DOCTOR OF PHILOSOPHY

Automotive cybersecurity management

a conceptual framework for improved cybersecurity knowledge sharing in the automotive industry

Madzudzo, Garikayi

Award date:
2020

Awarding institution:
Coventry University

Automotive Cybersecurity Management: A Conceptual Framework for Improved Cybersecurity Knowledge Sharing in the Automotive Industry

By

Garikayi Brasington Madzudzo

June 2019

Coventry University

A thesis submitted in partial fulfilment of the University's requirements for the Degree of Doctor of Philosophy

Content removed on data protection grounds

Certificate of Ethical Approval

Applicant: Garikayi Brasington Madzudzo

Project Title: Automotive Cybersecurity Management: A Conceptual Framework for Improved Cybersecurity Knowledge Sharing in the Automotive Industry

This is to certify that the above-named applicant has completed the Coventry University Ethical Approval process and their project has been confirmed and approved as Medium Risk

Date of approval: 31 May 2017

Project Reference Number: P53760

Declaration

I confirm that this is my work and the use of all material from other sources has been properly and fully acknowledged.

This work used a third-party proofreading service for quality improvement

Garikayi Brasington Madzudzo

Coventry University

17 June 2019

List of Publications

1. Morris, D., Madzudzo, G. and Garcia-Perez, A., 2018. Cybersecurity and the auto industry: the growing challenges presented by connected vehicles. *International Journal of Automotive Technology and Management*, *18*(2), pp.105-118.

2. Madzudzo, G., Morris, D. and Garcia-Perez, A., 2018. Supplier Delocalization: A Threat to Automotive Cybersecurity Knowledge Sharing? *26th Gerpisa International Colloquium 2018: Who drives the change? New and traditional players in the global automotive sector.*

3. Kalutarage, H., Al-Kadri, M., Cheah, M., Madzudzo, G., McCausland, R., 2019. Context-aware Anomaly Detector for Monitoring Cyber Attacks on Automotive CAN Bus. *In Proceedings of CSCS '19: ACM COMPUTER SCIENCE IN CARS Symposium (CSCS '19). ACM, New York, NY, USA.*

4. Morris, D., Madzudzo, G. and Garcia-Perez, A., 2020. Cybersecurity threats in the auto industry: Tensions in the knowledge environment. Technological Forecasting and Social Change, 157, p.120102.

5. Madzudzo, G., Cheah M. and Kukova, M., 2019. Consumer Car Owner Attitudes Towards In-Vehicle Privacy. *Journal of Consumer Research (JCR), 2020*

Abstract

The inclusion of new connected services and features embodying unfamiliar technologies has transformed the automotive industry. Vehicle manufacturers and component suppliers now develop and integrate ever more technologically complex components into the modern connected vehicle. In the unrelenting search for sustainable competitive advantage, automotive manufacturers are driven to develop more reliable and safer products; at the same time as promoting product personalisation, higher quality, increased functionality and, lower costs. The creation of new digital products is a complex task, characterised by uncertainty, variability and the threat of cybersecurity breaches. These innovations require cooperation across multiple fields of expertise, some of them new to automotive design, development and, production.

Even though the potential risks inherent in cyber-vulnerable connected and autonomous vehicles affect all stakeholders in the automotive industry from, vehicle designers and manufacturers to vehicle end-users, there are relatively few research contributions which focus on the wider social, economic and behavioural aspects rather than the technological. The varied and often competing incentives of different auto industry actors to invest in cybersecurity defences, and the sharing of component-related knowledge, in particular, the knowledge of potential cybersecurity threats and vulnerabilities of relevance for the digital security of connected and autonomous vehicles, are identified as a challenge to developing a specific and coherent industry response to the growing threats posed by cybersecurity breaches. This thesis summarises research conducted to investigate and analyse the sharing of knowledge related to component integration processes within the automotive industry as a potential factor for improving the cybersecurity of modern connected vehicles. The study focuses on the knowledge sharing aspects of the component integration problem, rather than investigating the technical aspects.

Fieldwork involving two original equipment manufacturers (OEMs), two automotive component manufactures, plus a number of knowledge experts from across a spectrum of automotive stakeholder institutions, was conducted to identify the most important factors, and management strategies, in an attempt to ensure auto security now and in the future. An interpretive paradigm using multi-method research was employed to collect qualitative data from experts within the auto-domain.

The research has resulted in a number of contributions and benefits for the automotive industry. A key contribution is the development of a conceptual framework for the sharing of knowledge related to components and their integration processes, which can help all relevant stakeholders; from vehicle manufacturers to their supply chain, dealers and their customers, to be better prepared to handle the complexities of the current cybersecurity landscape where the sector operates. The proposed knowledge sharing framework, which has been positively evaluated by experts from the automotive domain, is designed to assist the industry to develop, design and deliver more cyber-secure vehicles through better management of component integration processes by overcoming some of the limitations of existing techniques for knowledge sharing in the integration of components for connected vehicles as identified in the relevant literature. The proposed framework is supported by theory from both the automotive and the knowledge management domains and brings together the best practices established in this thesis through the literature review and the primary evidence from the semi-structured interviews and the online surveys.

Feedback provided by the study's participants suggests that the proposed framework overcomes some of the major challenges of component integration processes particularly those of relevance for the cybersecurity of the connected vehicle. In addition to its contribution to the emerging body of knowledge on the subject, the research has identified areas where there is significant scope for further research and investigation.

Table of Contents

List of Tables

List of Figures

List of Abbreviations

ACM	Association for Computing Machinery
ASCM	Automotive Supply Chain Management
AV	Autonomous Vehicle
Auto-ISAC	The Automotive Information Sharing and Analysis Center
BMW	Bayerische Motoren Werke
BO	Boundary Object
CAN	Controller Area Network
CAV	Connected and Autonomous Vehicle
CBiS	Centre for Business in Society
CIA	Confidentiality, Integrity and Availability
CS	Cybersecurity
CSCS	Computer Science in Cars Symposium
CV	Connected Vehicle
DOS	Director of Studies
ECU	Electronic Control Unit
EE	Extending Enterprise
ENISA	European Union Agency for Network and Information
EU	European Union
EV	Electric Vehicle
FBL	Faculty of Business and Law
FOTA	Firmware updates Over the Air
GDPR	General Data Protection Regulation
ICT	Information and Communications Technology
IoT	Internet-of-Things
IP	Intellectual Property
IT	Information Technology
ISACA	Information Systems Audit and Control Association
ISO	International Organisation for Standardization

KM	Knowledge Management
KS	Knowledge sharing
LIN	Local Interconnection Network
MOST	Media Oriented Systems Transport
NASA	National Aeronautics and Space Administration
NDA	Non-Discloser Agreement
NHTSA	National Highway Traffic Safety Administration
NIST	National Institute of Standards and Technology
OEM	Original Equipment Manufacturer
SAE	Society of Automotive Engineers
SOW	Statement-of-Work
V2S	Vehicle-to-Sensor-on-board
V2V	Vehicle-to-Vehicle
V2R	Vehicle-to-Road-infrastructure
V2I	Vehicle-to-Internet

Statement of Copyright

Acknowledgements

This thesis would not exist without experiences, insights and generosity of many people. I would like to express my deepest and sincere gratitude to all those I was fortunate to have in my life when I embarked on this journey and those I met along the way.

First and foremost, I thank the Lord Almighty for giving me the strength, knowledge, opportunity and ability to undertake this research study and to persevere through all these years so that today I can stand proudly with my head held high.

I express my heartfelt gratitude to my Director of Studies, Dr Alexeis Garcia-Perez for all the guidance and support l received throughout these years and for his enduring patience in many brainstorms that helped to crystalize the essence of this project. I am forever in your debt. In this area as well, my immense and sincere gratitude goes to my supervisor Professor David Morris for his ongoing interest in the research study, continuing encouragement, generous sharing of expertise and kindness. This work would not have been possible without his guidance and involvement.

To Kendra Kai "KiKi" Madzudzo, I want to say a very special thank you for putting up with me working very long hours and for making the times we could spend together so happy and memorable. This work is especially dedicated to her. Finally, there are not enough words to tell Mitchelle Madzudzo how grateful l am for her unwavering belief in anything being possible, and for her ongoing commitment to give me the space to get to the finish line "*Gratias ago tibi ubera mea*". You have been a constant source of support and encouragement and you have made an untold number of sacrifices. To Emmanual, you are still in my heart. But you are missed each and every day, for you were someone special.

Thank you to all of you

In Memory of my Mother

Lydia Madzudzo

I would much prefer it if you were alive and well

With you went so much of me

You were a fantastic mum

Chapter I
INTRODUCTION

1.1 Introduction

The trend towards connectivity in vehicle development has ushered the automotive industry into a new era of evolution and cybersecurity challenges. Estimates of the likely number of connected vehicles abound, but about one in five vehicles will have some sort of wireless connection by the end of 2020, which is a quarter of a billion connected vehicles on the roads. The value of the 2021 connected vehicle market is estimated at €122bn (Allied Market Research 2014). In the context of this study, “connected vehicle” refers to a vehicle equipped with internet access, a wireless local area network, and built-in capabilities that allow the vehicle to share digital information with other connected vehicles, physical devices, transport infrastructure, drivers and passengers. They can contain over 60 embedded electronic control units (ECUs), making the vehicle highly dependent on numerous complex software systems. Most high-end connected vehicles can embody software code that exceeds 100 million lines and have the computing power of approximately 20 personal computers (Mössinger 2010).

As vehicles increasingly incorporate in-vehicle computer systems to improve safety, security, comfort and performance, the threat and potential incidence for cybersecurity vulnerabilities increases. The creation of a new product in the automotive industry is a knowledge-intensive, complex task characterised by uncertainty and variability. The trend towards connected vehicles further emphasises these challenges. As vehicles become pervasively computerised and open to compromise from many attack vectors, the need to ensure that connected vehicles are protected against malfunction and/or manipulation has never been more important.

In the current context, intangible assets such as data, information, and knowledge not only become key sources of sustainable competitive advantage, but are important for security, and are particularly relevant for areas driven by the use of technology such as the automotive domain. Knowledge becomes important for effective cybersecurity management practices and the security of connected vehicles. Cooperation of OEMs and their suppliers in the form of knowledge sharing is an important aspect in the disciplines of component design, development, and integration.

This research captures a detailed exposition of an investigation into the sharing of knowledge related to component integration processes in the automotive industry. This research was undertaken to investigate and understand knowledge sharing challenges associated with component integration that lead to cyber-related challenges in connected vehicle development, and to develop a knowledge sharing infrastructure to support the sharing of relevant knowledge pertaining to component integration processes for addressing these challenges. It is an area that has received very little research yet is of increasing importance as the industry enters the era of connected and autonomous vehicles (CAVs). The phenomena under study defy explanation by a single theory, therefore the focus is positioned at the intersection of three evolving research disciplines that comprise the automotive industry, knowledge management discipline and, the cybersecurity domain as shown by the red area in Figure 1.1 below. This chapter outlines the context of the research and provides an overview of the importance of and difficulties in achieving successful component integration. This is followed by a summary of the importance of knowledge sharing, specifically, component integration-related knowledge. Finally, the research questions are presented, and the research aims and objectives are established.

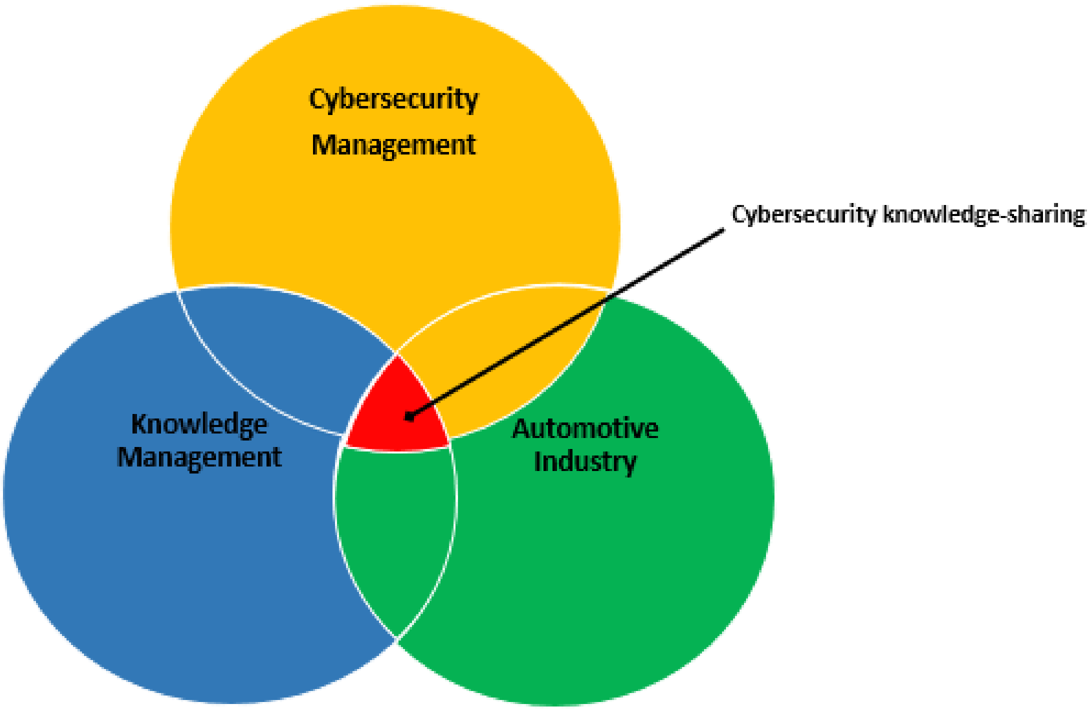

Figure 1. 1: Focus of the research

1.1.2 Research path

The study investigates the sharing of knowledge by original equipment manufacturers (OEMs), component suppliers and other relevant stakeholders in the integration of components for modern connected vehicles. The study explores:

- Component integration challenges that expose connected vehicles to cybersecurity vulnerabilities.
- Knowledge sharing inhibitors in automotive component integration processes.
- Strengths and limitations of component integration strategies in use within the automotive domain.
- Developments in the cybersecurity field in general and their potential impact on the automotive sector.

The investigations in this thesis centre on the sharing of relevant knowledge for component integration and the design and development of a conceptual framework to potentially assist with the secure integration of components for connected vehicles. The literature review identifies sources discussing how knowledge is used to benefit vehicle manufacturing (Ho & Ganesan 2013, Blome et al. 2014), but, notably, none on the sharing of knowledge in component integration processes, and how it can be employed to mitigate cybersecurity challenges in the automotive domain. Additionally, cybersecurity challenges due to insecure integration strategies and processes remain an area yet to be fully explored; the discussion in Chapters 2 and 6 examines this more fully.

During the fieldwork, the researcher engaged with individuals and organisations that are affected by the phenomenon to understand potentially effective approaches to develop a novel knowledge sharing framework and, for promoting its adoption by the automotive industry. The proposed framework developed; is based on an evidence collection process involving automotive knowledge experts, OEMs and component manufacturers. The proposed framework was designed and developed from information derived from the review of relevant literature (Chapter 2), and information provided by the study's participants who are involved with integrating components for connected vehicles. The proposed framework was evaluated by expert personnel in vehicle and component manufacturing organisations. However, areas where there is significant scope for further research and investigation still exist.

1.2 Research context

The trend towards the manufacture of connected vehicles has transformed the automotive industry, leading OEMs and their supply chains to develop and integrate ever-more technologically complex components, sub-systems, and systems into their products. In the unrelenting search for sustainable competitive advantage, automotive manufacturers are driven to develop more reliable and safer products, at the same time as promoting product personalisation, higher quality, improved environmental impact; increased functionality and lower costs. The creation of new digital products for smart, intelligent vehicles capable of absorbing information from the environment and other vehicles, and then feeding it to drivers and the transport infrastructure to assist with safe navigation, pollution control, and traffic management, is an expensive, competitive, complex task, characterised by uncertainty, variability and the threat of cybersecurity breaches. As a consequence of these technological advances, and component out-sourcing, modern connected vehicles have been ushered into the era of cybersecurity.

Historically, the automotive industry has been a network relying on the sharing of knowledge between the various tiers in the supply chain to obtain better component design and quality, thus ultimately manufacturing better vehicles. Studies in the European, Chinese and Japanese auto-industry provide evidence of the existence of knowledge sharing practices and highlight how knowledge was used to improve vehicle manufacturing (Cabigiosu et al. 2013, Khan et al. 2015 and Kochan et al. 2018). The drive towards connectivity in modern-day vehicles has re-structured the automotive supply chain and has adversely affected inter-firm relationships that existed when suppliers were in close proximity with OEMs, often in supplier-parks. In a bid to apply downward pressure on operating costs and to satisfy an over-arching need to remain competitive, OEMs and component suppliers have become more reliant on component out-sourcing (Woolliscroft et al. 2013). The design and development of connected vehicles is affected by an ever-increasing cybersecurity threat landscape which demands an effective sharing of cybersecurity-related knowledge between vehicle manufacturers and their tiered supply chain.

1.2.1 The cybersecurity concept

Cybersecurity is a broadly used term, whose definitions are highly variable, context-bound, often subjective, and at times, uninformative (Caldwell 2013, Baylon 2014). There is a substantial literature on what the term "*cybersecurity*" means and how it is situated within various contexts; however, there is an absence of a concise, broadly accepted definition that captures the multi-dimensionality of cybersecurity (Craigen et al. 2014, Westerlund et al. 2018). However, all attempts to define cybersecurity have one thing in common; they see cybersecurity as either being the security of systems or the security of individual components within a system. Within the context of connected vehicles and for the purpose of this study, cybersecurity is understood as:

> "*The protection of vehicular electronic systems, communication networks, control algorithms, software, users, and underlying data from malicious attacks, damage, unauthorized access, or manipulation*" (NHTSA 2017).

Designing and developing cyber-resilient components and systems for connected vehicles is a complex and challenging endeavour, in general, it is infeasible for a single supplier or OEM to design and develop a successful system or sub-system of any complexity for connected or autonomous vehicles without effectively cooperating with many suppliers. Therefore, from a cybersecurity perspective, knowledge related to the integration of components is key in the design and development of components and systems for connected vehicles. Nonetheless, cybersecurity knowledge is context-bound by the phenomenon being studied. The focus of this research is the sharing of knowledge related to component integration processes as a potential factor in improving the cybersecurity of modern connected vehicles, so for the purpose of this research, the author adheres to the definition of automotive cybersecurity knowledge as:

> *"Component and architectural knowledge used to protect connected vehicles, automotive integrated components, systems, sub-systems, and embedded software from unauthorised access and manipulation."*

1.2.2 Knowledge concepts

Defining the term "*knowledge*" is difficult as there is no universal definition of the term. Polanyi (2012) states that the definition of knowledge varies depending on the entity that created the knowledge. However, knowledge has been classified into two main types: tacit and explicit (Dalkir 2013). Tacit knowledge is not easy to capture and articulate as a valuable asset for others, but in dialogue and collaboration, specific meanings of words and actions are communicated and shared to a greater or lesser extent, allowing some tacit knowledge to be articulated (Holste & Fields 2010, Goffin & Koners 2011). Explicit knowledge is already codified and articulated and is available for transfer to others, leading to a potential growth of shared understanding (Greenhalgh 2010, Durisova 2011). Defining knowledge is difficult, nonetheless, knowledge will be defined in the context of this study as:

> *"The integration of ideas, experiences, intuition, assertions, skills, and lessons learned that have the potential to create value for an organisation, a business or company by informing decisions and improving performance" (Polanyi 2012).*

Knowledge management

Knowledge management (KM) is a concept that was initially defined as the process of applying a systematic approach to the capture, structure, management, and dissemination of knowledge throughout an organisation in order to work faster, reuse best practices, and reduce costly rework from project to project (Dalkir 2013). Knowledge management has been defined in different ways in the scientific literature. There are various concepts, conflicting definitions, and overlapping views, however, the general consensus across most definitions is that knowledge management involves people, technology and processes of creating, capturing, sharing and using knowledge to add value and benefit to an organisation, particularly in decision-making (Gasik 2011, Zaied et al. 2012). KM is viewed as an increasingly important discipline that simplifies the process of sharing, creating and transferring knowledge (Von Krogh et al. 2012).

Nonaka and Toyama (2015) state knowledge creation is a transcending process through which entities (individuals, groups, organizations, etc.) transcend the boundary of the old into a new self by acquiring new knowledge. Knowledge creation integrates context, knowledge assets, and knowledge creation processes throughout the organization. Alipour et al. (2011) state that knowledge transfer and knowledge sharing are sometimes used synonymously or are considered to have overlapping content and define knowledge transfer is a process by which knowledge, ideas, and experience move from the source of knowledge to the recipient of that knowledge. Evans and Ali (2013) demonstrated the key knowledge management activities, of which the most significant was that of knowledge sharing.

Knowledge sharing

The success of knowledge management activities and the value of knowledge depends on the sharing of relevant knowledge across all its potential stakeholders, be it within an organisation, sector or society in general. The sharing of knowledge is fundamental in gaining competitive advantage, promoting innovation and increasing production (Wang et al. 2010). A more specific view of knowledge sharing is that it describes a complex process involving the contribution of knowledge by an organisation or its personnel, and the collection, assimilation, and application of knowledge by the organisation or its people (Kimble et al. 2010). In the context of this study, knowledge sharing is individuals, organisations and systems sharing relevant knowledge with other individuals, organisations and systems to design, develop and integrate components for connected vehicles. The knowledge that is shared is in the form of cybersecurity knowledge.

Defining the concept of automotive cybersecurity knowledge

Automotive cybersecurity knowledge comprises component-specific knowledge on the one hand, and architectural knowledge on the other (Chapter 2, section 2.5). Component-specific knowledge, from a cybersecurity perspective, comprises security test results, technical safety test results, functional safety test results, performance specification test results, manufacturing processes, and design processes.

Architectural knowledge is knowledge about the vehicle's architecture (Chapter 2, section 2.6.2). This knowledge comprises design decisions, integration specifications and, interface specifications. Automotive cybersecurity knowledge is developed over time through experience and expertise, it can be complex in nature; nonetheless, it can be captured and codified in documents so that it can be stored, retrieved, reused and shared when required, therefore, cybersecurity knowledge is both, tacit and explicit.

The growing importance of the sharing of cybersecurity knowledge in the automotive ecosystem

The rate and extent to which automotive cybersecurity is changing is extremely variable and unpredictable; the sharing of cybersecurity-related knowledge is important in component manufacturing, and for creating secure component integration processes. In today's market, an OEM's ability to act as an integrator of systems, sub-systems, and modules, is a new core competence. Automotive component development is an information and knowledge-intensive activity, and a firm's superior product development capabilities are derived from its ability to create, distribute and utilise knowledge throughout the component development process (Pastor et al. 2010, Santos et al. 2012).

Chapter 2, highlights that, whilst there is a substantial body of literature on knowledge sharing in product development in various domains such as aviation (Siqing et al. 2013, Li et al. 2014), military, (Neches et al. 2013), and maritime transport (Nir et al. 2012, Argote 2012), much less attention has been focused on the sharing of knowledge in automotive component integration processes as a potential solution for improving the cybersecurity of modern connected vehicles. Few researchers have explicitly stressed the importance of knowledge sharing, however, their research remained predominantly conceptual or descriptive. From a cybersecurity perspective, the concept of knowledge sharing is vital in the automotive domain to ensure secure component integration practices.

The importance of cybersecurity knowledge in automotive component manufacture and its inclusion in component integration strategies

The business of making vehicles is now more based on the ability to integrate different components and different technologies provided by a plethora of geographically dispersed component suppliers. Studies in automotive component manufacture highlight the importance of detailed component-specific knowledge in ensuring secure component integration. Erdem et al. (2015) stress the importance of including the internal activities and processes of component manufacturers as they develop and integrate the inputs required to produce the final component. A component's functional and performance parameters are important in understanding whether it will comply with the expected overall functional performance parameters of the vehicle, while architectural knowledge is important in providing a holistic view of how the components will be integrated into modules, systems or sub-systems. This knowledge is important in identifying potential cyber-weaknesses in component manufacturing processes, integration processes and for designing and specifying the necessary functional and security tests and specifications.

1.3 Research problem

Automotive component design and development is rapidly evolving from a focus on aesthetics and functional requirements to the design and development of complete digital systems. Component out-sourcing has emerged as a primary vehicle for vehicle innovation and development. While component out-sourcing is not new, the various types of components being outsourced are. The modern connected vehicle, which has now become more than simply a mode of transportation, is built with digital components that are manufactured by a plethora of globally dispersed component suppliers.

Out-sourcing of complex digital components and technological advancements in vehicle manufacturing is new and exciting, however, the frequency and depth to which the automotive industry is embracing this dynamic practice compounds' cybersecurity challenges. OEMs are tasked with integrating outsourced digital components into systems or digital modules which are then integrated into the vehicle. Cybersecurity vulnerabilities are introduced into the automotive industry via insecure strategies when components are integrated into systems, subsystems or digital modules (Kosher et al. 2010, Checkoway et al. 2011 and Amin et al. 2015). Additionally, cybersecurity vulnerabilities exist at the interface between these systems or digital modules and the vehicle.

The extant literature highlights research conducted by academia and automotive R&D (research and development) departments on automotive cybersecurity aimed towards identifying different attack vectors capable of compromising connected vehicles and exposing the lack of security mechanisms in connected vehicles and their networks. The bulk of automotive cybersecurity research is focused on providing technical architectures of security solutions to support the management of vulnerabilities, threats, and incidents (Amin et al. 2015). Security vulnerabilities in connected vehicles have been identified and documented; however, research in the sharing of knowledge of relevance for component integration processes in the auto-domain is still in its infancy, and there is little exploration and investigation of sharing of knowledge related to component integration processes as a factor influencing cybersecurity in connected vehicles.

1.3.1 Research questions

The primary research question

How can the sharing of knowledge in component integration processes within the automotive industry be exploited to improve the cybersecurity of modern connected vehicles?

The main research question that drives this study was driven by knowledge sharing theory, recent events such as cybersecurity breaches, and technological developments that have occurred in today's automotive industry. Connected systems and the "Internet-of-Things" (IoT), that is the web of physical objects including vehicles, embedded with electronics, software, and sensors, although no longer new, influence component design requirements and integration processes, and expose connected vehicles to cybersecurity vulnerabilities (Patel & Patel 2016). Understanding how OEMs and component suppliers share component integration knowledge which could potentially improve the cybersecurity of connected vehicles requires research and an understanding of a number of areas which include the following:

- Existing knowledge sharing practices in the automotive industry, specifically in component integration.
- Component and system integration strategies
- Barriers to knowledge sharing and measurement of success
- Cybersecurity knowledge sharing platforms
- Changes and adaptations in the automotive supply chain
- Factors that contribute to effective knowledge sharing relationships and structures

This led to the development of more specific research questions that were derived from the main research question. These additional questions also needed to be answered during the research.

Additional research questions

Cybersecurity is a new phenomenon in the automotive industry, understanding how the trend towards connectivity in vehicle manufacture has changed the automotive supply chain will assist in understanding how cyber-related information is shared between all relevant stakeholders, this motived the outlining of the following research question:

RQ-1: *How has the structure of the automotive supply chain been affected by the design, development, and manufacture of increasingly connected vehicles?*

Knowledge sharing should be analysed in the context of the automotive industry, especially in component integration processes. Engagement with the relevant literature on knowledge sharing theory in the automotive industry highlights the existence of knowledge sharing strategies (Chapter 2). The researcher acknowledges that the concept and practice of sharing knowledge in component integration processes as a potential factor for improving the cybersecurity of modern connected vehicles is new and still very much under-researched, the need to engage with the industry to investigate if such knowledge sharing approaches exist motivated the following research question:

RQ-2: What types of knowledge does the automotive sector rely on and how is it shared amongst the different stakeholders involved in component design, development, and integration?

The following research question was motivated by the need to gain an understanding of how OEMs and component suppliers implement security measures to protect connected vehicles against cybersecurity vulnerabilities. This requires an understanding of the forms of cybersecurity knowledge that are adopted and applied to the manufacture of components for the connected vehicle.

RQ-3: How is cybersecurity knowledge adopted and applied in component design and development processes?

The following research question was motivated by the need to gain an understanding of the challenges and limitations of current standards, guidelines and best practices designed to inform knowledge sharing processes in the development of components for connected vehicles.

***RQ4:** What standards, best practices, and guidelines exist in the automotive industry to inform knowledge sharing in connected vehicle manufacture?*

A systematic and systemic framework is required for analysing the aspects of knowledge sharing in component integration within the automotive sector. To successfully design and develop a conceptual framework that will assist the industry to potentially address cybersecurity challenges due to insecure integration processes, an investigation of what is required to design such a framework outlined the following research question:

RQ-5: How can component related knowledge be shared effectively between OEMs, the automotive supply chain, and amongst suppliers, for improved digital security of connected vehicles?

By addressing these additional research questions, the researcher aims to contribute towards the understanding of the main research question and the research as a whole.

1.3.2 Research aim and objectives

The central focus of this research is to analyse the sharing of knowledge of relevance for component integration processes within the automotive industry as a potential factor for improving the cybersecurity of modern connected vehicles. The previous section provided the research problem, based on this, the research aims to develop a framework to support the sharing of knowledge related to component integration processes in connected vehicle development in the automotive industry.

In order to achieve the stated aim, the following objectives have been formulated:

Research Objective 1:

Explore and investigate the current state of the automotive sector to understand the effects caused by the trend towards connectivity.

In particular, to identify components and elements that have introduced changes to the automotive sector. Also, to understand how processes for sharing knowledge previously employed in vehicle development have been affected by changes to the industry. This objective will attempt to address research question 1.

Research Objective 2:
Review the main context in which knowledge sharing has arisen and the limitations they have encountered.

A review of this nature will focus on the context of this research, especially the key stages and the attempts to use models and frameworks to support knowledge sharing in the specified context of knowledge sharing. This objective will attempt to answer research question 2.

Research Objective 3:
Explore and investigate how cyber-related information is shared between vehicle manufacturers and the automotive supply chain for component integration.

In particular, investigate how component integrators acquire cyber-related information, and how that knowledge is adopted and applied to component integration processes.

Research Objective 4:

Critically review the literature on current automotive security standards, best practices and guidelines to explore how they inform approaches for sharing cybersecurity-related knowledge.

Research Objective 5:

Review the key areas that emerged from the empirical research that could potentially be beneficial to the development of the proposed framework.

Research Objective 6:

Develop a conceptual framework to support the sharing of relevant knowledge related to component integration processes in connected vehicle development in the automotive industry, which addresses cybersecurity challenges born out of insecure integration processes.

Research Objective 7:

Expose the conceptual framework to critique before critically evaluating the final framework to demonstrate an original and significant contribution.

1.4 Research contribution

Although still relatively new, research into automotive cybersecurity has been conducted from various perspectives by researchers in academia and experts within the automotive domain. Cybersecurity vulnerabilities due to the inclusion and presence of Bluetooth modules, on-board diagnostics systems, mobile communications and, electronic control units (ECUs) were highlighted by Lu et al. (2014), Parkinson et al. (2017) and, Cheah et al. (2017). Weaknesses surrounding the standard communication technology Controller Area Network (CAN), and affiliated automotive network communication protocols such the deterministic, fault-tolerant high-speed bus system; FlexRay, the serial communication system for transmitting audio, video and control data via fibre-optic cable; Media Oriented Systems Transport (MOST), and the low-cost embedded networking standard for connecting intelligent devices in automotive networks; Local Interconnection Network (LIN) have been documented by authors such as Yadron (2014) and, Zhang et al. (2014). Practitioners such as Koscher et al. (2010), Checkoway et al. (2011) and, Miller et al. (2014) have highlighted how vulnerable modern connected vehicles are to cybersecurity challenges, be they remote or local (originating from within the vehicle). To date, proposed solutions have focused on providing technical architectures of security solutions. Thus, this research makes contributions to both theoretical and practical bodies of knowledge. The practical contributions (i.e. findings from the research questions) are specific to the automotive industry, while the theoretical contributions are applicable to other organisations that wish to address cybersecurity challenges that are born out of insecure component integration processes.

The study attempts to fill a knowledge gap in the literature, by extending knowledge sharing theory into the contexts of component integration to address automotive cybersecurity challenges, while addressing inhibiting factors that do not favour the sharing of cyber-related knowledge. This contribution is important in that the study of knowledge sharing of cyber-related information in component integration processes as a potential factor to improve the cybersecurity of connected vehicles in the automotive industry is still under-researched and is yet to be fully explored. Especially when empirical studies of cybersecurity in automotive manufacturing have largely concentrated on identifying the consequences of a lack of appropriate security mechanisms. The study highlights the limitations of knowledge sharing practices prior to the introduction of connectivity modules and software in vehicle manufacture, in addition to partly filling the research gap, the study provides a practical approach to how the industry could address those limitations through knowledge sharing approaches.

The research contributes to the automotive industry through the development of a knowledge sharing framework designed to potentially assist the industry to manufacture cyber-secure vehicles through secure component integration processes. The conceptual framework, which was presented to personnel employed in the automotive industry and knowledge experts for refinement and evaluation, is designed to improve, extend and incorporate knowledge sharing in component integration approaches. If adopted by industry, the framework has the potential to affect policy and standards within the automotive domain. Policymakers and training providers and those associated with enforcing knowledge sharing approaches for the automotive industry may wish to incorporate some of the study's findings in their provisions. This contribution is important in that current frameworks fail to take into consideration the possibility of knowledge sharing as a potential factor for improving the cybersecurity of modern connected vehicles.

1.5 Thesis structure

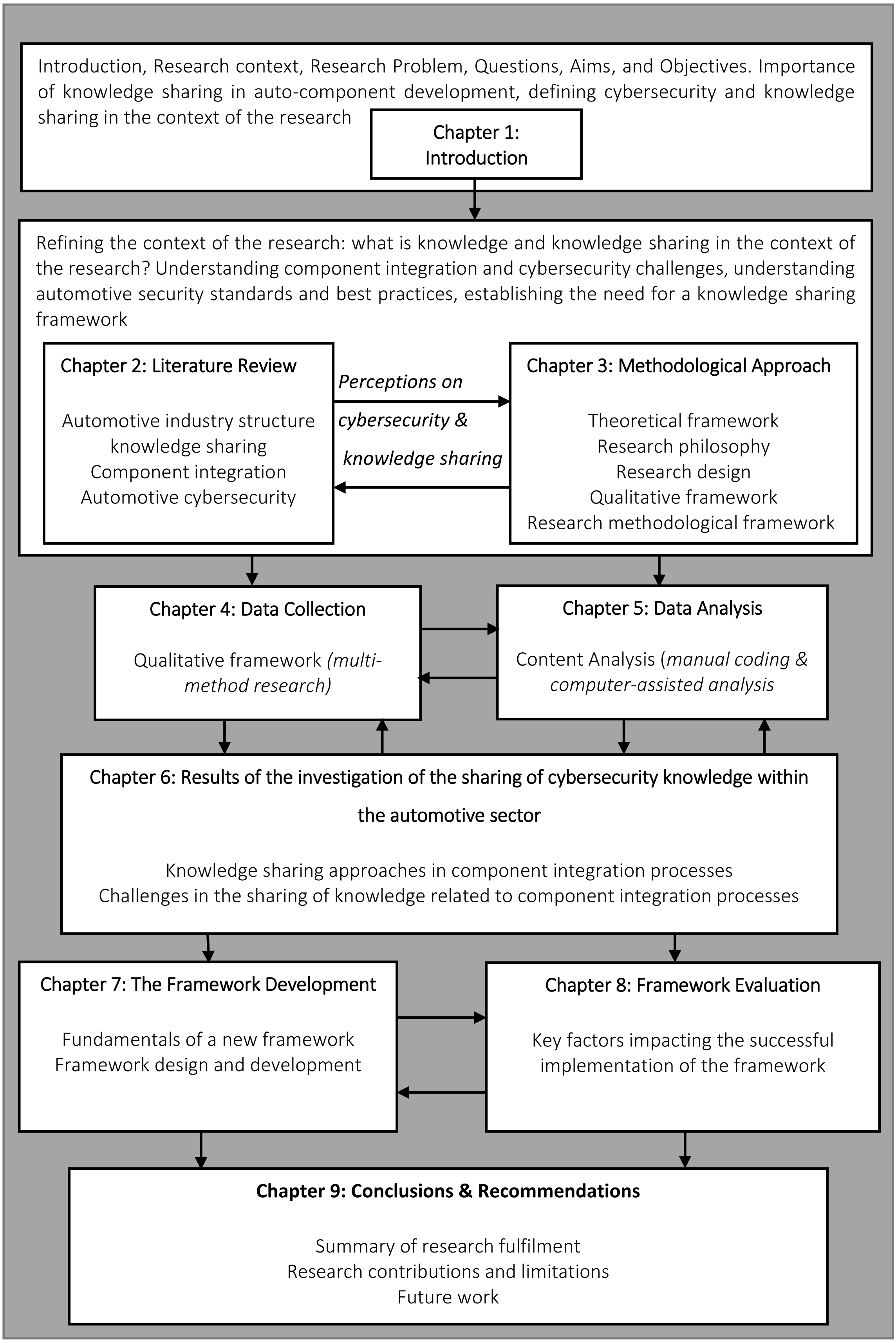

Figure 1. 2: Structure of the research thesis

The thesis consists of nine chapters, as depicted in Figure 1.2 above. Chapter 1 outlines the research problem and introduces the aim and objectives of the thesis as well as a broad introduction to the main issue of cybersecurity challenges in connected vehicles as a result of insecure component integration processes. The concepts of knowledge, knowledge sharing and cybersecurity in component integration are also introduced and discussed in Chapter 1. More specifically, Chapter 2 reviews the theoretical foundations of knowledge sharing and cybersecurity, drawing from knowledge sharing theories. Structural changes that have increased component out-sourcing and their effects on knowledge sharing are presented, before challenges relating to the sharing of cyber-related information within the automotive sector are; as the core research area of the study. Before outlining available research methodologies and philosophies, Chapter 3 discusses the research design and methods utilised to address the research problem. It provides justification for the path that the research took. Data collection methods and techniques employed to identify and select participants are presented in Chapter 4. Chapter 5 focuses on the analysis of the qualitative research data collected during the fieldwork. The chapter provides considerations for data validity and reliability, along with ethical considerations. Chapter 6 presents the results of the study. The quality of the findings of the research are presented and discussed in this chapter. The proposed framework is developed in Chapter 7, bring together the best practices identified in the literature review and the primary evidence from the fieldwork. The chapter also includes justification for the inclusion of all components of the framework. Chapter 8 focuses on the evaluation of the proposed framework. The framework is evaluated for its perceived value, usability and limitations by personnel employed in the auto industry. Chapter 9 presents a discussion based on the findings from the fieldwork and the study's results from the data analysis phase. Additionally, Chapter 9 concludes the thesis discussing the study's key contributions and outlining the study's limitations, as well as discussing avenues for future research.

