thus, the change of the supplier panel could include a costly adaption of the type certificate and is therefore largely avoided.[105, 106, 104] The experts' opinions differ for the purchase strategy inside the supplier panel. On the one side, Expert D formulates the need for diversification by including different components of certain competitors. In case, one component (e.g., the engine) breaks down, not the whole fleet of the same aircraft type would be grounded.[105] This would mean that only one metapath would not be feasible to represent the supply chain of an aircraft type. Hence, the possible combination of different undefinite purchasing decisions would let the number of metapaths increase sharply. On the other hand, Expert B mentions only one operating supplier for one component in a certain period of time [104]. Further, the suppliers in the qualified panel do not necessarily have to have a contract with the buyer for the component with which they have been certified for the panel.[104] This is another point for a small number of supply chain alternatives as the diversification strategy is limited to a few specific component types. Additionally, in higher tier levels, the buying in large quantities could also impact the decision to rely on one supplier instead of having several alternatives. Hence, a few possible metapaths in the qualified supplier panel should be taken into consideration and can also benefit the incidence response in the following scenarios.

5.4 Scenario 4: Reassessment Based on Certification Loss, Supplier Failure, and Certification Upgrade

The decision for the securest supply chain path has been made. Additional information about parts of the supply chain appears: A supplier is compromised causing unavailability and an alternative cyber secure supply chain path can be reassessed. Additional, suppliers can lose or enhance their cyber security maturity. The graph has to be updated by changing or adding attributes of the suppliers. The metagraph model must ensure traceability of changes (version controlling). A reassessment of possible secure supply chain paths shows a more secure alternative, or a chosen path turns insecure. This scenario relates to the taxonomy of supply chain attacks of ENISA [5] and the re-certification of certification standards [9].

5.4.1 Scenario 4: Implementation

With an established qualified supplier panel, this scenario assumes changes in the suppliers' cyber security maturity niveaus. This scenario is based on the context K_{S4} which is a copy of the context K_{L3} of the previous scenario and includes the qualified supplier panel shown in Figure 24.

The first case introduces the situation that one supplier of the established supply chain loses its cyber security maturity certification. Since certificates are renewed periodically, this case is feasible although it should not occur if the supplier was chosen carefully. In this example supplier 19 loses the approval for one or all of the three ISO 27001 practices (6.2.1, 6.2.2, 6.1.2, see Table 8). As suppliers in the qualified supplier panel are not easy to replace, supplier 19 remains in it but has to renew its certification in a given period of time. However, supplier 6 must find replacement for the subcomponent 302 in the supplier panel. Thus, the connection to the double sourcing alternative needs to be established. The second case assumes unavailability of supplier 23. The reason for this could be exemplary a ransomware attack. However, the approach is similar to the one of case 1. Supplier 6 also has to establish connection to the backup supplier of the qualified supplier panel. Both cases would trigger the following steps for the context calculation of the conditional metagraph:

1. Update of the following edges in context K_{S3} to:
   $e_{19} = \langle\{19\}, \{302\}, [IE1, CC0, L0]\rangle$,
   $e_{23_1} = \langle\{23\}, \{307\}, [IE1, CC0, L0]\rangle$,
   $e_{23_2} = \langle\{23\}, \{308\}, [IE1, CC3, L0]\rangle$

2. Build a context $K_{S3_{nL0}}$ on top of K_{S3} with $P = \{nL0\}$ and $Q = \{L0\}$ which deletes edges $\langle e_{19}, e_{23_1}, e_{23_2} \rangle$.
3. Generate a new metapath on $K_{S3_{nL0}}$ that has only one purchasing option for components $302, 307$ and 308. Sort the metapaths in descending order by highest maturity level and chose the highest one.

Figure 25 shows the change in the supply chain. Considered edges by the most secure metapath are thicker than the others. The substitute for supplier 19 is supplier 18, for 27 the alternative is 23. In both cases, the alternative has only a cyber security maturity niveau of $L1$. Thus, the supply chain significantly weakens through the loss of suppliers 19 and 23. Other contexts and the main conditional metagraph S_{AC} also have to be updated in case the loss of suppliers is long term. Further, the qualified supplier panel has to be extended by two additional backup suppliers.

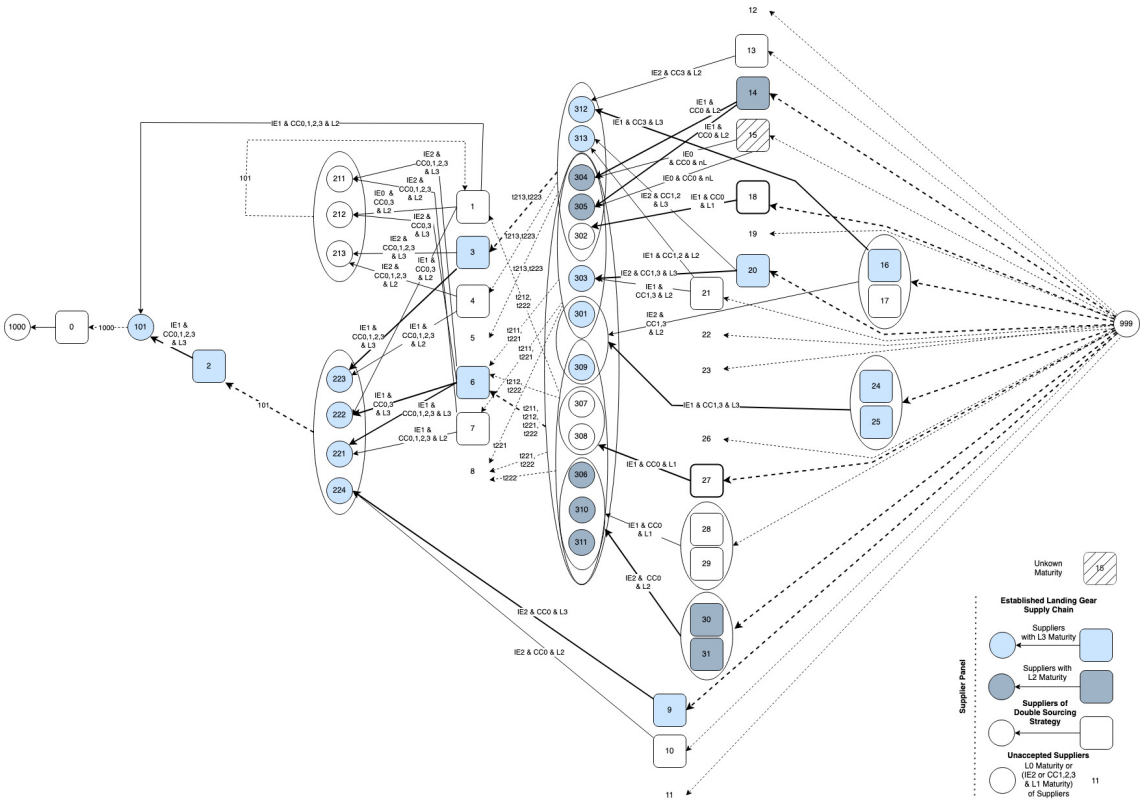


Figure 25. *Scenario 4: Context $K_{S3_{nL0}}$ with the Updated Metapath After Supplier Loss*

The third case assumes an increasing cyber security maturity niveau of a supplier which can change the order by highest maturity level of the metapaths. Thus, the metapath in use is no longer the most secure option of the supply chain path options in the qualified supplier panel. This can happen through a reassessment of a supplier who increased its cyber security practices since the last certification such that it has reached a new maturity level. Exemplary, an alternative option is introduced: The supply chain of the landing gear

contains a supplier who has not yet its cyber security maturity niveau revealed. We assume that the supplier (15) now contributes its maturity level which is a $L3$. Thus, the context $K_{S3_{nL0}}$, S_{AC}, and other contexts in use need to be updated in the following edges:

$$e_{15_1} = \langle\{15\}, \{304\}, [IE1, CC0, L3]\rangle, \text{previously } nL$$
$$e_{15_2} = \langle\{15\}, \{305\}, [IE1, CC0, L3]\rangle, \text{previously } nL$$

Additionally, the metapaths can be recalculated. The supplier option in use (14) has a maturity niveau of $L2$ and turns into the second best option to purchase from. Thus, the operating supply chain could be changed to the metapath shown in Figure 26. Scenario 4 is verifiable and reproducible based on the pythonscript[100].