Chapter II

LITERATURE REVIEW

2.1 Introduction

The focus of this research is to assist the automotive industry to address cybersecurity vulnerabilities in connected vehicles. More specifically, as detailed in Chapter 1, this research aims to design and develop a conceptual framework for the sharing of knowledge of relevance for component integration processes in the automotive industry.

The previous chapter offered an introduction to this research and provided the context in which the research was undertaken. The need for a framework for sharing knowledge was established, however, the discussions thus far would not be sufficient to provide a robust framework; therefore, this chapter provides a review of the key areas of related knowledge sharing in the automotive sector. Additionally, this chapter explores existing theories that underline issues and challenges in the sharing of cybersecurity-related knowledge in the automotive industry. Cybersecurity (CS), Knowledge management (KM), knowledge sharing (KS), automotive supply chain management (ASCM), Internet-of-things (IoT) and developments in vehicle manufacturing lay the theoretical foundations of this study. Critiques are drawn from some of these research areas to contextualise findings within the research problem. This review is important in that it shows that there is no single existing framework that addresses the sharing of knowledge in component integration processes that expose connected vehicles to cybersecurity threats in the automotive industry.

Accordingly, the chapter is structured as follows:

- Section 2.2 discusses knowledge management in organisations. The discussion starts with an introduction to knowledge from knowledge management literature. It gives an overview of the nature and management of knowledge.
- Section 2.3 addresses knowledge sharing, this discussion starts with an introduction to knowledge sharing before moving onto the importance of knowledge creation and sharing. Specific consideration is given to the relevance of knowledge sharing in the automotive industry.
- Section 2.4 gives an overview of the changes to the automotive industry and how those changes have affected knowledge sharing processes within the domain.
- Section 2.5 discusses cybersecurity management, defining the term “cybersecurity” and its relevant concepts.

- Section 2.6 addresses cybersecurity challenges that are born out of knowledge sharing challenges in component integration processes as the core research area of the study.
- Section 2.7 gives an overview of knowledge sharing frameworks in component integration.
- Section 2.8 concludes by summarising the key findings of the study.

2.1.1 Theoretical foundations for studying knowledge management

The purpose of this section is to provide a theoretical framework of knowledge and knowledge management and to assess the existing knowledge sharing approaches on the research topic, and to confirm the tentative belief of the need for research in this area. There are a few important issues that appear to be significant in the existing theory of knowledge management. These are associated with organisational knowledge and how knowledge is managed within organisations, these are discussed in subsection 2.2.2. Following this, the discussion moves onto the importance of knowledge sharing as a strategy for an organisation to succeed in today's business environment (subsection 2.3.1). Knowledge sharing in the context of the automotive industry is discussed in subsection 2.3.2. Research into component integration challenges that have resulted in cybersecurity challenges in the automotive domain are discussed in subsection 2.6.2. A review of frameworks that have addressed knowledge sharing in the automotive industry is presented in section 2.7.

2.1.2 Literature review methodology

The review of prior relevant literature was guided by the central research question, the need to establish a solid theoretical foundation to underpin and guide the research and to provide a firm foundation for the development of the study's research methodology. The initial selection of literature included studies focused on analysing knowledge management, knowledge sharing and frameworks for sharing knowledge in the automotive industry with a particular, but not exclusive emphasis on cybersecurity threats; this not only assisted in clarifying the context and identifying promising approaches, but also gaps in the existing literature. The identification of relevant literature that was used to define this piece of research was based on a keyword search which began with terms such as "knowledge", "knowledge management", "knowledge sharing", "component integration", "knowledge sharing frameworks". Once these terms identified appropriate literature, more specific terms were then used to narrow the searches. Appendix 1 shows the combinations of words, phrases and concepts used to identify relevant literature. Whilst the listing of search combinations may appear over-detailed and repetitive, it is useful to note that the list is a product of both ex-ante search terms and additional terms which emerged as the search progressed. The table in Appendix 1 is a summary, ex-post, listing of terms actually used in this study.

Academic literature

Locate; an on-line catalogue and bibliographic resource discovery system provided by Coventry University was used to gather a comprehensive collection of relevant sources. Locate provides access to published journal papers, conference proceedings, secondary references, theses and textbooks through well-known academic databases such as EBSCO, ScienceDirect, Springer, Web of Science etc. However, Locate only permits title, author and keyword search options. This allows a portfolio of databases to be searched and is useful in developing an overall picture of the available literature. Full-text searching was available at the individual database level and was undertaken guided by knowledge of the summary results from Locate. Given the recency of the phenomenon, only articles less than ten (10) years old were included, thus the review search started from 2010.

Industry and government reports

Given the novelty and complexity of the phenomena under investigation, industry and government reports provide valuable information not available elsewhere. Similar keywords to those used to search Locate; were used to search for relevant industry and government reports using Google Scholar and Google. Industry and government reports may often be associated with low theoretical background, but significant bias; however, they are produced by people close to the phenomena under investigation, and the inclusion of these non-academic sources allows for judgement to be made based on a wider range of opinions and evidence. Furthermore, the need to review industry and government reports was reinforced by the fact that most research in automotive cybersecurity centres on providing technical architectures of security solutions, but not much attention has been given to researching automotive cybersecurity as a knowledge sharing problem. Industry and government reports are often focused on knowledge sharing, although it is important to recognise that their development may be motivated for other than academic reasons, for example, policy development, political support or commercial gain. Two clear and important initial results from the bibliographical databases search were, firstly, that the bulk of extant literature focuses on the technical aspects of cybersecurity impacts and relatively little on the business, social, legal, strategic and management aspects and, secondly, that the concept and practices of knowledge sharing of cyber-related information are still very much in their infancy and not prominent in the existing discourse.

2.2 Defining knowledge

Defining knowledge is difficult because it is a fluid mix of information and intuition based on the person's own perceptions and experiences. There is no consensus on a definition of knowledge (Dalkir 2013). Yet, knowledge is one of the unique, valuable and critical resource that is central to developing and maintaining a competitive edge, it allows industries to provide better quality products at cheaper rates in a shorter amount of time (Goffin & Koners 2011, Wood 2017:891-903). Nonetheless, knowledge is defined in Webster's dictionary as; the fact or condition of knowing something with familiarity gained through experience or association. In practice, though, there are many possible, equally plausible definitions of knowledge. A frequently used definition of knowledge is "the ideas or understandings which an entity possesses that are used to take effective action to achieve the entity's goal(s)." This knowledge is specific to the entity which created it (Polanyi 2012). Knowledge comprises of different perceptions and classifications. It is therefore essential to make a proper distinction between the terms data, information, knowledge and wisdom. This section will define and illustrate these concepts and differentiate between them, as well as consider the hierarchical relationship between them.

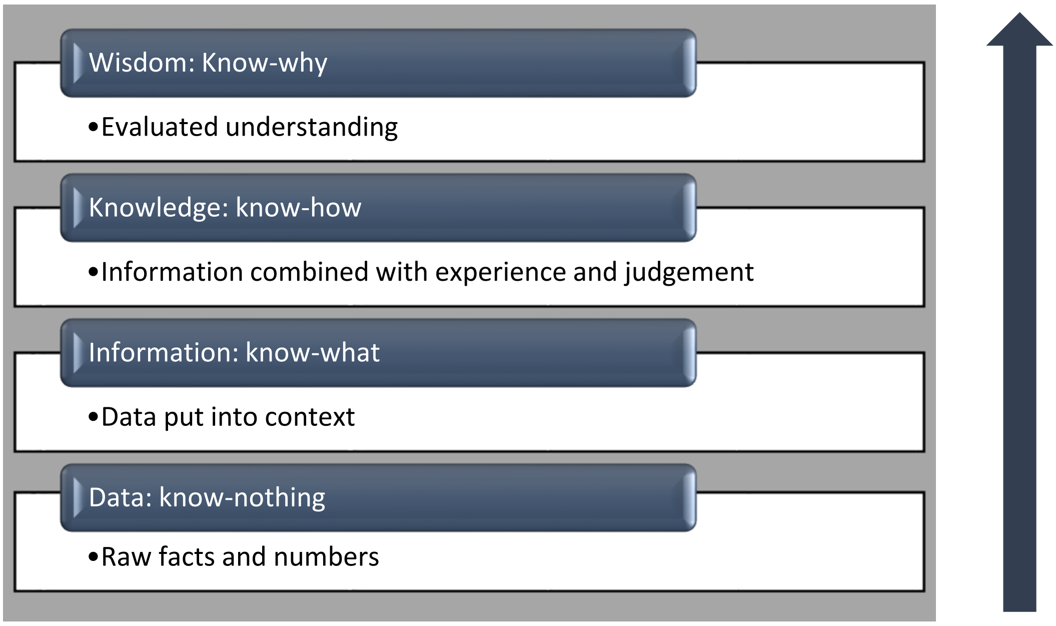

Figure 2. 1: Knowledge hierarchy
Source: Munir (2014)

The knowledge hierarchy is widely used to conceptualise knowledge. The hierarchy denotes the common notion of knowledge development in which data is converted into information, and information is converted into knowledge, which eventually develops into wisdom (Lambe 2014). As depicted in Figure 2.1, each phase is dependent upon the phase below.

The first phase of the knowledge hierarchy is data, from which an upward transition is made for data to be transformed into information. Data defines a set of discrete, objective facts about events that have not been organised and processed. Within the context of the automotive industry, data in their basic form carry no meaning and have little value for managers unless one understands the context in which the data were collected. The automotive industry captures vast amounts of data via the vehicle and vehicle manufacturing processes, the transport infrastructure, physically connected devices, component manufacturing processes etc. this data is valuable only if it is processed, analysed, synthesised and transformed into information and knowledge (Wang et al. 2012, Abdelhamid et al. 2015). The second phase of the hierarchy is information. When data is processed and structured it becomes information. Unlike data, information holds meaning and purpose to the individual. Information can thus be explained as data that has a function and significance that has been placed in context (Janich 2018). The core value of building activity around information is managing the content in a way that makes it easily accessible and reusable. Therefore, the context of cybersecurity in the automotive industry, information is useful for the purpose of problem-solving, threat analysis, and risk assessment (Natella et al. 2013).

Knowledge builds on information, and it is the third phase of the hierarchy. Information has little value and will not become knowledge until it is processed. Knowledge is essential information in the context which it is interpreted and acted upon by those who must perform a given function. Therefore, knowledge is the confident understanding of a subject with the ability to use it for a specific purpose. Knowledge is of greater significance, as it is derived from experts and is based on expert experience. It, therefore, demands a higher comprehension compared to information (Stehr & Grundmann 2011). Knowledge is context-specific and Hartwig and Granhag (2015) suggest that if knowledge is not put into context and combined with an understanding of how to utilise it, it is merely information. The fourth phase of the hierarchy constitutes wisdom, and according to Lambe (2014), is assumed to create a better understanding and ethical basis for action. In essence, it embodies more of an understanding of the fundamental principles embodied within the knowledge that are essentially the basis for the knowledge being what it is. It is sometimes added to the top of the data-information-knowledge hierarchy, but its appearance is less widespread in the literature. From the discussion above, it can be inferred that knowledge is fundamentally different from data, information and wisdom. However, data, information and wisdom in combination are essential to organisations. In this study, the definition that will be adopted is the one proposed by Polanyi (2012):

"*Knowledge is the integration of ideas, experiences, intuition, assertions, skills and lessons learned that have the potential to create value for an organisation, a business or company by informing decisions and improving performance*."

This definition has been adopted based on the fact that it more or less embraces the definition of knowledge given by various scholars (Polanyi 2012, Dalkir 2013, Harman 2015, Hislop et al. 2018, and Lehrer 2018).

2.2.1 Tacit and explicit knowledge

Knowledge is divided into two groups; explicit and tacit (see Table 2.1 below). Explicit knowledge is formal, systematic, expressed externally, and thus easy to capture, store, communicate and distribute (Durisova 2011). Sometimes referred to as know-what, explicit knowledge can be codified, digitised and, stored as information. It exists in organisations as reports, articles, manuals, patents, pictures, images, video, and software (Durisova 2011). From a managerial perspective, the greatest challenge with explicit knowledge is similar to information. It involves ensuring that people have access to what they need; that important knowledge is stored; and that the knowledge is reviewed, updated, or discarded.

Tacit knowledge which sometimes is referred to as know-how is often context-dependent and personal in origin, job-specific, related to context, difficult to fully articulate, and poorly documented but highly operational in the minds of the possessor. It combines individual experience and intuition, and it cannot be expressed externally. It is found in the minds of human stakeholders and includes cultural beliefs, values, attitudes, mental models etc. as well as skills, capabilities and expertise (Holste & Fields 2010). Goffin and Koners (2011) state that tacit knowledge is the most valuable source of knowledge, and the most likely to lead to breakthroughs within an organisation. However, Dalkir (2013) notes that tacit knowledge is quite a relative concept; what is easily articulated by one person may be very difficult to externalise by another. Thus, the same content may be explicit for one person and tacit for another.

Table 2. 1: Explicit vs tacit knowledge

	Explicit Knowledge (Documented)	Tacit Knowledge (know-how embedded in people)
Features	Easily codified Storable Transferable Easily expressed and shared	Personal Context-specific Difficult to formalize Difficult to capture, communicate, share
Sources	Manuals Policies and procedures Database and reports	Informal business processes and communications Personal experiences Historical understanding

2.2.2 Knowledge management in organisations

As with knowledge, there is no agreement on what constitutes knowledge management (Ragab & Arisha 2013, Rechberg & Syed 2014). There are many different definitions of knowledge management and there is a conceptual confusion of what knowledge management is. For example, according to Durst and Edvardsson (2012), knowledge management is a multidisciplinary discipline that employs a deliberate and systematic approach to the capture, structure, management, and dissemination of knowledge between individuals and groups within an organisation, consisting of four essential steps: acquisition, storage, distribution and knowledge utilisation. Hislop et al (2018) state that knowledge management is a mechanism that allows for the retention of tacit and explicit knowledge, so it may be distributed to individuals within the organisation for incremental improvement activities, thus providing a competitive advantage. Gonzalez and Martin (2014) state that knowledge management's main task is to create an organisational context that encourages the development of new knowledge through explorative and exploitative learning processes. Koenig (2012) provides a definition that has the virtue of being simple, stark and to the point, Koenig states that "knowledge management is the process of capturing, distributing, and effectively using knowledge." After conducting a formal survey, Dalkir (2013) identified over 100 published definitions of knowledge management and defines knowledge management as "the deliberate and systematic coordination of an organisation's people, technology, processes, and organisational structure in order to add value through re-use and innovation. This coordination is achieved through creating, sharing and applying knowledge as well as through feeding the valuable lessons learned and best practices into corporate memory to foster continued organisational learning." From the definitions highlighted above, the general consensus across most definitions is that knowledge management involves people, technology and processes of creating, capturing, sharing and using knowledge to add value and benefit to an organisation, particularly in decision making (Gasik 2011, Zaied et al. 2012). As illustrated above, various definitions and approaches to knowledge management exist, and it should be noted that each definition of knowledge management is dependent on the discipline of the organisation that engages with the concept (Cao & Xiang 2012, Ragab & Arisha 2013). Furthermore, each discipline approaches knowledge management with a different perception, for example, computer science focuses heavily on technology, human resources takes an individual and organisational approach emphasising learning and reward factors, and others focus on the explicit capture and registration of knowledge (Rechberg & Syed 2014).

2.2.3 Knowledge Management: taxonomy, processes and components

Knowledge management involves iterative processes that enable the application and development of knowledge in an organisation. Some of these processes are intertwined and can occur simultaneously. The premise of these processes is that knowledge management implies the continuous and ongoing renewal of organisational schemas to anticipate future opportunities and threats (Ma et al. 2014). These processes "link people and knowledge content" (Rodriguez & Edwards 2010) and are summarized in Figure 2.2 below.

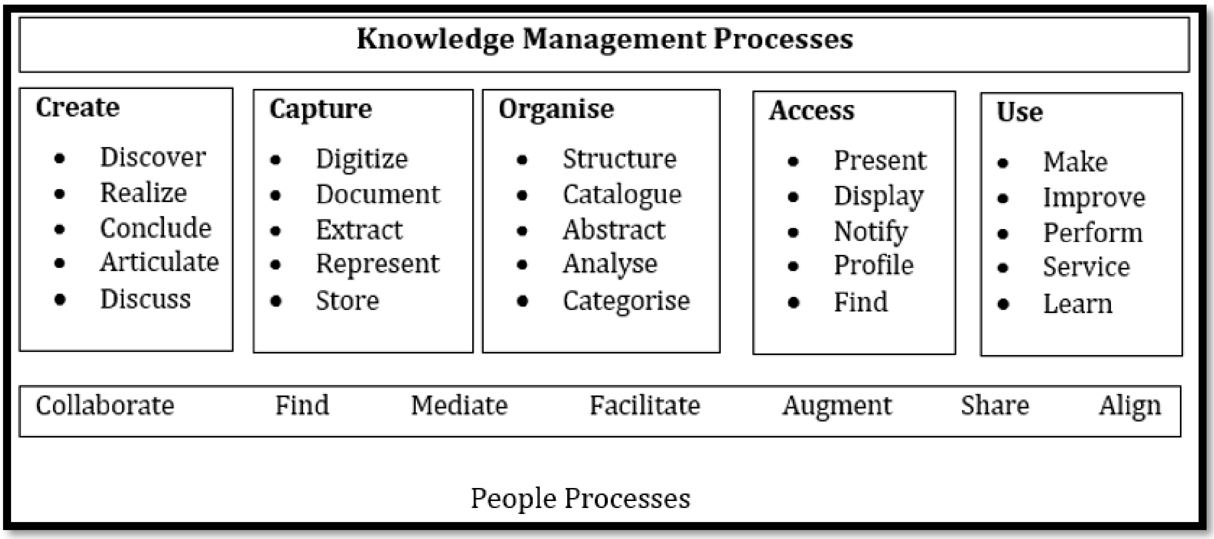

Figure 2. 2: Knowledge management processes
Source: Koulikov (2011)

Numerous knowledge management processes have been introduced from various authors, for example, knowledge capture, knowledge re-use, storage and retrieval of knowledge (i.e. knowledge repositories), sharing and distribution between individuals, creation of new knowledge, innovation

(Durst & Edvardsson 2012, Ma et al. 2014, Rechberg & Syed 2014), and knowledge application (Rechberg and Syed, 2014, Hislop et al. 2018). At the core of these processes is the creation of knowledge, all organisations, the automotive industry, in particular, create knowledge (Jurgens & Krzywdzinski 2013, Gonzalez et al. 2014). Creation of knowledge can occur through a variety of means, such as through technological discovery or discussions. However, knowledge can be easily lost if it is not captured and used. From a technological perspective, knowledge capture can be achieved via numerous methods such as digitisation, documentation, extraction, representation, storage etc. Technology has made it relatively easy to organize, post and transfer certain types of information.

One of the key activities in the processes of knowledge management is knowledge sharing. The tacit knowledge possessed by individuals is crucial and instrumental to an organisation's operations and continued existence (Evan & Ali 2013, Hislop et al. 2015). Knowledge sharing is perceived as an indicator of an organisation's accumulation of social capital because knowledge possessed by one member of an organisation can be shared easily and efficiently if there is sufficient social capital (Jo & Joo 2011, Witherspoon et al. 2013). However, reaching the point where employees willingly share tacit knowledge remains a challenge for organisations. The willingness to share knowledge among organisational members depends on the resources embedded in the organisation's social relations and structures (Jo & Joo 2011, Amayah 2013).

To share knowledge is not nearly the end of a knowledge management process. What often fails in knowledge management is the inability to shepherd the entire process. Lilleoere and Hansen (2011), Akhavan et al. (2013), Bashouri and Duncan (2014), found three barriers to successful knowledge sharing: the individual's ability to absorb and share knowledge, organisational learning mechanisms, and the ability to store and retrieve knowledge. Absorptive capability refers to the individual's ability to utilize available knowledge. Authors Connelly et al. (2012), Vuori and Okkonen (2012), Jo and Joo (2011), Kuo (2013), Paulin and Suneson (2015), and Weinberg (2015) identified five major barriers affecting knowledge sharing: individual motivation to share, opportunities to share, the nature of the knowledge, the culture of the work environment, and the large physical and social distances between individuals. Many organisations have tuned in to these five barriers. Based on these discussions on knowledge management, the next section discusses knowledge sharing.

2.3 Knowledge sharing

The term knowledge sharing implies the giving and receiving of information framed within a context by the knowledge of the source, it deals with how knowledge may be shared between individuals, teams and/or organisations (Suppiah et al. 2011). As a concept, "knowledge sharing" is now well established in knowledge management and information science literature, and numerous knowledge sharing definitions have been introduced by many authors, for example, Tangaraja et al. (2016) define knowledge sharing as the voluntary process of transferring or disseminating knowledge from one person to another person or group within an organisation. According to Wang and Noe (2010) and Gera (2012), knowledge sharing is a process through which an organisation or any of its departments is influenced or affected by another organisation or its departments. Peng et al. (2013) define knowledge sharing at an individual level as "a voluntary act which leads to new experiences or understanding for the knowledge sharing recipient". Sandhu et al. (2011) further explain that knowledge sharing occurs between at least two parties and is a reciprocal process that allows the reshaping and sense-making of the new knowledge in the new context. Nesheim and Gressgard (2014) distinguish knowledge sharing from information sharing by arguing that knowledge sharing contains an expectation of reciprocity, whereas information sharing is seen as unidirectional and unrequested. As illustrated above, various definitions to knowledge sharing exist, for the purpose of this study, knowledge sharing is defined according to Koulikov (2011), who comes closer to encompassing what knowledge sharing actually is, rather than what the process entails. He states that knowledge sharing consists of "voluntary interactions between human actors through a framework of shared institutions, including ethical norms, behavioural regularities, customs and so on, the subject matter of the interactions between the participating actors is knowledge. Such an interaction itself may be called knowledge". Based on this conceptualisation of knowledge sharing, the next section discusses the importance and the benefits of knowledge creation and sharing.

2.3.1 Importance of knowledge creation and sharing across organisations and sectors

The benefits of knowledge creation and sharing have been studied from different perspectives ranging from people management practices that encourage and sustain voluntary knowledge sharing, the paradox that arise when organisations simultaneously share and protect their knowledge in an alliance with other organisations (Bogers 2011), and knowledge sharing in teams to promote and enhance performance (Lee et al. 2010). Suppiah and Sandhu (2011) conducted studies on the influence of organisational culture on knowledge sharing initiatives and knowledge sharing behaviour. Authors Lam and Ford (2010) explored facilitating knowledge sharing within organisations and how organisations resolved the social dilemma of knowledge sharing. Carmeli et al. (2013) highlighted how knowledge sources are fundamentally building blocks in facilitating creativity and innovation in organisations. Wang and Noe (2010) demonstrated how the sharing of knowledge enables organisations to develop new platforms for the development and introduction of new products and services to the market. Tohindinia and Mosakhani (2010) stated: "knowledge creation and sharing can promote organisational innovation, enabling people to capitalize on existing knowledge bases residing within and outside the organisation, thus enhancing their capacity to come up with creative solutions". North and Kumta (2018) argue that "organisational knowledge needs to be managed as corporate assets and that knowledge creation and sharing should be harnessed as key organisational capabilities". Xue and Zhang (2010), Arduin et al. (2013) discuss the benefits of sharing knowledge in collaborative decision-making processes. This is supported by Shih et al. (2012) who also highlight the benefits of sharing knowledge to promote decision-making from a manufacturing perspective, they provide a case study of knowledge sharing at a U.S. Fortune 40 firm. The benefits of sharing knowledge in manufacturing are supported by Wang and Hu (2017), who identify knowledge sharing as the mechanism that introduces the development of new products and services quickly and efficiently to market in supply chain networks.

Knowledge creation and sharing in today's world stretches cultural and national boundaries, between geographically dispersed individuals and organisations. Knowledge sharing has emerged as a tool to enhance organisational performance, achieve and maintain a sustainable competitive advantage, while simultaneously creating innovation for tomorrow (Wang & Noe 2010, Urbancova 2013). Knowledge-creation and sharing influences organisational development and performance, assists and maximises the ability of organisations to meet the needs of the industry, and create solutions to problems for their business advantage (Tohndinia & Mosakhani 2010, Urbancova 2013, Shih et al. 2015). The discussion above highlights the importance of knowledge sharing from different perspectives, however, one thing they have in common is that knowledge sharing is important because it offers a link between the individual and the organisation by moving information that exists in the individual to the organisational level, where it is transformed into economic and competitive value for the organisation (Nonaka & Toyama 2015).

However, previous research also suggests that knowledge sharing can reduce the loss of intellectual capital due to people leaving the company, reduce costs by decreasing and achieving economies of scale in obtaining information from external providers, reduce the redundancy of knowledge-based activities, increase productivity by making knowledge available more quickly and easily and, increase employee satisfaction by enabling greater personal development and empowerment. The empirical results of this study regarding the significance (benefits and importance) of knowledge sharing approaches in the context of cybersecurity and component integration in the automotive industry are analysed and reported in Chapter 6.

2.3.2 Background of knowledge sharing in the automotive industry

While there is a substantial body of literature on work integration in new product development (NPD) in the automotive industry (Lawson et al. 2015, Tuli & Shankar 2015), much less attention has been focused on component manufacturing or NPD knowledge sharing (Blome et al. 2014). Cousins et al. (2011) also argue that extensive research in NPD has focused more on integrating customer requirements into NPD efforts, while the area of supplier integration has not received much attention (Yeniyurt et al. 2014).

Empirical studies of product development highlight the importance of integration of abilities of both upstream (e.g. design engineers) and downstream knowledge workers (e.g. manufacturing engineers) for competitive advantage and superior product quality. Christopher (2016) and, Fredrich and Pesch (2017) confirmed that shared knowledge is an important resource underlying product development capability. They define "glitches" as costly errors resulting from knowledge not being shared. However, the automotive industry is and has always been a knowledge sharing network (Khan et al. 2015, Loebbecke et al. 2016, Kotabe et al. 2017), as demonstrated by Monden (2011) and Vyas (2011) and Schulze et al. (2015) on the Japanese auto industry and studies of the Chinese auto industry by Jean et al. (2014), Corredoira and McDermott (2014), Khan et al. (2015). Evidence of knowledge sharing practices in the European automotive industry were highlighted by Schulze and Brojerdi (2014), Schulze et al. (2015), and Loebbecke et al. (2016). Exploratory studies of Toyota's knowledge sharing network routines (kyohokai, Jishuken etc.) highlight how the automotive industry has always relied on knowledge sharing. Collins et al. (2015), Chiarini and Vagnoni (2015) Filippini and Forza (2016), and Rinehart et al. (2018) among others, conducted exploratory and empirical studies on Toyota and highlight how Toyota created and used knowledge sharing routines to become one of the world's leading automotive manufacturers.

2.3.3 Factors which influence knowledge sharing

Research has shown that the role that knowledge sharing plays in an organisation is positively related to reductions in production costs, faster completion of new product development projects, team performance and, firm innovation capabilities (Wang & Noe 2010). There is increased recognition of the role that individuals play in knowledge sharing processes employed by an organisation, Tohidinia and Mohammad (2010), and Matzler et al. (2011) state that knowledge sharing between employees and within and across teams, allows organisations to exploit and capitalize on knowledge-based resources. Knowledge sharing is the fundamental means through which employees can contribute to knowledge application, innovation, and ultimately the competitive advantage of the organisation. Additionally, it offers a link between the individual and the organisation by moving information that exists in the individual up to the organisational level where it is transformed into economic and competitive value for the organisation. Empirical evidence also points to the importance of people and people-related factors as important to knowledge processes within the organisation (Henttonen et al. 2016).

2.3.4 Knowledge sharing behaviours

Knowledge has become a vital resource for organisations to achieve a competitive advantage and the primary force behind an organisation's continued success in a competitive and dynamic economy (Tohidinia & Mohammad 2010). Matzler et al. (2011) states that knowledge is now seen as an intangible asset that is unique, path-dependent, causally ambiguous, and hard to imitate or substitute and therefore a potential source of competitive advantage. According to Wang and Noe (2010), by developing positive knowledge sharing behaviours, organisations develop skills and competencies, furthermore, the productivity levels amongst workers increases. They further state that organisations that encourage knowledge sharing increase efficiency and effectiveness, speed up information and knowledge flow and react to customer needs faster (Lotfi et al. 2013, and Arnett & Wittmann 2014).

Organisational commitment

Organisational commitment is defined as the bond employees experience with their organisation. In organisational behaviour literature, organisational commitment is regarded as an important factor influencing participation, attitude, and organisational effectiveness. The added value of organisational commitment is that employees who generally feel connected to their organisation tend to be more determined in their work, showing relatively high productivity and are more proactive in offering their support. Iglesias et al. (2011) provide a useful distinction between different kinds of commitment that encourage knowledge sharing, which are:

Affective commitment – this relates to an individual's identification and involvement with the organisation and is defined as an employee's emotional attachment to the organisation which in most cases leads to the employee seeking to preserve and continue employment within the organisation.

Continuance commitment – relates to how much employees feel the need to stay with their organisation. Possible reason for the need to stay within the organisation vary, but the main reason according to Iglesias et al. (2011) relates to a lack of work alternatives and remuneration.

Normative commitment – relates to a feeling of obligation, employees that are normatively committed feel committed to staying within their employment due to guilt. Reasons for such guilt varies, but often employees feel that in leaving the organisation they would create a void in knowledge and skill, which would apply pressure on the organisation.

Individuals that are affectively committed feel they identify with the organisation's goals, view their jobs as encompassing a wider range of behaviours, thus, they commit themselves to extra tasks and roles. This kind of commitment is strongly related to a willingness to share and receive knowledge. Matzler et al. (2011) agree and further state that highly committed employees are more willing to engage in an extra effort to document their knowledge, as they believe that documentation of knowledge is beneficial to the achievement of organisational goals. Hur et al. (2010) argue that affective commitment is not only a form of social identification, but it is also the highest degree of attachment an employee can develop towards the organisation leading to a belief that their organisation has rights to the information and knowledge one has created or acquired. Various authors have specifically investigated the relationships between commitment and knowledge sharing (Eisenerger & Karagonlar 2010, Iglesias et al. 2011, Matzler et al. 2011, Morin et al. 2011) Affective commitment according to Gutierrez et al. (2012) leads to more documentation of knowledge, and it is positively associated with knowledge sharing.

Social environment

The social environment created within an organisation potentially encourages knowledge sharing. Several theories have been developed to explain why and how individuals share knowledge and information within an organisational setting. Three principal theories which explain the social interaction of people are economic exchange theory, social exchange theory and, social identity theory (Gursoy et al. 2010). While economic exchange theory concerns extrinsic benefits and reciprocation favours, social exchange theory concerns intrinsic rewards (Casimir et al. 2012, Cook 2013 and Blau 2017). Social exchange theory differs from economic exchange theory in that social exchange entails unspecified obligations. Social exchange theory argues that people work together to gain desired resources through social exchange (Burgess & Huston 2013). Social identity theory explains collaborative beliefs and why individuals share expertise, it is of the assumption that by demonstrating consistency with the organisation's goals, individuals revalidate their status in the organisation (Jenkins 2014).

Organisational structure

Doherty et al. (2010) and Maduenyi et al. (2015) argue that organisational structure influences the quality of knowledge being shared. Relationships often affect the kind and amount of information that is shared and exchanged between individuals. Positions in an organisation usually determine who controls, enables, impedes the information flow and who has similar information needs and uses. Maduenyi et al. (2015) argue that individuals are more likely to withhold information from others if they perceive that sharing of that information will eventually lead to loss of power, position or the opportunity to achieve promotion. To establish successful knowledge sharing processes, organisations need to understand the processes of learning, behavioural change, and performance improvement. These processes have been shown to exist in organisations that encourage and promote employees to share information.

Organisational culture

Organisational culture is the sum of shared philosophies, assumptions, values, expectations, attitudes and norms that bind an organisation together. According to Saifi (2015), it creates the context for social interaction that establish how knowledge is used, and it shapes the process by which new knowledge is created and distributed in organisations. In addition, it is affirmed that knowledge management is nested in social settings that greatly impact its process. There have been many studies over the years investigating the impact of organisational culture on firm performance (Nguyen et al. 2011, Suppiah et al. 2011, Omotayo 2015, Saifi 2015). The result is a widely accepted view that organisational culture facilitates more knowledge management practices and develops organisational performance. Organisational culture enables and motivates people to create, share, and utilise knowledge for the benefit and the enduring success of the organisation (Rasula et al. 2012).

In the automotive industry, the current trend towards connectivity means OEMs and their tiered supply chain are now located in dispersed geographic locations that have ethnic and cultural diversity (Madzudzo et al. 2018). Existing literature in knowledge management, rational view theory and supply chain management highlight that organisational culture that supports knowledge management can lead to more effective accomplishments. Instilling a culture of standardising and maintaining information is significant for the achievement of organisational goals.

Trust

Trust plays a more important role in social transactions than in economic transactions (Niu 2010, Casimir et al. (2012), trust can, therefore, facilitate knowledge sharing because voluntarily sharing one's knowledge with others is a social transaction. Various authors have described the need for trust to facilitate voluntary cooperation, especially under the context of complex independent actions (Lee et al. 2010). Casimir et al (2012) argue that individuals are more willing to engage in cooperative behaviours such as knowledge sharing when the relationship, they have with their organisation is characterised by a high level of trust. Additionally, Niu (2010) states that trust is a social phenomenon that makes collaboration among organisations possible, and it is an important prerequisite for developing inter-organisational relationships, which facilitate inter-firm knowledge sharing. Trust is likely to enhance collective learning and once established, trust stabilises exchange relationships, which, in turn, considerably increases the chances to enhance trust over time.

Incentives and rewards

Incentives and rewards for individuals as a result of sharing knowledge influences information and knowledge sharing processes (Lam & Lambermont-Ford 2010, Hau et al. 2013). The probability that individuals in an organisation will route information to other individuals is positively related to the rewards that they expect to result from knowledge sharing. In the economic exchange theory perspective, each person's behaviour is influenced by rational self-interest. When individuals feel that the obtained rewards are more than the cost, they will share their knowledge (Hung et al. 2011). Social exchange theory proposes that all human behaviour involves benefit maximisation and cost minimisation, and can influence knowledge contribution (Cook 2013, Blau 2017). The social capital theory perspective recognizes that social capital can promote knowledge sharing among partners because they possess common values, enabling them to build mutual trust (Hung et al. 2011, Lin 2017). Several prior studies used social capital theory to understand an organisations' knowledge creation and sharing process. Social capital theory argues that cooperation and tacit understanding are formed over a long period of time. This leads to the development of mutual trust and the establishment of long-term interpersonal relationships of reciprocity within and across groups (Hung et al. 2011, Cook 2013, and Blau 2017).

Technology

In recent years technology has increased the potential for intra-organisational knowledge sharing. Several of these technologies enable the sharing of knowledge regardless of time, location, and personal history (Di Gangi et al. 2012). The development and use of technology in collaborative information and communication systems to facilitate sharing of information beyond the traditional face-to-face environment has increased (Wang & Noe 2010, Panahi et al. 2013). Additionally, technology creates opportunities to share knowledge across organisational boundaries (Gibbs et al.

2013). In an exploratory study conducted by Faraj et al. (2011), four predictors of participation in computer-mediated knowledge sharing were presented. The predictors were: personal propensity to share information, experienced comfort and confidence with the use of technology, perceptions about the quality of content found in information systems, and the degree of task interdependence experienced by each user. Nonetheless, challenges in encouraging individuals to use such systems to share knowledge remain.

Motivation

The motivation that promotes knowledge sharing by individuals can be intrinsic or extrinsic. While intrinsic motivation concerns itself with internal rewards and provides an individual with a sense of immediate satisfaction, extrinsic motivation relates to intentional acts that are engaged in as a means to an end (Lam & Lambermont-Ford 2010). Research has shown that these two categories of motivation can lead to very different behaviours and performance (Hung et al. 2011). Intrinsically motivated individuals are more likely to generate and transfer tacit knowledge than those who are extrinsically motivated. Extrinsically motivated individuals are more conducive to the sharing of explicit knowledge (Lam & Lambermont-Ford 2010, Hau et al. 2013).

2.3.5 Knowledge sharing barriers

Authors Pirkkalainen et al. (2013), Angela (2013, Wendling et al. (2013) and Paulin and Suneson (2015) identified the following knowledge sharing barriers as illustrated in Table 2.2 below, that organisations need to address in order to achieve effective and efficient knowledge sharing.

Table 2. 2: Knowledge sharing barriers organisations must consider

Level	Barrier
Individual	• Lack of time (lack of time to identify colleagues in need of specific knowledge, and lack of time to share) • Trepidation (fear that sharing will jeopardise or reduce job security) • Low awareness and comprehension of the value and benefit of knowledge to others • Dominance in sharing explicit over tacit knowledge such as know-how and experience that requires hands-on learning, observation, dialogue and interactive problem solving • Use of strong hierarchy, position-based status, and formal power • Insufficient capture, evaluation, feedback, communication, and tolerance of past mistakes that would enhance individual and organisational learning effects • Differences in experience levels • Lack of contact time and interaction between knowledge sources and recipients • Poor verbal/written communication and interpersonal skills • Age and gender differences • Lack of social network • Differences in education levels • Taking ownership of intellectual property due to fear of not receiving just recognition and accreditation from managers and colleagues • Lack of trust in people because they may misuse knowledge or take unjust credit for it • Differences in national culture or ethnic background; and values and beliefs associated with it (language is part of this)
Organisational	• Integration of km strategy and sharing initiatives into the company's goals and strategic approach is missing or unclear • Lack of leadership and managerial direction in terms of clearly communicating the benefits and values of knowledge sharing practices • Shortage of formal and informal spaces to share, reflect and generate (new) knowledge • Lack of transparent rewards and recognition systems that would motivate people to share more of their knowledge • Existing corporate culture does not provide sufficient support for sharing practices • Knowledge retention of highly skilled and experienced staff is not a high priority • Shortage of appropriate infrastructure supporting sharing practices • Deficiency of company resources that would provide adequate sharing opportunities • High external competitiveness within business units, functional areas and subsidiaries • Communication and knowledge flows are restricted into certain directions • Physical work environment and layout of work areas restrict effective sharing practices • High internal competitiveness within business units, and functional areas • Hierarchical organisation structure inhibits or slows down most sharing practices • Size of business units often is not small enough and unmanageable to enhance contact and facilitate ease of sharing
Technical	• Lack of integration of IT systems and processes impedes on the way people do things Lack of technical support (internal or external) and immediate maintenance of integrated IT systems obstructs work routines and communication flows • Unrealistic expectations of employees as to what technology can do and cannot do • Lack of compatibility between diverse IT systems and processes • Mismatch between individuals' need requirements and integrated IT systems and processes restricts sharing practices • Reluctance to use IT systems due to lack of familiarity and experience with them • Lack of training regarding employee familiarisation of new IT systems and processes • Lack of communication and demonstration of all the advantages of any new system over existing ones

2.4 Research context where the knowledge sharing problem has arisen

Sections 2.2.2 and 2.3.1 discussed knowledge management and knowledge sharing in organisations, but the challenge in the automotive industry is different. In the automotive industry, the concept of knowledge management has always been employed as a tool to achieve organisational objectives (Moffett et al. 2014), boost innovativeness and cost control (Lli et al. 2010), improve inter-firm collaborations and inter-organisational relationships and, impact an organisation's financial performance (Vaccaro et al. 2010). However, in the past few years, a continual transformation of the automotive industry has been witnessed by the sector and its stakeholders, whereby new technologies are integrated into vehicles, changing the traditional concept. This section provides a literature review on the transformations that have occurred in the automotive industry, that have affected knowledge sharing within the domain.

2.4.1 Background on the automotive industry

The automotive industry is one of the world's longest established and successful industries, its success and continued survival can, in part, be attributed to the tiered supply chain structure. Prior empirical investigations into the automotive industry suggest that before the trend towards connectivity, the traditional automotive industry supply chain employed a tiered structure usually stretching from raw material suppliers (Tier 1-5) through to auto consumers (Kim et al. 2011, Thomé et al. 2014) as illustrated by Figure 2.3 below. The higher the number of the tier, the greater the commercial distance in the relationship between the OEM and the supplier (Christopher 2016). Tier-one suppliers are suppliers of large batches of identical components and modules, they were the largest and considered the most important suppliers due to their technical capabilities (Simchi-Levi et al. 2015). Suppliers gained tier-one status by demonstrating the credibility, reliability and commitment required by the manufacturer and its business partners. They integrated their supply chains for direct supply to the manufacturer and had significant technical influence with the manufacturer (Jain et al. 2015). The remainder of the actors in the automotive supply chain fell into either tier two, three, four and five depending on their outputs. Tier-five outputs were directed to tier-four suppliers while tier-four outputs were directed to tier-three suppliers and so forth. Lower tiers (such as three, four and five) supplied raw materials, close-to-raw materials, sub-assemblies, and components to tier-one suppliers (Rightmer 2012). Regardless of tier status, all suppliers were required to meet quality and production standards set by OEMs. Automotive dealerships sold vehicles supplied by OEMs and were a critical interface between the customer and the OEM (Ambe et al. 2010). Vehicle purchasers obtained their warranties and discounts through dealerships, customers had very little interaction with the OEM.

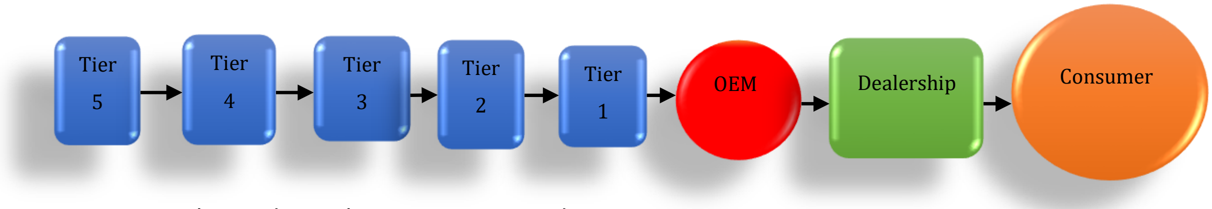

Figure 2. 3: The traditional automotive tiered structure
Source: Ambe et al. (2010)

The emergence of supplier parks

As demand for a diversified range of vehicles increased, supplier parks emerged as part of the auto industry supply chain. According to Marodin et al (2016) and, Qamer and Hall (2018), supplier parks emerged due to increased levels of out-sourcing, the use of sequential synchronous just-in-time deliveries, demand for greater interdependency between suppliers and assemblers, and the evolution of production methods such as the concept of modularisation (Qamer & Hall 2018). Modularisation is highly dependent on out-sourcing and interchanging of modules. Supplier parks were designed as a solution to problems of reliability in logistics and transportation, to lower capital and labour costs (Chung 2016), to fulfil customer orders in short lead times through responsive manufacturing and information exchange (Szmelter 2016), to closely tie supplier production schedules into customer production schedules (Bacchiocchi et al. 2014), to increase inter-firm cooperation and to address human capital demands (Marodin et al 2016). Furthermore, the presence of OEMs and suppliers within close proximity, encouraged knowledge sharing network creation for improved innovation in design and quality improvement, as skilled and professional employees could be moved to other production facilities (Piran et al. 2016). However, it is important to note that not all OEMs were wedded to the concept of supplier parks.

Globalisation in the automotive industry

Supplier parks encouraged efficient investments in dedicated assets, efficient product development and reduced transaction costs (Kim et al. 2011). However, some studies raise questions of whether or not suppliers within the chain became heavily dependent on the OEM for their survival. As the market grew, the need to reach a wider customer base coupled by inter-firm relationships and their inter-dependencies, economic geography and the inclusion of new entrants into the automotive tiered supply chain forced some OEMs to change their supply chain structure (Kito et al. 2014). Changes were in the form of new entrants that included national, regional distribution centres, and import and export ports. These changes forced some suppliers and manufacturers to increase out-sourcing, adapt their supply chain strategies and ushered the industry into a new round of globalisation.

Historically, leading vehicle manufacturers produced 60-70 percent of the value of the vehicles they manufactured in-house (Lema et al. 2015), however as competition and the need to reduce production cost increased and the industry shifted towards global value-chains. According to Mahutga (2012), Cârstea (2013), Woolliscroft et al. (2013) and Motoyama (2016), market saturation, the need to build vehicles where they are sold, and the need to establish firms in low-production and low-cost countries contributed in the drive towards globalisation in the auto-industry. Ofreneo (2016) further adds that the need to reduce risks associated with emerging market investment and the need to reduce an increasing reliance on suppliers further encouraged globalisation. Globalisation, which is a trend reflected in the reduction of trade barriers, de-regulation of commerce and the use of information technology (IT) to facilitate links to potentially anywhere in the world (Nachiappan & Gunasekaran 2015), afforded the automotive industry the opportunity to find synergies, and to reduce costs through integrating low-cost manufacturing locations, and spreading the cost of vehicle development across a greater number of markets (Lema et al. 2015). Although globalisation saw major auto-assemblers investing heavily in emerging markets, building new capacity and modernising existing plants, it is important to note that the automotive industry remained overwhelmingly concentrated in the developed economies of Japan, Europe and the United States (Motoyama 2016).

2.4.2 Digitalisation and its impact on the automotive industry

Vehicles were pure mechanical constructs until connected vehicle technology emerged in the mid-1990s, with a focus on technology-driven telematics concepts (Möller et al. 2017). Every component from engine to window and, steering to brakes, was a mechanical component working via gears and based on the principles of mechanics. Advances in information technology in the computing industry paved the way for the introduction of software in vehicle manufacturing. As a result, the automotive industry has undergone a radical transformation from the traditional automaker’s business into digital electronic component manufacturing, and software has been the enabling technology responsible this transformation in the auto-domain (Broy et al. 2014).

Automotive software

Software was first deployed into vehicles to control the engine and, in particular, the ignition approximately 35 years ago (Broy et al. 2014). The first software-based solutions were very local, isolated and unrelated. Since then, the amount of software in vehicles has grown exponentially, driven by cheaper and more powerful hardware, and the demand for new innovations and functionality (Grewe et al. 2017). This rapid increase in software and software-based functionality paved the way for connectivity, the inclusion of electronic components, innovative and sophisticated functions, and Internet access into vehicles (Kugele et al. 2017).

Connectivity

The inclusion of software-based functions and software-based electronic components was fundamental in the evolution of vehicles from completely mechanical to becoming electronic dominant devices (Sagstetter et al. 2013, Studnia et al. 2013). Vehicles became more connected internally and externally. Internal connectivity was achieved through the use of electronic control units (ECUs). ECUs can be defined as the vehicles' on-board computer tasked with controlling and monitoring the internal vehicle network and its various subsystems interconnected through several gateways (Koscher et al, 2010, Studnia et al. 2013, Loukas 2015). There are different ECUs used for different systems on the vehicle, these ECUs are interconnected through digital communication networks. Connectivity with the outside environment through the internet was achieved through the introduction of built-in Wi-Fi modules (Onishi 2012).

Internet-of-Things (IoT)

The joint connection of vehicles and the Internet resulted in a manifold of new physical characteristics for the automotive industry, such as the provision of low-level smart mobility, safety and comfort. The concept of IoT or pervasive computing was introduced to automotive manufacturing to promote more informed manufacturing processes, and to create new business models (Liu et al. 2012), to reduce costs and risks (Leminen et al. 2012), for real-time data collection processes, to achieve connectivity between different production devices, and to connect more and more software-based applications (Tenghong et al. 2012). The development of IoT was enabled by combining the Internet, hardware, embedded sensors with real-time localisation. Embedded sensors are physically small relatively inexpensive computers, each with a set of sensors. These sensor nodes are deployed in situ, physically placed in the environment near the objects they are sensing. Sensor nodes are networked, allowing them to communicate and co-operate with each other to monitor the environment (Jabeen et al. 2016). The use of the Internet in the vehicle and the use of Internet-based applications in vehicle manufacturing processes resulted in better product development and better product performance (Aris et al. 2015), however, it also resulted in an increase of engineering, production, and component out-sourcing.

The emergence of connected vehicles

Over the preceding decade, vehicle manufacturers have been increasingly equipping vehicles with capabilities to transmit and receive information (Trope & Smedinghoff 2018). In the process, hundreds of on-board computer-operated controls have replaced mechanical systems of old. The term "connected vehicle", refers to wireless connectivity-enabled vehicles that can communicate with their internal and external environments by supporting the interactions of vehicle-to-sensor-on-board (V2S), vehicle-to-vehicle (V2V), vehicle-to-road-infrastructure (V2R), and vehicle-to-Internet (V2I). The collective term for the networking terms is V2X (Diewald et al. 2012). A useful way of viewing connected vehicles is to see them as a collection of functionality bundles (He & Zhao 2018). These technologies (V2X), build on the familiar transport services to add driver assistance, passenger safety, vehicle security, improved mobility, entertainment, office and communication services, navigation and so on (Morris et al. 2018). Built with over 100 million lines of code, and more than 100 embedded and interconnected computerized ECUs, connected vehicles are considered as building blocks which have fuelled a plethora of innovations which have left the industry on the verge of introducing autonomous vehicles into the consumer market in the very near future (Gerla et al. 2014). Nonetheless, this digital transformation of the automotive industry has resulted in a steady increase in vehicle development outsourcing (Ciravegna et al. 2013, Cabigiosu et al. 2013, and Danese & Filippini 2013).

Component outsourcing

In the last decade, OEMs have had to re-evaluate their supply chain activities and relationships to adapt to the challenges of an ever-changing industry. This has resulted in a steady increase in vehicle component design and development out-sourcing (Danese & Filippini 2013), and a shift of both product development tasks and knowledge from vehicle makers to suppliers (Cabigiosu et al. 2013). Outsourcing has emerged as a vehicle to apply downward pressure on operating costs and to satisfy an overarching need to remain competitive (Woolliscroft et al. 2013). Outsourcing has emerged as a strategic necessity as can be gauged by the increasing size of the outsourcing industry. It is, however, important to note that component out-sourcing is not a new feature in the automotive industry, rather it is the inclusion of complex software systems in the vehicle architecture that has transformed the supply chain, defined new supply requirements, forced manufacturers to rationalise the supply base and increase the use of out-sourcing as a strategic alternative. (Ambe et al. 2010, Kim et al. 2011, Sturgeon & Van Biesebroeck 2011).

Badampudi et al. (2016), define component out-sourcing as "transfer of previously in-house activities to a third party" and infer that, at some time in the past, the out-sourcing organisation had a level of competence in the activity being out-sourced. Whilst Zirpoli and Becker (2011) refer to external third-party sources, Wilhelm and Dolfsma (2018) refer to a broader perspective known as *Internal Out-sourcing*, whereby out-sourcing can apply to internal business units or joint ventures. In addition to the definitions above, as Jacobides et al. (2016), suggest, "out-sourcing" is nothing less than the wholesale restructuring of the corporation around core competency and outside relationships." Schniederjans and Schniederjans (2015) define out-sourcing as "a multi-dimensional system involving an organisation, the supplier, the transporter/shipper, the storage provider and the customer." Out-sourcing is also defined as the procurement of products or services from sources that are external to the organisation (Gholz et al. 2018). Conventional out-sourcing arguments drawn from transactions cost literature, which are embodied in conventional supply chain structures, fail to clearly define out-sourcing in the context of the rapidly changing automotive industry. Out-sourcing in the automotive industry requires firms to develop more in-depth relationships with suppliers including strategic partnerships (Ciravegna et al. 2013), early involvement of suppliers in product development (Danese & Filippini 2013), open and inclusive innovation processes, and an increased modularity (Zirpoli & Becker 2011). What distinguishes out-sourcing in the automotive industry, is that compared to other industries that use modular supply networks, the automotive industry still retains some elements of product integrality and specificities, for example, the lack of standard interfaces (Ciravegna et al. 2013).

2.4.3 Changes to the automotive supply chain

ICT driven transformations, technological developments, increased component out-sourcing, the growing influences of cybersecurity, increased customer demands and the increase in the number of models and model variants have resulted in changes to the automotive supply chain structure (Schniederjans & Schniederjans 2015). Changes faced by the industry make the simple tiered configuration of Figure 2.3 unsuitable to service a modern-day business and customer requirement driven industry (Ambe et al. 2010 & Kim et al. 2011). The automotive supply chain has transformed from the traditional tiered structure to a network of multiple businesses and relationships. New roles have emerged in addition to the traditional first-tier suppliers that delivered physical products to the OEMs. Growing software system complexity and highly integrated hardware sub-systems, either at first-tier supplier or OEM level has paved the way for the introduction of new suppliers. The new suppliers do not supply physical products, they supply technical and software engineering skills (Loukas 2015, Manello & Calabrese 2018). Changes to the traditional tiered structure permit component out-sourcing, reduce production cost, improve responses to strict deadlines and product proliferation and encourage the production of quality products (Calabrese & Manello 2018). However, it introduces knowledge sharing challenges and does not allow OEMs to fully participate in the design and development of components, software systems and multi-technology products. Changes to the supply chain structure that affect tier one and two, include the following:

Tier-one suppliers

Global firms that specialise in complex systems and multi-technology assemblies are the new direct suppliers (Loukas 2015, Manello & Calabrese 2018). These firms, some of them new to automotive design, development and production, have a huge global presence and often locate their assembly plants in countries with a lower cost base (Woolliscroft et al. 2013), and take responsibility for designing and assembling of whole modules or systems of a vehicle. However, the major shifts in the nature of the auto-industry analysed above, have created new demands on, and opportunities for, tier-one suppliers, new and old. Tier-one now includes the following roles:

1. System Integrator

   System integrators' capabilities lie in design and component integration. They integrate sub-systems into complete system modules before being shipped directly to the OEMs (Amin et al. 2015). Most automotive manufacturers place design and development responsibilities of systems, sub-systems, multi-technology products and components on system integrators (Amin et al. 2015, Morris et al. 2018).

2. Global Standardiser

   Global standardisers are companies that set standards on a global basis for a component or system. They are capable of designing, developing and manufacturing complex systems or multi-technology products (Amin et al. 2015).

Tier -two suppliers

Tier-two suppliers provide the parts that are required by tier-one suppliers to make complete components, sub-systems, multi-technology products or complex software systems. They do not supply products directly to the OEMs (Amin et al. 2015). The tier-two status can be company-specific if the organisation supplies different components to different vehicle manufacturers. A company can also be a tier-one supplier for one component and a tier-two supplier for another component (Christopher 2016). Product quality assurance, meeting demands and responding to price issues are some of tier two's responsibilities. Most tier-two suppliers have established a presence in low-cost countries around the world as there is no pressure to be close to OEMs (Ambe & Badenhorst-Weiss 2011). In addition to the traditional tier-two supply chain structure-function of delivering components to tier-one suppliers, a new role of component specialist has emerged.

1. Component Specialist

   Component specialists are companies that design and manufacture specific components or sub-systems for a given vehicle or platform. These companies can also be suppliers to system integrators and system manufacturers (Liu et al. 2011). They command a huge global presence and design systems and multi-technology products from functional specifications and performance factors provided by automotive manufacturers (Amin et al. 2015). Component specialists can further be divided into the following:

   - *Component Manufacturer*: these companies are responsible for designing and testing components they manufacture, but not responsible for the design of the complete sub-system where the components will fit.

   - *Subassembly Manufacturer*: these are process specialists with additional assembly integration and design capabilities.

2. System Manufacturers

   System manufacturers are organisations that design, develop and manufacture multi-technology products. System manufacturers design systems and components from functional specifications and performance factors provided by automotive manufactures, however, at times system manufacturers make design decisions without the OEM's input (Amin et al. 2015). System manufacturers supply components to the system integrators or at times directly to the OEMs (Liu et al. 2011).

Summary of this section

This section introduces knowledge and the role it plays in organisations through the concept of knowledge management. Several definitions were presented; key knowledge processes and components for knowledge management are discussed. However, the automotive industry is changing rapidly; the digital transformation of the automotive industry, globalisation, the emergence of supplier parks and connected vehicles, and an increase in component outsourcing. All of these concepts have one thing in common: they have altered the structure of the automotive supply chain and as a result, introduced knowledge sharing challenges into the automotive domain. The manufacture of connected vehicles requires the integration of complex outsourced digital components and technological advancements. Knowledge regarding the design and development of these outsourced components needs to be shared with relevant stakeholders in order to manufacture secure vehicles, however, the knowledge sharing processes of old are no longer suitable due to changes that have occurred within the domain. This challenge to knowledge sharing processes within the automotive industry has contributed to the cybersecurity challenges faced in connected vehicles. The following section discusses cybersecurity and the importance of knowledge sharing in the context of the automotive industry.

2.5 Cybersecurity management

Cybersecurity within a business or organisation is protection that is focused on protecting proprietary information, maintaining the integrity of databases, ensuring timely access to systems and information by authorised users, preventing unauthorised access and damage to systems and their components (Raggad 2010). It aims to make an organisation more competitive and successful in a safe environment. This involves strategies that enhance confidence with shareholders, customers and stakeholders, for preventing damage to the business brand, actual losses and business disruptions.

Cybersecurity management provides an objective, systematic, and analytical approach to assessing system security risk to enable senior management to better understand system risks and allocate resources to reduce and correct potential losses and operational impacts (Katsumata et al. 2010). It involves a series of decision-making processes to select, implement, and maintain proper security controls based on three pillars: people, processes and technology (Goodyear et al. 2010, Fischer 2014). This three-pronged approach helps organisations protect themselves from both organised and opportunistic attacks, as well as common internal threats (Bayuk 2012). Cybersecurity threats are dynamic and constant, therefore there is no hard and fast rule regarding an evaluation of effective security. Nonetheless, Goodyear et al. (2010) argue that an effective cybersecurity management posture hinges on a systematic approach that encompasses application security, network security, operational security, end-user education, and leadership commitment and involvement. These elements are discussed in Table 2.3 below.

Table 2. 3: Elements of cybersecurity management

Elements for an effective cybersecurity management posture	
Application security	Web application vulnerabilities are a common point of intrusion for cybercriminals. As applications play an increasingly critical role in business, organisations need to focus on web application security to protect their customers, their interests and their assets.
Network security	Network security is the process of protecting the usability and integrity of network and data. This is usually achieved by conducting a network penetration test, which aims to assess networks for vulnerabilities and security issues in servers, hosts, devices and network services.
Operational security	Operational security protects an organisation's core functions by tracking critical information and the assets that interact with it to identify vulnerabilities.
End-user education	Human error remains the leading cause of data breaches. A cybersecurity strategy is only as strong as the weakest link, so organisations need to make sure that every employee knows how to spot and deal with the threats or risks they may encounter.
Leadership commitment and involvement	Leadership commitment is the key to a successful implementation of any cybersecurity project. Without it, it is very difficult to establish or enforce effective processes. Top management must be prepared to invest in appropriate cybersecurity resources, whether it's hiring qualified people, awareness training or technology.

Cybersecurity management consists of managing risks, and there are a number of risk management frameworks that have been proposed by government institutions (e.g. National Institute of Standards and Technology [NIST], the National Aeronautics and Space Administration [NASA]), international organisations (e.g. European Union Agency for Network and Information Security [ENISA]), or international professional associations (Information Systems Audit and Control Association [ISACA]), as well as prominent scholars (Katsumata et al. 2010, Raggad 2010, McCarthy & Harnett 2014, Ganin et al. 2017, Meszaros & Buchalcevova 2017).

The focus of this study does not extend to risk management frameworks; however, cybersecurity management involves cybersecurity, and thus it is important to define the term "cybersecurity". The following section defines cybersecurity.

2.5.1 Defining cybersecurity

The term "cybersecurity" is sometimes inappropriately conflated with other concepts such as privacy, information sharing, intelligence gathering, and surveillance (Fischer 2014). There is a paucity of literature on what the term actually means and how it is situated in various contexts. The absence of a concise, broadly acceptable definition that captures the multidimensionality of cybersecurity potentially impedes technological and scientific advances by reinforcing the predominantly technical view of cybersecurity while separating disciplines that should be acting in concert to resolve complex cybersecurity challenges (Cebula & Young 2010, Klimburg 2012, Craigen et al. 2014). For example, there is a spectrum of technical solutions that support cybersecurity. However, these solutions alone do not solve the problem; there are numerous examples and considerable scholarly work that demonstrate the challenges related to organisational, regulatory and legal, collaboration and cooperation effort built upon knowledge-based solutions, skilled personnel, a trusted environment and other human dimensions as highlighted by Figure 2.4 below, that are inextricably tied to cybersecurity efforts (Deibert 2012, Von Solms & Van Niekert 2013, Craigen et al. 2014, Garcia-Perez 2019).

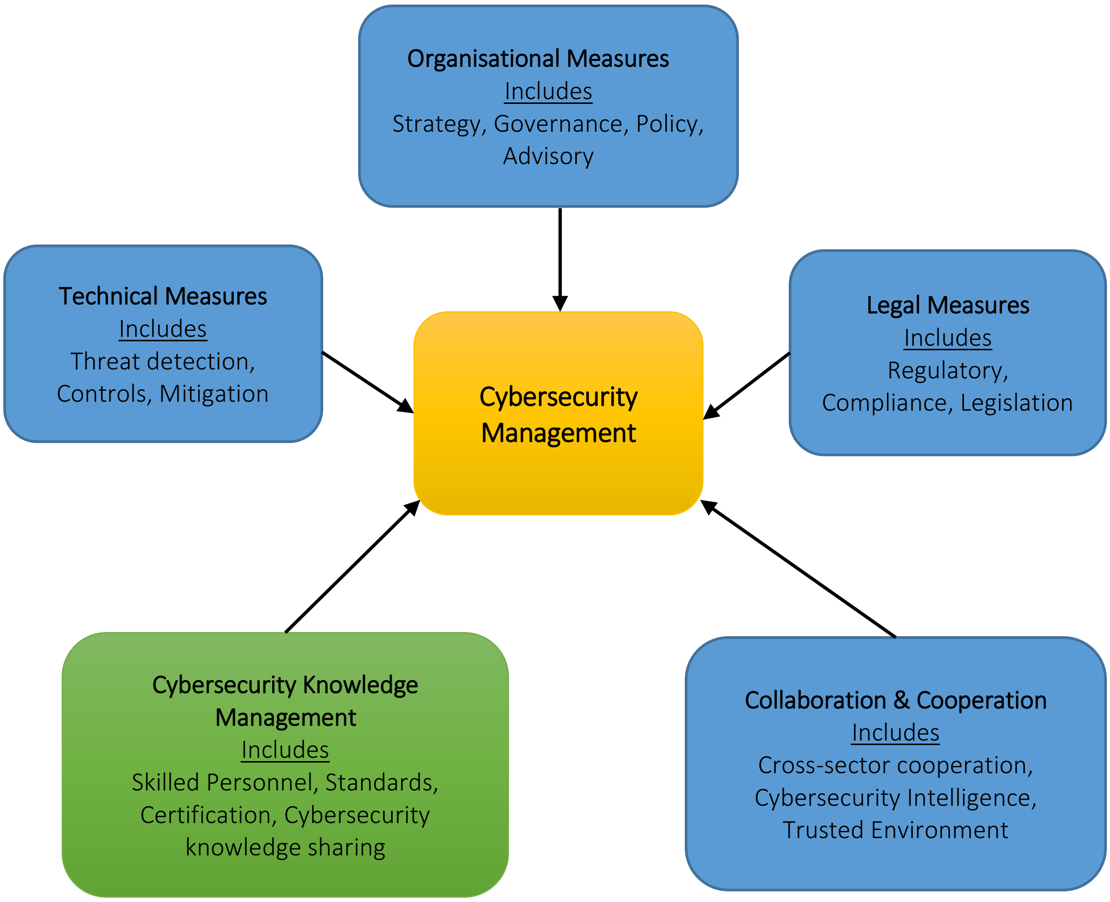

Figure 2. 4: Cybersecurity posture
Source: Garcia-Perez (2019)

An additional, although less impacting, issue is the inconsistent use of syntax for cybersecurity. Across the literature, both versions, cybersecurity and cyber security, are used. The lack of a uniformly accepted definition of cybersecurity as described in the previous section has been recognized across professional (Barzilay 2013, Stubley 2013, Walls et al. 2013), governmental (Falessi et al. 2012, Wamala 2011) and academic (Baylon 2014, Giles & Hagestad 2013). According to Craigen et al. (2014), part of why cybersecurity lacks a concise definition is because cybersecurity is an evolving and complex challenge requiring interdisciplinary reasoning, therefore any definition must attract currently disparate cybersecurity stakeholders while being unbiased, meaningful and fundamentally useful. Schatz et al. (2017) conducted various lexical and semantic analysis techniques in an attempt to better understand the scope and context of available definitions and their relevance. The researcher has adopted the following working definition of cybersecurity, based on the work of Schatz et al. (2017):

> *"The approach and actions associated with security risk management processes followed by organisations and states to protect confidentiality, integrity and availability of data and assets used in cyberspace. The concepts include guidelines, policies and collections of safeguards, technologies, tools and training to provide the best protection for the state of the cyber environment and its users."*

The definition addresses the cybersecurity phenomenon from various perspectives which include industrial, organisational, governmental, and academic and, the user perspective. It is expected that this definition will become less fitting or relevant as social, political and technological developments in this space progress.

2.5.2 Conceptual aspects of cybersecurity

Cybersecurity is an interdisciplinary field comprising a wide variety of topics such as information security (Julisch 2013, Von Solms & Van Niekerk 2013), and risk management (Cebula & Young 2010). While the distinction between cybersecurity and related concepts such as information security is often missed (Burgess 2010). Information security concerns itself with maintaining the CIA triad of confidentiality, integrity and availability of information (ISO/IEC 27000, Dardick 2010, Von Solms & Van Niekerk 2013), cybersecurity involves applying those elements to cyberspace (Bayuk 2012, Klimburg 2012). Cyberspace is the virtual and automated information network supported by information technology (IT) infrastructures that include the Internet, computer systems and telecommunication systems. Theoretically, cybersecurity involves protecting information systems and technology against threats from cyberspace. Technology also includes non-information-based assets, however, cybersecurity does not include protecting information that is not within the extent of cyberspace (e.g. a document stored in a safe), although this is still an information issue (Klimburg 2012).

Other concepts closely related to cybersecurity are cyber-defence, cyber-attack and cyber-war. Cyber-defence is the use of technical and non-technical measures that allow a nation, an organisation or individual to defend in cyberspace, information systems that it considers to be critical (Farwell &

Rohozinski 2012), while the term 'cyber-attack' is used to describe a variety of harmful activities taking place in the cyberspace (Clarke & Knake 2012, Cornish et al. 2010). Cyber-war is described as actions by a nation, an organisation or individual to penetrate computers or networks that belong to another nation, organisation or individual to cause damage or disruption (Cornish et al. 2010, Farwell & Rohozinski 2012, Klimburg 2012). A cyber threat in the technical domain is treated as a potential event, which, if actualised could cause an unwanted incident that negatively affects the security of a system (ISO/IEC 27001). Appendix 2 presents a list of cybersecurity-related definitions for further reference.

2.6 Cybersecurity and the automotive industry

The rapid growth in the development of computing technologies has transformed the automotive industry, leading vehicle manufacturers and component suppliers to develop and integrate ever-more technologically complex components into modern vehicles. These connected vehicles, which represent current technological advancements in the automotive industry, are electromechanical constructs with highly integrated hardware and software (Sagstetter et al. 2013, Leenstra 2017). This means that such vehicles are highly complex machines with many potential vulnerabilities. Protecting connected vehicles is a challenging task, and prior research shows that there are cybersecurity concerns regarding the design, development and integration of components for connected vehicles and the vehicle as a whole (Checkoway et al. 2011, Sagstetter et al. 2013, Studnia et al. 2013, and Amin et al. 2015). The potential cybersecurity risks inherent in vehicle manufacture affect all stakeholders in the automotive industry from vehicle designers and manufacturers to vehicle end-users, this brings cybersecurity knowledge sharing in the automotive industry to the fore.

2.6.1 Defining cybersecurity knowledge in the automotive industry

To define cybersecurity knowledge in the automotive industry, it is necessary to define cybersecurity in the context of connected vehicles in the automotive industry first. For the purpose of this study, the researcher has adopted the following working definition based on the work of the National Highway Traffic Safety Administration (NHTSA).

> *"The protection of vehicular electronic systems, communication networks, control algorithms, software, users, and underlying data from malicious attacks, damage, unauthorized access, or manipulation" (NHTSA 2017).*

The investigations of this study focus on the sharing of knowledge relevant for component integration processes. It is therefore important to define cybersecurity knowledge within the context of component integration in connected vehicle development.

Automotive cybersecurity knowledge

In the context of this research, cybersecurity knowledge can be framed as information required to successfully address cybersecurity issues through secure component integration processes. Cybersecurity knowledge assists component manufacturers and OEMs to identify integration weaknesses that can potentially expose integrated components, sub-systems and systems to cyber-related threats and comprises of component-specific knowledge and architectural knowledge. Component specific knowledge concerns itself with the following:

- **Security test results** – contain information relating to how a component satisfies security requirements, and security testing techniques employed to address the security requirements. The security test results include documentation relating to risk and hazard analysis, threat analysis, fault injection tests and, residual risk documentation (SAE J3061, ISO26262). Fault injection or stress testing is the deliberate introduction of faults to test a component's robustness and error handling capabilities (Natella et al. 2013). Residual risks are the risks remaining after risk management (ISO 27001).
- **Safety test results** – comprise respective documentation from tests conducted to verify that a component fulfils its safety requirements. The results include all the results from all the tests conducted from the initial design stage to the final stage of component development (Ericson 2015). Safety test results also comprise functional safety and technical safety results. Functional safety aims to address risks due to hazards caused by unwanted behaviour (Birch et al. 2013).
- **Performance specification test results** – contain documents that specify the operational requirements of a component. Performance specification test results are measured against the component's specified requirements that describe how the component is expected to perform and behave (SAEJ 3061).
- **Manufacturing processes** – these contain information on how the component was manufactured, including information relating to the tools used within the manufacturing environment. A flowchart or some form of diagrammatic representation highlighting the steps, processes and or phases employed to manufacture the component are normally included with

the documentation. The manufacturing processes may at times, include development information of tools developed specifically for the manufacturing of a specific component.

- Design processes –these are documents that define the processes adopted in designing the component. Design processes also include the rationale for identifying, characterising and, the general development of the process (Kaluza et al. 2016).

Architectural knowledge, on the other hand, focuses on vehicle architecture, and comprises of the following:

- Design decisions – define the design and development activities of the vehicle's architecture. This knowledge resides with vehicle manufactures, and it specifies the architecture's operational requirements and associated risks (Soliman et al. 2015). Architectural patterns, design patterns and design tactics are also contained in the design decisions data.
- Integration specifications - these specifications provide coding guidelines for modelling and programming languages for component-to-architecture integration. Integration specifications also define existing component-to-architecture integration processes, modelling and programming languages.
- Interface specifications – define the interplay between the architecture's interface and the component's interface, based on the component's requirements, expected performance and behaviour. Interface specification documentation also defines a component's portability, reconfigurability and extensibility, together with guaranteed reliability and performance levels in the context of the vehicle architecture (Di Natale & Sangiovanni-Vincentelli 2010).

In the next section and chapter 6, the researcher will discuss how the sharing of relevant knowledge related to component integration processes enhances cybersecurity challenges in connected vehicle manufacturing.

2.6.2 Component integration challenges and cybersecurity

Bonjour et al. (2013) conducted research on component integration challenges before the era of cybersecurity; although their findings are still relevant in the integration of mechanical constructs, they may not be so with electro-mechanical systems. However, they propose a decomposition methodology to improve product design and to ease the substantial coordination demands that are required when sub-systems interact. Yağdereli et al. (2015) view the component integration challenge from a different perspective and state that remote diagnostic and firmware updates over the air (FOTA), as proposed by Idrees et al. (2011) are not feasible due to component integration challenges. Yagdereli et al. (2015)

state that a key problem for software updates is that all different components need to be updated together to a known global configuration to ensure that the whole system will work as expected. With each component being developed in isolation from different providers, this is an area that affects the integration challenge. Farcas et al. (2010) state that component integration is an intricate task, it requires complex interactions with different suppliers to guarantee that the final product is successful. Jacobides et al. (2016), state that component integration comprises a set of different technological and organisational skills ranging from component manufacture and assembly through the understanding and integration of the technological disciplines underlying a product to project management.

However, according to Checkoway et al. (2010) and Amin et al. (2015), design decisions can at times be left at the discretion of the component manufacturer by the OEM, and because component manufacturers do not have a holistic view of all the different components that make up the final module, they are forced to assume those particular components in the vehicle work in certain ways. Potentially, this may result in incorrect performance and functional specifications leading to incorrect binding of components that results in weak integration processes. Amin et al. (2015) and Checkoway et al. (2010) state that component integration challenges in vehicle manufacture are enhanced by the use of “glue-code”. Glue-code is a custom-written code that is intended to meld existing systems and new technologies to form sub-systems or systems capable of taking additional tasks, exhibiting improved performance and enhancing existing systems. When applied with the relevant component integration knowledge, glue-code can be used to tie together automotive systems and to connect disparate software and hardware modules (Tanev et al. 2015).

However, if not properly managed, glue-code can become excessively complicated and can negatively affect performance and introduce cyber-related vulnerabilities (Amin et al. 2015). They argue that the true source of the glue-code problem can be traced back to the structure of the automotive supply chain and that glue-code integration problems are a consequence of knowledge sharing challenges in component integration processes facing the automotive industry. The lack of knowledge sharing in component integration results in glue-code integration problems that lead to cybersecurity vulnerabilities at the interfaces between digital modules and the vehicle as an entity. Furthermore, cybersecurity vulnerabilities also occur between distinct modules designed by external suppliers (Checkoway et al. 2010, Amin et al. 2015).