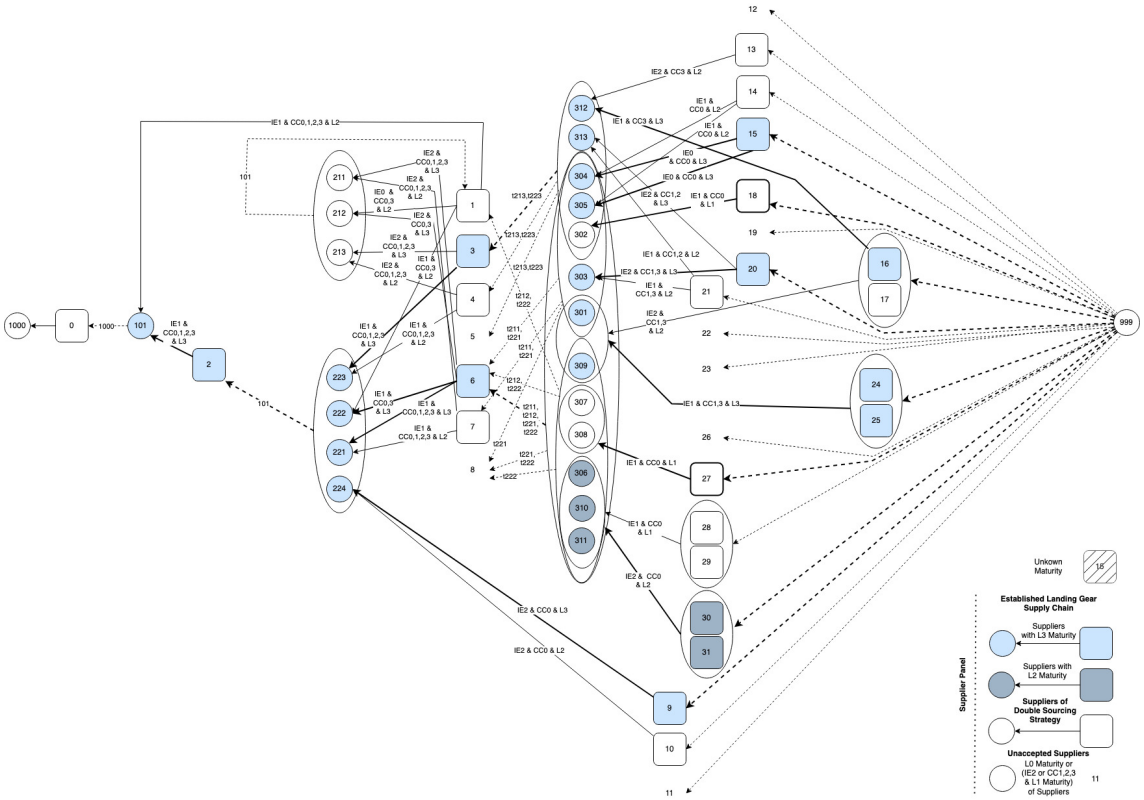


Figure 26. *Scenario 4: Context K_{S2} with the Securest Metapath in Updated $K_{S3_{nL0}}$*

5.4.2 Scenario 4: Discussion

This scenario describes different situations in which the chosen supply chain path changes its properties: First, a the break down of a supplier causes disruption in the current operational supply chain path. Second, a supplier loses its cyber security maturity niveau which causes the current supply chain path to turn less secure than other alternatives. The last situation describes a supplier upgrading in its cyber security maturity causing an alternative supply chain path to become more secure than the current one.

Overall, the experts agree on the importance of failure and loss of cyber security maturity of suppliers for call for action in the supply chain path decision [105, 106, 108, 103, 107]. In case of an indirect supplier failure, the buyer would have the responsibility to find a new alternative and also to inform the buyers of its product based on the contractual requirements (see Expert B in scenario 1) [104]. Expert B mentions further, that in case of a direct supplier failure, it has to be assessed whether the supplier has a temporary problem as, e.g., a problem of processes where it can recover from. Mostly, the buyer prefers to support a direct supplier rather than changing the supplier which could cause in worst case the need for a re-certification of the airworthiness type certification.[103, 104] Hence, in case the supplier is willing and able to turn back its availability or certification maturity in a certain time period, the supplier will stay in the qualified supplier panel. Expert D supports this perspective and adds that even when issues are found in the auditing process of suppliers, there shall be given room for justification even when they do not meet the target and the possibility for these suppliers to resubmit compliance with relevant requirements.[105] While supporting or waiting for the supplier to recover, the buyer selects the backup supplier option which depends on the situational context, the time required for recovery, and the component complexity [105, 104]. In case the supplier loses its cyber security maturity niveau, the change to the backup supplier depends on the proportionality of the effort to change compared to the possible impact of the missing cyber security practices. A risk assessment should be carried out whether the risk depending on the level of insecurity is acceptable or not [107]. In case the supplier is not able or does not want to comply in the long term with the cyber security maturity requirements or is not able to recover, the supplier is dropped from the qualified supplier panel [104]. Hence, the first part of the scenario is validated as important and applicable to the supply chain of the aviation industry.[105, 106, 107, 103] Expert C mentions further, that the accountability for failure lies within the aircraft OEM and hence, validates the chosen perspective of the metagraph by pointing out that the identification for secure supply chains through the use of a conditional metagraph should be interesting for aircraft manufacturers.[106]

The third alternative assumes a change of the supply chain paths as a result of, e.g., a re-certification, since the cyber security maturity of another purchasing option is higher than the current one. The approach of adapting to the securest purchasing option is not feasible for most of the interview partners. Expert E sees this option as a desirable outcome but mentions that the industry would not allow this to happen. To convince the management of a cyber security related change in the purchase option without negative harm is only applicable when an assessment shows that the change to the other purchasing option would be done cost-neutral or the costs would be less than the potential impact of staying with the current purchase option in a risk assessment.[107] Expert B finds clear words for a future scenario: "It won't be possible to purchase from suppliers without cyber security

maturity on the niveau of the Part-IS regulation. Hence, the decision would only lie between suppliers mapping the minimum requirements and a supplier that is willing to invest additionally in cyber security."[104] The purchase decision would ultimately depend on further parameters as cyber security never becomes a major paramater compared to capability, experience, or costs. Hence, cyber security would be one parameter equally significant as other parameters.[104] Therefore, this part of the scenario is less applicable in the aviation supply chain and less important compared to the business continuity approaches mentioned above. However, the update of the graph structure stays important to support the versioning of the metagraph structure even though the necessity of calculating the metapath is omitted.

5.5 Scenario 5: Analysis of a Security Breach

A security breach of one of the suppliers goes viral. How should the direct supplier behave and could it have been possible that the attacker already cascaded through the supply chain? These questions can be answered through the use of the conditional metagraph, its properties, and its propositions (e.g., IE and CC). This scenario illustrates a showcase of how to interpret the metagraph's supply chain paths and is based on the threat landscape of ENISA [5]. Further, the scenario relates to approaches of cooperation in the supply chain as, e.g., CSASC [40] or the coordinated cyber security investment [34].

5.5.1 Scenario 5: Implementation

The last scenario describes a possible attack of the supply chain which does not harm necessarily the availability (already covered in Scenario 4) but rather the integrity or confidentiality. Especially, the concern whether the attacker was able to cascade through the supply chain towards the landing gear OEM is not insignificant. Essentially, the metagraph can be used to quickly assess the risk of an attack's expansion taken place in the supply chain based on three characteristics:

1. Information exchange between suppliers
2. Cyber security maturity niveaus of relevant suppliers
3. Importance of the compromised supplier to the supply chain
   (including the cyber secure criticality of the produced component)

Assuming that supplier 17 was compromised being part of the qualified supplier panel. Thus, the risk of, e.g., a potential espionage is not unreasonable on the first thought. However, the conditional metagraph may provide more insight. Hence, the edges of

context $K_{S3_{nL0}}$ are first filtered for supplier 17. It turns out that supplier 17 is not part of the established operating supply chain, as it does not appear in the edges. Thus, supplier 17 is a backup supplier. However, the filtering for supplier 17 in the edges of K_{S2} shows, that supplier 17 is cooperating for the production of sensors (301) and the brake caliper (309) with supplier 16 who is part of the established supply chain (filtering the edges of $K_{S3_{nL0}}$ for 16). Since they are cooperating, it is assumed that they communicate in a close manner. Thus, the risk of supplier 16 being also compromised is higher than through information exchange $IE2$. However, the collaboration must have taken place recently, as - at least for the landing gear in this example - they did not have to communicate, as the 301 and 309 components were sourced through an alternative (suppliers 24 and 25).

Nevertheless, a metapath between supplier 16[3] and the landing gear component 101 in the established supply chain context $K_{S3_{nL0}}$ is calculated and has the following edges:

$$\begin{aligned} m_1 = \; & [\langle\{16\},\{312\},[IE1,CC3,L3]\rangle, \\ & \langle\{312,313,304,305,302\},\{3\},[t213,t223]\rangle, \\ & \langle\{3\},\{223\},[IE1,CC0,CC1,CC2,CC3,L3]\rangle, \\ & \langle\{223,222,221,224\},\{2\},[t101]\rangle, \\ & \langle\{2\},\{101\},[IE1,CC0,CC1,CC2,CC3,L3]\rangle] \end{aligned}$$

Out of curiosity, a metapath is also calculated on the qualified supplier panel context K_{S2} between suppliers $16, 17$ and 101[4] with the following edges:

$$\begin{aligned} m_2 = \; & [\langle\{16,17\},\{301,309\},[IE2,CC1,CC3,L2]\rangle, \\ & \langle\{301,302,303,304,305,306,307,308,309,310,311\},\{6\}, \\ & [t211,t212,t221,t222]\rangle, \\ & \langle\{6\},\{222\},[IE1,CC0,CC3,L3]\rangle, \\ & \langle\{6\},\{221\},[IE1,CC0,CC1,CC2,CC3,L3]\rangle, \\ & \langle\{223,222,221,224\},\{2\},[t101]\rangle, \\ & \langle\{2\},\{101\},[IE1,CC0,CC1,CC2,CC3,L3]\rangle] \end{aligned}$$

First, the information exchange between the suppliers is analysed. On the one hand, m_1 is equipped with $IE1$ all the way to the aircraft manufacturer. Thus, the communication between the suppliers is as low as necessary and could present a first barrier for an attacker to traverse the supply chain. On the other hand, the analysis of m_2 holds more potential for an attacker. Suppliers 16 and 17 would have communicated through an $IE2$ with supplier

[3] As the suppliers of the other components also have to be known, the process is a bit more complex but traceable in the pythonscript[100].