The notion that cybersecurity vulnerabilities are a result of a lack of knowledge sharing that eventually leads to insecure component integration processes is supported by Farcas et al. (2015) who conducted studies on component integration in both the avionics and automotive domains. Their research focused on complex distributed safety-critical systems in aeroplanes and vehicles developed independently by different organisations. They state that, although avionics and automotive domains have different business models and certification regulations, both face challenges in the integration of heterogeneous and distributed components into highly complex system-to-systems with a wide variety of functional and non-functional requirements, especially when many failures depend on the way components are integrated. Baheti and Gill (2011) state that vehicle control systems rely on system components manufactured by different vendors with their own software and hardware; a major challenge for the industry is not only the ability to securely integrate those components into systems or subsystems but on how to integrate them securely into different vehicles without the relevant integration knowledge. Both the supplier and the integrator need new system science that enables reliable integration knowledge sharing and cost-effective integration of independently developed system components (Baheti & Gill 2011).

2.6.3 Towards a knowledge-based economy

Today knowledge is considered to be the driving force of economic growth, productivity growth and a resource that can offer a sustainable competitive advantage in a competitive and dynamic economy (Lee et al. 2010, Wang & Noe 2010, Tocan 2012, and Carmeli et al. 2013). The change towards a knowledge-based economy is happening on a global scale, transformation is taking place in all advanced industrialised economies and many developing economies are also aspiring to reach this target. It is a deep and general process which operates across all sectors of the economy: manufacturing and services, high tech and low tech, domestic and internationally traded, public and private, large corporation and small enterprise (Schiliro 2012). This is evidenced by the rise in high-technology investment, the growth of the service sector, the rise in self-employment and start-up companies, and a rise in the number of patents. Knowledge has always played a vital role in the technological and innovation advances that have been experienced in most critical sectors and economists Kanellos (2013) and Zieba (2013) argue that in the past few decades most crucial sectors have transitioned to a knowledge-based economy, where sources of knowledge such as tacit and explicit knowledge are crucial and considered important.

Knowledge-based economies rely on the use of knowledge to create goods and services and it is defined as "as a system of consumption and production that is dependent on the quantity, quality, and accessibility of the information available, rather than the means of production" (Araya & Peters 2010, Edmondson 2012, Tocan 2012). According to Kanellos (2013), it is a very important socio-economic phenomenon that drives innovation, economic growth and development, characterised by high potential technology upgrading, moreover, it is an effective mechanism for the transformation of knowledge into innovation and new economic activity.

In the automotive domain, the knowledge-based economy is transforming not only the structure of the automotive supply chain and operational performance measures used to measure success (Chapter 2 section 2.4.3) but also the adoption of new methods and technologies in the design and development of digital components for connected vehicles (Alguezaui & Filieri 2014). In the unrelenting search for sustainable economic and competitive advantage, automotive manufacturers have transitioned to a knowledge-based economy relying on knowledge sharing for the development and integration of ever more technologically complex components into the modern connected vehicle.

2.6.4 The Importance of cybersecurity knowledge sharing in component manufacturing

In connected vehicle manufacture OEMs no longer manufacture vehicles, they are now tasked with integrating various components manufactured by different organisations; a connected vehicle is a vehicle that supports connection and communication with the transport infrastructure and other connected vehicles (Woo et al. 2016). Component integration was and is one of the most often used terms in automotive component manufacture, yet a poorly defined notion (Liu et al. 2011). However, it is widely accepted that integration is a property of interrelations, and the specifications of those relationships between the components holds the key for integration. Vehicle components have been defined in supply chain management literature and vehicle manufacturing literature (Rusinek & Zaera 2018), as physical portions of a product that carry out specific functions and are linked to each other through a set of interfaces defined by the product architecture. However, due to recent developments within the industry, this definition is no longer valid as vehicle components are no longer simply physical constructs (Moazed 2016). Connected vehicles are manufactured with software modules, hardware modules, applications, services, and technologies that connect the vehicle to its surroundings (Uhlemann 2015, Bryans 2017), therefore for the purpose this study, a component is defined as:

> *"A uniquely identifiable, functional input, code, piece, assembly or subassembly, system or subsystem, which is designed and developed to perform a distinctive and necessary function in a connected vehicle environment."*

Similar to software and hardware modules used in connected vehicles manufacturing, automotive systems change over time, however, in the context of connected vehicles, automotive modules and systems are defined as follows:

> *"Software modules are software components or part of a program, while a hardware module is an independent physical entity which can be used as part of a more complex system. A system is an organised purposeful structure that consists of interrelated and interdependent elements*

(components, modules etc.). These elements continually influence one another to maintain their activity and achieve the goal they have been designed to fulfil."

2.7 Automotive standards, best practices and guidelines

The following section reviews current standards, best practices and guidelines in the automotive industry that cover automotive cybersecurity, including sharing practices of knowledge related to component integration processes, to determine if any are designed to address the sharing of knowledge relevant for component integration.

Standardization and best practices are designed to assist manufacturers, suppliers and developers to demonstrate compliance to a standard or practice; it is a belief that when a product or component follows the standard or practice, particular properties are present and associated threats have been considered. Table 2.4 below provides a list of some of the standards currently being employed to attempt to address cybersecurity challenges in the automotive industry. Table 2.4 presents some of the best practices and guidelines in use. However, not all the standards and guidelines are directly applicable to the automotive domain in their current states (Macher et al. 2017). Nevertheless, currently available standards and guidelines are at times frequently fragmented or incomplete (Kreiner 2017, Macher et al. 2017). Standard and guideline providers typically assume that their open issues are covered by other guidelines or standards.

Table 2. 4: Current automotive cybersecurity standards

Standard	Name
ISO/SAE 21434	Automotive Cybersecurity Standard *(expected to be published in 2020)*
SAE J3061	Cybersecurity Guidebook for Cyber-Physical Vehicle Systems
SAE J3101	Requirements for Hardware-Protected Security for Ground Vehicle Applications
SAE 2945	Dedicated Short Range Communication (DSRC) Minimum Performance Requirements
ISO 26262	International standard for functional safety of electrical and electronic systems in production vehicles
ISO 12207	Systems and software engineering - Software lifecycle processes
ISO 27001	Information security management
ISO 27002	Information technology - Security techniques - Code of practice for information security management
ISO 29119	Software testing standard
ISO/*IEC* 15408	Information Technology – Security Techniques – Evaluation Criteria for IT Security

As shown in Tables 2.4 and 2.5, while vehicle development faces a merger of security and safety, many of the standards, guidelines and best practices cross industry and device boundaries. For instance, the standards and best practices that relate to software development lifecycles apply to all industries that include software in their components and products, and not just vehicle development. Nonetheless, existing standards and guidelines place an extra focus on the need to ensure data privacy in connected vehicles.

Table 2. 5: Current automotive cybersecurity guides and best practices

Organisation	Best Practice/ Guidelines
Alliance of Vehicle Manufacturers	Consumer Privacy Protection Principles for Vehicle Technologies and Services
NIST	Framework for Improving Critical Infrastructure Cybersecurity
NIST	Security and Privacy Controls for Federal Information Systems and Organisations
NIST	Computer Security Incident Handling Guide
NIST	Guide for Conducting Risk Assessments
NHTSA	Cybersecurity Best Practices for Modern Vehicles
Auto-ISAC	Automotive Cybersecurity Best Practices
MISRA-C	Guidelines for Safety Critical Software

The automotive domain had already well-established safety standards and guidelines, which have been in use for designing safety-critical components and systems that ensured that all safety risks were reduced to tolerable levels, however as vehicle manufacturing now includes modules that permit connectivity to the outside world, these safety standards can no longer guarantee safety if the vehicle's cybersecurity is compromised. The automotive domain requires standards and guidelines that integrate cybersecurity best practices, security and functional safety engineering approaches for connected vehicles and autonomous vehicles (Kreiner 2017, Macher et al. 2017).

There is, however, a new standard that is being developed specifically for connected vehicles which aims to address cybersecurity challenges. The Automotive Cybersecurity Standard (ISO/SAE 21434) is the first domain-specific cybersecurity engineering standard to be created under a collaboration between ISO (International Organisation for Standardization) and SAE (Society of Automotive Engineers). The standard, which is expected to be published in 2021, aims to define a structured process to ensure cybersecurity is designed upfront, to maintain consistency across a global industry, and to be complete and to promote conscious decision making. Nonetheless, standards, best practices, or guidelines that address knowledge sharing within the domain are non-existent.

The review of automotive standards, best practices and guidelines above, highlights the absence and need for automotive-specific standards, best practices and guidelines. None of the reviewed standards, best practices and guidelines address cybersecurity-related challenges that are a result of the lack of knowledge sharing in component integration processes.

2.8 Knowledge sharing frameworks

Based on the review carried out of the literature on this topic, knowledge sharing has been addressed in many different contexts. Many different frameworks address knowledge sharing which are:

1. Frameworks that focus on knowledge sharing in new product development

Le Dain and Merminod (2014), investigated knowledge sharing between suppliers and customers in an inter-organisational new product development (NPD) context, and developed a conceptual framework for knowledge sharing according to the suppliers' involvement. New product development (NPD) is an iterative process of gathering, creating and evaluating information for developing new, quality and defect-free products. Le Dain and Merminod (2014), introduce three supplier involvement configurations to knowledge sharing in NPD: black box, grey box and white box. According to Le Dain and Merminod (2014), supplier involvement in NPD can take the form of a variety of configurations: the simple consultation of suppliers about customer design ideas *(white box),* the joint development of an outsourced product *(grey box),* or delegation to the supplier of full design responsibility for an outsourced product *(black box).* They argue that in NPD, most novelty arises at the boundaries between the specialised knowledge emanating from different company departments involved in the NPD process. Effectively managing knowledge across these organisational boundaries is a daunting task that is, however, critical to successful product development. Le Dain and Merminod's (2014) conceptual framework (Figure 2.5 below), which was adapted from Carlilie's (2004) integrated framework for managing knowledge across boundaries, distinguishes three levels of cross-knowledge sharing complexity: transfer, translation and transformation.

Some materials have been removed from this thesis due to Third Party Copyright. Pages where material has been removed are clearly marked in the electronic version. The unabridged version of the thesis can be viewed at the Lanchester Library, Coventry University.

Figure 2. 5: The conceptual framework for knowledge sharing across boundaries
Source: Le Dain and Merminod (2014)

These levels have been the subject of several other knowledge sharing studies (Koufteros et al. 2010, Le Dain et al. 2010, Nicolini 2011 and, Merminod & Rowe 2012). In the context of inter-organisational NPD, Le Dain and Merminod (2014) state that knowledge transfer is supported by storage and retrieval technologies and operationally consists of exchanging boundary objects. Boundary objects (BOs) are objects or documents that are created and used during collaborative design across functions (Paulin & Suneson 2015). Knowledge translation relates to issues that arise from bad knowledge circulation between different project members, while knowledge transformation is an activity analysed through a number of complex problem-solving situations encountered during a project which may result in the building of a new solution.

The framework by Shanker et al. (2013) was based around the concept of "collaborative networks" and is concerned with creating collaboration pools that provide systematic channels of information flow helping mitigate knowledge loss through the value-chain. Shanker et al. (2013) argue that the only effective way to create long-lasting "intelligence" within an organisation where knowledge is gathered, stored and retrieved effectively, and knowledge losses are minimised, is to create collaborative networks in a knowledge management cycle as shown in Figure 2.6 below. Knowledge sharing in NPD has been the subject of several other knowledge sharing studies (see Fuchs & Schreier 2011, Esper et al. 2010, Trkman & Desouza 2012). Shanker et al. (2013) conclude by stating that the agility of NPD is governed by the efficiency of knowledge management skills and knowledge creation cycles, which are largely and directly impacted by the organisation's internal and external collaboration capability.

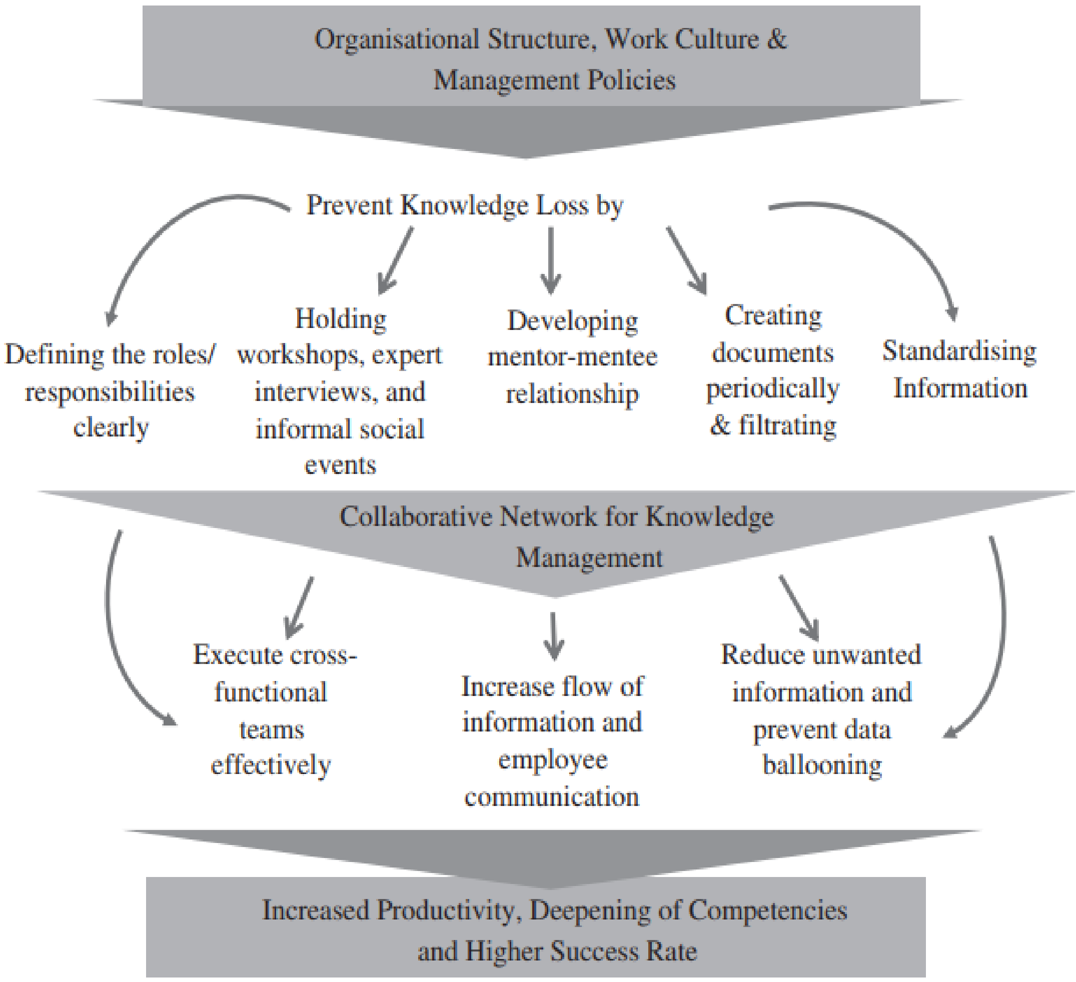

Figure 2. 6: Collaboration framework to minimise knowledge loss in new product development
Adapted from Shanker et al. (2013)

Shanker et al. (2009) proposed a knowledge management framework for intra-level and inter-level knowledge flow in new product development. Intra-level knowledge flow focuses on knowledge flow within different levels within an organisation (i.e. group-level, departmental-level and team-level). The proposed framework assumes that organisational knowledge is the collective sum of individual knowledge assets, which is embedded in people, product, process and structure. Therefore, knowledge can be captured from organisational systems, processes, products, rules and culture. The knowledge management framework aims to link knowledge management initiatives with key organisational goals like new product development, customer satisfaction and manufacturing excellence. As shown by Figure 2.7 below, the proposed framework highlights the hierarchal nature and bi-directional flow of knowledge.

Figure 2. 7: Proposed KM system framework in the context of NPD for engineering firms
Source: Shanker et al. (2009)

2. Frameworks designed to improve performance through knowledge sharing

Advancing on Ipe's (2003) conceptual work that opines that individual knowledge sharing is influenced by motivation to share, the nature of knowledge, opportunity to share and culture, Eaves (2014) developed a multidimensional model of individual knowledge sharing influences. In the first dimension, Eaves (2014) states that to share knowledge, opportunities must be available for the organisational actors to do so *(opportunities to share*), these may be formal or informal in nature and span individual, social, organisational and technological dimensions including physical and virtual contexts, that are designed specifically to facilitate the acquisition and dissemination of knowledge. The second dimension, *(motivation to share),* facilitates knowledge sharing behaviour through complex processes of socialisation, externalisation or both processes. The third dimension, *(nature of knowledge)* is influenced by the nature of the knowledge; tacit or explicit, as well as the value of the knowledge. Culture is presented as the primary factor in knowledge sharing behaviour, influencing all others. Individuals possess personal values, beliefs and experiences which influence their perception, interpretations and actions. These combined with collective norms, practices, values and history which intimate organisational culture, along dimensions such as espoused corporate vision and views of support from management, can facilitate and contribute to knowledge sharing.

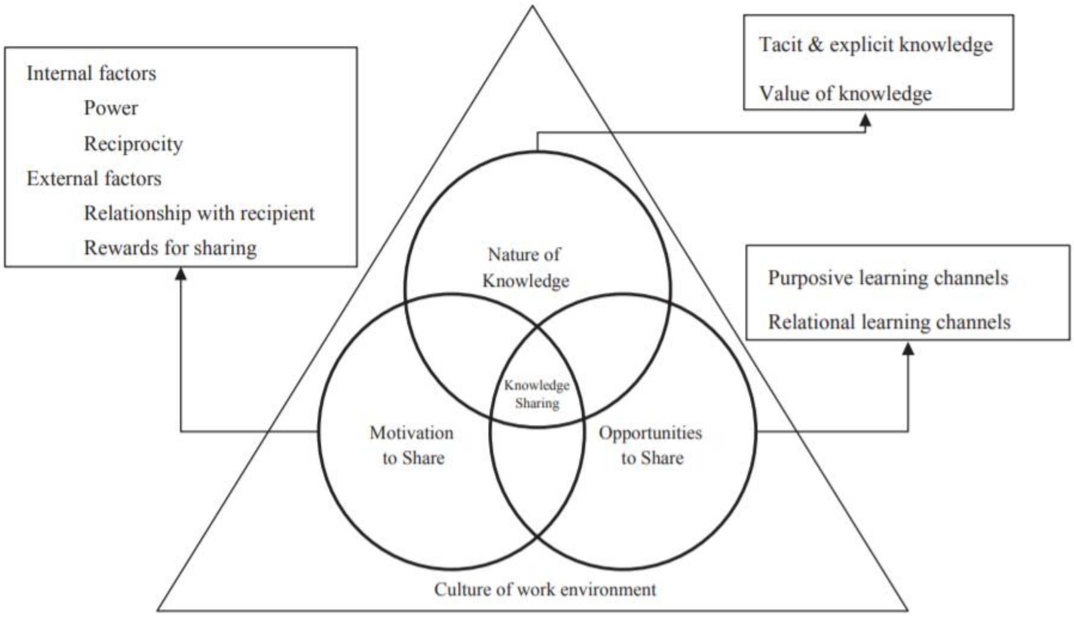

Figure 2. 8: Factors that influence knowledge sharing between individuals within an organisation
Adapted from Ipe (2003)

Ghobadi and D'Ambra (2012) integrated the Competitive Model of Knowledge Sharing and Social Interdependence theory to explain the forces behind high-quality knowledge sharing and propose a framework for predicting effective knowledge sharing behaviours in cross-functional project teams. The framework proposes three dimensions of cross-functional cooperation: cooperative task orientation, cooperative communication, and cooperative interpersonal relationships. They argue that the framework can be used by managers to facilitate problematic knowledge sharing processes and to directly drive effective knowledge sharing behaviours within cross-functional teams.

López-Cuadrado et al. (2012) present a framework based on ontologies, for Business Processes Modelling (BPM) that allows experts to represent and to share their knowledge with other experts utilizing shared and controlled vocabularies. The framework also allows for the execution of business processes represented by the experts.

Matzler and Mueller's (2011) theoretical framework identifies how personality traits impact effective knowledge sharing via goal orientations. They identify two goals; learning orientation and performance orientation, and state that there is a significant positive relationship between knowledge sharing behaviour and learning orientation. On the contrary, a significant negative relationship between performance orientation and knowledge sharing exists. Matzler and Mueller (2011) state "learning-oriented people perceive their and others' capabilities as shapeable and which requires their engagement in knowledge sharing processes, while performance-oriented people regard their abilities as fixed and in the case of negative feedback regarding their activities, they might avoid these situations instead of investing time into learning and knowledge sharing activities."

Fernandez-Fernandez et al. (2010) describe business process modelling as a group of techniques that allow modelling those business aspects necessary for correct performance of the business process applications. The model offers users the capability to model business processes through notations that are agile, easy to understand and design, and capable of providing semantic information about the process.

Drawing from research on achievement motivation and social exchange, Swift et al. (2010) discuss how goal orientations provide a framework for an individual's knowledge sharing by shaping how they cognitively value the cost and benefits associated with sharing their knowledge. They argue that each of the goal orientations is associated with preferences for sharing specific types of knowledge. Their model considers both personal and contextual factors in explaining an individuals' motivation to share their knowledge. It conceptualizes an individual's motivation to engage in knowledge sharing as a function of a cost-benefit analysis within the context of their goal orientation. Goal orientations represent individuals' general tendency to pursue performance or learning goals when they are in achievement situations.

3. Knowledge sharing frameworks that address innovation and competition

Alguezaui and Filieri's (2014) extending enterprise (EE) framework adapted from Browne (1995), discusses challenges related to innovation and competition in new product development in the knowledge economy. The term extended enterprise was coined by Chrysler to define businesses with an extended supply chain composed of thousands of suppliers and globally dispersed distributors. The framework is designed to promote a collaborative innovation advantage derived from collaboration between manufacturers and suppliers in high-tech industries, such as aerospace, automotive and pharmaceutical sectors. The framework describes the adoption of new methods and technologies for the sharing of knowledge, and the outsourcing and offshoring of value-creating activities.

He et al. (2014) state that hyper-competition is characterised by team members' need to out-perform other members on the same team with little concern for the collective benefit. He et al. (2014) highlight how according to the theory of competitive orientation, individuals can learn through the socialisation process, to fit into a workgroup in which they compete with, rather than against to accomplish collective goals. They propose a framework of various factors focusing on team collectivism, within team competition and team empowerment and their impact on knowledge sharing and team flexibility. He et al. (2014) suggest that team development competition and team hyper-competition has an indirect relationship with knowledge sharing and team flexibility through team empowerment.

Pratrap's (2014) framework for performing outsourcing capability seeks to address the importance of knowledge sharing to avoid "outsourcing failure." The framework was proposed to address two challenges in capability outsourcing. The first challenge revolves around the need to access the market for external, specialised and responsive sources of cutting-edge knowledge, and at the same time, ensure that this diverse knowledge base works intimately and passionately for the focal firm. The second dilemma concerns the problem of losing a part of the organisation's informal knowledge sharing mechanism, its wide perceptive ability, its idiosyncratic communication codes and coordination mechanism, every time a process is outsourced. The framework employs a matrix which, taking into account the potential gains and perils of outsourcing, and depending on the particular context which the focal firm finds itself in, informs about the specific facet of the outsourcing capability to be deployed to reap the benefits of outsourcing and mitigate associated risks.

4. Frameworks that focus on knowledge sharing for risk management

Trkman and Desouza (2014) developed an exploratory framework that categorises knowledge sharing risks across multiple dimensions. The framework outlines various kinds of knowledge risks that organisations face by employing a structured approach to knowledge risk management that complements the practised-based approach to knowledge risk management that is presented by Marabelli and Newell (2012). They use a combination of knowledge-based and transaction cost theories to demonstrate how knowledge risks impact knowledge transfer among entities within a team or within an organisation. The proposed framework classifies knowledge sharing risks according to five dimensions: the nature of the collaboration; the nature of the network; proximity; the type of action, and the range of risk. Trkman and Desouza (2014) state that the development of the framework is important in the context of strategic information management for three main reasons. First, the identification of risks is vital for their communication and management in the network. The framework provides a common language that all of the participants can use to describe the basic elements. Second, a proper approach for either proactive or reactive risk management may differ considerably for various types of risk. Third, the potentially prohibitive effect on the trust-building needed for continuous organisational collaboration and knowledge sharing may vary for different types of risk.

Existing knowledge sharing frameworks in the automotive industry can be classified according to:

- frameworks focusing on knowledge sharing in new product development
- framework designed to improve performance through knowledge sharing
- frameworks that focus on knowledge sharing for risk management
- knowledge sharing frameworks that address innovation and competition

This section reviewed knowledge sharing frameworks that have been developed for component development, however, none of the available frameworks address the sharing of knowledge relevant for component integration processes in the context of the automotive industry and, how sharing of knowledge could potentially improve the cybersecurity of modern connected vehicles. Nonetheless, these frameworks provide input to the development of the proposed research. The lack of frameworks that explore knowledge sharing in component integration highlights the need for a knowledge sharing framework and justifies the path that the research took.

2.9 Lessons Learnt from the literature review

The review introduced foundations of knowledge and presented a selection of the many knowledge concepts. The concepts of knowledge management and knowledge sharing are presented incorporating an overview of the various approaches that have been developed to guide scholars and practitioners in knowledge management research and practice. The section also identified the key knowledge processes as determined by a range of scholars. Of these processes, knowledge sharing forms the basis of this research and further elucidation was provided through a more in-depth view of this process.

The review presented several important approaches to knowledge sharing and highlighted a range of factors that have been identified in the literature as pertinent to the knowledge sharing domain. The identification of useful elements and concepts to be considered in the development of the proposed framework was achieved by identifying elements of best practice within the reviewed frameworks. Overall, the majority of academic papers and industry publications present aspirational frameworks for implementing knowledge sharing, with sparse theoretical and empirical underpinning. The frameworks do not consider the challenge of knowledge sharing in the integration of components for connected vehicles. The lack of industry-specific standards, best practices and guidelines, and the lack of knowledge sharing frameworks focused on component integration processes demonstrates the importance and need to improve the security of vehicles through the sharing of knowledge of relevance for component integration processes.

2.10 Chapter conclusion

The chapter presents an extensive review of the key points of focus pertaining to the research topic and presents evidence of the literature gaps identified in Chapter 1, section 1.3. It identifies the need for a greater research focus on knowledge sharing in the automotive industry, specifically in the integration of components manufactured by a plethora of globally dispersed component suppliers. The chapter introduces the foundations of knowledge, presenting a selection of knowledge concepts whilst incorporating an overview of their importance and background in vehicle manufacturing. A brief history and the current state of the industry is presented highlighting the changes that have occurred in the sector as a result of the trend toward connectivity. Knowledge sharing challenges that are a result of the transformations experienced by the sector are presented and discussed thereby, supporting the relevance and need for the research topic.
The review introduces and, provides an overview of cybersecurity management. The section also provides a discussion on the various definitions of cybersecurity from different scholars and practitioners. It defines cybersecurity and cybersecurity knowledge in the context of the automotive industry. The concepts of cybersecurity knowledge and cybersecurity knowledge sharing are introduced. Component integration challenges that introduce cybersecurity challenges are discussed before the importance of sharing knowledge related to component integration, which forms that basis of this research is discussed.

The review provides an overview of the various knowledge sharing frameworks that have been developed to guide scholars and practitioners in knowledge management research and practice, with special attention afforded to knowledge sharing frameworks that are specific to the automotive domain. The frameworks discussed highlight knowledge sharing at the organisational, team and individual levels in different manufacturing processes. However, none of the available frameworks adequately consider and address the sharing of component integration knowledge in connected vehicle manufacture. It is clear as demonstrated by the review that there is no unified approach to component integration knowledge sharing in the automotive industry, however, this thesis does not advocate for a prescriptive approach for knowledge sharing within the auto-domain. The challenge is to establish a generic framework with appropriate theoretical underpinning that is understandable and provides guidance for management to consider in component integration approaches as a potential factor for improving the security of modern connected vehicles.

This review of the literature reinforces the model in Figure 1.1. The three domains of cybersecurity management, knowledge management and the automotive industry all feature strongly in the extant literature. However, they are often considered in isolation from one another whereas their significance can only be seen fully when they are considered together, as in the red area of Figure 1.1. The remainder of this thesis describes how the lessons learnt from the literature were applied to the design of a knowledge sharing framework that focuses on component integration in the automotive sector. Accordingly, the next chapter discusses a wide range of research philosophies and methodologies to aid in the research data collection and data analysis for the creation of a knowledge sharing framework.

Chapter III

METHODOLOGY

3.1 Introduction

This chapter guides the reader through the research methodology adopted within the study, and the design of such a framework. It first outlines the philosophy that underpins the approach, discussing the researcher's interpretivist stance and the consequent choice of a multi-method research approach. The chapter also provides an overview of the data collection methods that the study employs, as well as the means used to analyse the data. Additionally, the chapter outlines the research design, a methodological framework, and the advantages and limitations of the chosen research method to provide valid and reasonable conclusions.

3.1.1 The need for a methodological approach

The key issues of this study, as discussed in the previous chapters, include the sharing of cyber-related information for secure component integration processes. To understand how these issues have been studied and reported, it is of great importance that the overall strategy adopted for the collection and analysis of data is outlined. This will allow the reader to consider the relevance of the strategies and methods and their analysis to address the research questions.

To effectively collect data with richness and information depth, that identifies how a complex set of circumstances come together to produce a particular manifestation, the use of a data collection strategy that is versatile and deploys many methods of gathering information is needed, and hence the adoption of a multi-method research approach (Erickson 2012). This chapter also explains why a multi-method research approach has been chosen and follows the viewpoints of Silverman (2016) providing answers to the following questions:

- What are the theoretical assumptions that shaped the data collection and analysis reported in this study?
- What are the factors that influenced the researcher to choose to work with these particular data?
- How did the overall strategy adopted, and the research design and techniques used by the author affect the conclusions of the research and, how can the author still generalise from his analysis?

These questions will be partially answered in this chapter, Chapters IV and V will then focus on a detailed description of the data collection and data analysis processes. Chapters VI and VII will focus on presenting the results of the data collection and analysis, as well as the development of the framework. Accordingly, this chapter is structured as follows:

- Section 3.2 discusses key concepts that support the conduct of this study.
- Section 3.3 presents theoretical assumptions that determine the research.
- Section 3.4 discusses the approaches taken to collect and analyse the study's data.
- Section 3.5 presents the chapter conclusion.

3.2 Key concepts supporting the conduct of this research

Defining the author's theoretical assumptions and the main issues affecting the data collection and analysis processes would be difficult without referring to terms such as the author's mental model of research; the concepts related to the sharing of knowledge in component integration processes; theories supporting the study of such concepts, and the methodologies and methods used. A review of the literature shows there is no general consensus as to how these terms are understood and used. This section explains how these terms relate to one another in the context of this research and how they are understood in the remainder of the thesis.

Mental models

A researcher's understanding of the reality surrounding phenomenon under investigation influences the research process. Mental models are internally held and are typically the first ideas that are formed in developing the research, however, they are not always made explicit in the research design (Magzan 2012). This research, like most other research, is influenced by the researcher's understanding of the reality surrounding the problem. The authors' involvement with the automotive industry, specifically, automotive cybersecurity, has shaped his experiences, beliefs and views. This will have an impact on this research. This understanding is referred to in the literature as mental models. Although the concept of a mental model has been researched in various disciplines, the definition of what a mental model encompasses remains indistinct. However, the author adheres to Rook's (2013, p.38-47) definition of mental models as "a concentrated, personally constructed, internal conception, of external phenomena (historical, existing or projected), or experience, that affect how a person acts".

Models are also referred to as research paradigms. They provide an overall framework for how reality is viewed (Silverman 2016). A research paradigm is a set of fundamental assumptions and beliefs as to how the world is perceived, which then serves as a thinking framework that guides the behaviour of the researcher (Wahyuni 2012, Marshall & Rossman 2014). A model, therefore, describes the following:

- Epistemology: the philosophy of knowledge or how we come to know (Ferber & Harris 2013)

Epistemology refers to the theory of knowledge, more specifically, how we acquire knowledge. Knowledge is the driving force behind research and, it is known through the subjective experiences of people (Creswell 2013, Pritchard 2013). To understand the complexity of the phenomenon under investigation, the research was conducted within the context in which the phenomena occurs. The research was conducted within the automotive industry; this provided the researcher with a clear understanding of the environment affected by the phenomena.

- Ontology: the philosophy of reality and what there is to know about the world (Heywood 2012)

Ontology involves the philosophy of reality. In this research, it is considered that there are multiple realities that need to be understood. The researcher sought to gain different perspectives on the sharing of knowledge related to component integration processes; the perspectives of OEMs involved in integrating components from their supply chain, suppliers that integrate components from other suppliers, the perspectives of automotive knowledge experts involved in component integration strategies, all different perspectives embracing the same challenge.

Concepts

Concepts are clearly specified ideas deriving from a particular model that provides a general sense of reference and guidance in approaching an empirical stance by assisting in identifying and defining what needs to be searched for, where to search, with whom and in what relationships (Silverman 2015). Once the researcher had established a mental model, the concepts that emerged are "knowledge management", "knowledge sharing", "cybersecurity", "component integration", and "automotive industry."

Theories

A theory is a set of concepts which are intended to provide a plausible or rational explanation to a phenomenon (Bell et al. 2018). Theories are living entities focused on providing an impetus for research. According to Silverman (2015), theories are mental models of the perceived reality and provide a framework for critically understanding a certain phenomenon.

Methodology

Miles (2015) and Kaplan (2017), noted that the terms "method" and "methodology" are often used interchangeably. However, methodology defines the overall approach taken to research the phenomenon, as well as to the theoretical basis from which the researcher comes. According to Kaplan (2017), methodological choices should be consequential to the researcher's philosophical stance and the phenomenon being investigated.

Methods

Methods are the various means by which data is collected and analysed Bryman (2016). Research methods can either involve qualitative and quantitative techniques, or both and are instruments for collecting the data.

3.3 Theoretical assumptions

The theoretical assumptions in this research are determined by the following:

- The research paradigm (also referred to as the researcher's mental model).
- The research ideas in the field of knowledge sharing in component integration that acted as a starting point of the research.
- The concepts derived from the idea stated above
- The theories supporting the sharing of knowledge in component integration processes

This section aims to define the researcher's theoretical assumptions by outlining each of the component mentioned above.

3.3.1 Research paradigms

The sharing of knowledge of relevance in component integration processes is the primary focus of this study, more specifically, the sharing of information related to secure component integration strategies that obstruct cybersecurity. Chapter 2 outlined the importance of sharing information by OEMs, component manufacturers and other relevant stakeholders in the integration of components for connected vehicles. The automotive industry has transformed due to the trend towards connectivity, and the author understands that this transformation has affected knowledge sharing processes of old. OEMs and component suppliers are now located in different geographical locations and operate in different environments. Each of these locations and environments operate differently and has factors which impact on how knowledge relating to the integration of components is shared. In the author's view intra-organisational, inter-organisational and cross-organisational sharing of component integration-related knowledge can have a significant effect in the cybersecurity of connected vehicles. The author's view is supported by authors in the field of social studies such as Kosher et al. (2010), Checkoway et al. (2011), Zirpoli et al. (2011), Sagstetter et al. (2013), Studnia et al. (2013), and Amin et al. (2015).

3.3.2 Research ideas

During the early stages of the research, the work that was conducted helped the researcher understand the need and importance of sharing knowledge related to component integration processes for potentially addressing cybersecurity challenges in connected vehicles. This understanding led to the definition of the main research question. However, other ideas also emerged from the early work carried out. They include:

- The sharing of knowledge in component integration is a process that can benefit from lessons learnt from other sectors of the industry were knowledge sharing has been applied.
- Although cybersecurity is still relatively new to the automotive industry, other industries have encountered the challenge of cybersecurity. The automotive industry can learn from such domains.
- Successful knowledge sharing practices will require the support of top management within vehicle manufacturing organisations and organisations that manufacture components for connected vehicles.
- Certain standards and indicators need to be in place to ensure and support the automotive industry with its sharing of component integration-related knowledge practice.

3.3.3 Research concepts

The key concepts that emerged from the set of ideas outlined above and therefore represent the key points around which this research was conducted include knowledge, knowledge management, knowledge sharing, component integration processes, cybersecurity and connected vehicles in the automotive industry. This was supported by the literature review in Chapter 2 and these concepts became part of the main research problem.

3.3.4 Theories

The focus of this research was defined by combining a review of relevant literature with empirical work on the research topic of knowledge sharing. Bell and Bryman (2018) state that instead of theories, the literature can inform the generalisation of research questions in what the authors perceive to be a relevant research topic. Thus, appropriate background literature on existing approaches to knowledge sharing, specifically the sharing of component integration-related knowledge in different areas and organisations and their limitations were the equivalent to theories supporting the identification of the research problem.

3.4 Methodological approach to data collection and analysis

The theoretical assumptions of the researcher and the practical issues which will be discussed in the body of the thesis informed the data collection and evaluation processes carried out to address the main aim of the research study.

This section discusses the approaches taken to collect and analyse data using the terms; research strategy, research design and research methods as described in section 3.3.