[4] Assuming that the supplier on tier 2 level is the one of the established supply chain: supplier 6.

6 which could have caused more weak links for an attacker to find access into the systems of supplier 6 through increased communication. However, the attacker would not have to migrate to supplier 6 to cause a breach. The exchange of information in the manner of $IE2$ means supplier 6 has to disclose design information to suppliers 16 and 17 which could have led to an unauthorized leak of information if the attacker had been able to capture this information in supplier 17's system (loss of confidentiality).

Secondly, the cyber security maturity niveaus of supplier 17 and the potentially attacked suppliers should be analysed. m_1 reveals that the whole supply chain has the highest possible maturity of $L3$. Thus, this could be another barrier for an attacker to cascade through the supply chain as the employees are well trained to identify, e.g., phishing emails. However, in m_2 exists only a $L2$ for both suppliers $16, 17$. Supplier 17 has a maturity of $L2$ and based on the conditional metagraph setup of Subsection 4.2.3, the lower maturity niveau of suppliers 16 and 17 is embedded in the edge from $\{16, 17\}$ to $\{301, 309\}$. The rest of the supply chain's suppliers have a maturity niveau of $L3$. Hence, 17 is the weakest link in the supply chain path of m_2 and being the only supplier with a critical information exchange of $IE2$.

The importance of supplier 17 can be analysed through the amount of produced components for the landing gear component and their cyber secure criticality. m_1 shows that supplier 16 only produces one component for supplier 3 which only affects the control unit 223 of the landing gear component. Thus, $1/5th$ of the subcomponents of the control unit are produced by 16. However, 312 produced by 16 are sensors which have exemplary critical connections ($CC3$) to systems outside of the aircraft embedded. Thus, should the attacker have penetrated 16's systems to access the sensor design or production facilities, this could compromise the integrity of the sensors or the confidentiality of the aircraft's system parameters in operation.

The alternative in m_2 looks worse. If suppliers $16, 17$ had been chosen for the production of $301, 309$, this could have resulted in serious consequences, since these components supply both the brake system component (221) and the wheel (222) component of the landing gear component. This could have led to a considerable amount of know-how being lost. As the produced subcomponents of 16 and 17 would have been sensors (301) a similar scenario as in m_1 could have taken place with a higher probability as it is known that the attacker is in the systems' of supplier 17. Additionally, the brake caliper (309) is produced by 16 and 17. A misconfiguration in this subcomponent could cause a serious threat to the airworthiness safety of the landing gear component (loss of integrity).

Another point that should be considered is the influence of supplier 6 to the landing gear supply chain as it is also part of the established landing gear supply chain. The supplier produces two of the four components of the landing gear (the wheel and the brake caliper) whereby the fourth component represents already the assembly of the landing gear. Thus, only the control unit is not supplied by supplier 6. Hence, the supplier and its suppliers have the highest impact on the components of the landing gear and supplier 6 could become a point of failure or even a target for espionage. In case supplier 6 had purchased 301 and 309 through suppliers 16 and 17, the supplier would have exchanged critical information via $IE2$. As this supplier is a key supplier, it should be reconsidered if it is allowed that 6 could engage in purchases with critical information sharing ($IE2$) and through suppliers possessing a lower maturity niveau.

Overall, choosing supplier 16 for the established supply chain path was a valuable decision. The alternative would have made the supply chain more vulnerable. Recommendations for action should definitely include that supplier 3 is warned and increases its cyber security practices as direct buyer of supplier 16. Also, the landing gear OEM should advocate further strengthening of cyber security practices of supplier 6. One could consider switching to supplier 13 as alternative for 16, depending on the individual situation of the attack (how long the attack has been going on, and whether a switch to supplier 13 could be done within a reasonable time). In any case, it would be important to observe supplier 17 and its measures for mitigation and emergency response management.

The current decision for the supply chain to be as secure as in $K_{S3_{nL0}}$ with m_1 is only possible because suppliers can integrate SMBs that do not have certifications but nonetheless integrate cyber security practices. Thus, the established supplier for 301 and 309 is a cooperation of 24 and 25 having cyber security maturity of $L3$ through the integration of cyber security practices without one of the four certification standards.

Scenario 5 is verifiable and reproducible based on the pythonscript [100]. This analysis bears further analysis potential in case the metagraph would also encompass suppliers and their connections of different aircraft components or competitors aircraft components. For this example, the metagraph is narrowed down to analyse suppliers which are part of the same supplier panel of the landing gear.

5.5.2 Scenario 5: Discussion

The last scenario investigates the potential of a conditional metagraph structure in case an attacker is assumed or detected in a compromised supplier of the qualified supplier panel. The potential of the conditional metagraph is confirmed valuable by all industry

experts [105, 106, 107, 103, 104, 108]. Expert B states that when a compromised supplier is present in the established qualified supplier panel, the aim is to collect as much information as possible to understand the attack vectors, aim, and motivation.[104] Here, the metagraph can support by analysing the supply chain paths for potential targeted customers or suppliers. Further, the information exchange and component criticality properties allow to assess attack targets of the ENISA taxonomy. Overall, the communication with potential compromised suppliers because of their closeness to the known compromised supplier is an important point for Expert B, D, and F.[105, 104, 103] Expert F and E mention investigations which are established to analyse the criticality of the security breach [103]. Expert E adds a risk assessment which is done to assess whether the breach causes a change of the purchasing option or not.[107] Expert B and F differs between an attack of a direct and an indirect supplier. In case a direct supplier is compromised, the supplier is supported with incident response and also the own organisations is analysed with regard to an cyber attack. For the second option, meetings with the direct supplier of the compromised purchase option (the compromised metapath) are established to let the supplier justify why the contract is continued or stopped. Here, the buyer largely an impact on the purchase decision of the direct supplier as the direct supplier does not want to lose its customer.[104, 103] Overall, Expert C mentions again that this scenario would be relevant for aircraft OEM because the mentioned accountability of the supply chain's reliability also includes cyber security attacks.[106]

To sum up, the industry experts state that in this scenario the conditional metagraph would be beneficial to understand possible explanations of how the attacker could have propagated through the supply chain [105, 106, 107, 103, 104, 108]. This scenario is applicable as a decision support for current supply chain purchase options but also able to analyse supply chain cyber attacks that may have happened in the past in order to initiate possible MRO measures in the active fleet.[108]

6. Discussion

The scenarios presented in Chapter 5 provided an introduction to the potential of the conditional metagraph model applied to the supply chain of an aviation landing gear component and were evaluated by the interviewed experts. This chapter answers the research questions and situates the results of this thesis and its relevance into scientific research.

Overall, the case study methods form the foundations for the results of this thesis. The literature review and the semi-structured interviews provide the basis for the application of the conditional metagraph to the aircraft landing gear supply chain and the integration of cyber security properties in form of certification standards. The scenarios are designed as snapshots of the case study and close the gap between the graph-theoretical construct of the conditional metagraph and the visualisation of possible application fields. They serve as ground for the evaluation of the conditional metagraph's benefits by the six industry experts interviewed.

The first research question as how the application of the conditional metagraph looks like was answered in Section 4.2. Through the definition of the characteristics of the aviation supply chain, specifications for the conditional metagraph in its application to the aviation supply chain were defined (i.e., subset and edge patterns) without contradicting the graph-theoretic literature. Based on the graph-theoretic specifications, the conditional metagraph was applied to the exemplary key case of the case study's subject, the segment of a landing gear supply chain. Additionally, cyber security properties in form of certification standards were integrated into the conditional aviation metagraph. Therefore, the second research question about how cyber security is applicable to the metagraph model is also answered in Section 4.2. The application of the conditional metagraph to the aviation supply chain and cyber security certification standards is feasible and graphical visualised in Figure 19 of Subsection 4.2.3. The third research question, which benefits the conditional metagraph offers for enhanced cyber security in the aviation supply chain, is demonstrated through the scenarios in Chapter 5. Subsequently, the relevance of cyber security in the aviation industry, the conditional metagraph model's relevance to supply chain cyber security research, and its benefit are discussed and summarised.

The importance and criticality of cyber security in aviation is growing with the rising integration of aircraft components and the increasing complexity of ICT technologies used in an aircraft [106]. Expert F places cyber security on the same critical level as airworthiness safety and reliability of aviation systems, as the identification of a vulnerability could threaten not just one aircraft, but an entire fleet of the same type of aircraft. [103] Expert E adds that the whole aviation industry evolves towards an increased deployment of COTS software (see, e.g., the SolarWinds' attack [2]) which originates from benefiting of the advantages of the electronic markets: Instead of redeveloping software components for the aircraft, the purchase of COTS software is cheaper and faster deployed.[107] Thus, the production of the aircraft is efficiently improved by using, e.g., pre-existing code and software libraries which are part of the common supply chain attack targets of the ENISA taxonomy [5]. Expert B and D see cyber security as part of the aviation safety as cyber security incidents could have an airworthiness safety impact [105, 104]. In the last six to seven years, cyber security was an additional factor rather than a major one, especially in the context of deciding for subcontractors. As more incidents of cyber attacks in the aviation industry are reported by the media, organisations are searching for cyber security experts and cooperation within the supply chain to tackle the issue.[105]

None of the experts mentions that cyber security and airworthiness safety could be seen on the same level of significance. Instead cyber security is seen as part of the airworthiness safety. [105, 106, 107, 103, 104, 108] Only Expert F describes potential conflicts between cyber security and airworthiness safety [103]. Main focus of the interview partners lay on the components' cyber security [107]. Through the introduced Part-IS regulation [11], the organisational cyber security moves into focus. Here, the difference between security and safety is visible as the thought of insider threat is contra-intuitive to an industry where the human was more in focus to be saved from harm. [104] Nevertheless, intentional unauthorized electronic interaction was already introduced with Acceptable Means of Compliance (AMC), e.g., AMC 20-42 [103]. Further, Expert F adds the corporate IT and OT infrastructure which has to be considered but not necessarily has an impact on the airworthiness safety which is supported by Expert D [105, 103]. However, cyber security for aviation safety is distinguished by Expert B into three categories: The final component, its life cycle (design, production), and the organisation. All of them can have a negative impact on the airworthiness safety and have to be considered for fulfilling Part-IS requirements.[104, 11]

From aircraft OEMs, cyber security had already a greater significance for the last years as these organisations are responsible for the airworthiness safety of their aircraft types and further had requirements imposed by their customers, the operators of the aircrafts. Hence, confidentiality and integrity were in focus to prevent operational delays and safety

critical harm. Safety critical harm was further regulated through, e.g., EASA [6]. The aircraft component OEMs on the other side, did not focus on cyber security and are in a transformation phase by analysing gaps to the introduced regulation (Part-IS [11].[107, 104]

With increasing significance of cyber security, the question of responsibility has to be raised. Expert E and B mention responsibility in the context of a risk management which is based on a distributed balanced monitoring and implementation responsibility. Aim is to distribute the responsibility of cyber security through the supply chain which aligns with the approach of CSASC (see Melnyk et al. (2021) [40]) and the approach of an optimal cyber security investment by Simon and Omar (2019) [34].[105, 107] Alternatively, Expert A, B, and C represent the opinion that the aircraft OEM is responsible for pushing cyber security through the supply chain as they cascade their (product) requirements forward and will held accountable in case a cyber security incident occurs.[108, 104, 106].

In total, the industry experts' point of views align with the outcome of the supply chain literature in Section 2.1(see e.g., Ukwandu et al. (2022) [14]) in giving cyber security an increasing relevance. However, the definition and focused aspects of cyber security vary broadly and also the allocation of responsibilities. With the help of the integration of the new cyber security regulation, a definition of cyber security can be harmonised and responsibility distributed. However, the challenge of managing accountability and demonstrating compliance with cyber security requirements in the supply chain remains.

The scenarios in Chapter 5 demonstrate that the challenge of managing accountability and demonstrating compliance with cyber security requirements in the supply chain can be mitigated through the use of a conditional metagraph. However, the approach to only implement cyber security related properties is reasonable for a concept of proof but not applicable into praxis. Overall, the interview partners agree on the fact that cyber security is only one of a variety of different parameters in the purchase decision of an aircraft.[105, 106, 107, 103, 104, 108] Expert B mentions parameters as capability, cost, or experience of the supplier which have currently a higher relevance as cyber security. However, cyber security will evolve to an equally significant parameter in the next few years. [104] Scenarios 1, 2, and 5 were confirmed applicable by the interview partners. Hence, the prioritisation of suppliers with cyber security maturity above the ones without is considered important (scenario 1). The cyber secure maturity ranking of suppliers is possible through the harmonisation of cyber security certification standards which is defined as significant by the experts. Further, also the filtering for certain cyber security maturity niveaus conditioned by a cyber secure criticality of the produced component and the information exchange type between supplier and buyer (scenario 2) is seen relevant

by the experts. Scenario 3 establishes one operating supply chain which needs further extension of alternatives for certain diversification strategies of the aircraft OEM. Scenario 4 was validated in its first part but not confirmed in its second part. Hence, the experts preferred the reassessment of the supply chain due to supplier failure and certification loss instead of a certification upgrade. The fifth scenario introduced an ex-post analysis of a cyber incident and was considered valuable. To sum up, the interview partners see the potential of the conditional metagraph to enhance cyber security hygiene in the qualified supplier panel but also state some challenges which are explained in Subsection 6.1.2.[105, 106, 107, 103, 104, 108]

The conditional metagraph was applied onto the aviation industry through requirements defined in the industry. As the aviation industry handles safety criticality, the metagraph is tested in a tertiary propagation zone in which cyber security could have an impact on a society's safety (see Dolgui, Ivanov, and Sokolov (2018)).[17, 35] It integrates cyber security on an organisational and technical level which can be linked to the research of Urciuoli and Hintsa (2017)[36]. Further, the points of penetration (human, technical, and physical) mentioned by Ghadge et al. (2020) are covered by the introduced conditional metagraph based on the implementation of the C-SCRM approach [28]. Through the implementation of different certification standards, expertise of cyber security practices, supply chain management, and enterprise risk management (also often referred to by Expert E [107]) can be combined as attributes on the conditional metagraph's edges. Further, the properties of information exchange and component cyber secure criticality on the conditional metagraph's edges are technical parts which, however, were presented at a very high level for comprehensibility needs (see Urciuoli and Hintsa (2017) [36]). The CSASC approach relates partly to the mentioned trust framework of the aviation industry (mentioned by, e.g., Expert D and E [107, 105]). However, the metagraph includes further potential to be adapted for this approach (see Section 7). Benefits of the metagraph are shown in the implementation of cyber security practices for SMBs in combination with the research result of Boyson et al. (2021) showing that cyber security practices based on standards can enhance the cyber security hygiene [26]. Hence, the inclusion of secured SMBs over unsecured, properties of information exchange, and component characteristics could place the weakest links in the supply chain at higher levels. However, considering state sponsored APTs as attackers (see the threat landscape of ENISA [5]), buyers should not lull themselves into a false sense of security. Therefore, the traceability of cascading attackers in the supply chain through the use of the conditional metagraph can strengthen the incident response and business continuity management of the supply chain. Finally, the supply chain cyber security system shows three parts to be integrated which is introduced by Dolgui, Ivanov, and Sokolov (2018) (see Figure 1)[17]. The "IT security system"[17] consists of hardware, software, and broad technology which is covered by requirements

of certification standards. Additionally, the organisational security system is also handled in certification standards as those encompass the requirement for rules and guidelines, physical asset protection, and employee awareness. The last system contains the supply chain security system which includes information sharing, agility and adaptability, and a collaborative risk management.[17] The information sharing is enhanced through the use of the conditional metagraph in scenario 4 [104, 105]. Further, the conditional metagraph is able to support the agility and adaptability of the supply chain by using its metapath calculations [15]. Adding certain cyber security maturity niveaus as contexts underneath the metapath calculation forms a tool which supports the introduction of a collaborative risk management, which has been so far only done with direct suppliers (see Expert B and E [104, 107]) and approaches of CSASC (see Melnyk et al.(2021)[40]).

The conditional metagraph to the aviation supply chain holds an added value in providing information to enable cyber secure purchasing decisions and ex-post analysis of cyber security incidents in the supply chain. Based on the scenarios this statement was confirmed by the industry experts interviewed and underpinned in its relevance by the mapping to the scientific discourse of the cyber security supply chain.

6.1 Challenges and Limitations

The limitations of this thesis are split into ones connected to the methodology and ones connected to the applied graph-theoretic construct of the conditional metagraph mapped onto the aviation supply chain.

6.1.1 Reliability and Validity of the Methodology

The concept of reliability in qualitative research deals with the replicability of the researcher's result. Thus, it addresses the truthfulness and credibility of the case study. [113] The inquirer needs to be consistent in conducting research procedures and observations. This is achieved through clarity in the procedures of data collection, access, sampling, and analysis.[102, 114] For a case study, this involves the documentation of an iterative design process. However, the inquirer enhanced the reliability of the study with the documentation of the development process of the metagraph model in an excel sheet as a study case protocol (recommended by [82, pp. 43]). The reliability of the data collection was strengthened through the description of the expert recruitment procedures in Subsection 3.2.6 and the description of the flow diagram of the literature review (see Figure **??**). Additionally, explicit interview questions which are anchored in the interview guide (see Appendix A1) as an entry point for the semi-structured interviews were used. The main

risk in the data collection was the use of the same set of interview partners for the setup of the requirements for characteristics of the aviation supply chain and the evaluation of applicability of the scenarios. The inquirer was carefully separating the requirements from the feedback of the scenarios. Another challenge was the normalisation of security and safety perspectives of the industry experts. The proportion of interviewees with aviation safety and aviation cyber security background was equally distributed with two experts having expertise from both fields.

Validity questions whether the inquirer has taken the right idea or the right construct to approach the research problem.[113] To satisfy the validity of the case study, the researcher provides two approaches: The four triangulation types by Denzin (1970) [115] and three case study design tests of Yin [82, pp. 43] which give a guideline for judging the criteria of the research design quality.