3.4.1 Research strategy

All research is guided by a defined research methodology. The methodology prescribes the methods by which research data are gathered and analysed. To achieve research aims, every research must first identify and use suitable tools and techniques. These tools may either be qualitative or quantitative in nature. Qualitative research is primarily exploratory research. Silverman (2015) emphasize that to realise the benefits of qualitative research methods, understanding and listening to individuals, societies and organisations affected by the phenomena is required. According to Miles et al. (2014) qualitative research is a craft that assists in developing concepts, insights and understandings from patterns in the data rather than collecting data to assess preconceived theories. Quantitative research is used to quantify the problem by way of generating numerical data or data that can be transformed into usable statistics (Brannen 2017). Quantitative techniques conclude by proving or disproving a specific theory that was tested (Yilmaz 2013).

The nature of the research problem coupled with the epistemological and ontological orientations of the study, backed by extensive literature review, influenced the choice to employ a qualitative methodology or research strategy. The main reasons supporting this argument, included as outlined by Bryman (2016) are:

- The research is not involved with the testing of existing theory as quantitative research does. Emphasis is placed on the use of existing theory already available in the literature relevant to knowledge management and knowledge sharing.
- The author sought to understand the sharing of knowledge in automotive component integration processes from different organisations using more than one source of data and, applying a variety of qualitative analytical methods. This approach permitted data triangulation and, to a lesser extent, methodological triangulation, thereby promoting reliability and validity.
- The research focuses on the generation of findings that are likely to contribute to the development of new theories related to how component integration processes can be improved through knowledge sharing in connected vehicle manufacture.

3.4.2 Research design

Empirical research methods exist in both qualitative and quantitative divides, and Yin (2011) suggests that within social science, five major research methods can be distinguished: experiments, surveys, archival analysis, histories and case studies. Within qualitative research Creswell (2013) distinguishes five research traditions: the historian's biography, the psychologist's phenomenology, the socialist's grounded theory, the anthropologist's ethnography and, the social scientist's case study. Myers (2019) discusses action research, case study research, ethnographic research and grounded theory research. Each of these research methods has its focus, discipline origin, and the method of data collection and analysis. The biography method describes the life of an individual, the ethnography method describes and interprets a cultural and social group, the case study method develops an in-depth analysis of one or more cases, the action research method is focused on solving actual problems by actively participating and the grounded theory method develops a theory grounded in data from the field.

None of the methods discussed above are adequate for the type of research proposed. The research seeks to understand the sharing of knowledge relevant for component integration processes in the automotive sector from different organisations using more than one source of data and, applying a variety of qualitative analytical methods. This motivated the consideration of a multi-method research design, which would permit data triangulation and, to a lesser extent, methodological triangulation, thus, promoting reliability and validity. A key rationale behind the choice of a multi-method research design is the explanatory nature and form of the research questions coupled with the sensitive nature of the study. Additionally, the use of a multi-method research approach allows for the exploration of potentially multiple perceptions of the phenomenon within the automotive sector, a characteristic that further re-enforced the validity of the research method.

As described before, the scope of methods is limited to qualitative research methods. The research aims to explore whether the sharing of cyber-related information in component integration processes can potentially improve the cybersecurity of connected vehicles, grounded theory is not appropriate. Although case study would be an option (spending a significant amount of time in a single organisation setting, while immersing oneself in the organisation's knowledge sharing practices), just like an ethnography method, however, this research does not focus on a single organisation's knowledge sharing practices, furthermore, available time and resources do not permit for either case study research or an ethnography method. Action research is not appropriate, because this research does not intend to contribute to the practical concerns of people in an immediate problematic situation. Multi-method research was chosen as this method best matches the capability of the researcher and the requirements of the research situation.

3.4.3 Research methods

Given the novelty of the research study and the secretive nature of the auto-industry, multi-method research is an appropriate fit for the study as the phenomenon under investigation does not clearly fit within one research method. The study also requires multiple data sources to answer the research questions; a single data source will be inadequate for generalising exploratory findings and results analysis. Furthermore, multi-method research involves philosophical assumptions that guide the direction of data collection and analysis in many phases of the research process (Creswell et al. 2011). As a research approach, multi-method research can be defined as:

> *"A detailed investigation that is based on a combination of complementary empirical research methods that encompass a wide range of research methods, each conducted rigorously and complete in itself. The results are then refined to form a complete whole. The intention is that the complementary nature of the research methods compensate for weaknesses inherent in mono-methods. It is argued that multi-method research approaches provide potential benefits in terms of more robust conclusions, development and investigation questions, and increased understanding of the research findings" (Wisdom & Creswell 2013).*

Multi-method research is an approach that breaches the qualitative-quantitative research divide, and according to Morse (2016) and Hammersley (2017), can be practised in both camps. It is a research approach that takes a non-purist or compatibilist stance, this allows for the mixing and matching of design components which, together, offer the best chance of answering the questions posed by the phenomenon under investigation.

The study makes use of semi-structured interviews and online open-ended questionnaires to collect data. This process was informed by the research questions and the relevant background literature on knowledge sharing in automotive component integration processes. The combination of semi-structured interviews and questionnaire survey data collection techniques enabled methodological triangulation and a richer understanding and analysis of the concepts of knowledge sharing. According to O'Cathain et al. (2010) and Denzin (2012), this triangulation of research methods not only promotes a leading strategy for starting a research study, but it also stimulates a follow-up strategy for widening the enquiry and rounding out the research study. Terrell (2012), Fetters et al. (2013) and Venkatesh et al. (2013), argue that the uncertainty of a proposition is greatly reduced when the proposition and its interpretations are confirmed by two or more independent research approaches. The strengths of multi-method research demonstrate that it can and should qualify as a suitable research design for the phenomenon under investigation.

Reliability, validity and credibility issues relating to the study are addressed in Chapter 4 section 4.4. The study adopts data collection methods that fall within qualitative interactionism. According to Corbin et al. (2014), qualitative interactionism gains knowledge through the use of authentic experiences, by employing semi-structured interviews and open-ended questionnaires. Data collection methods and analysis approaches are discussed in the sections below.

Semi-structured face-to-face interviews

Interviews are a ubiquitous way of collecting data (Friend & Caruthers 2015, DiCicco-Bloom 2016), and this study employs semi-structured interviews as one qualitative data collection method. There are three generic forms of interviews according to Corbin et al. (2014), Brinkmann (2014), and Merriam and Tisdell (2015), which comprise of unstructured, semi-structured and fully structured interviews. Corbin et al. (2014), Brinkmann (2014), and Merriam and Tisdell (2015), further state that the different interview approaches are linked to a certain extent, to the type of inquiry being conducted and the depth of response sought to address the inquiry. The principal objective for employing semi-structured interviews is to collect expert experiences and views, to gather data that provides reliable, comparable, genuine and trustworthy insight into people's experiences regarding the phenomenon under investigation (Silverman 2015). Nagy et al. (2010) and Brinkmann (2014) state that when researching sensitive issues whereby confidentiality, anonymity and a more intimate setting for data collection is important, such as this study, then semi-structured interviews are better equipped.

Semi-structured interviews potentially allow the researcher to take advantage of social cues (Irvine et al. 2013). Social cues such as voice, intonation, body language etc. of the interviewee provides the interviewer with a lot of extra information that can be added to the verbal answer. This is very important to the study as there is a potential participation reluctance due to the nature of the phenomenon being investigated. The ability of semi-structured interviews to permit respondents to provide much more detailed information about their interactions and experiences with the phenomenon absent the rigidness offered by unstructured interviews paves the way for follow-up questions tasking the respondent to provide more valuable data (Brinkmann 2014, Mann 2016), thus making the research approach suitable for this investigation. Additionally, more often than not, information obtained from semi-structured interviews provides not just answers and the reasons for the answers, but an opportunity for further probing and learning (Rowley 2012).

Galletta (2013), McIntosh and Morse (2015) suggest that semi-structured interviews can be viewed as a special kind of knowledge-producing conversation, or as a meaning-making partnership where the interviewer and the interviewee co-create knowledge in an interview setting, thereby co-constructing reality. The semi-structured interview approach employed by this study targets senior management personnel within the study population. The roles vary from company directors, chief executive officers, project managers and, department managers. Targeting such a range of roles permits the investigation and collection of a variety of perspectives, opinions and understandings regarding the sharing of knowledge in automotive component integration processes. Such a diverse group of study participants not only allows the researcher to compare different participant views but also permits and develops better approaches that help to identify emergent patterns and themes (Brinkmann 2014).

However, as with most data collection approaches, semi-structured interviews do possess some weaknesses which are highlighted by Doody and Noonan (2013) and Creswell (2017), who state that although semi-structured interviews provide rich and thick qualitative data which reduces researcher bias, it can be quite difficult to filter through all the narrative responses to accurately reflect on the overall interview activity. Due to the large amounts of data acquired via semi-structured interviews, coding issues are a common weakness associated with semi-structured interviews, extracting similar codes or themes from interview transcripts can be a daunting task (Creswell et al. 2017). Another weakness is highlighted by Silverman (2015) who states that social categories such as age, race, gender and class of the interviewer can influence how an interviewee responds, additional factors such as the relationship the interviewee has with the interviewer may affect the participant's responses. These weaknesses are not only practical concerns but are also epistemological and theoretical ones as well.

Online Open-ended questionnaires

The study also makes use of online open-ended questionnaires to gather valuable data from relevant personnel not amenable to semi-structured face-to-face interviews, employed in the automotive industry located in hard to reach areas or being otherwise unavailable for face-to-face interaction. The need to employ online open-ended questionnaires was driven by the geographic nature of the automotive supply chain, the complexity of the phenomenon being studied and the study population. The study population comprises of a society that has internet access and can be labelled "tech-savvy". Due to the novelty and complexity of the study, online open-ended questionnaires are preferable to closed-ended questionnaires because they allow the respondent to express an opinion without being influenced by the researcher (Bryman 2017). They are exploratory in nature, asking for critical thinking and uncut opinions from the participants, thereby providing more detail and depth, revealing the participant's thinking process. Online questionnaires have numerous strengths and potential weaknesses as highlighted by Bryman and Bell (2015), and McGuirk and O'Neill (2016), these are highlighted in Table 3.1 below. One of their main attributes is that they are ideal for gaining information from specialists in a given field, potentially producing information of great wealth that leads to the creation of new ideas and perspectives. They allow respondents partaking in the study to provide a more diverse set of answers, thus avoiding the bias that may result from suggested responses, a bias that may occur in the case of closed-ended questionnaires (Roberts et al. 2014). Their ability to automate data provided justification and reason to use them as a survey modality. This, in turn, reduces time and effort in data sampling and analysis (Sue & Ritter 2012). Online questionnaires are cost-effective when data from a large sample of respondents is required. Online questionnaires were the preferred choice compared to postal questionnaires because of the geographical nature of the automotive industry, the time and resources available to the researcher, and the high non-response rates associated to postal questionnaires (Van Gelder et al. 2010).

Table 3. 1: Comparison of strengths vs weaknesses of online questionnaires

Strengths vs Weaknesses of Online Questionnaires		
Major Strengths		Major Weaknesses
Global Reach		Perception as Junk Email
Flexibility		Privacy Issues
Speed and Timeliness		Low Response Rate
Ease of Data Entry and Analysis	Online Questionnaire Attributes	Technological Variations
Low Administration Cost		Impersonal
Ease of Follow-up		
Controlled Sampling		
Fast Response Rates		

Although online questionnaires offer many advantages, they do, however, in most cases encounter data sampling issues. According to Harris and Brown (2010), and Krosnick (2018) the validity of data obtained from online communities raises concern, as the characteristics, basic demographic variables and credentials of people in online communities and groups may be questionable, however, these sampling problems can be controlled to various degrees depending upon the data collection techniques employed. Other disadvantages of online questionnaires include the design, implementation and evaluation of online data (Fink 2015), however, modern software packages and applications alleviate the burden, making online open-ended questionnaires a solution for data collection targeting a substantial respondent sample.

Data analysis

Qualitative data analysis approaches come in different forms and vary depending on the nature of the research phenomena and have been widely debated (Silverman 2011, Neuendorf 2016, Bryman 2017). Qualitative data acquired through online open-ended questionnaires are analysed through the use of Nvivo (Chapter 5, section 5.4). Semi-structured interview data is analysed through the use of qualitative content analysis (Chapter 5, section 5.2). As a research strategy, content analysis is a suitable analysis modality for this study as it allows for the testing of theoretical issues to enhance understanding of the acquired data (Elo et al. 2014). Data analysis is discussed in more detail in Chapter 5.

Participant selection criterion

The selection of participants in this study is conducted using criterion-based or purposive sampling. According to Symon and Cassell (2012), qualitative criteriologists debate on the appropriateness of purposive sampling over criterion-based sampling, however, for this study, and because all sampling is purposive, the term purposive sampling will be used (Bryman & Bell 2015). Miles et al. (2014) identify seven strategies of purposive sampling; maximum variation sampling, homogeneous sampling, typical case sampling, deviant case sampling, total population sampling, critical case sampling and expert sampling. This study employs the use of expert sampling. Expert sampling is a positive tool to use when investigating new areas of research and when selecting candidates across a broad spectrum relating to the topic of study (Etikan 2016). According to Miles et al. (2014), the relevance of each strategy is reliant on the study's objectives, purpose and questions. The purposive sampling strategy employed by the study was implemented before the data collection phase was begun. The choice to employ purposive sampling is driven by the principal aims of the study and, existing knowledge and theories about the study population.

Appropriate number of interviews

According to Mason (2010), Dworkin (2012), Baker et al. (2012), and Marshall et al. 2013) qualitative research studies do not place too much emphasis on the number of interviews. There are no guidelines or requirements for sample size, however, Mason (2010) states that the purpose of the inquiry, what is deemed to be useful and credible, available resources and time, determine the sample size. The premise for this relative lack of focus on sample size appears sound and valid according to Marshall et al. (2013) who state that the observational and analytical capabilities of the researcher contributes to the reliability, validity and information richness of the phenomenon under investigation than the sample size. However, Francis et al. (2010) state that in a qualitative inquiry sample sizes should not be too small such that it is challenging to achieve saturation. Due to the novelty, complexity, sensitivity of the research study, and the potential reluctance of industry to participate, the size of the sample is considered less important than locating and selecting participants that are willing to provide credible and meaningful data that will aid the study. The deliberative and flexible purposive recruitment approach focused on selecting participants with adequate understanding, experience and exposure in the sharing of knowledge within the automotive continuum, automotive component integration, automotive cybersecurity and, automotive component manufacturing.

3.4.4 Overall research process

A research plan consisting of a research design was devised once the research questions had been defined, and the theoretical assumptions and issues affecting the data collection had been fully understood. A research design also known as a plan for investigation provides a framework for the collection and analysis of data. The research design was continually evolving as learning and understanding developed. Creswell (2013) states that a research design is the logical sequence that connects the empirical data to a study's initial research questions and ultimately, to its conclusions. It includes specific design features from the broad philosophical and theoretical perspectives to the quality and validation of a study. Creswell (2013) asserted the importance of illustrating the research approach as an effective strategy to increase the validity of social research. Figure 3.2 below provides an overview of the overall research process, showing how the investigation was conducted. The research process is identified as having various stages that exist in three key stages.

The first stage; establishing the research problem, began with a description of the different elements of the literature review that were required to place the research in context. The stage identified the initial idea starting with a preliminary research of the chosen area. A review of the literature in knowledge management, knowledge sharing, automotive cybersecurity and component integration, provided clarification of the wider issues and led to the research questions and subsequently the aim and objectives of the study. This stage also established the need for a knowledge sharing framework as a potential factor for improving the cybersecurity of connected vehicles.

Stage 2, research methods, was concerned with incorporating the elements identified in the initial stage into a system capable of supporting the sharing of relevant knowledge in automotive component integration processes. Data collection and data analysis was conducted at this stage and contributed to the formulation of the conceptual framework. The study's data was gathered through the use of semi-structured interviews and an online survey instrument (these are discussed in detail in subsections 3.4.3.1 and 3.4.3.2). Component suppliers, OEMs, knowledge experts in automotive manufacture are the data sources for the study.

The third and final stage; framework development and evaluation were concerned with the formulation of the conceptual framework, undertaken through an iterative cycle of development, critique and improvement. This phase of the study took criteria and dimensions identified during the data collection and analysis stages and applied them into the construction of the conceptual framework. The role of the development phase was to construct a model based on the data provided by the study's respondents and, improve the framework's initial design based on the study's evaluation phase.

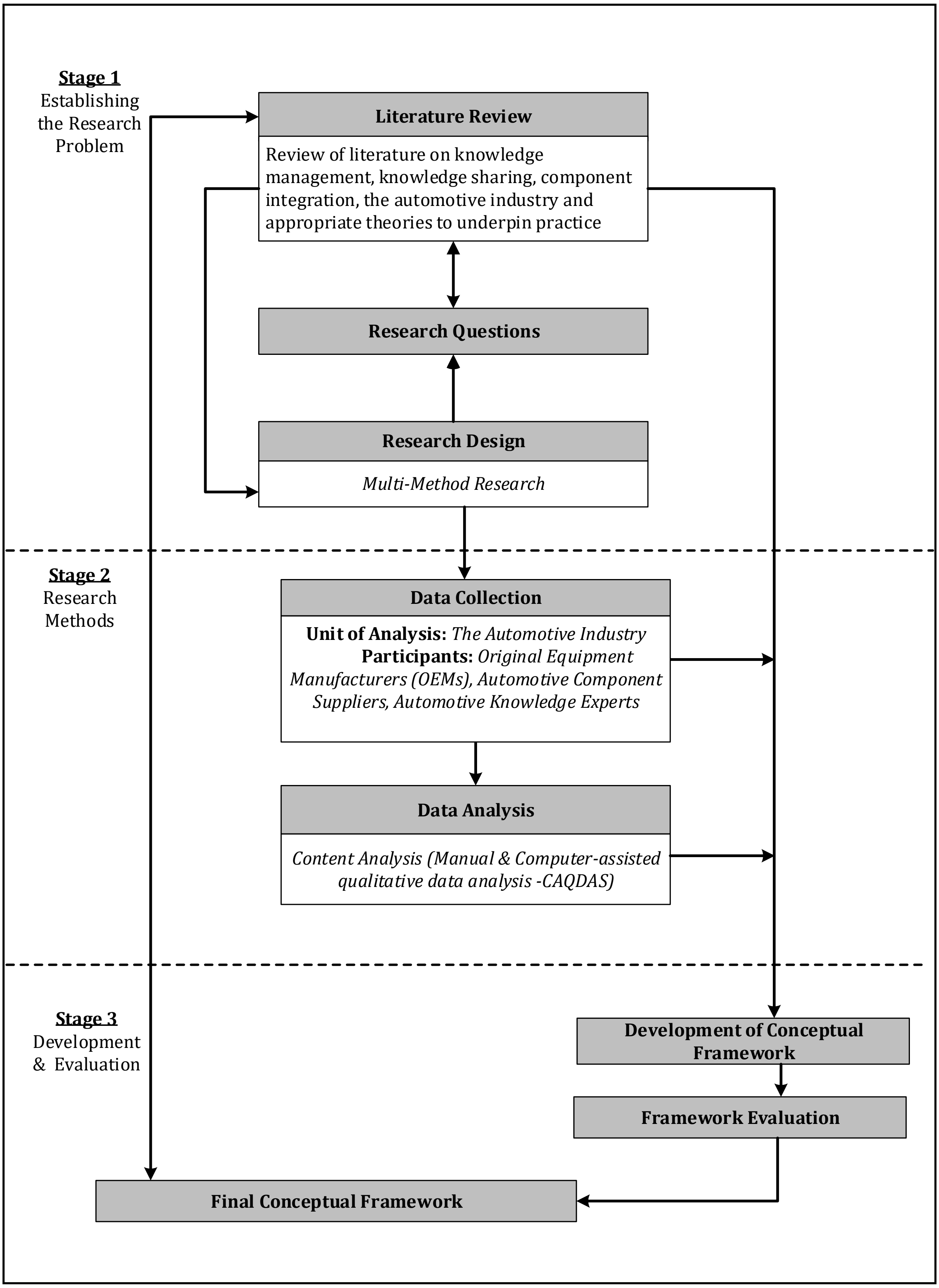

Figure 3. 1: Overview of the research process
Source: Author (2018)

3.5 Chapter conclusion

This chapter described the methodological characteristic of this research. The research is qualitative in nature and it is based on qualitative interactionism. It employs a multi-method research approach because it validates data and results by combining a range of data sources and methods (triangulation), allowing for the discovery of fresh or paradoxical factors that stimulate further work and expansion (creativity), permitting a widening of the scope of the study to take in contextual aspects of the research. The following chapter focuses on the study's data collection approach.

Chapter IV

DATA COLLECTION

4.1 Introduction

The main aim of this section is to describe the data collection processes that enabled the creation of a framework for sharing knowledge related to component integration processes in the automotive industry. The description of the data collection process will begin with the identification and selection of participants in section 4.2. Section 4.3 reports on data collection methods implemented in this study. Ethical, reliability, validity and bias considerations are discussed in section 4.4 before the chapter conclusion in section 4.5.

4.1.1 Overall data collection process

In line with the focus of the research (Figure 1.1) and, the findings of the review of the literature on cybersecurity and knowledge management in the automotive sector, data was collected in two phases. Phase one of the data collection process was exploratory and primarily focused on cybersecurity management. The purpose of the first phase of data collection was to develop a better understanding of the phenomenon under investigation, ensure the relevance of the research problem, formulate the final research questions, triangulate findings from the literature, and elicit preliminary requirements for developing a conceptual view of the solution.

From the preliminary analysis of data collected at phase 1, the key issue that emerged which required further investigation was that of cybersecurity knowledge within the industry. This necessitated further investigation, which was carried out under phase 2. Given the relevance of knowledge management practices for cybersecurity management in the automotive industry, the rationale behind the second data collection phase was to gain a better understanding of the sharing of knowledge of relevance for component integration processes. The two data collection phases complement each other in providing the basis of the research's contributions. The two phases of the data collection process used a similar methodological approach, as detailed in the following sections.

4.1.2 Data collection methods

Data collection methods and techniques differ subject to the nature of the phenomenon under investigation, and research goals to be achieved (Christensen et al. 2011). Other differences exist in reliability, validity, flexibility and, cost of resources required to collect the data. Data collection methods and techniques must be conducted in the context of the research goal (Bryman & Bell 2015, Creswell & Clark 2017). In this study, the research objectives drive the formulation of the research questions, which in turn determine the research design, which then, in turn, dictates the choice of data collection techniques. According to Neuman (2013), Marshall and Rossman (2014), and Glaser and Strauss (2017), data collection techniques can be grouped into two categories: qualitative and quantitative. This research adopts a data collection method that falls within qualitative interactionism. Qualitative interactionism gains knowledge by employing semi-structured interviews and questionnaires on how individuals and societies are shaped by interacting with a given phenomenon (Silverman 2015). The research achieved methodological triangulation through a combination of semi-structured interviews and questionnaire survey data collection techniques, which in turn provided a richer understanding and analysis of the concept of knowledge sharing in component integration approaches within the automotive industry.

4.2 Identification and selection of participants

The research's target audience is senior management; therefore, a deliberative and flexible purposive recruitment approach was employed to recruit a diverse range of senior management who were "*information-rich*" on knowledge sharing and component integration in the automotive sector (Ritchie et al. 2013). To deliberately seek out participants at both ends of the spectrum (component design, development and integration), and to ensure that all viewpoints are adequately represented, the recruitment approach took into consideration the context and the individual. The selection of the research's target audience was not restricted to a particular geographical or socio-economic context. Participants were recruited from automotive component manufacturing organisations, original equipment manufacturers (OEMs), and knowledge experts from the auto-domain. The respondents that assisted with the study were selected because they met the specific requirements sought for the research.

Participants were recruited from the following key areas:

- Software Engineering, Testing and Software Integration
- Component manufacture and integration
- Component integration knowledge management
- Automotive cybersecurity and diagnostics
- Automotive systems development and integration

- Automotive cybersecurity knowledge management
- Automotive knowledge sharing/management

Participants selected to assist with the research study had to meet the following requirements:

- Be employed in the automotive industry.
- Provide consent to either take part in the semi-structured interview or questionnaire survey.
- Be actively involved with connected vehicle manufacturing or connected vehicle component manufacturing, or
- Be involved in knowledge sharing approaches or management and/or were involved in knowledge transfer processes in the automotive industry or,
- Their employer/organisation had to be involved in connected vehicle development research, and/ or automotive cybersecurity research.

4.2.1 Participating organisations

This section provides a brief description of the organisations that participated in the study.

Company 1: one of the leading global suppliers of technologies for the automotive market, which provides more connected solutions for connected vehicles than most component manufacturers. One of the main reasons for selecting personnel from Company 1 for the study was because it manufactures connected automotive components prone to cyber-attacks such as ECUs, infotainment systems and vehicular telematics technology. Besides being one of the world's largest and most diversified automotive parts manufacturer, it employs personnel with skill and experience in component integration, software integration, automotive software development and, software testing and validation.

Company 2: one of the leading global suppliers of automotive technology and services. It offers the automotive industry innovative solutions and expertise in connected mobility through its expertise in sensor technology, sensor software, and services. Company 2 services most of the OEMs that are leading in the connected vehicle and autonomous vehicle development, making personnel from Company 2 suitable for the research study. Employees at Company 2 involved with connected component manufacture are aware of cybersecurity policies and procedures demanded and employed by the various automakers that the company services.

OEM 1: a multinational automotive company that focuses on designing and building internet-enabled and connected vehicles. It is one of the largest vehicle manufacturers. OEM 1 is a listed member of the Alliance of Vehicle Manufacturers who created ISAC (Information Sharing and Analysis Centre) (Wilson et al 2010, Auto-ISAC 2016). ISAC's aim focuses on providing security for communication systems and user data by collecting, cataloguing and sharing threat information and vulnerabilities with members (Choucri et al. 2016). OEM 1 is heavily involved in automotive research with plans of launching a state-of-the-art technology research hub that aims to advance connected and autonomous vehicle research by combining automotive expertise nationally and internationally, providing a unique resource capability along with an environment to foster collaboration, cohesion and cross-fertilisation of cybersecurity knowledge. Personnel involved with, or working on cybersecurity projects, system and vehicle integration projects, automotive software engineering, in-vehicle security, automotive infotainment and Telematics, and information security were recruited for the research.

OEM 2: one of the world's leading vehicle manufacturers in the field of technology. OEM 2 is a member of the Alliance of Vehicle Manufacturers (Wilson et al 2010, Auto-ISAC 2016). The organisation maintains an educational system for basic technical skills delivery that ensures a higher quality of engineering than is usual in the production of vehicles. The organisation has been involved in automated driving and intelligent driver assistance research since 2000. Employees from OEM 2 with skills and experience in in-vehicle security and diagnostics, automotive software design and development, component and software integration, and vehicle information security were approached to participate in the research study.

Knowledge experts: Viewed as the gatekeepers of knowledge, this group comprised of personnel employed in academia engaged in teaching and working with leading manufacturers in delivering automotive engineering excellence, members of national councils that help to inform legislation and the formation and amendments of automotive cybersecurity standards such as ISO26262, and employees working for automotive consulting organisations involved in knowledge sharing initiatives.

4.2.2 Selection criterion

Participants were chosen because they possess particular skillsets and experiences which enable a detailed exploration and understanding of the phenomenon under investigation. Members of the sample were selected with a purpose to represent a type in-relation to the key criteria's set out in Chapter 4.2 above. This was done to address two principal aims. First and foremost, to ensure that all significant areas of the subject matter are addressed (Ritchie et al. 2013, Bryman & Bell 2015), and secondly, to ensure, that within each significant area of the subject matter, some degree of diversity exists, so that the breadth of impact of the characteristics concerned can be explored.

4.3 Methods for collecting data

The following section discusses the methods (semi-structured face-to-face interviews and online questionnaires) employed to collect data from senior management employed in the automotive domain.

4.3.1 Semi-structured interviews

A draft list of questions relating to the research study was designed and compiled before the interview process began. The questions were then grouped into three sets, one for participants employed by OEMs, a set for participants employed by component manufactures and a final set for knowledge experts employed in the automotive domain. The reasoning behind the creation of separate although overlapping question sets is because the three categories, although all affected by the phenomenon under study, do not face the same challenges. The questions were passed to the researcher's research team, to check if they satisfied the research's aims and objectives. The interview protocol and the three sets of questions were then refined from the feedback provided by the researcher's research team.
To test the interview questions and to improve the researcher's existing interviewing skills, pilot interviews were carried out (Jacob et al. 2012, Galletta 2013, Brinkmann 2014, and Creswell 2017). Emails were sent to potential participants requesting their participation in the research study. To ensure that the respondents were clear about the interview process and that they fully understood why they had been selected for the study, the interview request email contained a participant information sheet that clearly outlined the aims and purpose of the research and interview. The interview dates, place of interview and interview timeslots were arranged taking into consideration the respondents' work and life commitments. This was to ensure that postponements were reduced, and cancellations were avoided. Once the respondent had agreed to participate, interview arrangements were then made either via email or by telephone. The interview time slots were scheduled according to the respondent's availability and convenience. The interviews lasted between 40-50 minutes and were all conducted at the respondent's place of work. Before commencing the interview process, a signed copy of the participant's consent form was obtained. This was important because it provides proof that the respondent was a willing participant in the study, and it also informed the interviewer as to whether the respondent was comfortable with their true name being used in the research study.

To build a good rapport, the initial interview process began with an introduction and a brief background about the researcher, the university associated with the research, the nature of the research (in non-academic jargon), the research's ethical considerations, the interview approximate duration, how the data will be used, stored, disseminated, and whether the information will be attributed or anonymised. At the end of the interview, participants were asked if they wanted to be informed of the outcomes and findings of the research when the study concluded.

The interview process

Permission to record the interview sessions was obtained verbally and via the consent form from each respondent. Harvey (2011), Marshall et al. (2015), and King et al. (2018) state that a major advantage of audio recording in interviews is that it allows the interviewer to engage more with the interviewee. It allows the interviewer to listen to the interviewee and to probe further and ask full-on questions that lead to more valuable information. Harvey (2011) flags the dangers of not employing audio recording devices in interviews and highlights the loss of some qualitative data regardless of how fast the interviewer can write. During the interview process, building a good rapport with the respondents was important. It allowed the respondents to speak freely and to provide important information that led to additional follow-on questions being included in the interview.

Two devices were employed for audio recording, the first was the interviewer's mobile phone, which recorded the interviews via an application that permits the transfer of the audio recordings to an encrypted storage device issued by Coventry University. The second device was an audio recorder provided by Coventry University. The audio recorder also allows for the transfer of the audio files to the encrypted storage device. The choice to employ digital audio recording was influenced by the need to maintain data accuracy, reliability, to ensure that all data could be accurately transcribed and so that the recordings could be made available to support the research's findings and results. Furthermore, the choice to employ two recording devices was to cater for any device malfunctions and loss of power. After the interviews, the audio files were labelled, time-stamped and stored on the encrypted device.

In two cases participants were interviewed by telephone. The content of the interviews was identical to that used in the semi-structured face-to-face interviews. In both cases, the decision to use telephone interviews was that of the interviewee and based on convenience and availability factors. Holt (2010) and Vogl (2013) state that telephone interviews should not be seen as a "second-best option", as in certain circumstances they are the most favourable option. The telephone interviews were recorded, and the recordings stored in an encrypted drive for further analysis.

4.3.2 Online questionnaires

The geographically dispersed nature of the automotive industry and the sensitivity of the study encouraged the use of an online questionnaire. According to McGuirk and O'Neill (2016), online questionnaires have numerous strengths and potential weaknesses as discussed in Chapter 3, however, their strengths outweigh their weaknesses, and this further encouraged their use in the study. The selection requirements for participants were discussed in section 4.2 above. As with the study's semi-structured face-to-face interview questions (Chapter 4, section 4.3.1), a two-phase process was used to design and develop the online questionnaire. Similar to the semi-structured interviews, three sets of questionnaires were constructed for the three participant groups. The online questionnaire was designed and distributed using the online application Qualtrics (Chapter 4, sub-section 4.3.2.3). The questionnaire was designed such that if the respondent failed to provide consent to participate, the survey terminated. Potential respondents were contacted via email to ask if they were willing to participate in the research by completing the online survey. Once the respondent agreed to participate in the study, a participant information sheet and a personalised link to the survey was generated in Qualtrics and sent via email to the participant.

Questionnaire design and development

As highlighted in Chapter 2, the available academic literature highlights a significant lack of sharing of knowledge for component integration processes within the automotive industry. This made the challenge of developing a questionnaire suitable for addressing the research's objectives and aims of the utmost importance. The initial questionnaire development process was based on the review of the limited existing literature in the automotive industry, and knowledge sharing approaches from the computing industry, aviation, maritime industry and the defence sectors. The questionnaire design stage also comprised of knowledge transfer approaches, activities, challenges and attitudes within the automotive industry (Cabigiosu et al. 2013, Teece 2013, Jean et al. 2014, Nonaka & Toyama 2015), component out-sourcing activities and their effects on the sharing of knowledge (Wynstra et al. 2010, Christensen et al. 2011, MacDuffie 2013, Brown et al. 2015). The questions posed by the online questionnaires were similar to the questions in the semi-structured interviews, they aimed at gaining an understanding of knowledge approaches, and current component integration strategies for the connected vehicle. Appendix 9 provides a sample of the questionnaires. The questionnaires consisted of five sections:

Section one: this section requested the respondent's consent to participate in the study. It also checked to ensure that the participant was fully aware of what the study was about, and how the collected data would be used. This section comprised closed questions.

Section two: this section contained a mixture of open-ended and closed questions. The general information questions asked about the participant's job role, title, duties and the length of time they had been employed in their current role.

Section three: contained open-ended questions on component integration. The questions were designed to gain an understanding of the type of components the participant's organisation out-sourced and the kind of integration approaches employed to integrate both out-sourced components and components manufactured by the participant's organisation. The section also sought to understand the type of information provided to aid with the process of integration.

Section four: contained open-ended questions focused on approaches for sharing knowledge, if any, used by the participant's organisation. The section aimed to gain an understanding of knowledge sharing challenges and limitations within the automotive industry. The section also investigates the potential of knowledge sharing in addressing cybersecurity-related threats in connected vehicles.

Section five: this section focuses on the creation of a knowledge sharing framework and poses questions on what is required to design a knowledge sharing framework. The questions focus on the type of information and processes required to design and develop a framework to share component integration-related knowledge.

Questionnaire pre-test study

A pre-test study was conducted to refine and improve the survey questionnaire according to Sue and Ritter (2012), and Blair et al. (2013). Van-Teijlingen and Hundley (2010) compare and contrast the pros and cons of pre-testing and pilot tests. According to Van-Teijlingen and Hundley (2010), a pilot test is deployed before the actual study to solicit feedback while pre-testing aids in improving planned data collection techniques concerning both the processes to be followed and the data content type to be collected. This is supported by Millar and Dillman (2011), who state that pre-testing must be conducted using proposed data collection methods on different groups that resemble the study population. The questionnaire was pre-tested on colleagues involved in research non-related to knowledge management, primarily to ensure that the questionnaire instructions and questions were clear and understandable. The pre-test was conducted to ensure that the questionnaire avoided the use of jargon or specialist language, negative, impersonal, suggestive or double-direct questions. The main objective of the pre-testing process was to ensure that the questions contained in the questionnaire were readable, clear and appropriate. The pre-test process also aimed at improving the questionnaire's format, and to test and check the time taken to complete the survey. In the context of the study, the pre-test was conducted to ensure the questionnaire allowed the participants to respond to the questions without violating company policy and non-disclosure agreements. The questionnaire was refined and re-designed according to the outcomes of the pre-test to ensure that it could be completed within 30-40 minutes.

Questionnaire distribution – Qualtrics

The online questionnaire was designed in and distributed by an online application called Qualtrics. The choice of Qualtrics was partially driven by the fact that respondents need not install any software to access the questionnaire. Qualtrics is a powerful, easy to use web-based research suite used to build and conduct survey research, conduct evaluations, analyse responses and other data collection activities (O'Neill et al. 2018, qualtrics.com 2018). It has a simple user interface, with built-in capabilities that permit respondents to stop in-mid-survey and resume later where they left off. This built-in feature is designed to reduce low-response rates. Training, permission and licencing for the application was obtained through Coventry University.

Potential respondents were contacted via email to ask if they were willing to participate in the research by completing the online survey. Once the respondent agreed to participate in the study, a participant information sheet and a personalised link to the survey was generated in Qualtrics and sent via email to the participant. Personalised links in Qualtrics are tied to a specific survey recipient, this functionality offered by Qualtrics is extremely useful in sensitive research topics whereby confidentiality, privacy and anonymity is of extreme importance. The questionnaire was designed such that if the respondent failed to provide consent to participate, the survey terminated. Upon completing and submitting the survey, the responses are sent and stored against the researcher's Qualtrics account, ready for evaluation and analysis. The respondent is unable to access the survey once it has been submitted as complete. A thank you letter was sent via email to participants upon completion of the survey.

Low and non-response rates

To maximise the questionnaire's response rate and to avoid zero or low response rates, the study employed several strategies which include the following:

Pre-contact – emails were sent in advance to potential participants requesting their participation in the research study, and to check if the contact details were current and correct. Their current job role, job title and involvement with automotive cybersecurity, component integration and knowledge sharing was also checked to ensure that they were suitable and could contribute to the research.

University name and logo – the name and logo of Coventry University appeared in all communications, and on the questionnaire to inspire feelings of reliability.

Coventry University ethic approval - the research participant information sheet and the research invitation email stated that the research had been approved through the formal Research Ethics procedure at Coventry University to demonstrate the level of importance afforded to the research topic.

Appeal **–** within the pre-contact email, included was an explanation on the importance of the research, the importance of the participant's participation and the research's aims and objectives.

Stimulus – a summary of the survey results was promised on the conclusion of the research study as a gesture for their participation and contribution.