Triangulation describes the combination of different data types of various sources to analyse a research problem. First, the data triangulation [113] points towards the use of different data sources in a study.[82, 116] This is done as the inquirer was conducting interviews with industry experts from different organisations and European member states with varying expertise. Secondly, the investigator triangulation recommends to use multiple investigators to study a research problem.[116] As this thesis has one inquirer, the lack in quality of the research is mitigated through two procedures. First, the interviews were recorded which gave the possibility to review the observer's perceived content against the recordings afterwards. Secondly, the interview partners were consulted on the outcome to identify possible misinterpretation of the investigator. This procedure also supports the construct validity, as according to Yin (2018) the key informants should be included in the review process of the case study report [82, pp. 43]. The risk of defining wrong questions for the interviews by one inquirer was reduced by conversations beforehand with experts at the conferences [93, 94]. The third triangulation type is not applicable for a case study. The last type of triangulation focuses on using multiple methods in the execution of the research study.[113, 116] This is achieved by using the method of semi-structured interviews and literature reviews as well as scenario designing. The third quality test for case studies of Yin is the internal validity test. This test describes the risk of misleading to inferences which are originated by an unknown impact factor.[82, pp. 43] The risk is less severe in non-experimental, e.g., explanatory studies. As this case study does not respond to the question of why the aviation supply chain can be mapped onto a metagraph rather than descriptive explaining how it is possible, this risk is negligible. Additional, different cognitive biases could have influenced the inquirer of the thesis. This was mitigated by establishing breaks in the research process in order to approach the topic from different perspectives.[117]

6.1.2 Conditional Metagraph Applied the Aviation Supply Chain

The most critical limitation that the experts attribute to the metagraph structure is the supply chain disclosure, i.e. transparency [104, 107]. Since the supply chain is often part of the competitive advantage, disclosure has critical implications that could be similar in impact to over-regulation [105], especially for SMBs. The graph-theoretic property of a projection allows to conceal suppliers by building a view on components and their interconnections (edges with suppliers are hidden). This approach needs to be further explored with focus on a scalability analysis.

An approach to implement an industry wide metagraph for enhanced cyber security is challenged by the following aspects:

The technical implementation would not be feasible because the conditional metagraph, in its lack of scalability, could not handle the processes of metapath calculations on the scale of an entire industry. This problem is exacerbated by the fact that suppliers in edges $\in E_{A2}$ which hold *false* propositions are not deleted when contexts are created. Moreover, the choice of components in higher tiers could affect the properties of components in lower tier levels. This is applicable but means that context generation depends on metapath calculations and not as it is done in this work. In addition, the maturity of the supplier is mapped to the information exchange and criticality of the components, while the maturity of the buyer is not. However, it can be argued that buyers are closer to the final product and already pressured to have a higher cyber security hygiene.

Another challenge is the concept of the graph setup which could be error-prone. Assuming a graph structure based on different supplier inputs (tables with information of their cyber security maturity, direct suppliers (and information exchange), purchased components (and their properties) (see Subsection 4.2.3). To deploy a graph structure which is reliable, the input files have to be reliable. This includes the uniqueness of a supplier ID and the correctness of content submitted by suppliers in their inputs. Hence, an central independent authority would need to certify the correctness of the documents and distribute the IDs of suppliers. If this idea is taken further, the central authority would need to be contacted in case an organisation's supplier would change and the authority could distribute updates if needed to affected organisations. Exemplary, EASA could represent this authority. Expert B states that such a graph structure in the aviation industry would be beneficial. Especially in the transformation phase, the graph could be used as a reference tool to identify suppliers with already established cyber security maturity niveaus.[104, 107] On the other side, Expert D and C see a possible implementation of such a graph structure only feasible when it develops bottom up from the aircraft OEMs. Also the manpower of the

maintenance of such a graph is criticised and not available on the side of authorities.[105, 106] However, the implementation from inside the supply chain is not feasible as the disclosure of information would need to be imposed and then privacy concerning stored. Expert F adds that even if EASA would be capable to implement a metagraph structure, it would still not feasible to integrate the whole supply chain as EASA is only regulating the EU and suppliers under other regulation (e.g., FAA or CAAC) would not be imposed to submit the needed information.[103] Additionally, the graph also relies on the quality of the certification standard mapping tables, which also would need to be reviewed. Some certification standards might also be limited in their mapping possibilities as their scopes would not overlap. The harmonisation of cyber security certification standards could also be investigated further with focus on supply chains.

7. Conclusion

This thesis shows that the graph-theoretic construct of a conditional metagraph is applicable to the aviation industry exemplified by the landing gear. With increasing importance of cyber security in the aviation industry and the regulator exerting pressure on the industry and authorities through the enactment of Part-IS, the enhancement of cyber security maturity in the aviation supply chain becomes relevant. The conditional metagraph performs algebraic calculations on cyber secure properties of suppliers and their components. Further, it integrates cyber security certification standards and cyber security practices which are harmonised to compare different suppliers in their cyber security maturity. The integration of cyber security practices allows SMBs to participate in the metagraph without the need for an extensive certification. The graph structure and its algebraic calculations further allow to filter for the securest suppliers conditioned on their properties. Alternative purchase options are identified in a reassessment of the conditional metagraph model in the event of a failure of confidentiality, availability or integrity, or loss of a particular cyber security maturity of a supplier. Additionally, the conditional metagraph allows to analyse ex-post cyber incidents of suppliers and its potential harm to the supply chain. The characteristics of the conditional metagraph application fields are evaluated by six industry experts. The mentioned topics are defined as significant by the experts. The thesis identifies limitations and challenges of the conditional metagraph applied to the aviation industry and suggests further research directions.

7.1 Outlook

Fundamentally, the introduced conditional metagraph model is limited in its attributes. The attributes can be extended by non-secure but purchase related attributes and additional cyber secure attributes. Further, the mentioned technical aspects (e.g., scalability enhancement of the metagraph construct) in Subsection 6.1.2 should also be considered for further research.

On the one hand, the conditional metagraph construct enables the representation of further restrictions, e.g., cost aspects or experience [104]. These could be supplemented by quantitative properties which could be algebraic used in a quantitative conditional metagraph. Exemplary, cyber security maturity could be the leading filter on a context which already filtered for the cheapest suppliers. Whether the cheap offers provide cyber security that

exceeds a certain threshold remains to be seen. However, this example should illustrate that the metagraph must not be limited to cyber security attributes.

On the other hand, cyber security attributes could be further extended. It would be interesting to see to what extent standardised platforms or interfaces between suppliers could protect them from vulnerabilities. Spear phishing could be mitigated and advantages could also be drawn from standardised technical security measures. Additionally, key suppliers would need to comply to a higher cyber security maturity conditioned by the number of edges they are included in. The information exchange about cyber security (e.g., ECCSA) can be added and hence, extend the graph away from a single purchase perspective. Further, the integration of two metagraphs as established supplier panels through a mergers and acquisitions could highlight further limitations and challenges of the metagraph. Additionally, also MRO certified suppliers could be implemented through sub-metagraphs in current individual supplier nodes.[108] Additionally, the transparency issue could be addressed and tested for feasibility in the context of homomorphic encryption or secure multi-party computation starting from the perspective of projections. Furthermore, the question should be asked whether airworthiness security and cyber security are in conflict with each other and whether it would be possible to apply a metagraph structure to address this issue. Following this thought, it would be interesting to see whether the regulator takes points into account which have not been addressed yet, such as the cyber security of aircrafts that are certified for new leasing agreements (e.g., whether and how implications for cyber security requirements of reused aircafts change) [108].This work could be extended with a longitudinal study by repeating the interviews with the industry experts in 2025 to analyse the transformation towards the Part-IS compliance.[104]

This work has shown that by applying a conditional metagraph to the supply chain, the aviation industry can be used as an example to increase cyber security maturity. The application to other industries can be considered as a call for research, as characteristics of the aviation industry can also be found in other industries: An antitrust exclusion of competitors defines the exclusion of communication between competitors and the solicitation of bids from multiple suppliers is graphical comparable to the double-sourcing strategy of the aviation industry. Thus, the graph structure can conceptually be applied to other industries.

Bibliography

[1] J. Cianci. *The SolarWinds Software Hack: A Threat to Global Cybersecurity, 08.02.2021*. URL: https://jolt.law.harvard.edu/digest/the-solarwinds-software-hack-a-threat-to-global-cybersecurity. (accessed: 09.04.2023).

[2] J. Martínez and J. M. Durán. "Software Supply Chain Attacks, a Threat to Global Cybersecurity: SolarWinds' Case Study". In: *International Journal of Safety and Security Engineering* 11.5 (2021), pp. 537–545.

[3] CERT-EU. *Airbus supply chain hacked in a cyberespionage campaign [190927-2]*. URL: https://media.cert.europa.eu/static/MEMO/2019/TLP-WHITE-CERT-EU-MEMO-190927-2.pdf. (accessed: 09.04.2023).

[4] A. Janofsky. *Cyber incident at Boeing subsidiary causes flight planning disruptions*. URL: https://therecord.media/cyber-incident-at-boeing-subsidiary-causes-flight-planning-disruptions,%2003.11.2022. (accessed: 09.04.2023).

[5] European Union Agency for Cybersecurity (ENISA). "ENISA Threat Landscape for Supply Chain Attacks". In: (2021). DOI: 10.2824/168593.

[6] European Union Aviation Safety Agency (EASA). *Overview: Product certification library*. URL: https://www.easa.europa.eu/en/document-library/product-certification-overview. (accessed: 09.04.2023).

[7] A. Brintrup, Y. Wang, and A. Tiwari. "Supply Networks as Complex Systems: A Network-Science-Based Characterization". In: *IEEE Systems Journal* 11.4 (2017), pp. 155–173.

[8] T. M. Sobb and B. Turnbull. "Assessment of Cyber Security Implications of New Technology Integrations into Military Supply Chains". In: *Symposium on Security and Privacy Workshops (SPW)*. 2020.

[9] International Organisation for Standards (ISO). *ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls*. URL: https://www.iso.org/standard/75652.html#page-top. (accessed: 15.03.2023).

[10] National Institute of Standards and Technology (NIST). *NIST Special Publication 800-171 Revision 2: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*. 2020. URL: https://doi.org/10.6028/NIST.SP.800-171r2. (accessed: 25.08.2022).

[11] European Union Aviation Safety Agency (EASA). *Part-IS regulation published, completing regulatory framework for cyber-resilient aviation [02.02.2023]*. URL: https://www.easa.europa.eu/en/newsroom-and-events/news/part-regulation-published-completing-regulatory-framework-cyber-resilient. (accessed: 09.04.2023).

[12] U.S. Department of Defence (DoD). *Cyber Security Maturity Model Certification*. URL: https://dodcio.defense.gov/CMMC/. (accessed: 25.08.2022).

[13] Federal Office for Information Security (BSI). *Guide to Basic Protection based on IT-Grundschutz: 3 Steps to Information Security*. URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/Basic_Security.pdf?__blob=publicationFile&v=2. (accessed: 15.03.2023).

[14] E. Ukwandu et al. "Cyber-Security Challenges in Aviation Industry: A Review of Current and Future Trends". In: *Information* 13.3 (2022), p. 146. DOI: https://doi.org/10.3390/info13030146.

[15] A. Basu and R.W. Blanning. *Metagraphs and their applications*. Vol. 15. New York City: Springer Science and Business Media, 2007.

[16] A. Shelupanov et al. "Information Security Methods—Modern Research Directions". In: *Symmetry* 11.150 (2019). DOI: doi:10.3390/sym11020150.

[17] A. Ghadge et al. "Managing cyber risk in supply chains: a review and research agenda". In: *Supply Chain Management: An International Journal* 25.2 (2020), pp. 223–240.

[18] International Telecommunication Union (ITU). *Definition of cybersecurity, referring to ITU-T X.1205, Overview of cybersecurity*. URL: https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx. (accessed: 22.03.2023).

[19] A. Yeboah-Ofori and S. Islam. "Cyber security threat modeling for supply chain organizational environments". In: *Future Internet* 11.3 (2019), p. 63.

[20] Justia U.S. Law. *2010 US Code, Title 44, Chapter 35, Subchapter III, Sec. 3542 - Definitions*. URL: https://law.justia.com/codes/us/2010/title44/chap35/subchapiii/sec3542. (accessed: 22.03.2023).

[21] M. Gasser. *Building a secure computer system*. NY: Van Nostrand Reinhold Company New York, 1988.

[22] T. Ncubukezi, L. Mwansa, and F. Rocaries. "A Review of the Current Cyber Hygiene in Small and Medium-sized Businesses". In: *15th International Conference for Internet Technology and Secured Transactions (ICITST)*. 2020, pp. 1–6. DOI: 10.23919/ICITST51030.2020.9351339.

[23] S. J. Shackelford. "Business and cyber peace: We need you!" In: *Business Horizons* 59.5 (2016), pp. 539–548. DOI: doi:10.1016/j.bushor.2016.03.015.

[24] S. Pandey et al. "Cyber security risks in globalized supply chains: conceptual framework". In: *Journal of Global Operations and Strategic Sourcing* 13.1 (2020), pp. 103–128.

[25] National Institute of Standards and Technology (NIST). *NIST Special Publication 800-161: Supply Chain Risk Management Practices for Federal in-Formation Systems and Organizations*. 2015.

[26] S. Boyson, T. M. Corsi, and J.-P. Paraskevas. "Defending digital supply chains: Evidence from a decade-long research program". In: *Technovation* 118 (2022), p. 102380.

[27] K. C. Kim and I. Im. "Research letter: issues of cyber supply chain security in Korea". In: *Technovation* 34.7 (2014), pp. 387–387.

[28] S. Boyson, T. M. Corsi, and H. Rossman. "Building a cyber supply chain assurance reference model". In: *Science Applications International Corporation (SAIC)* (2009).

[29] S. Simpson et al. "Software integrity controls: An assurance-based approach to minimizing risks in the software supply chain". In: *SAFECode* (2010).

[30] T. Sobb, B. Turnbull, and N. Moustafa. "Supply chain 4.0: A survey of cyber security challenges, solutions and future directions". In: *Electronics* 9.11 (2020).

[31] D. Miorandi et al. "Internet of Things: Vision, application and research challenges". In: *Ad Hoc Networks* 10.7 (2012), pp. 1497–1516.

[32] M. N. A. Latif et al. "Cyber security in supply chain management: a systematic review". In: *LogForum* 17.1 (2020), pp. 49–57.

[33] G. Li et al. "Joint supply chain risk management: An agency and collaboration perspective". In: *International Journal Production Economies* 164 (2015), pp. 83–94.

[34] J. Simon and A. Omar. "Cybersecurity investments in the supply chain: Coordination and a strategic attacker". In: *European Journal of Operational Research* 282 (2020), pp. 161–171.

[35] A. Dolgui, D. Ivanov, and B. Sokolov. “Ripple effect in the supply chain: an analysis and recent literature”. In: *International Journal of Production Research* 56.1/2 (2018), pp. 414–430.

[36] L. Urciuoli and J. Hintsa. “Adapting supply chain management strategies to security – an analysis of existing gaps and recommendations for improvement”. In: *International Journal of Logistics Research and Applications* 20.3 (2017), pp. 276–295.

[37] Ngoc T. Le and Doan B. Hoang. “Can maturity models support cyber security?” In: *2016 IEEE 35th International Performance Computing and Communications Conference (IPCCC)*. 2016, pp. 1–7. DOI: 10.1109/PCCC.2016.7820663.

[38] K.-F. Cheung, M. G. H. Bell, and J. Bhattacharjya. “Cybersecurity in logistics and supply chain management: An overview and future research directions”. In: *Transportation Research Part E* 146 (2021).

[39] S. Boyson. “Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems”. In: *Technovation* 34.7 (2014), pp. 342–353.

[40] S. A. Melnyk et al. “New challenges in supply chain management: cybersecurity across the supply chain”. In: *International Journal of Production Research* 60.1 (2021), pp. 162–183.

[41] A. B. D. Gani et al. “Interplay between cyber supply chain risk management practices and cyber security performance”. In: *Industrial Management and Data Systems* 123.3 (2023). Cited by: 0; All Open Access, Green Open Access, pp. 843–861. DOI: 10.1108/IMDS-05-2022-0313.

[42] PwC Germany GmbH. *Zahlungsbetrug in der Lieferkette – Zunehmender Einsatz von Cybercrime-Methoden. (German) [Payment fraud in the supply chain - increasing use of cybercrime methods]*. URL: https://www.pwc.de/de/managementberatung/forensic-services/zahlungsbetrug-in-der-lieferkette-zunehmender-einsatz-von-cybercrime-methoden.html. (accessed: 09.04.2023).

[43] CERT-UK. *Cyber-Security Risks in the Supply Chain*. 2015. URL: https://www.%20ncsc.gov.uk/content/files/protected_files/guidance_files/Cy%20ber-security-risks-in-the-supply-chain.pdf. (accessed: 05.11.2021).

[44] L.-W. Wong et al. “The role of cybersecurity and policy awareness in shifting employee compliance attitudes: Building supply chain capabilities”. In: *International Journal of Information Management* 66 (2022), p. 102520. ISSN: 0268-4012. DOI: https://doi.org/10.1016/j.ijinfomgt.2022.102520.

[45] International Organisation for Standards (ISO). *ISO/IEC 27001 – Information Security Management*. 2021. URL: https://www.iso.org/isoiec-27001-information-security.html. (accessed: 05.11.2021).

[46] C. Toppinga et al. "Beware suppliers bearing gifts!: Analysing coverage of supply chain cyber security in critical national infrastructure sectorial and cross-sectorial frameworks". In: *computers & security* 108 (2021), p. 102324.

[47] European Union Agency for Cybersecurity (ENISA). *NIS Directive*. 2021. URL: https://www.enisa.europa.eu/topics/nis-directive. (accessed: 05.11.2021).

[48] EUR-Lex. *Document 32016L1148, EUR-Lex: Access to European Union Law*. 2021. URL: https://eur-lex.europa.eu/eli/dir/2016/1148/oj. (accessed: 05.11.2021).

[49] Federal Office for Information Security (BSI). *IT-Grundschutz (German) [IT Baseline Protection Manual]*. 2021. URL: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-%20Zertifizierung/IT-Grundschutz/it-grundschutz_node.html. (accessed: 05.11.2021).

[50] Federal Office for Information Security (BSI). *IT-Sicherheitsgesetz 2.0 (German) [IT-Security Act 2.0]*. 2021. URL: https://www.bsi.bund.de/DE/Das-BSI/Auftrag/Gesetze-und-Verordnungen/IT-SiG/2-%200/it_sig-2-0_node.html. (accessed: 05.11.2021).

[51] European Commission. *Proposal for directive on measures for high common level of cybersecurity across the Union*. 2020. URL: https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-%20common-level-cybersecurity-across-union. (accessed: 05.11.2021).

[52] Federal Ministry for Economic Cooperation and Development (BMZ). *Supply Chain Law FaQs*. URL: https://www.bmz.de/resource/blob/60826/89631a44cf2ac8ca0d7dc45c6b0ed197/supply-chain-law-faqs-data.pdf. (accessed: 09.04.2023).

[53] Federal Ministry for Economic Cooperation and Development (BMZ). *Gesetz über die unternehmerischen Sorgfaltspflichten in Lieferketten, 16.07.2021 (German) [Law on corporate due diligence in supply chains, 16.07.2021]*. URL: https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl121s2959.pdf#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl121s2959.pdf%27%5D__1681653228064. (accessed: 09.04.2023).

[54] European Union Agency for Cybersecurity (ENISA). *IT-Grundschutz (IT Baseline Protection Manual)*. URL: https://www.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_it_grundschutz.html. (accessed: 21.03.2023).