Confidentiality, anonymity and privacy – the pre-contact email explained how the data collected was to be stored and processed to ensure confidentiality, anonymity and privacy

Reminders - gentle reminders were sent out to participants who had received the questionnaire link and were yet to complete the questionnaire, and to those that had completed part of the survey. The reminders were sent on a weekly basis over a period of four months.

4.3.3 Data collection – Phase 1

Table 4.1 below summarises phase 1 of the data collection process conducted between June 2018 and October 2018.

Table 4. 1: Summary of phase 1 data collection process

Source	Data Collection Method		
	Semi-Structured Interviews	Online Questionnaires	Totals
OEMs	7	22	**29**
Component Manufacturers	4	19	**23**
Knowledge Experts	2	4	**6**
Totals	**13**	**45**	**58**

The initial data collection process employed by the study comprised participants from nine different countries. Table 4.2 below provides a breakdown of the participant's locations and data collection methods used.

Original Equipment Manufacturers (OEMs)

Semi-structured interviews

A total of 120 semi-structured face-to-face email requests were sent to potential participants employed by OEMs located in the United Kingdom (UK) between June 2018 and October 2018. 39 declined, citing NDAs as the reason, 38 failed to respond to the request, 12 declined stating they felt they were not well qualified for the task, 24 declined without providing a reason. Seven participants accepted the request; hence seven face-to-face semi-structured interviews were conducted with senior management employed by the two vehicle manufacturing organisations involved with the study. The researcher is situated in the UK, and the option to participate in face-to-face interviews was only extended to potential participants located in the UK due to resource constraints such as time and costs associated with travel and accommodation.

Online questionnaires

200 emails were sent to potential participants employed by vehicle manufacturing organisations requesting their participation in the research's online survey. The emails were sent to potential participants world-wide. From the 200 potential participants who were contacted, 22 accepted and completed the survey, 45 potential participants accepted the request but did not complete the survey or provide a reason as to why they did not complete the survey. 52 potential participants declined due to NDAs that they had signed with their employer. A total of 43 potential participants rejected without providing a reason, while 38 incomplete surveys were received that could not be used for the study.

Table 4. 2: Breakdown of participants by geographical location

Country	Data Collection Source			Collection Method
	OEMs	Component Manufacturers	Knowledge Experts	
United Kingdom	7	7	4	Semi-structured Interviews, Online Questionnaires
Germany	6	2	1	Online Questionnaires
United States	3	3	0	Online Questionnaires
India	0	3	0	Online Questionnaires
South Africa	2	0	0	Online Questionnaires
Korea	1	0	0	Online Questionnaires
Italy	4	2	1	Online Questionnaires
Luxemburg	0	6	0	Online Questionnaires
Sweden	6	0	0	Online Questionnaires
Totals	29	23	6	

Component Manufacturers

Semi-structured interviews

The researcher sent a total of 120 emails to management personnel employed by component manufacturers in the UK, requesting to conduct face-to-face semi-structured interviews. Similar to OEMs, only potential participants located in the UK were contacted due to constraints in resources available to the researcher. 55 potential participants stated that they were not permitted due to NDAs that they had signed with their employer, 29 potential participants declined without providing a reason. The study received 32 non-responses, nonetheless, four face-to-face semi-structured interviews were conducted with managers from the two component manufacturing organisations involved with the study.

Online questionnaires

A total of 200 emails were sent requesting potential participants to take part in the study's online survey. 19 surveys were completed by respondents located in 6 different countries (Table 4.2). 39 of the participants that were contacted declined as a result of the NDAs, and 30 potential participants rejected without providing a reason for the rejection. A significant number (41) of the participants accepted to complete the survey but failed to do so, and no justification was provided. 33 non-responses were received and 38 spoilt surveys that could not be used were also received from the participants.

Automotive Knowledge Experts

Semi-structured interviews

Similar to OEMs and component manufacturers, a total of 120 emails requesting to conduct semi-structured interviews were sent to potential participants in the UK. Two participants accepted to conduct the interviews via Skype. Skype is a telecommunication application designed to provide video and voice calls between mobile devices and computers. 20 potential participants declined due to NDAs, while 18 rejected without providing any justification. 14 rejected stating that they did not feel well suited to answer the interview questions, and 61 failed to respond to the participation request.

Online questionnaires

200 requests were also sent requesting potential participants to take part in the study's online survey. 40 surveys were returned incomplete, with some questions not answered which resulted in the surveys being discarded. 59 of the participants accepted the request to complete the survey, however, they did not complete the survey or justify as to why. 75 of the participants contacted declined due to NDAs and 22 rejected without providing a reason. Four surveys were completed by knowledge experts employed in the automotive domain.

4.3.4 Data collection – Phase 2

Phase 2 of the data collection process was conducted between August 2019 and October 2019. Table 4.3 below summarises the final data collection activity.

Table 4. 3: Summary of phase 2 data collection process

Source	Data Collection Method		
	Semi-Structured Interviews	Online Questionnaires	Totals
OEMs	5	20	25
Component Manufacturers	5	11	16
Knowledge Experts	8	23	31
Totals	18	54	72

The final data collection activity collected data from participates located in seven different countries. Table 4.4 below provides a breakdown of the participant's locations and data collection methods used.

Table 4. 4: Breakdown of participants by geographical location

Country	Data Collection Source			Collection Method
	OEMs	Component Manufacturers	Knowledge Experts	
United Kingdom	5	4	11	Semi-structured Interviews, Online Questionnaires
Germany	4	3	4	Semi-structured Interviews, Online Questionnaires
Brussels	3	2	2	Semi-structured Interviews, Online Questionnaires
Italy	4	1	3	Semi-structured Interviews, Online Questionnaires
Luxemburg	2	6	4	Online Questionnaires
France	3	0	5	Online Questionnaires
Sweden	4	0	2	Online Questionnaires
Totals	**25**	**16**	**31**	

Original Equipment Manufacturers (OEMs)

Semi-structured interviews

The researcher attended the Third Association for Computing Machinery (ACM) Computer Science in Cars Symposium in Germany in October 2019 and conducted three face-to-face semi-structured interviews with senior management employed by vehicle manufacturing organisations. The participants that participated in the data collection process had been contacted before the symposium and had agreed to be interviewed by the author. An additional two semi-structured interviews were also conducted by the researcher after sending a total of 60 emails to potential participants located in the UK. From the 60 emails, 30 declined due to NDAs, 20 non-responses were received and 8 declined without providing justification.

Online questionnaires

60 emails were sent to potential participants employed by OEMs requesting their participation in the online survey. From the 60 emails, 20 online surveys were completed, 35 non-responses were received, and five incomplete surveys were received and discarded.

Component Manufacturers

Semi-structured interviews

Two Face-to-face semi-structured interviews were conducted with participants employed by component manufacturing organisations at the Third ACM Computer Science in Cars Symposium in Germany. Similar to the participants employed by OEMs, the researcher had contacted the participants before attending the symposium. Three more face-to-face semi-structured interviews were conducted after 60 emails were sent to potential participants. From the 60 emails, 27 declined due to NDAs, 17 declined without providing justification, and 13 non-responses were received.

Online questionnaires

60 emails were sent to potential participants requesting their participation in the online survey. From the 60 emails, 27 participants declined without providing justification, 15 declined due to NDAs and seven returned incomplete surveys that were discarded. A total of 11 surveys were completed by the study's respondents.

Automotive Knowledge Experts

Semi-structured interviews

60 emails requesting to conduct semi-structured interviews were sent to senior managers in the UK. 19 participants declined without providing a reason, 12 declined due to NDAs and 21 non-responses were received. Nonetheless, a total of eight face-to-face semi-structured interviews were conducted.

Online questionnaires

An additional 60 emails were sent to potential participants requesting their participation in the online survey. 23 surveys were completed, 17 participants did not respond to the email request, 15 declined citing NDAs and five declined but did not provide a reason or justification.

Data collection summary

In summary, 31 participants participated in the face-to-face semi-structured, while 99 participants participated in the online survey, giving an overall total of 130 participants from eleven different countries as illustrated by Table 4.5 and Table 4.6 below.

Table 4. 5: Data collection summary

Source	Data Collection Method		
	Semi-Structured Interviews	Online Questionnaires	Totals
OEMs	12	42	**54**
Component Manufacturers	9	30	**39**
Knowledge Experts	10	27	**37**
Totals	**31**	**99**	**130**

Table 4. 6: Overall breakdown of participants by geographical location

Country	Data Collection Source			Collection Method
	OEMs	Component Manufacturers	Knowledge Experts	
United Kingdom	12	11	15	Semi-structured Interviews, Online Questionnaires
Germany	10	5	5	Semi-structured Interviews, Online Questionnaires
Brussels	3	2	2	Semi-structured Interviews, Online Questionnaires
Italy	8	3	4	Semi-structured Interviews, Online Questionnaires
United States	3	3	0	Online Questionnaires
India	0	3	0	Online Questionnaires
South Africa	2	0	0	Online Questionnaires
Korea	1	0	0	Online Questionnaires
Luxemburg	2	12	4	Online Questionnaires
France	3	0	5	Online Questionnaires
Sweden	10	0	2	Online Questionnaires
Totals	54	39	37	

4.4 Validity, reliability, bias and ethics

Validity determines whether the research truly measures that which it was intended to measure, or how truthful the research results are, while reliability is defined as the extent to which results are consistent over time and an accurate representation of the total population under study (Flick 2018, Saunders et al. 2018). Ethics pertains to doing good and avoiding harm. Harm can be prevented or reduced through the application of appropriate ethical principles. Thus, the protection of participants in this research study was imperative. Bias is defined by the Oxford Dictionary as: "an inclination or prejudice for or against one person or group, especially in a way considered to be unfair"; "a concentration on an interest in one particular area or subject"; "a systematic distortion of statistical results due to a factor not allowed for in their derivation. Section 4.4.3 outlines the actions taken to minimise bias and ensure that the findings accurately reflect the data.

4.4.1 Validity

To provide evidence of effort to obtain validity, the following steps were taken to ensure that the study measures accurately that which it was intended to represent and that it operates in a set of relationships representative of the developed theory.

1. To ensure that the study participants provided honest answers to the survey questions, the participants were informed about the broad aims of the study and were provided with the opportunity to decline the request to participate in the study. Furthermore, the participants were made aware of their rights to withdraw from the study at any point of the interview. The researcher's Director of Studies (DOS) contact details were also provided to the participants in the event they required further assurances and information. These measures assured that data were obtained through voluntary contribution. The interview contained an introductory section designed to establish a good rapport with each respondent. The interview was also designed to employ neutral phrases that do not create impressions of approval or disapproval that could potentially result in bias of the offered answers.
2. The information gathered for the study was obtained from appropriate; data-rich sources. The contexts of the study participants were adequately described in section 4.2. A deliberative and flexible purposive recruitment approach was employed to recruit a diverse range of people capable of providing information that will aid in answering the question posed by the study topic (Ritchie et al. 2013).

3. The online questionnaire was designed to follow the same interview protocol as that which was used in the semi-structured interviews. It started with a series of questions about the respondent's employment history and related duties followed by probes to elicit participants' perceptions of knowledge sharing phenomena in question, and views on the use of that knowledge in component integration processes.
4. By choosing semi-structured interviews and questionnaire surveys; established techniques for data collection, the researcher was able to obtain thick and rich descriptions of the phenomena without imposing any constraints on participants' discourses.
5. The interview questions and the survey questions were exposed to pre-testing, to check for consistency and validity. The questions were checked to gauge if they were appropriate to answer the research questions and to meet the research objectives.

4.4.2 Reliability

To provide evidence of effort to obtain consistent and comparable data, the following steps were taken to minimise error at the design, data collection and analysis stages.

1. Interview training for the researcher was conducted before the data collection process begun, to advance the researcher's interviewing skills, mainly on the conventions of note writing and transcription rules. The underlying idea is that the conventions for how to write notes increase the comparability of the perspectives which have led to the corresponding data. In particular, the separation of concepts of the interviewed from those of the interviewer in the notes makes re-interpretation and assessment by different analysts possible. Transcription rules that clarify procedures for transcribing conversations have a similar function to conventions for writing notes in such a way (Flick 2018).
2. To increase the reliability of the data collection process, all semi-structured interviews were audio-recorded with the respondent's permission. The audio recordings were then transcribed for coding and analysis before being stored on a secure encrypted drive provided by Coventry University.
3. Regular debriefings (supervisory meetings) were held every fortnight with the Director of Studies and the researcher's supervisor, to discuss the relevance and appropriateness of interview procedures and to scrutinise the appropriateness of the study participants.
4. Multi-method data collection was employed. Data was collected by combining several qualitative methods which included online questionnaires and face-to-face interviews. This

triangulation according to Flick (2018) enlarges the focus of the study permitting the researcher to access participants in far to reach areas.

5. The distribution process for the online survey was conducted through the use of reliable software that creates an individual link to the participant. Once the participant has completed and submitted the survey, the application does not permit alterations to the data.
6. The interview recordings and transcripts were stored on an encrypted drive provided by Coventry University. Silverman (2015) points out that checking for reliability is closely related to assuring the quality of recordings and transcripts and guaranteeing access to the process of their production.
7. Multiple analysis techniques were employed to analyse the collected data. The analysis techniques are highlighted in Chapter 5.

4.4.3 Bias considerations

Bias exists in all study designs, and it is difficult to eliminate. It can occur at all stages of the study and impacts on the validity and reliability of the study findings. However, the study attempts to minimise bias both researcher and participant biases through the following actions:

1. An introductory section to the interview was designed to establish a good rapport with each participant, and in encouraging participants to elaborate on their answers researcher utilised neutral phrases so not to create impressions of approval or disapproval that could potentially result in bias of the answers offered by the participants.
2. Similar data sampling and analysis tools and techniques were used for both the semi-structured datasets and the online survey datasets. This was to safeguard against sampling errors and response recording bias.
3. Similar administration assurance of protecting respondents ‘anonymity and assurance that there are no right or wrong answers to the posed questions were implemented to encourage non-biased responses and to minimise interviewer bias.
4. The participants were selected through a purposive sampling approach. To safeguard against participant selection bias, selection guidelines that guided the selection and recruitment of a diverse range of participants capable of providing valuable information relevant to the study was employed.

4.4.4 Ethical considerations

Research ethics is specifically interested in the analysis of ethical issues that are raised when people are involved as participants in research, and Miller at al. (2012) state that ethical concerns are likely to occur at all stages of a research study. Saunders et al. (2018) highlight three main ethical issues that the researcher must consider, these are:

1. Protection of human participants
2. The research must serve the interests of individuals, groups and/or society.
3. The management of risk, protection of confidentiality, well-grounded data collection processes, data storage and the process of informed consent.

To ensure that the study is not in violation of research ethics, the following steps were followed to meet the contingent criteria in qualitative data collection and analysis:

1. **Voluntary participation** - participants participated in the study voluntarily and signed a consent form as confirmation and proof that they understood why they were taking part in the research, furthermore, no incentives or reward was offered. All participants were informed of their right to withdraw from the study at any point during the interviews or after. Participants were also informed of their right not to answer questions that they felt infringed their rights or those of their employer. A copy of the consent form and invitation email explaining the purpose of the research is available in Appendix 8.
2. **Non-maleficence** - the researcher adhered to the principle of non-maleficence during the data collection and data analysis phases to ensure that participants did not face any harm due to their participation in the research study. Participants taking part in research studies face three forms of harm; physical, mental and legal harm (Tracy 2010, Sarantakos 2012). The threat of physical harm was minimal as participants of online questionnaires completed the survey at a location and time of their choosing, while the face-to-face interviews were conducted at the participant's workplace during the day with other company employees present on the site. The health and safety rules set by the participant's employer were observed and adhered too at all times. The study's questions were designed not to explore personal or sensitive issues, participants were treated with the utmost respect, and communication channels to the researcher or the researcher's Director of Studies were available in case participants needed additional information, thus eliminating the potential of mental harm. The data collection process avoided asking questions that violated or forced participants to violate their

employer's rights, non-disclosure agreements or their employer's terms and conditions, thus eliminating any potential legal harm.

3. **Ethical approval** - The research was allocated ethical approval after a completed research ethical application was submitted to Coventry University's Applied Research Committee before the commencement of the data collection process.

Summary of validity, reliability, bias and ethics considerations

Although great attention is applied to reliability and validity, within this study, the researcher is aware of the contemporary dialogue and debates that centre on the difficulty of establishing validity and reliability criteria in qualitative research. Developing reliability and validity standards in qualitative research is challenging because of the necessity to incorporate rigour and subjectivity (Leung 2015). Some researchers opined from a purist ontological and epistemological angle that qualitative research is not unified, but ipso facto diverse field (Thomas & Magilvy 2011), hence any attempt to synthesize or appraise different studies under one system is impossible and conceptually wrong (Leung 2015).

4.5 Chapter conclusion

This chapter presented the data collection methods employed to select participants and to collect data. The rationale for selecting the participants for the study was discussed and justified. This chapter also discussed the design and development of the data collection instruments (online questionnaires, semi-structured interviews) used to collect data, together with how these instruments were deployed in the data collection process. Justification for the chosen data collection methods and selection of the study population was provided before, reliability, bias, validity and ethical considerations from the perspective relevant to qualitative research, and the steps followed to minimise bias and error were discussed and summarised.

The following chapter discusses how the collected data was analysed.

Chapter V
DATA ANALYSIS

5.1 Introduction

Chapter 4 presented the methods employed to collect data; this chapter presents the techniques employed to analyse the collected data. The chapter is structured as follows: Section 5.2 discusses the content analysis approach and the rationale for its selection as an analysis instrument. Sections 5.3 and 5.4 present the analysis of the data and outlines how all forms of data were analysed. Finally, the chapter conclusion is presented in section 5.5.

5.1.1 Content analysis

Data were collected in two phases (see Chapter 4, section 4.1.1), however, all collected data were treated as a single unit to inform the development of the framework (Chapter 7).

Content analysis was employed to analyse the qualitative data of the study (Sections 5.3 and 5.4). Content analysis identifies and determines structures and discourses of communication, frequencies of words and their relationships. Vaismoradi et al. (2013) note that content analysis is a term used to describe a variety of text analysis strategies. Elo et al. (2014), Neuendorf (2016), and Gaur and Kumar (2018), state that content analysis is an efficient methodical coding and categorising strategy. It is mainly used in analysing textual data unobtrusively to identify patterns and themes. Pfarrer et al. (2010) state that content analysis allows researchers to recover and examine nuances of organisational behaviours, stake-holder perceptions and societal trends. The purpose of content analysis is to describe the characteristics of a document's content by examining who says what, to whom, and with what effect (Vaismoradi et al. 2013). Content analysis aims to make sense of text, symbols, media content, information, technology-supported social interactions or messages that are interceded between people. It bridges the gap between qualitative and quantitative research approaches (Elo et al. 2014, Stemler 2015, and Neuendorf 2016). Content analysis is deemed appropriate in dealing with studies that are under-researched or when they are fragmented (Elo et al. 2014). The sharing of knowledge in component integration is a complex, multi-disciplinary problem that is largely under-researched. This makes content analysis more suitable for this study. Thematic analysis was considered for this study however, content analysis became the preferred option over thematic analysis for the reasons and differences that are highlighted by Figure 5.1 below.

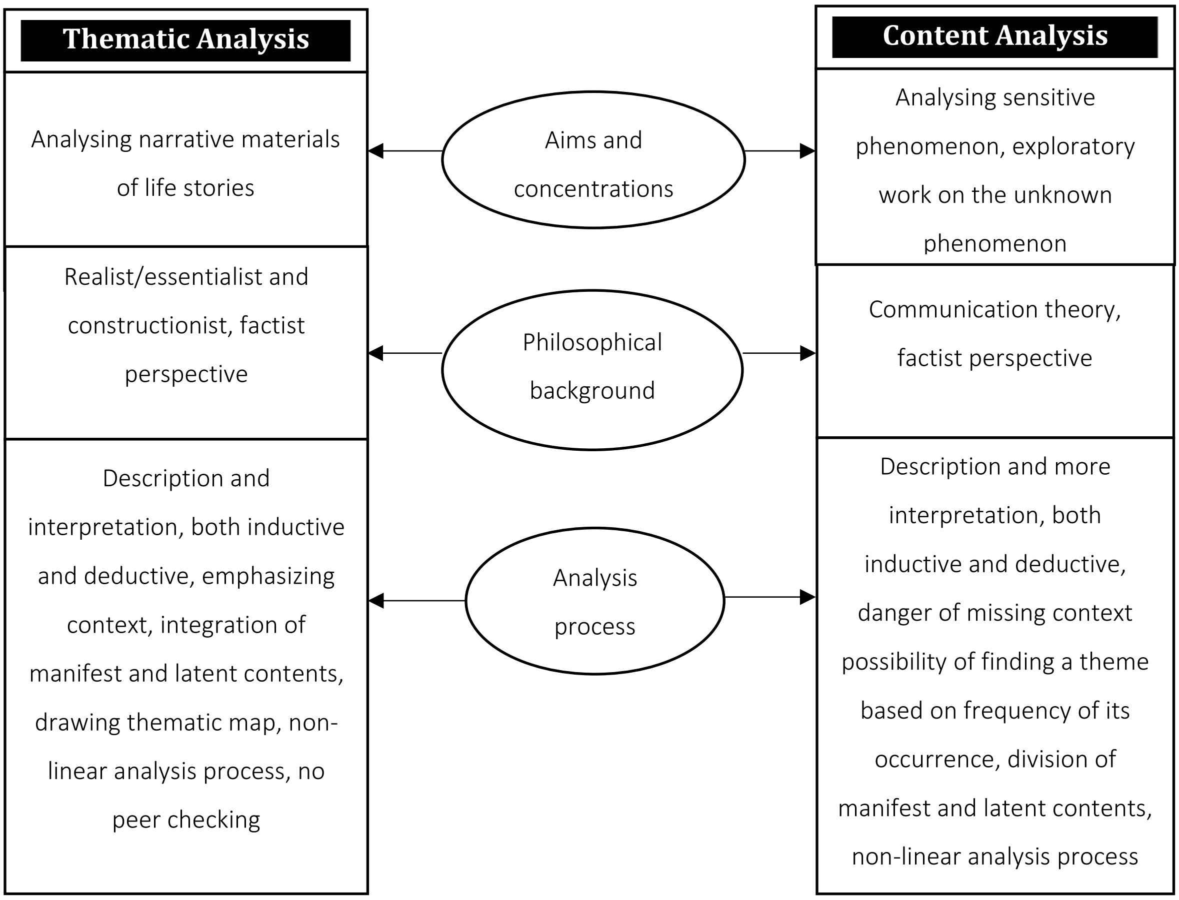

Figure 5. 1: Content analysis vs thematic analysis
Adapted from Elo et al. 2014

5.2 The content analysis approach

Qualitative research's Achilles heel has always been data analysis. Scott and Garner (2013), Corbin et al. 2014, and Miles et al (2014) describe a number of data analysis tools and techniques that can be used to analyse qualitative data. The tools vary based on the aims and objectives of each study. This study is predominantly exploratory, thus inductive content analysis became the logical option for analysing the data collected via face-to-face interviews and questionnaires. In inductive content analysis, coding categories are derived directly and inductively from the raw data. Researchers avoid using preconceived categories, allowing the categories and names for categories to 'flow from the data' instead (Moretti et al. 2011). A total of 31 semi-structured face-to-face interviews and 99 online surveys were collected for the study. The content analysis and coding guidelines provided by Neuendorf (2016) are employed to code and analyse the interview transcripts from the face-to-face interviews, while computer-assisted qualitative data analysis (CAQDAS) was used to analyse the online surveys. However, as, Elo et al. (2014) point out, the software does not code the data, however, it efficiently stores, organises, manages and reconfigures the data for human analytic reflection. Table 5.1 below presents an outline of the data analysis approaches employed to analyse the semi-structured interviews and surveys.

Table 5. 1: Summary of the data analysis approaches

Methodology Issues	Contents			
Research Design				
Research Design	Multi-Method Research			
Research Philosophy	Qualitative Interpretivism			
Research Methods	Semi-structured Interviews & Online Questionnaires			
Unit of Analysis	Automotive manufacturers / Component manufacturers/ Knowledge Experts			
Respondents	Directors, CEOs, Senior Managers			
Data Collection	Main Study			
	Online Questionnaires		Semi-structured Interviews	
Interview Time	30-40 minutes	30-40 minutes		
Recording Instrument	Digital voice-recorder	Skype in-built call recorder	Mobile Phone	Excel Database
Sampling Strategy	Deliberative and flexible purposive sampling			
Sample Location	Eleven (11) Countries			
Sample Size	130 Participants *(OEMs, Component manufacturers, knowledge experts)*			
Data Analysis				
Analysis	Qualitative Content Analysis			
Analysis Tools	Manual Coding		Computer-assisted NVivo coding	

The categorisation of verbal or behavioural data for classification, summarization and tabulation was conducted at two levels; the manifest level and the latent level as suggested by Thyme at al. (2013) and Neuendorf (2016). The manifest level was conducted immediately after each interview, to provide a descriptive account of the data, such as what was said, but no comments or theories as to why or how. This assisted in identifying continuous patterns and consistent themes and was followed by an inductive process that seeks to identify continuous patterns and regular themes that emerge from the data. To ensure that the data was not misinterpreted or misconstrued, the inductive process was complemented by a deductive approach, which is often referred to as latent level analysis. The latent level is a more interpretive analysis that is concerned with the responses as well as what may have been inferred or implied (Corbin et al. 2014). According to Miles et al (2014), the phase maintains the rich quality of the data by focusing on the identification of emergent themes and the formation of clusters. Themes are often referred to as "categories".

Coding of the semi-structured face-to-face interview data was conducted manually rather than using a computerised coding process. In the context of qualitative research, manual coding involves a thorough reading of the transcripts before mining relevant user-specific information (Lewis et al. 2013). Saldana (2015) supports manual coding in content analysis over computerised coding and states that although time-consuming and tedious, manual coding is more reliable and valid. The following are the reasons that influenced the choice of manual coding:

- Feasibility in terms of the volume of the collected data.
- There were different groups of participants involved (Automotive knowledge experts, component manufacturers, and OEMs).
- Different terminology relating to the same subject was used by the different groups of participants (for example, knowledge transfer for knowledge sharing or knowledge management).
- The different groups of participants were presented with different sets of questions.

5.3 The analytic process – semi-structured interviews

An inductive analysis process, using three main phases as illustrated by Figure 5.2 below was used to analyse the data. The three main phases are preparation, organising and reporting. The inductive content analysis employed by the study involved open manual coding, category creation and abstraction. During the open manual coding process, notes and headings were captured and written in-text during the reading process. This was followed by the abstraction phase; a process of formulating general descriptions of the research topic through the generation of categories (Polit & Beck 2010). At the initial stage of the content analysis, the interview transcripts were read through thoroughly, and headings that described aspects of the content were captured and written down in the margins as suggested by Elo et al. (2014). The headings were then collected from the margins, transferred on to a coding sheet for category generation as depicted by Figure 5.2 below.

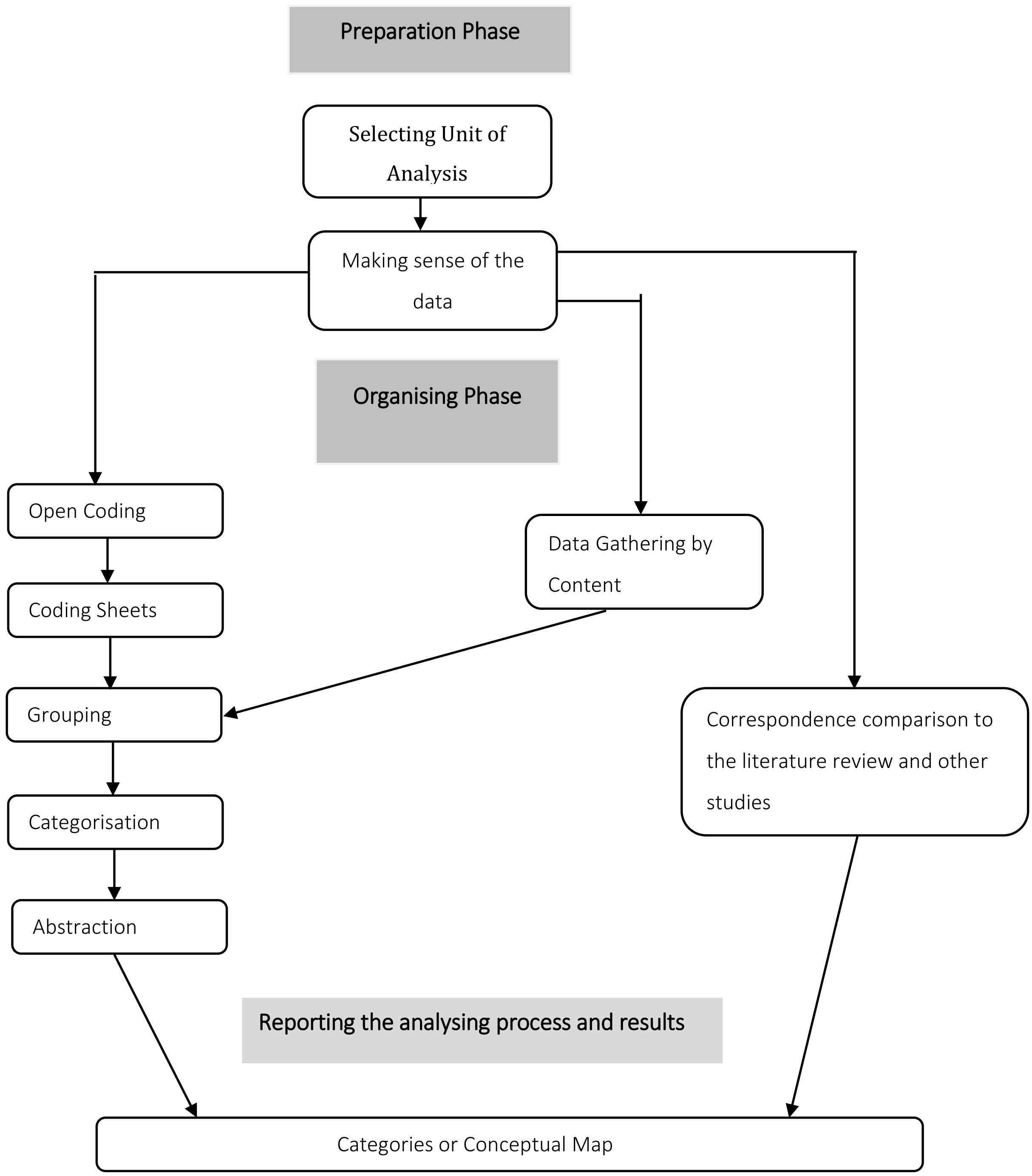

Figure 5. 2: The qualitative content analysis process
Source: Adapted from Elo et al. (2014)

After the open manual coding, the lists of categories were grouped under higher-order headings. The purpose of combining data was to condense the number of categories by collapsing those that were similar or dissimilar into broader higher-order categories and to classify data that belonged to a particular group. The creation of categories was to facilitate a means or a process of defining the phenomenon, to generate theory and to gain a better understanding. Elo et al. (2014) and Neuendorf

(2016) argue that an understanding of the phenomenon increases when creating categories, as decisions are made through interpretations, as to which things to put in the same category. Content-characteristic words were used to name the categories, sub-categories with similar events and conceptions were created and grouped. Figure 5.3 summarises the abstraction process.

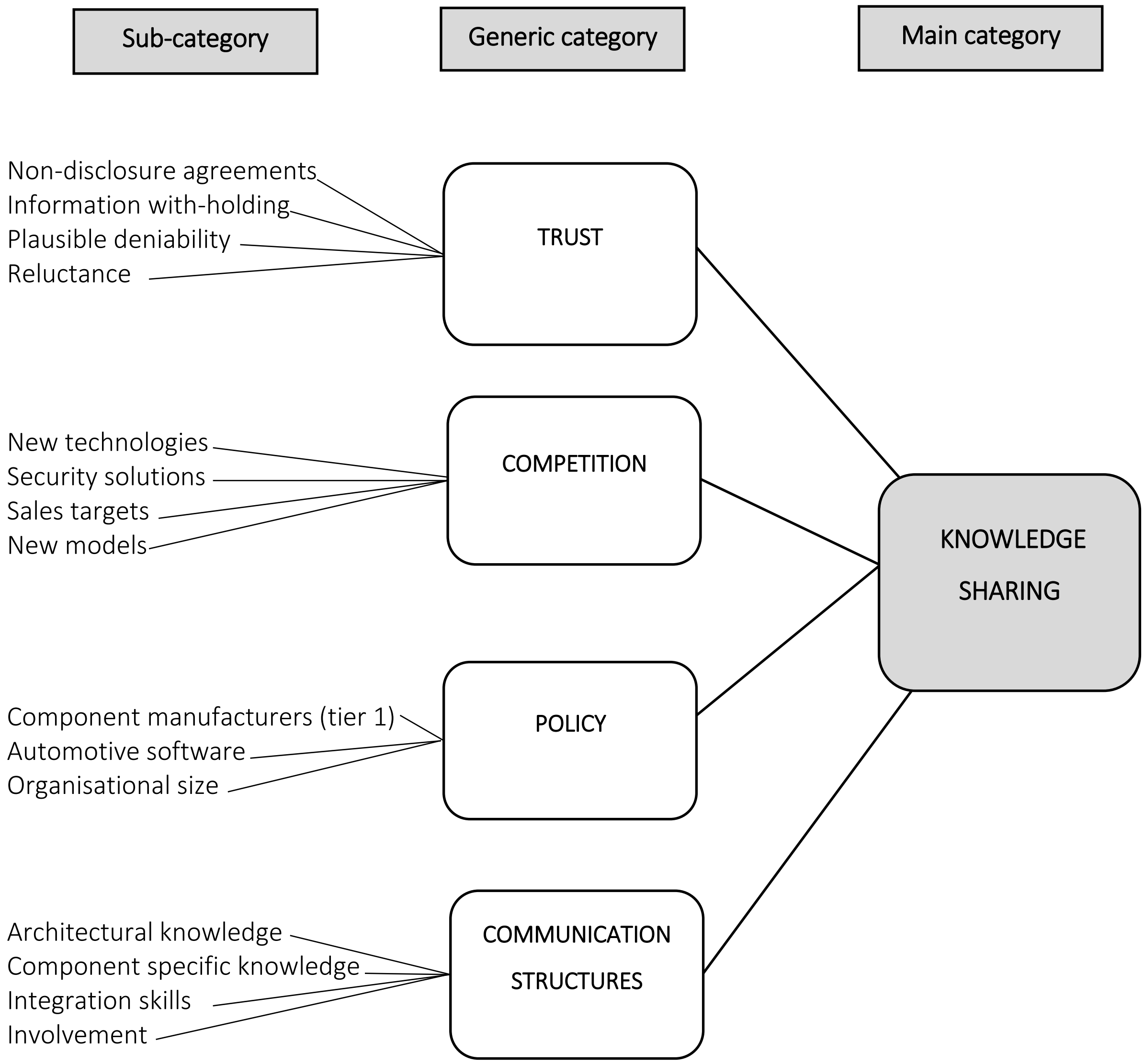

Figure 5. 3: The abstraction process
Source: Adapted from Elo et al. (2014)

5.4 The analytic process – online surveys

Computer-assisted qualitative data analysis (CAQDAS) was employed to code survey data collected via online questionnaires. CAQDAS enables the researcher to code and categorise collected data, as well as to organise, and attribute meaning and relationships between codes (Gilbert et al. 2014). To code, categorise, reshape, reorganise, examine relationships and subtle connections, and to compare coding nodes, a powerful efficient analytic tool called NVivo was used. NVivo became the preferred choice because it allowed for re-organisation, re-shaping and comparison of coding nodes. Figure 5.4 below presents the processes followed in coding the collected data. The coding processes used to code the online surveys, which include the first cycle and second cycle coding methods are explained below.

5.4.1 Data coding process defined

A code in qualitative inquiry is a researcher-generated construct that symbolically assigns a summative, salient, essence-capturing, and/or evocative attribute for a portion of language-based or visual data (Charmaz 2014, Vogt et al. 2014, and Saldana 2015). Numerous researchers and authors have described qualitative data coding as noticing relevant phenomena, collecting examples of those phenomena, and analysing those phenomena in-order to find commonalities, differences, patterns and structures (Marshall & Rossman 2014). Coding is a useful tool for data reduction and data analysis, it can either be concept-driven or data-driven (Miles et al. 2014). Concept-driven coding involves codes derived from theory (prior codes), while data-driven codes are derived from the participant data (emergent codes).

Both approaches were used to generate and create codes employed in this study. A codebook was developed to capture codes generated from the coding process. The codebook includes six basic components: the category, a brief definition, detailed description, inclusion criteria and exclusion criteria (Saldana 2015, Bernard et al. 2016). The code-book was designed to facilitate the codes "purpose" and "performance through a systematic and analytic approach by providing a template that prompts for key components (Guest et al. 2011). Please refer to Appendix 3 for a complete copy of the codebook.