[55] Federal Office for Information Security (BSI). *Mindeststandard des BSI für Schnittstellenkontrollen (German) [BSI minimum standard for interface controls]*. URL: https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/Schnittstellenkontrollen/Schnittstellenkontrollen_node.html. (accessed: 23.03.2023).

[56] B. Willemsen and M. Cadee. "Extending the airport boundary: Connecting physical security and cybersecurity". In: *Journal of Airport Management* 12.3 (2018).

[57] European Union Aviation Safety Agency (EASA). *Regulations*. URL: https://www.easa.europa.eu/en/regulations. (accessed: 25.08.2022).

[58] European Union Aviation Safety Agency (EASA). *Airworthiness*. URL: https://transport.ec.europa.eu/transport-modes/air/aviation-safety-policy-europe/aviation-safety-rules/airworthiness_en. (accessed: 15.04.2023).

[59] EUR-Lex. *Document 32023R0203, EUR-Lex: Commission Implementing Regulation (EU) 2023/203 of 27 October 2022*. 2022. URL: https://eur-lex.europa.eu/eli/reg_impl/2023/203. (accessed: 10.05.2023).

[60] Office of the Under Secretary of Defense for Acquisition & Sustainment. *CMMC Model and Assessment Guide*. 2021. URL: https://www.acq.osd.mil/cmmc/draft.html. (accessed: 05.11.2021).

[61] J. Horne. *The Fascinating History of CMMC as Told by Jacob Horne*. 2021. URL: https://www.youtube.com/watch?v=jbY2irZ1ePg. (accessed: 05.11.2021).

[62] National Institute of Standards and Technology (NIST). *Special Publication 800-171: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*. 2020. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf. (accessed: 05.11.2021).

[63] Agile Insider Blog. *CMMC 2.0 Announced – Changes from CMMC 1.0 to CMMC 2.0*. 2021. URL: https://www.agileit.com/news/cmmc-2-0-%20announced-changes-from-cmmc-1-0-to-cmmc-2-0/. (accessed: 05.11.2021).

[64] National Institute of Standards and Technology (NIST). *NIST Special Publication 800-171 Revision 2: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*. 2021. URL: https://csrc.nist.gov/publications/detail/sp/800-172/final. (accessed: 15.03.2023).

[65] A. Basu and R.W. Blanning. "Metagraphs". In: *Omega - International Journal of Management Science* 23.1 (1995), pp. 13–25.

[66] C. Berge. *Graphs*. 2nd ed. Amsterdam: North-Holland, 1985.

[67] Zihai Shi et al. "3 - Resilience assessment methodology and fundamentals of graph theory". In: *Structural Resilience in Sewer Reconstruction*. Ed. by Zihai Shi et al. Butterworth-Heinemann, 2018, pp. 79–111. DOI: https://doi.org/10.1016/B978-0-12-811552-7.00003-1. URL: https://www.sciencedirect.com/science/article/pii/B9780128115527000031.

[68] C. Berge. *Hypergraphs*. Amsterdam: North-Holland, 1989.

[69] M. Ramaswami, S. Sarkar, and Y.-S. Chen. "Using directed hypergraphs to verify rule-based expert systems". In: *IEEE Transactions on Knowledge and Data Engineering* 9.2 (1997), pp. 221–237.

[70] M. Ward et al. "Finding Input-Dominant Hyperpaths and Metapaths is NP-Hard". In: *in print* tba.tba (2023), tba.

[71] D. Harel. "On visual formalisms". In: *Communications of the ACM* 31.5 (1988), pp. 514–530.

[72] A. Basu, R.W. Blanning, and A. Shtub. "Metagraphs in Hierarchical Modeling". In: *Management Science* 43.5 (1997), pp. 623–639. DOI: https://www.jstor.org/stable/2634400.

[73] A. Basu and R.W. Blanning. "The Analysis of Assumptions in Model Bases Using Metagraphs". In: *Management Science* 44.7 (1998), pp. 982–995. DOI: https://www.jstor.org/stable/2634512.

[74] A. Basu and R.W. Blanning. "Model Integration Using Metagraphs". In: *Information Systems Research* 5.3 (1994), pp. 195–218. DOI: http://www.jstor.com/stable/23010889.

[75] A. Basu and R.W. Blanning. "Synthesis and Decomposition of Processes in Organizations". In: *Information Systems Research* 14.4 (2003), pp. 337–355. DOI: https://www.jstor.org/stable/23015678.

[76] A. Basu and R.W. Blanning. "Metagraph Transformations and Workflow Management". In: *Proceedings of The Thirtieth Annual Hawwaii International Conference on System Sciences*. 1997.

[77] A. Hamza et al. “Clear as MUD: Generating, validating and applying IoT behavioral profiles”. In: 2018, pp. 8–14. DOI: 10.1145/3229565.3229566.

[78] D. Ranathunga, M. Roughan, and H. Nguyen. “Verifiable Policy-Defined Networking Using Metagraphs”. In: *IEEE Transactions on Dependable and Secure Computing* 19.1 (2022), pp. 482–494. DOI: 10.1109/TDSC.2020.2974727.

[79] M. Saunders, P. Lewis, and A. Thornhill. *Research Methods for Business Students*. 6th ed. London: Pearson, 2007.

[80] D. Silverman. *Doing Qualitative Research: A practical handbook*. London: Sage Publications, 2013.

[81] A.K. Carstensen and J. Bernhard. “Design science research – a powerful tool for improving methods in engineering education research”. In: *European Journal of Engineering Education* 44.1-2 (2019), pp. 85–102. DOI: https://doi.org/10.1080/03043797.2018.1498459.

[82] R.K. Yin. *Case Study Research and Applications: Design and Methods*. 6th ed. Thousands Oaks: Sage Publications, 2018.

[83] G. Thomas. “A Typology for the Case Study in Social Science Following a Review of Definition, Discourse, and Structure”. In: *Qualitative Inquiry* 17.6 (2011), pp. 511–521. DOI: 10.1177/1077800411409884.

[84] R.K. Yin. *Case Study Research: Design and Methods*. 5th ed. Thousands Oaks: Sage Publications, 2014.

[85] H. Simone. *Case study research in practice*. London: Sage Publications, 2009.

[86] R.E. Stake. “Qualitative case studies.” In: N. K. Denzin & Y. S. Lincoln (Eds.), The SAGE handbook of qualitative research (3rd ed.) (pp. 443–466). Thousand Oaks: Sage Publications, 2005.

[87] M. Jarke, X.T. Bui, and J. M. Carroll. “Scenario Management: An Interdisciplinary Approach”. In: *Requirements Engineering* 3 (1998), pp. 155–173.

[88] S.B. Merriam. *Case study research in education: A qualitative approach*. San-Francisco: Jossey-Bass, 1988.

[89] S.B. Merriam. *Case study research in educational settings*. Maidenhead: Open University Press, 2000.

[90] Prisma Statement. *Flow Diagram*. URL: https://www.prisma-statement.org//PRISMAStatement/FlowDiagram. (accessed: 10.05.2023).

[91] A. Basu and R.W. Blanning. “Enterprise modeling using metagraphs”. In: T. Jelassi, M.R. Klien and W.M. Mayon-White (Eds.), Decision Support Systems: Experiences and Expectations, (pp. 183–199). Amsterdam: North-Holland, 1992.

[92] A. Basu and R.W. Blanning. “Doing mixed methods research pragmatically: Implications for the rediscovery of pragmatism as a research paradigm”. In: *Journal of Mixed Methods Research* 4.1 (2010), pp. 6–16.

[93] BSides. *BSides Tallinn 2022*. URL: https://www.eventyco.com/event/bsides-tallinn-2022-tallinn-estonia. (accessed: 10.10.2022).

[94] Behörden Spiegel (Organiser). *Berlin Security Conference: Europe – Developing capabilities for a credible defence*. URL: https://euromil.org/event/berlin-security-conference/. (accessed: 15.02.2022).

[95] Airframer Limited. *Supply Chain Directory*. URL: https://www.airframer.com/sector_front.html. (accessed: 01.11.2022).

[96] Infodas. *Download of the Infodas CMMCv1 Mapping with ISO27001 and NIST SP 800-171*. URL: https://www.infodas.com/wp-content/uploads/2021/08/CMMC_V1.02_Mapping_ISO_27001_IT-Grundschutz_infodas.xlsx. (accessed: 25.08.2022).

[97] BSI. *Zuordnungstabelle ISO zum IT-Grundschutz. (German) [Mapping table ISO27001 to IT Baseline Protection Manual]*. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/Zuordnung_ISO_und_IT_Grundschutz.html. (accessed: 25.08.2022).

[98] J.P.C. Kleijnen. “Theory and Methodology: Verification and validation of simulation models”. In: *European Journal of Operational Research* 82 (1995), pp. 145–162.

[99] D. Ranathunga. *mgtoolkit: Tutorial*. URL: https://mgtoolkit.readthedocs.io/en/latest/tutorial.html. (accessed: 15.02.2022).

[100] Luisa Caretta Hopp. *Aviation Supply Chain Cyber Security Metagraph*. URL: https://github.com/carihopp/AvSCCySecMetagraph.git. (accessed: 17.04.2023).

[101] E. Parsonage. *mgtoolkit Upgrade Python3*. (accessed: 15.03.2023).

[102] J.W. Creswell. *Research design: Qualitative, Quantitative, and Mixed Methods Approaches*. Thousands Oaks: Sage Publications, 2003.

[103] L. C. Hopp. *Interview: Aviation Expert F, see Appendix A2 [confidential]*. 17.12.2022.