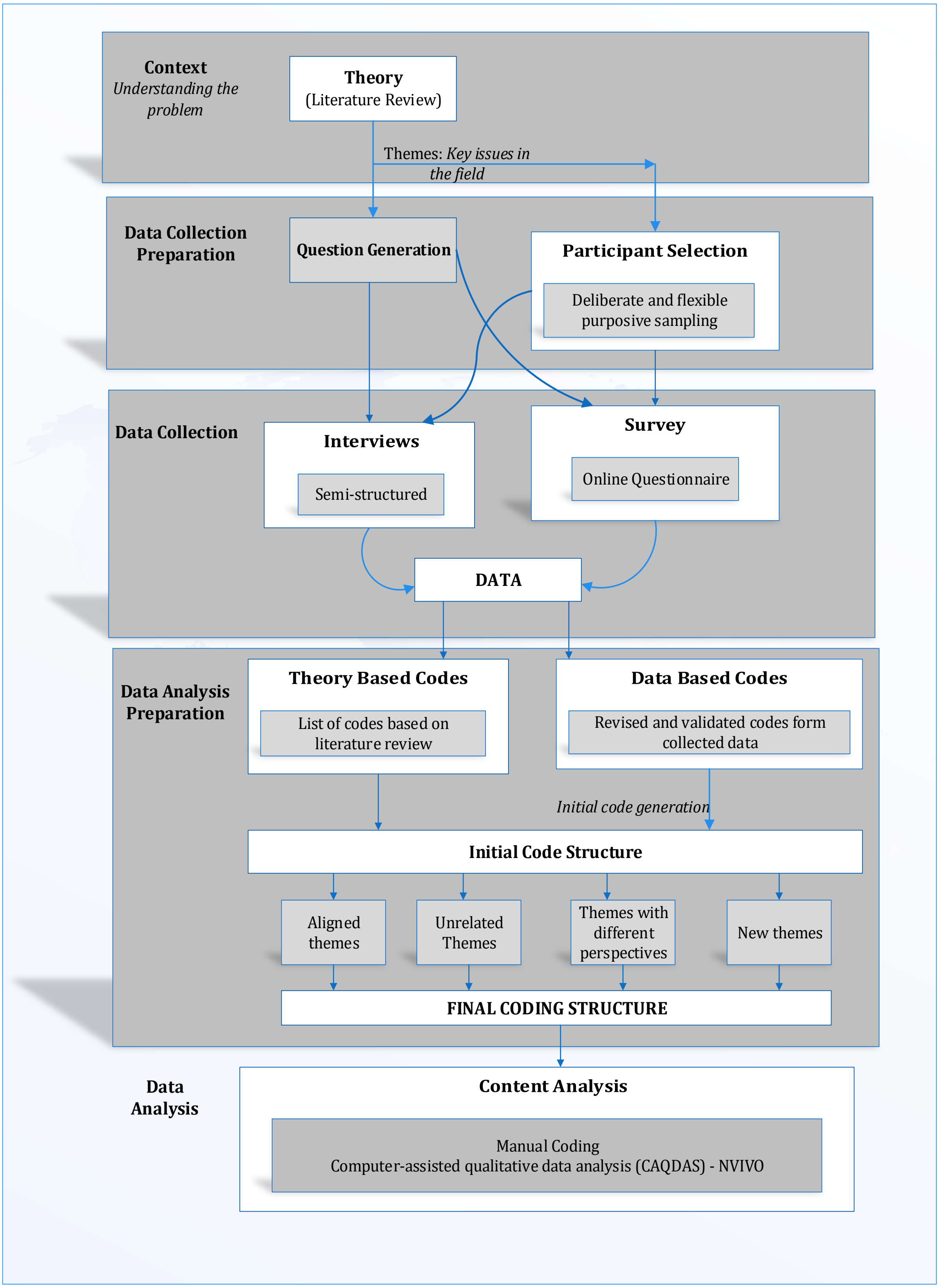

Figure 5. 4: The coding flowchart
Source: Author (2018)

5.4.2 First cycle coding methods

Grammatical methods and elemental methods were the first cycle coding methods employed to code the online survey data. Grammatical coding methods refer not to the grammar of language but the basic grammatical principles of a technique. Elemental methods are the primary approaches to qualitative data analysis. They have basic but focused filters for reviewing the corpus and they build a foundation for future coding cycles (Saldana 2015).

- **Grammatical methods** – the grammatical coding methods used within this study comprise of attribute coding and magnitude coding. Magnitude coding was used on a limited number of semi-structured interview questions and on some data captured via online questionnaire surveys, to capture and display basic statistical information such as frequencies and percentages. Attribute coding logs essential information about the data and demographic characteristics of the participants for future management and reference, and it was used to capture participant details, interview locations, dates and times.
- **Elemental methods** - elemental coding methods employed by the study include In Vivo coding, process coding and descriptive coding. In Vivo coding draws from the participant's own words for codes. Participant's statements, views and experiences noted in the surveys were coded using the In Vivo coding method. Descriptive coding assigns basic labels to data to provide an inventory of their topics. Descriptive coding was used because the data was collected across various time periods. Process coding uses gerunds ("ing" words) exclusively to connote action into the data. Process coding was employed to search for routines, repetitive forms of action-interaction and changes that have been introduced by the sharing of knowledge in component integration processes within the automotive sector.

5.4.3 Second cycle coding methods

First cycle coding methods allowed for the summarization of a substantial amount of the data, however, due to the large amount of analysed data, conceptually similar data and duplication of ideas, it was important to re-organise and re-analyse data coded through first cycle coding methods. Second cycle coding is a method that condenses large amounts of data into a smaller number of analytic units (Miles et al 2014, Saldana 2015). Its primary goal is to develop a sense of categorical, thematic, conceptual, and/or theoretical organisation from the array of first cycle codes (Saldana 2015). Pattern coding; a coding process for second cycle coding, was used to identify similar coded data and, to organise and reduce the corpus of the data into a smaller number of categories while attributing meaning to the data from the first cycle coding (Schreier 2012). Please refer to Appendix 4 for a complete second cycle coding list. Pattern coding methods make use of prior codes and emergent codes. Prior codes are codes and categories generated before the data collection activity. They comprise of key concepts and variables identified as initial coding categories through the use of existing theory and prior research. A full list of the study's prior codes is available in Appendix 5. During the coding process, data that could not be coded were classified and coded under emergent codes. Emergent codes were derived by applying code generation methods according to Miles et al. (2014) and Saldana (2015). The study's data was read whole, word by word to derive codes, first highlighting the exact words from the text that appear to capture key thoughts or concepts. Codes that were reflective of more than one key thought became the initial coding scheme. The codes were then sorted into categories based on how they were related and linked. The emergent categories were used to organise and create sub-codes. The emergent codes were kept in a separate file from the codebook as recommended by Saldana (2015). A full list of the study's emergent codes is available in Appendix 6.

First prior codes and emergent codes were then revised based on the theory and by re-reading the collected data for the creation of the initial coding structure. The creation of the initial coding structure involved a cyclic process that required revisiting the theory and the collected data. On completion of creating the initial coding structure, the structure was queried for unrelated themes, new themes, aligning themes and for themes with a different perspective. A finalised coding structure used to code the collected data was developed upon completion of all queries.

5.5 Chapter conclusion

This chapter presented the data analysis processes employed by the study to analyse data collected through semi-structured interviews and online surveys. A total of 31 face-to-face semi-structured interviews were conducted to gather perception regarding the phenomenon that is the sharing of knowledge in component integration processes in connected vehicle development. Additionally, 99 online questionnaires were completed. The chapter also outlined the different data analysis approaches employed to analyse the different forms of data. The next chapter employs the primary evidence from the data collection and analysis stages, and the theory from the literature review, to develop a new framework that promotes the sharing of knowledge of relevance for component integration in the automotive industry.

Chapter VI

ANALYSIS AND RESULTS

6.1 Introduction

In line with the two-phase data collection process as highlighted in chapter 4, this chapter presents the analysis and results from the data collection process focused on the sharing of knowledge of relevance for component integration processes within the auto industry. The detailed evidence gathering process which employed the use of semi-structured interviews and online surveys focused on senior management employed by vehicle manufacturers, component suppliers and knowledge experts within the automotive domain.

Phase 1 of the data collection process was primarily focused on cybersecurity management, and revealed different dimensions of the problem, in particular, the lack of component integration-related knowledge across the sector. Given the relevance of knowledge management practices for cybersecurity in the automotive industry, phase two was set to gain a better understanding of knowledge management. The two phases of the data collection complement each other, therefore, to cater for reliability and to assist with assessing for validity, the data were analysed using similar methods. The purpose of this part of the study is to appraise and document the different formal and informal approaches employed by the automotive industry for the sharing of knowledge of relevance for component integration processes. Accordingly, the chapter is structured as follows:

Section 6.2 presents approaches and challenges to the sharing of knowledge in the context of component integration derived from semi-structured face-to-face interviews and online surveys conducted on participants employed by vehicle manufacturing organisations. Section 6.3 presents results from participants employed in automotive component manufacturing. Section 6.4 presents results obtained from knowledge experts within the auto-domain. Section 6.5 addresses vehicle manufacturer-component supplier co-development relationships. The section highlights an awareness of the existence of knowledge that is relevant for the digital security of the integrated components and presents a discussion on how involved OEMs are with integration strategies employed within their supply chains. Section 6.6 outlines and details the integration approaches employed to integrate components as reported by the three sets of respondents. Suggestions for the potential knowledge sharing framework as noted by the participants are discussed in section 6.7. The conclusions of the chapter are presented in section 6.8.

6.2 Knowledge sharing from the perspective of OEMs

To investigate and gain an understanding of the level of sharing of knowledge in component integration processes, participants were polled via a mixture of semi-structured interviews and online surveys on knowledge sharing approaches that exist between the following:

a) Externally, between their organisation and its supply chain.
b) Externally, between their organisation and other vehicle manufacturers, and
c) Internally, between different branches or departments within their organisation (inter-departmental).

6.2.1 Approaches for knowledge sharing in OEMs

A total of 12 semi-structured interviews and 42 online surveys were conducted with respondents with senior managerial roles, employed by leading vehicle manufacturers. The data collection activity identified 11 approaches used by OEMs to disseminate knowledge. A majority of these approaches are also used in inter-departmental knowledge sharing sessions. The approaches identified by the study's respondents are:

Best practices – best practices and guidelines from existing standard-setting bodies, organisations and regulatory groups such as the National Institute of Standards and Technology (NIST), Automotive Information Sharing and Analysis Centre (Auto-ISAC), The National Highway Traffic Safety Administration (NHTSA), and The Alliance of Vehicle Manufacturers (TAVM) were identified as forms of knowledge transfer mechanisms in component integration by 58% of the study's participants.

Working groups - the interview and survey results identified knowledge sharing through the use of working groups. According to 54% of the study's participants, these working groups are a means to transfer and share information regarding the integration of components for connected vehicles. These working groups hold discussions on specific issues, and possible solutions. Some standards and specifications relating to certain and specific designs are at times discussed, formulated and written by such working groups before being disseminated to various stakeholders within the industry. Some of the working groups mentioned include the following: The Automotive Working Group (AWG), International Council on Systems Engineering (INCOSE), the Eclipse Automotive Industry Working Group (EAIWG), and the North East Automotive Alliance (NEAA).

Internal standards – internal standards affiliated to quality, design, development and security standards are highlighted as avenues some organisations employ to share knowledge in cross-functional teams. 51% of the polled respondents stated that internal standards are made available to personnel involved within the specific project or collaboration.

Statement of Work (SOW) – 32% of participants highlighted the use of SOWs as a knowledge sharing mechanism in collaborative projects with external suppliers, cross-functional teams and/or on inter-departmental collaborations. These SOWs routinely include detailed project requirements, standard regulatory requirements, project-specific integration strategies, governance terms, and conditions that are specialised and customised for the project under execution.

Industrial standards – standards such as the ISO26262 functional safety standard, SAE-J3061 (cybersecurity guidebook for cyber-physical vehicle systems) by regulatory and non-regulatory organisations for standardisation such as the International Organisation of Standardization (ISO), and the International Society of Vehicle Engineers (SAE) are used as a means to transfer and share knowledge. 59% of the participants highlighted the use of industry standards as an approach used to share knowledge that is relevant for secure integration of digital automotive components. The study results show that industry standards are the most used knowledge sharing mechanism.

Training sessions – 34% of the participants stated that training sessions to share information and to update personnel on new standards and requirements are a common feature in the auto industry. Nonetheless, training sessions are normally conducted in a controlled environment to ensure that only authorised personnel have access to the training and information under discussion. Although technological advances make it virtually easy to reach globally dispersed engineers, designers, suppliers etc. some organisations still prefer to hold face-to-face training sessions.

Joint projects – project-specific information is shared by OEMs and component suppliers. Information that is shared is to enable project completion, and it is in-line with the project contract signed by all stakeholders involved in the joint project. As noted by 38% of the participants, the information and the amount of information shared is determined and encouraged by the project activities, either varying on a point-to-point dimension or on a time dimension. The sharing of knowledge for component integration processes in collaborative or joint projects can be undertaken on a one-to-one, one-to-many or many-to-many basis, it can be either synchronous or asynchronous.

Recruitment – recruitment of personnel with relevant knowledge and expertise allows an organisation to benefit from the knowledge that the recruited individual brings. Some OEMs have adopted the approach of recruiting knowledge or integration experts with the aim of encouraging or persuading recruited personnel to transfer, teach, co-create and share the knowledge they have amassed over time. 33% of the polled participants highlighted the use of recruitment as an approach used to share knowledge of relevance that pertains to the integration of automotive digital components.

Secondment – the global dispersed structure of the automotive industry allows for organisations to send personnel on secondment to other departments or organisations located locally or externally. 29% of the respondents highlighted that secondments are routinely used were a persistent problem exists, and expert knowledge is required. Secondments aim to transfer and share knowledge, formulate mitigation solutions and to conduct training and/or knowledge sharing sessions.

Conferences – 24% of the study's participants highlighted the use of both practice-oriented and, research-oriented conferences as a means of informal and formal sharing of knowledge. Some of the study's respondents reported attending conferences to find solutions to a specific problem, share ideas, co-create knowledge and discover research agendas that other OEMs were engaged in.

Knowledge sharing sessions – knowledge sharing sessions have been adopted by some OEMs as a means to share knowledge, according to 38% of the respondents. The knowledge sharing sessions are routinely used during joint project sessions involving personnel from the same or different departments. At times, personnel from different organisations, branches or departments involved in the collaboration project access the sessions through the use of Internet technologies (emails, video calls, teleconferences, etc.), or in-person through face-to-face meetings. Other forms of conducting the knowledge sharing sessions involve the use of telephone calls or exchanging drawings via telephonic transmission. Similar to training sessions, knowledge sharing sessions are very controlled and only information that is deemed to be relevant to that particular project is discussed. If the sessions involve a third-party organisation or contractor, then Non-Disclosure Agreements (NDAs) and Confidentiality Agreement Contracts are signed before the commencement of the knowledge sharing sessions.

Summary of approaches to knowledge sharing in OEMs

OEMs have long engaged with component suppliers, third party security technologists and government initiatives to secure vehicles from unauthorised physical access. The approaches for sharing knowledge discussed above have long existed before the technological transformation facing the automotive industry. The study's results on the sharing of knowledge of relevance for secure component integration processes reveal that current approaches to share relevant knowledge capable of assisting the sector to mitigate threats born out of insecure integration approaches capable of exposing connected and autonomous vehicles to cyber-related threats are insufficient and constrained, as noted by a senior manager from OEM 1, who mentioned the following:

> "*I sit in a lot of these project meetings and vehicle manufacturers are very specific about how they pass their information on, very controlled but to the point where it's not very useful, so they have gone really sort of introvert such that I can't even ask them questions about specifications, provide aspects or anything, they just won't engage*."

Knowledge sharing approaches between vehicle manufacturers and component suppliers are almost only existent in joint project collaborations. Each organisation is expected and expects to address challenges that arise from insecure integration challenges individually, even in cases where the challenge affects more than one vehicle manufacturer. However, the results highlight greater use and appreciation of best practices and industry standards designed and produced by working groups and regulatory bodies such as the NHTSA and NIST.

Challenges of knowledge sharing in OEMs

The semi-structured face-to-face interviews and online surveys captured a number of challenges and barriers relating to the sharing of relevant knowledge that relates to the integration of automotive digital components. Although the data collection process focused mainly on the sharing of relevant knowledge for component integration processes, some of the challenges highlighted by the respondents affect the sharing of knowledge in most areas of vehicle manufacturing. The challenges to the sharing of relevant knowledge related to component integration processes as highlighted by the participants are presented in Table 6.1 below and are grouped according to the context in which they occur. According to the OEM respondents, the main challenges as highlighted in Table 6.1 below are trust, competition, over-reliance on suppliers, out-sourcing due to the supply chain structure and, a lack of processes and mechanisms that encourage the sharing of knowledge of relevance for component integration processes within the sector.

Table 6. 1: Knowledge sharing challenges related to component integration according to OEMs

Context	No of participants	Challenges of knowledge sharing in OEMs
Environmental Context	8 *(F2F interviews)* 38 *(Online surveys)*	***Insufficient investment*** - insufficient and inadequate investments to promote and encourage knowledge sharing
	12 *(F2F interviews)* 40 *(Online surveys)*	***Trust*** – lack of trust between different stakeholders due to other factors such as competition hinders the sharing of knowledge
	11*(F2F interviews)* 41*(Online surveys)*	***Competition*** - the main goal for OEMs is to manufacture and sell vehicles, sharing knowledge with a competitor is still a huge challenge
	6 *(F2F interviews)* 32 *(Online surveys)*	***Lack of incentives*** - lack of incentives to encourage and motivate organisations to partake in knowledge sharing processes
Knowledge Context	9 *(F2F interviews)* 39 *(Online surveys)*	***Lack of integration knowledge*** – most of the relevant and critical knowledge resides with component suppliers
	9 *(F2F interviews)* 38 *(Online surveys)*	***Skills shortage*** – insufficient skills and knowledge on component integration and knowledge sharing approaches
	10 *(F2F interviews)* 38 *(Online surveys)*	***Human capital*** - there are low numbers of personnel with vital and relevant skills and knowledge across the industry
	9 *(F2F interviews)* 36 *(Online surveys)*	***Insufficient understanding of associated risks*** - cybersecurity still a new phenomenon and the auto-industry is yet to fully appreciate the threats of cybersecurity that occur as a result of insecure integration processes
	10 *(F2F interviews)* 40 *(Online surveys)*	***Over-reliance on suppliers*** – vehicle manufacturers over relay on component suppliers to provide integration solutions and to lead in knowledge sharing approaches
Organisational Context	7 *(F2F interviews)* 36 *(Online surveys)*	***Organisational structures*** – organisational structures that do not promote or encourage the sharing of knowledge
	9 *(F2F Interviews)* 38 *(Online surveys)*	***Time and cost*** – the time and cost for implementing knowledge sharing mechanisms demands time and money
	12 *(F2F interviews)* 39 *(Online surveys)*	***Out-sourcing*** – knowledge sharing, and component integration challenges introduced by component and knowledge out-sourcing
	6 (*F2F interviews*) 32 (*Online surveys*)	***Change resistance*** – resistance to change from old manufacturing processes that did not incorporate knowledge sharing

	8 (*F2F interviews*) 37 (*Online surveys)*	***Restrictions via contracts*** - restrictions imposed on individuals by organisations through the use of NDAs, design contracts, etc.
	9 (*F2F interviews*) 38 (*Online surveys*)	***Lack of components specific information*** - component suppliers or manufacturers do not share component-specific information which in turn creates a culture of over-relying on component suppliers for solutions
Diversity Context	5 (*F2F interviews*) 29 (Online surveys)	***Cultural diversity*** - differences in culture and beliefs affects and influences perspectives and approaches to the sharing of knowledge
	6 (*F2F interviews*) 31 (Online surveys)	***Legislation and law*** – differences in legislation and laws between countries, at times restrict secure and timely sharing of relevant information between geographically separated organisations
	4 (*F2F interviews*) 24 (*Online surveys*)	***Language*** – technical terms and words may not be present in other languages or may not have the same meaning and definition
Technological Context	10 (*F2F interviews*) 41(*Online surveys*)	***Poor communication mechanisms*** - existing communication mechanisms are insufficient for knowledge sharing in the modern-day automotive industry
	9 (*F2F interviews*) 29 (*Online surveys*)	***Incompatible communication structures*** - different and incompatible communication structures that introduce challenges to knowledge sharing approaches

Summary of challenges of knowledge sharing in OEMs

The automotive industry used to be oligopolistic, implying domination by a small number of vehicle manufacturers. The introduction of connectivity in vehicles has seen new players enter the automotive domain, thereby increasing sales and manufacturing competition. The main objective for automotive manufacturers is to manufacture and sell vehicles, OEMs compete to bring the latest intelligent vehicle to market, and as a result, the sharing of knowledge is seen as training the competition and weakening an organisation's potential to become a market leader, a director from OEM 2, one of Europe's leading vehicle manufacturers stated the following:

> *"It is very important for an organisation not to give too much information. We are aware that most of the suppliers we work with, collaborate with, or are also working with our immediate competitors, so we have to be very careful on how much information we allow them to access. We do not want our technology, our processes and our designs to fall into the wrong hands."*

The results of the study highlight several challenges facing the automotive industry that hinder the sharing of knowledge relevant for integration processes. Challenges ranging from lack of investment, lack of incentives and lack of knowledge related to component integration, to challenges that have legal ramifications and regulatory hurdles such as NDAs and legislation. The results further highlight how component suppliers exploit integration knowledge as a driver of value and use knowledge retention as an instrument to gain a competitive advantage, as noted by a manager from OEM 1, a multinational automotive company, who stated:

> *"A component supplier might provide an OEM with a component and they will not tell the OEM how they have designed and manufactured the component. It might seem like that is good for business, but it is really not a good situation from my perspective because I am thinking, well there is software in there, for example, the OEM knows it is there (software) but they do not know anything about it, they do not know what it does, there is no understanding on what it should do or not do, which again is a threat according to threat analysis."*

However, the results also highlight new opportunities to raise awareness, develop and promote knowledge sharing approaches that can assist in extenuating the challenges stated by participants.

6.3 Knowledge sharing from the perspective of component manufacturers

Similar to participants employed by vehicle manufacturing organisations, participants from component manufacturing organisations were also polled via a mixture of semi-structured interviews and online surveys on knowledge sharing approaches that exist between the following:

a) Externally, between their organisation and its supply chain.
b) Externally, between their organisation and other component manufacturers, and
c) Internally, between different branches or departments within their organisation (inter-departmental).

6.3.1 Approaches for knowledge sharing in component manufacturing organisations

A total of nine semi-structured interviews and 30 online surveys were conducted with respondents with senior managerial roles, employed by component manufacturing organisations. The data shows a total of eight approaches used by component suppliers to propagate knowledge related to component integration processes. The approaches identified consist of working groups, best practices, industry standards, training sessions, knowledge sharing sessions, secondment, recruitment and joint projects; the knowledge sharing approaches are discussed below.

- *Component supplier and supply chain knowledge sharing approaches*

Joint projects and or collaborations (Chapter 6 section 6.2.1) were identified as avenues for sharing knowledge between component suppliers. Within these joint projects and collaborations, only the information that relates to components associated with the project under execution is shared. Study participants also identified industrial standards and best practices produced by standard-setting bodies, organisations and regulatory groups, as means of disseminating knowledge related to component integration processes.

- *Component supplier and OEM knowledge sharing practices*

Participants identified working groups, best practices and joint projects (Chapter 6 section 6.2.1) as mechanisms employed to share knowledge between component suppliers and vehicle manufacturers. Similar to knowledge sharing approaches employed by OEMs, only project-specific information is shared in joint projects to aid project completion.

- *Component supplier inter-departmental knowledge sharing approaches*

To share knowledge that is related to component integration processes between different departments and branches that are owned by the same organisation, polled participants highlighted the use of training sessions, knowledge sharing sessions, secondment and recruitment (Chapter 6 section 6.2.1).

Summary of approaches for knowledge sharing in component manufacturing organisations

The results on approaches to share knowledge of relevance related to the integration of automotive digital components demonstrate that component manufacturers recognise the need to share component integration-related knowledge, this is demonstrated by the number of inter-departmental knowledge sharing approaches noted by polled respondents. Furthermore, the limited number of processes employed to share knowledge related to component integration processes with OEMs highlights how component suppliers exploit component integration-related knowledge as a modern-day source of competitive advantage to remain relevant. These results are supported by a senior manager from Company 1, one of the leading global suppliers of technologies for the automotive market, who stated:

> *"The transfer of knowledge is too oriented around the suppliers and not so by the vehicle manufacturers. OEMs are too reliant on suppliers, for example, if OEM X (name provided) is supplied with a component which is generic, OEM X is not big enough to go back to the component supplier and dictate to them and say this is what we need, and these are the requirements, no, the component supplier will provide OEM X with a pre-defined solution because they (OEM X) cannot provide the information themselves. They are then forced to re-factor their architecture to accommodate the solution in, basically, they might be creating holes in their security architecture by doing so. So basically, they get what they are given."*

Another senior manager from Company 2, another leading component manufacturer, stated:

> "*When we talk to OEMs, from the questions they ask, you can tell they do not know, they do not have the information if l may say. They need to go and get the knowledge so that they can ask the right questions. They need to find some time and resources to go and find details of each component to be able to discuss at the same technical level as us.*"

Challenges of knowledge sharing in component manufacturing organisations

Fifteen likely determinants that affect and challenge the sharing of knowledge related to component integration processes were highlighted by the polled respondents. The challenges that affect and hinder the sharing of knowledge that pertains to component integration according to component suppliers are displayed in Table 6.2 below. The challenges that are highlighted by most polled participants are trust, competition, the automotive supply chain structure, restrictions and knowledge retention.

Table 6. 2: Knowledge sharing challenges related to component integration according to component suppliers

Context	No of participants	Challenges of knowledge sharing in component manufacturing organisations
Environmental Context	8 *(F2F interviews)* 29 *(Online surveys)*	***Competition*** – competition to design, develop and bring the latest technology to market
	9 *(F2F interviews)* 28 *(Online surveys)*	***Lack of trust*** – lack of trust created by competition and the need to remain relevant
	7 *(F2F interviews)* 24 *(Online surveys)*	***Inadequate industry standards*** – current and existing standards within the automotive domain do not cater, encourage or enforce the sharing of relevant component integration knowledge
	8 *(F2F interviews)* 30 *(Online surveys)*	***Supply chain structure*** – the current supply chain structure does not promote the sharing of knowledge for component integration processes
Knowledge Context	9 *(F2F interviews)* 29 *(Online surveys)*	***Knowledge retention*** – lack of architectural knowledge and, component-specific knowledge sharing retention due to trust and competition challenges
	4 *(F2F interviews)* 26 *(Online surveys)*	***Skills shortage*** – insufficient number of personnel with skills and knowledge on component integration strategies and relevant knowledge sharing approaches
Organisational Context	9 *(F2F interviews)* 28 *(Online surveys)*	***Restrictions*** - restrictions via contracts (NDAs, design contracts etc.) imposed on component integration, collaboration, or joint projects related discussions
	6 *(F2F interviews)* 23 *(Online surveys)*	***Time and cost*** – the time and cost associated with the creation and use of knowledge sharing mechanisms
	8 *(F2F interviews)* 30 *(Online surveys)*	***Component out-sourcing*** – challenges associated with component out-sourcing do not encourage knowledge sharing.
	4 *(F2F interviews)* 21 *(Online surveys)*	***Change resistance*** – resistance to change from old manufacturing processes that did not incorporate component integration knowledge sharing
Diversity Context	5 *(F2F interviews)* 19 *(Online surveys)*	***Cultural diversity*** - differences in nationality, language, culture and beliefs affects and influences perspectives and approaches to knowledge sharing
	3 *(F2F interviews)* 29 *(Online surveys)*	***Legislation and law*** – differences in legislation and laws between countries, at times restricts sharing of relevant knowledge and information
	6 *(F2F interviews)* 26 *(Online surveys)*	***Obsolete software*** – components or vehicle architectures running obsolete software whose functionality is not understood due to obsolete coding language
	7 *(F2F interviews)*	***Coding standards*** – different coding methods, styles and languages create component integration challenges

Technological Context	24 *(Online surveys)*	
	6 *(F2F interviews)* 23 *(Online surveys)*	***Communication platform***- lack of a communication platform away from potential hackers to discuss component integration approaches

Summary of challenges of knowledge sharing in component manufacturing organisations

Knowledge sharing challenges related to component integration processes highlighted by component manufacturers involved with connected vehicle development highlight how cyber-related threats that are born out of insecure integration processes are perceived by component suppliers. Challenges such as trust, competition and knowledge retention highlight how this challenge is viewed, as noted by a director from Company 1, one of the world's leading manufacturer of components for connected vehicles, who stated:

> "*I remember the first man on the moon, l don't know who was the second, so it's like that, it might seem like an extreme scenario but that is how people will remember. We are in a very competitive industry, very fast-moving industry so we have to make sure we are doing all we can to stay ahead, trust does not put us ahead of our competition."*

This finding was further supported by a senior manager from Company 2, one of the leading global suppliers of automotive technology and services, who stated the following:

> "*I would not say there is much sharing because it is a rat race to see who is going to bring the product first to market. I don't think It's only in the automotive or component manufacturing industry, I think this is the same in other industries where competition is high too, consumers don't ask if the car or product you are selling is very secure, no, buying decisions are not based on how secure the car is to cyber-attacks, no. People buy cars because of the technology that comes with the car.*"

Component suppliers are more focused on designing and developing new technological innovations, the sharing of knowledge related to component integration is viewed as giving the competition an unnecessary advantage.

6.4 Knowledge sharing from the perspective of automotive knowledge experts

A total of ten face-to-face semi-structured interviews and 27 online questionnaires were completed by knowledge experts with unique and necessary combination of technology, engineering and manufacturing abilities.

6.4.1 Approaches of knowledge sharing of knowledge experts

All polled participants were aware of the various mechanisms employed to share component integration-related knowledge with OEMs, component manufacturers and in-house with colleagues. Four approaches to share knowledge were highlighted by the respondents, they are listed and explained below.

Direct communication via letters – component integration-related information sent via letters to clients. This approach is normally used to relay non-urgent information and/or new information that may arise after project completion. Communication via letters is also employed to inform clients of new updates to regulations, standards or best practices that may have an immediate impact on a project.

Knowledge sharing sessions – normally organised and led by consultants or knowledge experts. These sessions normally entail a consultant or expert visiting the vehicle manufacture or component supplier's site and conducting knowledge sharing session(s). As noted by one respondent, the knowledge shared is project-specific as defined by the contractual agreements signed by participating organisations.

Collaboration with automakers/component suppliers – a collaboration with vehicle manufacturers or component suppliers in joint projects, however, the knowledge shared is governed by contractual agreements, with the owner of the project retaining performance specifications, test results and development processes. Collaborations or joint projects are one of the main mechanisms employed to disseminate project-specific knowledge.

Training sessions – automotive knowledge experts and consultants at times conduct training sessions to assist OEMs and component suppliers with integration challenges. Training sessions are conducted to explain policy, regulation, demonstrate procedures, and to explain the purpose of the procedures to ensure effective execution of the integration process. Training sessions are also used to measure and weigh an organisation's integration and knowledge dissemination procedures in-order to identify required future training.

Summary of knowledge sharing approaches of knowledge experts

Automotive knowledge experts gain valuable insight to how components are integrated and how relevant knowledge for component integration processes is shared within the domain, from their involvement with both OEMs and component suppliers as noted by a senior manager involved with conducting knowledge-sessions with both OEMs and components suppliers, who states:

"If I was to choose a side on who will be the first to come up with better solutions to address cyber-related challenges that are a result of insecure component integration, I would probably be on the side of component suppliers. They seem to be more open to sharing information than vehicle makers. They are not saddled with the same pressures that affect OEMs, so they are in a better position to talk to one another and work on a solution. From the training sessions that I have conducted, the component suppliers are not exposed to so many gagging orders as the OEMs and I think due to that, they are more open to sharing".

Knowledge sharing challenges of knowledge experts

Automotive knowledge experts' highlight similar challenges as those mentioned by OEM participants (Chapter 6 section 6.2.1.1), and participants employed by automotive component suppliers (Chapter 6 section 6.3.1.1). However, challenges not previously mentioned by the above-mentioned stakeholders were highlighted by the knowledge experts. The challenges are listed and explained below.

Inadequate legislation to enforce knowledge sharing – respondents highlight inadequate legislation to encourage or enforce sharing of component integration-related knowledge. The threat of cybersecurity that results from insecure integration processes affects all stakeholders in the automotive spectrum, yet the industry is yet to develop some form of automotive-specific legislation, regulation or standard to encourage sharing of such knowledge.

Contractual agreements – legally binding agreements with specific terms that gag organisations from discussing, re-using designs and specifications do not encourage the sharing of knowledge relevant for component integration, according to some respondents. Restrictions on sharing of solutions relating to threats affecting all stakeholders that affect consumer lives should not be included in contractual agreements or design contracts.

Intellectual property rights – the use of IP rights to prevent the sharing of relevant knowledge necessary for securing the digital component for connected vehicles. A number of respondents surveyed in both the semi-structured interviews and the online questionnaire highlighted how component-specific information and architectural information is retained and not shared, resulting in cyber-vulnerable component manufacturing.

Summary of knowledge sharing challenges of knowledge experts

The study's participants demonstrate awareness on the need for sharing knowledge that relates to the secure integration of digital components within the automotive continuum, however, due to the challenges identified via both modes of inquiry, the industry does not possess sufficient and effective knowledge sharing mechanisms. Processes for sharing knowledge currently in use are inadequate, constrained and were designed to address the integration of mechanical constructs that the auto-industry was accustomed to, as noted by one senior knowledge expert who stated:

> *"Some organisations are not willing or prepared to share knowledge. In some of the projects I have worked on, if I give them proposals on knowledge sharing approaches or integration strategies, they will just respond with yes or no answers, they won't give any details, which is great from a purist approach, but from a "we need to get them done" stance, it is not very useful."*

Another senior knowledge expert stated:

> "*There is not a lot of sharing between vehicle manufacturers and component manufacturers because most OEMs do not have the technical knowledge. Suppliers have the knowledge, but they really don't want to share the knowledge, I mean they just want OEMs to sign the contract, win their confidence and tell them that everything is fine. Some Germany suppliers are starting to be a little bit flexible, which is a good thing but the information they provide is very much limited to be useful."*

6.5 Vehicle manufacturers and component supplier co-development strategies

A total of 54 participants from vehicle manufacturing organisations were polled on how involved or intrusive their organisation was with integration strategies employed by component suppliers that manufacture and integrate components for their connected vehicles. Additionally, a total of 39 participants from automotive component manufacturing firms were also polled on how intrusive OEMs were in the integration processes they employ. Figure 6.1 below compares the pre-coded responses captured using a Likert scale with the following pre-coded scale: *extremely involved, very involved, moderately involved, slightly involved and not involved*.

Intrusiveness or involvement within the research context is defined as the level of detail and the amount of co-ordination the manufacturer employs in defining the design of the respective artefact, the level of control over the supplier's design decisions and component integration processes.

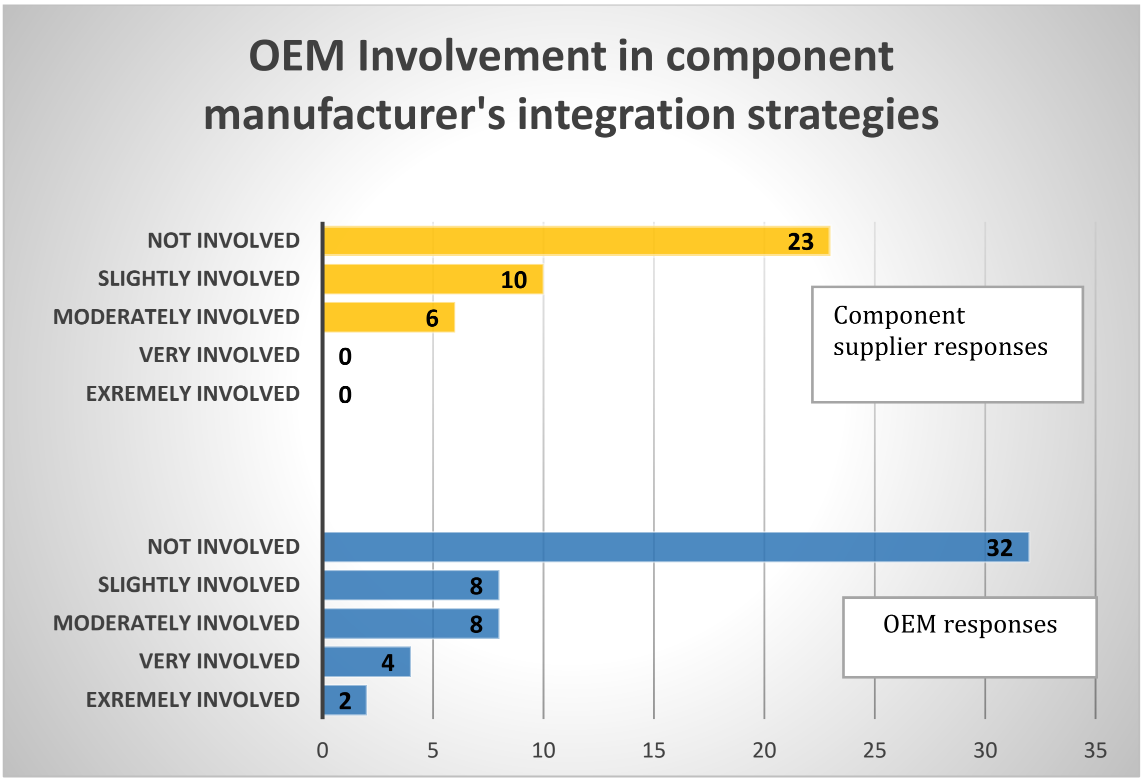

Figure 6. 1: OEMs and component suppliers' responses to OEM involvement in a component supplier's integration strategies

The results displayed by Figure 6.1 above illustrate very clearly the lack of involvement with or the lack of intrusion by OEMs in integration strategies employed by their supply chain. 59% of component supplier respondents stated that OEMs were not involved in integration strategies they employ. More so, 59% of OEM respondents highlighted that OEMs were not involved in integration strategies employed by suppliers who manufacture and integrate cyber-vulnerable digital components used in connected vehicle manufacture. However, Figure 6.2 below illustrates how intrusive and involved component suppliers are with integration strategies employed by OEMs and by suppliers in lower tiers (tier 2, 3 etc.). 55% of OEMs highlight that component suppliers are extremely involved with their integration strategies, while an additional 22% stated they are very involved. 46% of component suppliers are extremely involved in integration strategies employed within their supply chain, while 28% are deemed to be very involved with integration strategies employed within their supply chain.