[104] L. C. Hopp. *Interview: Aviation Expert B, see Appendix A2 [confidential]*. 9.12.2022.

[105] L. C. Hopp. *Interview: Aviation Expert D, see Appendix A2 [confidential]*. 16.12.2022.

[106] L. C. Hopp. *Interview: Aviation Expert C, see Appendix A2 [confidential]*. 14.12.2022.

[107] L. C. Hopp. *Interview: Aviation Expert E, see Appendix A2 [confidential]*. 16.12.2022.

[108] L. C. Hopp. *Interview: Aviation Expert A, see Appendix A2 [confidential]*. 23.11.2022.

[109] T.-C. Horng. *A Comparative Analysis of Supply Chain Management Practices by Boeing and Airbus: Long-term Strategic Implications*. Massachusetts Institute of Technology, 2007.

[110] Airframer Limited. *Airbus 320*. URL: https://www.airframer.com/aircraft_detail.html?model=A320#76. (accessed: 01.11.2022).

[111] Beuth Verlag GmbH. *DIN EN 9100:2018-08*. URL: https://www.beuth.de/de/norm/din-en-9100/289865083. (accessed: 22.03.2023).

[112] European Union Aviation Safety Agency (EASA). *Notice of Proposed Amendment 2019-01: Aircraft cybersecurity*. 2019.

[113] W.L. Neuman. *Social research methods: Qualitative and quantitative approaches*. 7th ed. London: Pearson, 2010.

[114] J.W. Creswell. *The art of case study design*. Thousands Oaks: Sage Publications, 1995.

[115] N.K. Denzin. *The Research Act: A Theoretical Introduction to Sociological Methods*. Aldine Publishing Company, 1970.

[116] Joint United Nations Programme on HIV/AIDS (UNAIDS). "An Introduction to Triangulation". In: *UNAIDS Monitoring and Evaluation Fundamentals* (2010).

[117] University of North Carolina. *Cognitive Bias Codex*. URL: https://www.sog.unc.edu/sites/www.sog.unc.edu/files/course_materials/Cognitive%20Biases%20Codex.pdf. (accessed: 15.04.2023).

School of Information Technologies

Appendix 1 - Interview Guide

Master Thesis

Cyber Security in the Aviation Supply Chain

Luisa Caretta Hopp, 202107IVCM

Introduction to the Research Topic

This interview is conducted for scenario validation of a case study covered in a master thesis. Using the landing gear supply chain as a case study, the aviation industry supply chain is mapped to the graph-theoretic construct of a metagraph. Three scenarios are presented below that illustrate the applicability of the metagraph. This interview is intended to validate the exemplary supply chain and the utility of the scenarios from the perspective of industry experts. The fundamental question is whether a metagraph supports the integration of cyber security certificates and practices within aviation supply chains.

By using the metagraph[1], possible supply chain paths can be represented with supplier characteristics. Requirements (go's and no-go's) for supplier attributes are defined. By excluding the no-go characteristics of suppliers, all possible supply chain paths are displayed (containing the go's and neutral characteristics of suppliers).

Scenario 1: Different cyber security certificates (exemplary: Cybersecurity Maturity Model Certification (CMMC), ISO 27002, NIST SP 800-171, BSI IT Basic Protection) and practices of suppliers are mapped to be comparable integrated into the metagraph model. Requirement of this scenario is a high level of cyber security maturity of the suppliers. All supply chain paths which include suppliers with a low cyber security maturity are dropped. Add-Ons: Handling of incompleteness of the supply chain paths' suppliers or their attributes and the introduction of certificate expiration warning.

Scenario 2:
A cyber secure supply chain can be conditionally selected on information sharing between supplier and buyer or component production. A certain level of information sharing between buyer and supplier requires a certain level of cyber security maturity. Manufacturing a specific component (e.g., software) necessitates a certain level of cyber security maturity. On these requirements, possible supply chain paths can be determined.

Scenario 3:
The decision for supply chain paths has been made. Additional information about parts of the supply chain appears: The supply chain path extends by additional suppliers or characteristics of the suppliers are added. A re-assessment of possible secure supply chain paths shows a more secure alternative, or a chosen path turns insecure.

Scenario 4:
The decision for supply chain paths has been made. Suddenly a supplier fails, or the data communication interface between two suppliers in a path is unreachable. A re-assessment of alternative secure supply chain paths is possible.

[1] Basu, A. and Blanning, R. W. Metagraphs and their applications, volume 15. Springer Science Business Media, 2007.

1 Introduction Questions

The information from the interview is presented as personal view of yours and detached from your employer. Is it possible to mention the functionality of your employer (not the employer's name) as scope of experience of the expert group to demonstrate the reliability of the study?

1. Can you please introduce your area of expertise? Please introduce the area of your profession. If this is not possible for confidentiality reasons, the question will be omitted.
2. How critical is cyber security to the aviation industry and its supply chain?
3. To what extent do you view cyber security as a supplier selection criterion?
4. Who bears responsibility for cyber security in the supply chain? E.g., the sourcing company, the respective supplier, the legislator or regulator, etc.?
5. Do you know companies who consider supplier cyber security when purchasing products? Do they have to follow any legal regulations concerning cyber security? If so, which ones?
6. What is the company's influence and insight on supplier cyber security practices in the supply chain (tier level, impact influence)? How far does the impact reach, and how strong is it (change in practices, veto power, etc.)?
7. Do airline or aircraft leasing companies have influence on the security of the aircraft? If so, how much?
8. Can previous owners/lessees (airlines) influence the security/safety of an aircraft?

2 Specific Questions about the Aviation Supply Chain

The following characteristics of the an aviation supply chain have been identified to set up the metagraph model. Can you confirm these?

1. The number of competing suppliers rises with the increase of tier levels. A few suppliers are close to the airframe manufacturer, taking a lot of responsibility as OEMs of airframe components.
2. Dependencies of suppliers of the same tier level can have three forms: (1) Suppliers can cooperate in a close alignment, (2) have different variants of products depending on the cooperation partner, or (3) their products have standardized interfaces making them independent from other components.
3. A supplier can have multiple supplier options. The number of options increases when standardized components are purchased and decreases for customzed components.
4. A component can be exactly assigned to its manufacturer(s) and its airworthiness certificate.

Do you have further characteristics of the aviation supply chain in mind?

3 Specific Questions about the Cyber Security Scenarios

3.1 Scenario: Cyber Security Assessment based on Harmonization of Cyber Security Practices and Certificates

1. Did you hear about different cyber security practices and certificates used by suppliers in the aviation industry?

2. Do you see the need for unification of cyber security practices to create clarity and comparability of supply chains' cyber security?
3. Would you decide on a supply chain dependent on cyber security requirements?

3.2 Cyber Security Assessment based on Information Exchange or Component Manufacturing

1. What types of information exchange between suppliers in the aviation industry exist? Do the types of communication vary? Are systems between suppliers linked to core supplier systems?
2. Do suppliers near the own company's core systems require cyber security practices?
3. Is the level of information exchange between supplier and buyer known at the time of proposal and contract signing?
4. How important is an electronic data interchange interface between supplier and buyer as a gateway or transmission path for cyber threats in the supply chain?
5. How important do you consider cyber security maturity for suppliers of critical components (E.g., control units)?
6. What would you consider more important: Cyber security based on
   a) information exchange between buyer and supplier,
   b) the manufacturing of a specific critical component,
   c) or both?

3.3 Cyber Security Assessment: Handling of Incompleteness

1. How does an aviation company deal with the incompleteness of supplier cyber security attributes and level of information sharing for an aircraft component in general (if known, specifically a landing gear component)?
2. Would it make a difference to a component's decision-making process if its supply chain and the cyber security practices of its suppliers were known or if parts of it were unknown?

3.4 Cyber Security Re-Assessment based on Additional Information About the Supply Chain

1. Is it still possible to change supply chain paths once contracts are signed?
2. Would you change an established supply chain path if
   a) a more secure alternative supply chain path was established in the supply network?
   b) the existing supply chain path was revealed to be more insecure than initially thought?

3.5 Cyber Security Re-Assessment based on Failure of Parts of the Supply Chain

1. Who is responsible for finding a new supplier in case of a supplier failure? Would there be differences between a close supplier and a more distant supplier? If so, what are they?
2. In the case of a compromised supplier, how important would you consider the possibility of obtaining information about the supplier's connectivity to other suppliers (regarding possible distribution of malicious software or component availability)?
3. How would an aviation company react in case of compromised data exchange between two suppliers (changing the suppliers or the information exchange channel, etc.)?
4. Do you know impact factors concerning supply chain unavailability that could limit cyber security (existing contractual relationships with other suppliers, time factor, component availability, etc.)?

4 General Closing Questions

1. Do you consider cyber security becoming more important in purchasing in the next few years? If so, at what point? E.g., organizational, component, or interface security?
2. Who will/should be responsible for cyber security in the supply chain?
3. What is your opinion of an industry-wide graph of supplier cyber security maturity levels?
4. Does an exchange of supply chain cyber security already exist within the aviation industry? If so, how is transparency dealt with within this approach?
5. How would you assess the feasibility of implementing an update structure for supply chains within the aviation industry (e.g., ECCSA members)?
6. How would you evaluate a central authority as authorisation unit for cyber security certifications and as a supply chain graph merger of the industry?
7. Is EASA a possible central authority to consider?
8. Do you have further comments and ideas in building a network for traceable cyber security maturity in the aviation supply chain?

Thank You for Participating in This Interview!

Appendix 2 - Interviews

Appendix 3 - The Uncensored Supply Chain of the Landing Gear