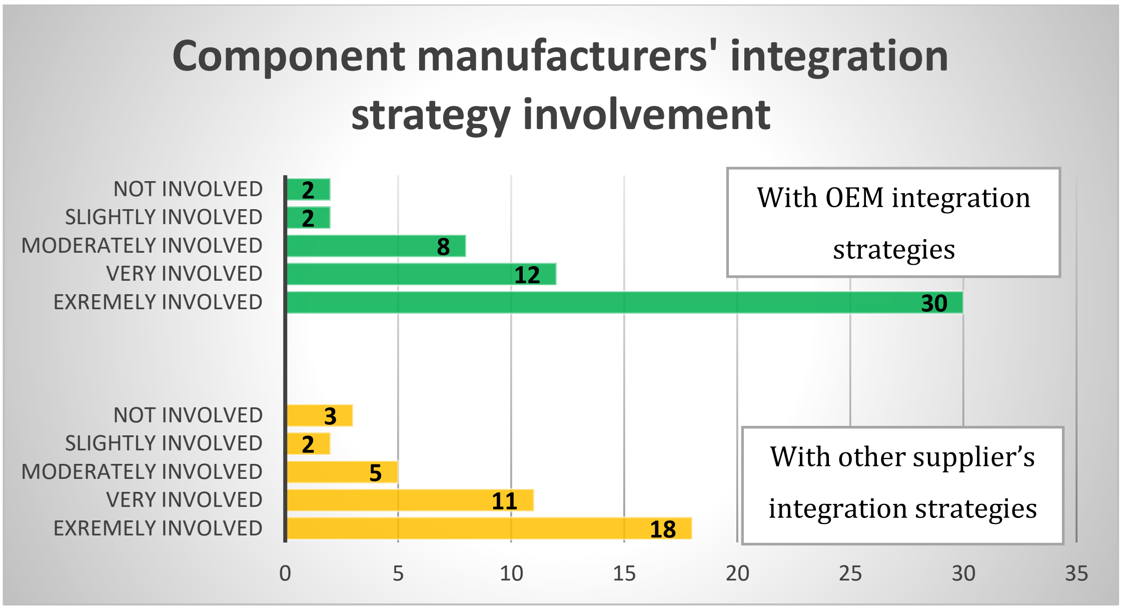

Figure 6. 2: Component supplier (Tier 1) involvement with integration strategies employed by OEMs and component suppliers in lower tiers

The results in Figure 6.2 above indicate disturbingly low levels of OEM involvement in component integration strategies employed within the automotive supply chain. The results show that OEMs are not highly intrusive in design and integration processes employed by component suppliers, however, Figure 6.2 shows that component suppliers are extremely involved in integration strategies employed by OEMs and suppliers in lower tiers, highlighting why most knowledge of relevance for component integration processes resides with suppliers, and why there is an over-reliance on suppliers to provide solutions to address the challenge of sharing knowledge related to component integration processes and strategies.

6.6 Component integration approaches currently in use

The study's participants were polled on component integration approaches that their organisation employs to integrate components in a sub-system or a system. The online surveys and the semi-structured interviews also aimed to gain an insight into the processes employed to integrate components into the vehicle architecture, and the information provided by component supplying organisations to aid with integration. Table 6.2 below presents and discusses the approaches currently employed to integrate components. The table presents the integration processes, their strengths and weaknesses as noted by the study's participants. Additionally, the various forms of information that are shared to aid with the integration process, and those which are not, as noted by the study's participants are also presented.

Table 6. 3: Current component integration strategies used in the automotive industry

Approach	Definition	Strengths	Weaknesses
Computer Integrated Manufacturing (CIM)	A programmable computer-based manufacturing system designed with CAD software, which uses computers to integrate the processing of production, business and manufacturing	• Automation: ability to create automated manufacturing processes • Efficiency: faster and less prone to manufacturing errors due to the integration of computers in the production process • Great machine utilisation • Quality: improvements in productivity and quality control	• Knowledge management: it is not able to adequately address knowledge management issues, and also it is not possible to solve problems related to decision and control even though there has been an increasing interest in subjects like artificial intelligence (AI), knowledge-based systems (KBS), and expert systems • Integration: integration of components from different suppliers • Data integrity: the higher the degree of automation, the more critical is the integrity of the data used to control the machines • Human labour: requires extra human labour in ensuring that there are proper safeguards for the data signals that are used to control the machines • Process control: computers may be used to assist the human operators of the manufacturing facility, but there must always be a competent engineer on hand to handle circumstances which could not be foreseen by the designers of the control software • Suitability: not suited for non-complex products yet requires highly skilled employees
Component information provided for integration	• Performance specification test results: performance tests measured against how the component is expected to perform within a system, module or subsystem. At times simulation test results are also produced for the customer • Safety test sheets/results: lists of the type of safety tests conducted and the results of the safety tests compared against safety regulatory requirements • Quality inspection results- results from quality tests highlighting the quality score achieved by the component. The quality test results are measured against an expected quality rating		

Important information required for integration not provided	• Component manufacturing processes: details of the processes followed to manufacture the component. Some respondents mentioned that this information can at times be held back if the component is a system, subsystem or module depending on the NDA or design contract • Security tests results: these are sometimes provided on request; most component suppliers seek justification before providing security test results • Integration specifications: coding guidelines for modelling and programming languages required for integration • Architectural information: information that relates the architecture/platform where the component, integrated system will function from • Interface specifications: information concerning the interface(s) that the component will interact with • Design decisions: decisions that influenced the design and development decisions • Design processes: the component's design and development activities, including the rationale for the implementation of the processes		
Enterprise Application Production (EAI)	It is an integration framework that comprises a collection of technologies and services designed for the integration of systems and applications	• Data sharing: provides unrestricted sharing of data and business processes among connected applications or data sources within an organisation • Data integration: ensures that information in the organisation's systems are kept consistent. • Vendor Independence: extracts and maintains an organisation's business policies, practices etc. such that when one of the organisation's applications is replaced, polices do not need to be re-implemented	• Limits: only capable of linking applications and business processes within a single organisation • Human Labour: requires expert knowledge and specialised training to operate and maintain EAI applications
Component information provided for integration	• Component design processes: design and development activities followed in the development of the component • Component performance specification: information on how the performance performed under the relevant tests that apply to the component are made available. Additionally, there are times when the customer will provide components that are meant to interface with the component for testing. The component supplier will then provide test results relating to how the component performs within such an environment • Integration specifications: coding guidelines for modelling and programming languages used for integration		
Important information required for integration not provided	• Design decisions: decisions that influenced the design and development decisions • Interface specifications: information concerning the interface(s) that the component will interact with • Architectural information: information that relates the architecture/platform where the component, integrated system will function from		

	• Manufacturing processes: information on how the component was manufactured including information on the tools employed to design, develop and manufacture the component • Security tests results: these are sometimes provided on request; most component suppliers seek justification before providing security test results • Design processes: the component's design and development activities, including the rationale for the implementation of the processes		
Product Lifecycle Management (PLM)	It is software that is used for the management and publication of product data. Production data usually involves technical specifications of the product, specifications for product development and manufacture	• Enhances collaboration: ensures that all stakeholders share a common understanding of product data • Archiving: can be employed as a central knowledge repository, storing process and product history. • Integration: promotes integration and data exchanges between personnel engaged in the project	• Compatibility: not designed to serve automotive component integration requirements, therefore requires modification which at times affects performance • Human labour: constantly requires human labour and expertise to organise and track design data
Component information provided for integration	• Manufacturing processes: information on how the component was manufactured including information on the tools employed to design, develop and manufacture the component. If the component comprises other components from other suppliers, this information can be provided upon request. These processes are available for stakeholders to view via the communication medium offered by PLM • Component performance specification: information on how the performance performed under the relevant tests that apply to the component are made available. Additionally, there are times when the customer will provide components that are meant to interface with the component for testing. The component supplier will then provide test results relating to how the component performs within such an environment • Safety test sheets/results: lists of the type of safety tests conducted and the results of the safety tests compared against safety regulatory requirements • Integration specifications: coding guidelines for modelling and programming languages used for integration		
Important information required for integration not provided	• Security tests results: these are provided on request; most component suppliers seek justification before providing security test results • Design decisions: decisions that influenced the design and development decisions • Design processes: the component's design and development activities, including the rationale for the implementation of the processes • Interface specifications: information concerning the interface(s) that the component will interact with • Architectural information: information that relates the architecture/platform where the component, integrated system will function from		

Product Data Management (PDM) or Product Information Management (PIM)	It is a software approach that is part of Product Lifecycle Management (PLM), AND Configuration management (CM) mainly used by engineers in organisations whose focus lies with manufacturing and retailing. PDM is used to manage, track the creation, change and archive information related to a component	• Enhances collaboration: ensures that all stakeholders share a common understanding of product data • Archiving: can be employed as a central knowledge repository, storing process and product history • Integration: promotes integration and data exchanges between personnel engaged in the project • Automation: creates automatic reports on product cost	• Compatibility: not designed to serve automotive component integration requirements, therefore requires modification which at times affects performance • Human labour: constantly requires human labour and expertise to organise and track design data
Component information provided for integration	• Product cost reports- automated reports on product costs, these are at times used to calculate product cost reduction • Component integration reports- integration reports that contain integration processes are shared with relevant stakeholders • Manufacturing processes: information on how the component was manufactured including information on the tools employed to design, develop and manufacture the component. If the component comprises other components from other suppliers, this information can be provided upon request. These processes are available for stakeholders to view via the communication medium offered by PLM • Component performance specification: information on how the performance performed under the relevant tests that apply to the component are made available. Additionally, there are times when the customer will provide components that are meant to interface with the component for testing. The component supplier will then provide test results relating to how the component performs within such an environment • Safety test sheets/results: lists of the type of safety tests conducted and the results of the safety tests compared against safety regulatory requirements • Integration specifications: coding guidelines for modelling and programming languages used for integration		
Important information required for integration not provided	• Safety test sheets/results: lists of the type of safety tests conducted and the results of the safety tests compared against safety regulatory requirements • Security tests results: these are provided on request; most component suppliers seek justification before providing security test results • Design processes: the component's design and development activities, including the rationale for the implementation of the processes • Design decisions: decisions that influenced the design and development decisions • Interface specifications: information concerning the interface(s) that the component will interact with • Architectural information: information that relates the architecture/platform where the component, integrated system will function from		

Integration Platform	It is software that is used to integrate different applications and services.	• Data integration: data management processes that ensure that engineers are using the same datasets • Interoperability: integrates applications independent from the platform, programming language or resources • Collaboration: permits collaboration between distributed applications and engineers • Simplicity: employs visual aids and interactive interfaces	• Limits: functions are restrained to software and application integration alone, does not apply to hardware components • Security: does not take security into consideration, for example, resources used to share data is not security checked • Human labour: constantly requires human labour and expertise to organise, code, encode and de-bug software applications
Component information provided for integration	• Coding information: information regarding the programming language and the binding code used to integrate the different application and services • Architectural information: information that relates the architecture/platform where the component, integrated system will function from • Performance test results: results from the different performance tests conducted. The testing approach employed is also provided highlighting how the applications performed when additional applications were integrated • Safety test sheets/results: lists of the type of safety tests conducted and the results of the safety tests compared against safety regulatory requirements		
Important information required for integration not provided	• Design processes: the component's design and development activities, including the rationale for the implementation of the processes. • Design decisions: decisions that influenced the design and development decisions • Interface specifications: information concerning the interface(s) that the component will interact with • Security tests results: these are provided on request; most component suppliers seek justification before providing security test results • Manufacturing processes: information on how the component was manufactured including information on the tools employed to design, develop and manufacture the component • Component integration reports- integration reports that contain integration processes which should be shared with relevant stakeholders		

6.7 Key factors to be considered by a new approach to improve knowledge sharing within the sector

The study's online questionnaire and the semi-structured interviewing process tasked participants to provide insight into the processes and strategies for the sharing of relevant knowledge that promotes the secure integration of digital components for the connected vehicle. The section below captures and discusses responses provide by participants employed by vehicle manufacturing organisations, component manufacturers and knowledge experts within the auto-domain. The section begins by discussing knowledge sharing from an organisational perspective first before discussing knowledge sharing from the industry's perspective.

Intra-organisational knowledge sharing

The results highlight the need for communication and knowledge transfer between different functions, departments and teams within organisations. 81% of managers in vehicle manufacturing organisations and 90% of managers involved with component manufacturing highlighted the need for intra-organisational knowledge sharing to aid with component integration processes. Similar to component manufacturers, 90% of Knowledge experts highlighted the need for intra-organisational knowledge sharing as illustrated by Table 6.4 below.

Table 6. 4: Number of participants that highlighted the need for intra-organisational knowledge sharing

Intra-organisational knowledge sharing			
	OEMs	Component manufacturers	Knowledge experts
No of respondents (%)	81%	90%	90%

The study's participants highlighted the need for an approach to share knowledge which has provisions that permit the sharing of explicit and tacit knowledge between the various departments, divisions and functions within the organisation. Component integration is a knowledge-intensive activity that requires constant communication between the various functions involved in the activity. However, according to the literature on knowledge management, and feedback from the study's participants, intra-organisational knowledge sharing requires an environment that has the following factors:

- **Organisational structure** – the organisation should create a structure that encourages and promotes knowledge sharing (Chapter 2 section 2.3.4 and Chapter 7 section 7.2.2). This potentially decides the organisation's ability to learn from other functions, projects, and to perform core functions related to the sharing of knowledge. Additionally, the organisational structure should be constructed to assist with solving problems encountered, define and achieve objectives concerning the project at hand.

- Human resources – the study's participants also highlighted the need for a human resources department that is tasked with staff development. This is critical, as it is within this remit that staff are motivated and satisfied to perform core functions related to the various phases of the component integration and knowledge sharing life cycles.
- Financial resources – the development of an appropriate knowledge sharing structure will require support and financial input. The study's respondents highlighted the challenge of insufficient investment in knowledge sharing structures. The knowledge sharing framework must consider how the financial needs are met within knowledge sharing processes. Insufficient or the lack of adequate financial resources can impact on creating an effective knowledge sharing framework.
- Communication processes –the study's participants highlighted that the framework should possess adequate processes of sharing information and knowledge (verbally, non-verbally or via other mechanisms). The organisation should have communication processes in place that facilitate the sharing of knowledge relevant for component integration within the internal environment (intra-organisational) and the external environment (inter-organisational).
- Leadership – the organisation's leadership plays a vital role in the development of knowledge sharing processes, integration strategies, staff development, and resource mobilisation as noted by the study's participants. The organisation's leaders should be motivated, and dynamic individuals focused on promoting the sharing of knowledge and, the creation of a knowledge sharing culture.
- Technology – a majority of the study's participants highlighted the need for a technological environment that is suitable for and promotes the sharing of knowledge. The communication media used to share knowledge in component integration processes should be suitable for secure information transfer and should be capable of communication within and outside the organisation (external environment) with relevant stakeholders not located within the organisation. The technology should be scalable and easily adaptable to changes to knowledge sharing requirements and processes.

Inter-organisational knowledge sharing

The results from the data collection process highlighted the need for a process to share knowledge related to component integration between different organisations. As illustrated by the results in Table 6.5 below, 95% of knowledge experts and 92% of managers employed by component manufacturing organisations highlighted the need for inter-organisational knowledge sharing. Additionally, 80% of managers in vehicle manufacturing organisations also highlighted the need for knowledge sharing between organisations, stating that the knowledge sharing framework should have provisions that permit the sharing of knowledge across different organisations.

Table 6. 5: Number of participants that highlighted the need for inter-organisational knowledge sharing

Inter-organisational knowledge sharing			
	OEMs	Component manufacturers	Knowledge experts
No of respondents (%)	80%	92%	95%

To ensure that knowledge was shared between different organisations, the study's participants highlighted the need for regulatory compliance. The knowledge sharing framework should be designed to address regulatory requirements that are specific to the auto-domain, in particular, the knowledge that relates to component integration processes.

- Regulatory requirements – knowledge sharing approaches proposed by the potential framework should consider and adhere to the industry's regulations, best practices and standards that have been designed to assist with knowledge creation, transfer and knowledge management.

External environment knowledge sharing

The knowledge sharing framework must be capable of addressing factors that are external to the organisation's structure and functional processes. The study's participants referred to factors that an organisation has very little or no control over such as changes in legislation or law as the 'external environment'. As highlighted by Table 6.6 below, 92% of participants from vehicle manufacturing organisations, 97% from component manufacturing organisations and 93% of knowledge experts highlighted the need for the framework to cater for changes in the political and legal landscape.

Table 6. 6: Number of participants that highlighted the need for external environment knowledge sharing

External environment knowledge sharing			
	OEMs	Component manufacturers	Knowledge experts
No of respondents (%)	92%	97%	93%

- *Political and legal requirements* - as noted by a majority of the study's participants, the knowledge sharing framework should be capable of addressing and adhering to requirements imposed by the political and legal environment. The approaches proposed by the potential framework should be capable of adapting to any changes that may result from changes to legislation or the political environment from which the organisation resides and operates in.

Figure 6.3 below presents the summary of requirements (intra-organisational, inter-organisational and external environment) that the potential framework should consider as noted by the study's participants.

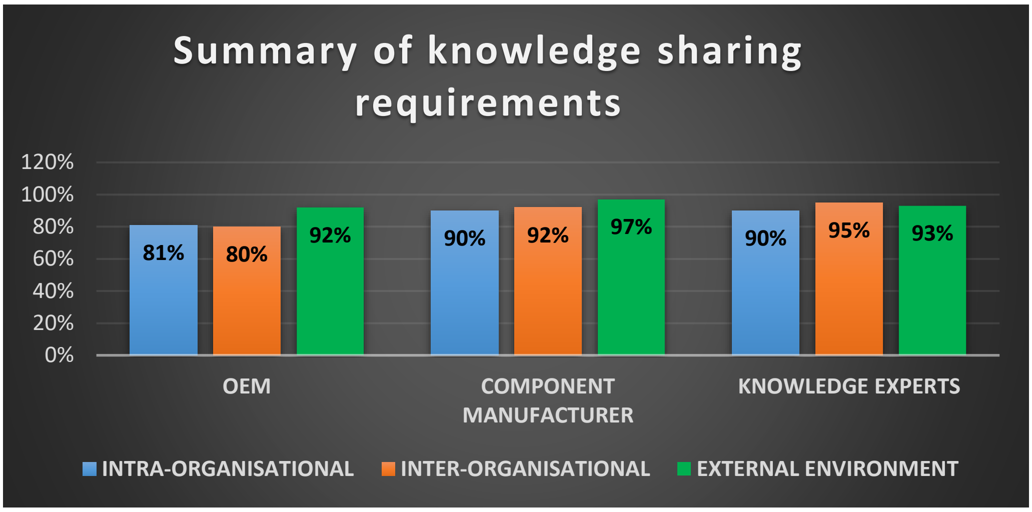

Figure 6. 3: Summary of requirements for the potential framework

6.8 Chapter conclusion

This chapter presents a detailed analysis of the data collected via semi-structured interviews and the online survey. It explores the different approaches employed by vehicle manufacturers, component suppliers, and automotive knowledge experts to share knowledge concerning component integration processes. The chapter identifies manufacturer-supplier development competition thereby presenting the challenges affecting the sharing of relevant knowledge related to the integration of automotive digital components. One of the main aims of the chapter was to gain an understanding of integration strategies in use in integrating the cyber-vulnerable components used in connected vehicle manufacture. The chapter fulfils this aim through information gathered via the interviews and online surveys. Unexpected and new findings were discovered in the data collection and analysis phases. These unexpected findings are taken into consideration in the creation of a potential framework for knowledge sharing (Chapter 7). Drawing together the learning gathered from the literature review and, the data collection process, the development of a framework to share knowledge of relevance for component integration processes is important for the following reasons:

- Security culture: The framework will assist with decision making, which in turn will potentially cultivate and foster a culture of security that recognises that cybersecurity is not just about technology, but also about psychology and sociology (Morris et al. 2018). As highlighted by the literature review, a security culture is greatly lacking, vehicle manufacturers are more concerned with safety and sales, security is and has always been viewed as an after-thought that delays production and increases development costs (PWC 2014).

- Facilitating communication: the framework will promote and advocate the sharing of relevant knowledge in component integration processes. Stakeholders will need to engage, collaborate, share and disseminate knowledge that is related to component integration processes. The framework defines the required steps or procedures to adhere to, thus providing a common process for all users.

- Determining the scope of integration: the framework sets the virtual boundaries of knowledge sharing for organisations to employ, and the processes to employ in component integration. It sets the requirements for integrating components and it outlines the phases and activities to be addressed, as well as the knowledge sharing factors and influences to be considered.

- Increasing understanding: The framework will help in improving security awareness and understanding of the cybersecurity phenomenon; e.g. how things work, where threats can come from, and the impacts of those threats, and to demonstrate the links between them. It provides definitions and approaches to knowledge sharing, and it will assist in defining knowledge elements that require sharing in component design and development. The data collection phase highlighted a seriously low level of cybersecurity awareness within the industry, mainly with OEM employees. The conceptual framework aims to create awareness of cybersecurity threats and mitigation processes made available by their employing organisation.

- Knowledge integration: the proposed framework will provide a more holistic view of processes that allow for the sharing of knowledge in integration processes across the auto industry. It will enable people within the auto-domain to consider the sharing of knowledge related to component integration facets from a broader perspective. The framework will highlight the need for OEMs to share automotive architectural knowledge and the need for suppliers to share component-specific knowledge. The framework will inform all automotive stakeholders on the use of the various forms of knowledge provided and obtained from OEMs and suppliers, thus alleviating the misperceptions surrounding this discipline, as it will provide clarification of the component integration knowledge sharing phenomenon.

- Facilitating participation: the implementation of a framework can facilitate the participation of managers and those who are in a position of power and responsibility, capable of promoting and ultimately enforcing knowledge sharing practices and encouraging the use of the framework within the organisation.

The next chapter focuses on the development of a framework that attempts to address some of the main limitations of existing techniques for knowledge sharing in component integration processes as identified in the relevant literature and by the study's participants.

Chapter VII
DEVELOPMENT OF THE FRAMEWORK

7.1 Introduction

The research presents a framework that has been developed to promote the sharing of knowledge in automotive component integration processes. This framework has been developed in an attempt to assist the automotive industry to overcome some of the limitations of existing techniques for knowledge sharing in the integration of components for connected vehicles as identified in the relevant literature. This new framework is supported by theory and brings together the best practices established in this thesis through the literature review and the primary evidence from the semi-structured interviews and the online survey.

7.1.1 The need for a component integration knowledge sharing framework

The evidence gathered and presented in previous chapters demonstrates the need for sharing knowledge related to component integration processes as a key factor to influence and improve the security of modern connected vehicles. However, due to a number of various constraints identified in the research, both avoidable and non-avoidable (trust, competition, insufficient investment, skills shortage, contracts, out-sourcing etc.), the sharing of knowledge that is relevant for secure integration of components is not common practice within the automotive ecosystem; furthermore, most organisations do not possess necessary mechanisms to capture, store and share component integration-related knowledge.

As the automotive industry prepares for and draws nearer and nearer to the age of driverless vehicles, it has become more evident to stakeholders in the auto industry that the sharing of knowledge related to component integration processes is a critical subject which will impact on the security of both connected and fully autonomous vehicles (Colquitt et al. 2017). As noted by Kuar and Rampersad (2018), to remain competitive in a hypercompetitive environment, organisations are becoming increasingly aware of the importance of addressing the challenges introduced by cybersecurity. The sharing of component integration-related knowledge in the design, development and manufacture of components for CAVs (connected and autonomous vehicles) has the potential to address cybersecurity challenges in vehicle manufacture. However, the sharing of knowledge of relevance for component integration processes in the automotive industry, have been found to be lacking (Madzudzo et al. 2018). As highlighted in Chapter 2 and Chapter 6, reasons such as the lack of incentives to participate in knowledge sharing initiatives (Choucri et al. 2016), reluctance to share knowledge which relates to cybersecurity due to the competitive nature of the industry (Ambe et al. 2010), and a dearth of relevant and meaningful cybersecurity knowledge (Mundhenk et al. 2015). The comprehensive and detailed evidence gathering undertaken and, the literature review, suggests that none of the available knowledge sharing frameworks explore knowledge sharing in component integration in the context of the automotive industry and, how sharing of this knowledge could potentially improve the cybersecurity of modern connected vehicles. Additionally, a knowledge sharing framework to support the secure integration of components susceptible to cyber-threats has not yet been widely attempted.

There is currently no systematic technique, practice or mechanism for collecting and disseminating relevant and useful knowledge concerning component integration between relevant stakeholders, as demonstrated by the evidence provided by the study's participants. Each stakeholder (OEM, component supplier, automotive knowledge expert) applies an approach they deem appropriate and necessary. From the data collection process conducted, respondents agree that in the absence of knowledge sharing, the threat of cybersecurity vulnerabilities that emerge from insecure integration mechanisms will remain a challenge to vehicle manufacturers and suppliers of both hardware and software components. Therefore, there is an urgent need for a knowledge sharing framework for automotive digital components which correspondingly addresses cybersecurity challenges born out of insecure component integration processes.

7.1.2 Fundamentals of the knowledge sharing framework

Drawing together the learning, information and evidence gathered to this point, the actual development of the conceptual framework is the focus of this chapter. The framework developed from theory and practice, addresses:

- How component integration knowledge is shared in the automotive industry (inter and intra-organisational)
- What processes are used and how they work?
- Which factors can improve these processes?

Conceptual frameworks are products of qualitative processes of theorisation and can be defined as networks of interlinked concepts that together provide a comprehensive understanding of a phenomenon or phenomena, by explaining either graphically or in a narrative form; the main things to be studied, the key factors, construct or variables, and the presumed relationships among them (Miles et al. 2013). The concepts that constitute a conceptual framework support one another, articulate their respective phenomena and establish a framework-specific philosophy. Conceptual frameworks possess ontological, epistemological, and methodological assumptions, and each concept within a conceptual framework plays an ontological or epistemological role (Eizenberg & Jabareen 2017). The major focus of this research is the exploration of knowledge sharing in the automotive industry, specifically, the way knowledge associated with component integration is shared, and the support needed for effective and efficient knowledge sharing to take place.

In this research the conceptual framework is used to draw together the researcher's thoughts about the process of knowledge sharing and to connect these to the key themes of interest from the extensive and detailed review of the existing literature, the comprehensive evidence-gathering undertaken, and from the evaluation that took place at the latter stage of the research. The development of the framework permitted for the encapsulation of ideas and concepts and presents the core components of knowledge sharing in component integration processes in terms of practices for sharing knowledge internally within an organisation or externally with other organisations.

The framework consists of three parts:

- The first part describes the knowledge sharing components needed within the automotive industry for intra and inter-organisational knowledge sharing. It also describes the required components for knowledge sharing with external organisations (See section 7.2.1 below).
- The second part further expands on each knowledge sharing component by identifying elements required to contribute to the effective sharing of knowledge in the integration of components for connected vehicles and suggests possible indicators which can be used measure these components against.
- The third part describes a method for implementation based on the knowledge sharing process.

To address these issues, this chapter is structured as follows:

- Section 7.2 discusses the design and development of the framework. It starts by capturing the automotive environment before identifying core components, elements and indicators for successful sharing of knowledge concerning component integration processes.
- Section 7.3 discusses how the conceptual framework was revised based on the critique and feedback received from the study's respondents. A new and final framework is then presented (see Figure 7.8).
- Section 7.4 discusses a possible method for implementation based on what is identified as the knowledge sharing process (see Figure 7.15).

The conceptual framework encapsulates the main concepts drawn from the literature and the data collection activity. It focuses on three key areas see Figure 7.1 below, which are:

- The key components of a solution for consideration to the lack of sharing of knowledge related to components and their integration across the automotive sector.
- The design and development of the infrastructure required to facilitate the sharing of knowledge of relevance for component integration processes within and between organisations of the automotive industry.
- A method for implementation based on a knowledge sharing process. For each phase and subsequent steps, components and knowledge sharing factors are identified and mapped back onto the knowledge sharing process to show the necessary support organisations in the auto-domain require.

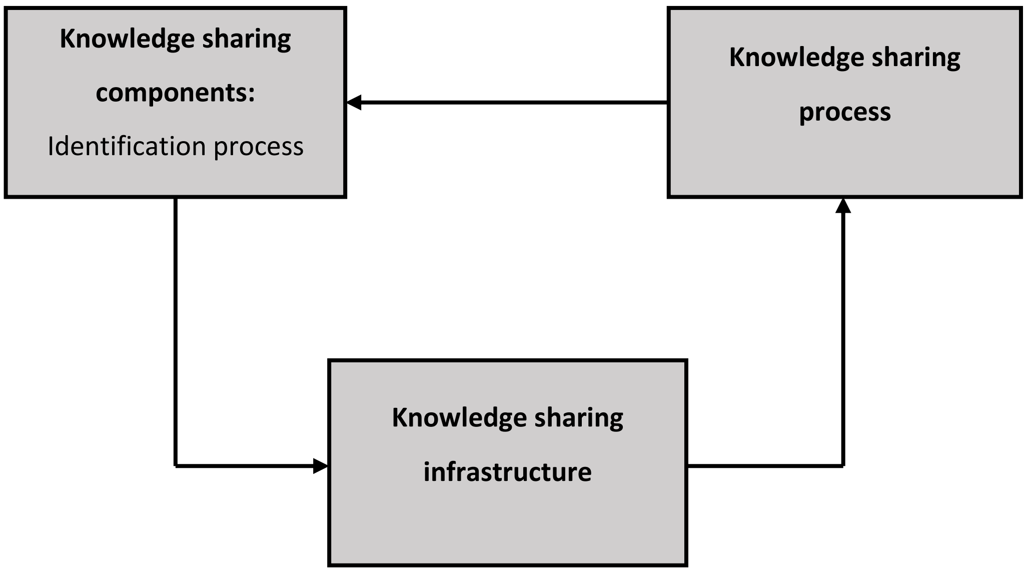

Figure 7. 1: Conceptual knowledge sharing framework

7.2 A conceptual framework for knowledge sharing: Initial version

Based on the evidence-gathering process involving experts from the automotive industry, and an extensive literature review process, the sharing of knowledge can occur between different functions, or between managers and employees *(intra-organisational*), between two or more different organisations *(inter-organisational)*, or with external factors that influence the organisation's decision making *(external environment).* This section focuses on the actual development of the conceptual framework. The key components for consideration in the sharing of knowledge related to component integration processes that have emerged from the research so far are presented in Chapters 2. Using this as a starting point for the development of the conceptual knowledge sharing framework, the following sections will explain how the framework was developed.

7.2.1 Automotive environment

As mentioned by some of the research participants and highlighted in the literature review chapter, various factors that influence the way knowledge for component integration processes is shared within and amongst vehicle manufactures and component suppliers. These occur in three discrete environments: the inter-organisational environment, the intra-organisational environment, and the external environment. The following sections discuss each environment and the knowledge sharing factors to be considered within each environment.

Intra-organisational environment

This refers to an environment within an organisation that permits sharing of explicit and tacit knowledge. The opportunities to share knowledge between different teams, divisions, functions and/or between levels in the hierarchy within the organisation are a key factor in achieving and improving on component integration processes. The intra-organisational environment is at times referred to as an internal environment that provides the physical opportunity for formal and informal interaction to support knowledge sharing. Factors to be considered within an intra-organisational environment include but are not limited to; opportunities to exchange ideas, concepts, experiences, integration processes and, processes for disseminating knowledge. As noted by some of the studies participants, opportunities within an organisation to share both tacit and explicit knowledge are key, and organisations that fail to exploit lose out on vital opportunities to improve on existing integration strategies.

Inter-organisational environment

The inter-organisational environment refers to an environment that allows the sharing of knowledge between different organisations. Opportunities to share knowledge with different organisations can have substantial implications because it can influence decisions related to the processes required for effective knowledge sharing and, decisions related to the type of knowledge to be shared. Golinelli et al. (2011) discuss how inter-organisational relationships result in managers making better decisions about collaboration initiatives and alliances.

External environment

This element is used to refer to external and uncontrollable factors which can potentially influence an organisation's component integration decisions, policy, strategy and /or performance. These external factors can also determine how knowledge is shared, and the form in which knowledge is shared. External factors such as legislation, regulatory, political, economic and social factors, which influence how knowledge is shared in the automotive continuum fall within this environment.

Another popular approach is to look at knowledge management in terms of people, processes and technology. As discussed in Chapter 2 section 2.2.3, knowledge sharing is a key activity in the processes of knowledge management and as such, people, processes and technology should also be considered in knowledge sharing.

People: creating the "right" culture which includes values and behaviours ideal for knowledge sharing is usually the most challenging yet the most important task. An organisation's management is tasked and required to play a huge role in creating, maintaining and encouraging the continued existence of this culture. A culture of knowledge sharing often starts with the creation of a vision statement and it is further strengthened by the organisational structure. This knowledge sharing culture can be further strengthened or hindered by policies and initiatives relating to rewards, incentives, and benefits designed to enhance organisational learning and the sharing of knowledge. The automotive industry needs to create and adopt a culture of security through knowledge sharing. As revealed by some of the study's participants, a culture of security through knowledge sharing is yet to fully embed itself within component integration in vehicle development. A culture that allows and permits the sharing of relevant knowledge related to component integration, designed to assist with the mitigation of cybersecurity challenges facing connected vehicles, needs to be encouraged by management.

Processes: For component suppliers and vehicle manufactures to share component integration-related knowledge, they need to ensure that there are systems and processes in place to support knowledge sharing. As illustrated by Figure 7.2 below, knowledge sharing processes should take into consideration individual factors, organisational factors and technological factors that support the sharing of knowledge. Individual factors consist of processes that permit employees to share knowledge, organisational factors relate to the way the organisation is structured and supports knowledge sharing, and technological factors relate to the media (information and communication technology) that is used to capture and share knowledge.

Technology: A common misconception is that knowledge sharing is primarily about the technology used to capture and share knowledge. Technology is often a vital enabler of knowledge sharing, it often assists in allowing people to collect, process and share information. Nonetheless, it is crucial that any technology an organisation adopts fits the people, the processes and the type of knowledge to be shared.

The components discussed above are crucial for successful knowledge sharing. If one component is missing, then the potential benefits associated with knowledge sharing are not fully realised. Arguments between researchers as to which component is more important than the others favour the people component (Holste & Fields 2010, Wiig 2012). The development of a friendly knowledge sharing culture among vehicle manufacturers and component suppliers, which is supported by processes that allow for secure knowledge sharing and, which are enabled by technology should be the focus of the automotive industry.

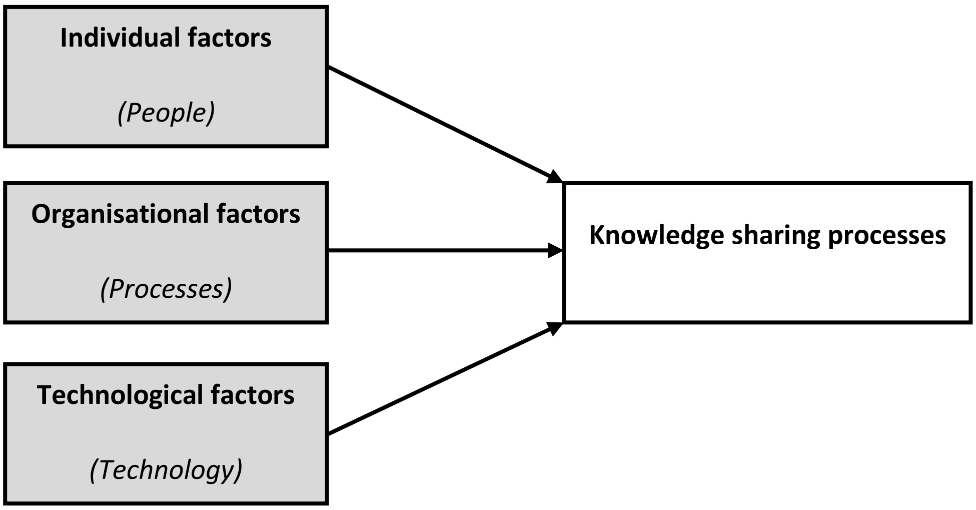

Figure 7. 2: Factors required for knowledge sharing processes

7.2.2 Identification of core components

Components in the context of this thesis define the set of core features that are required to be present and effectively functioning together for effective knowledge sharing to occur. The primary functions constitute the core components that are necessary for effective knowledge sharing to occur. The following areas were identified as being core components for the sharing of knowledge in component integration processes in the automotive sector:

Organisational structure

Refers to the broad purpose and vision of the organisation (vehicle manufacturer or component supplier), how the different segments of the business are organised and, how they relate to one another. It also extends to how the employees within the organisation and the different business segments are organised and, how they relate to one another. The organisational structure potentially decides the ability of the organisation in learning from its environment, which includes other vehicle manufactures, other component suppliers, and the various stakeholders affiliated with component manufacturing, to perform core functions related to secure component integration. Additionally, it has the potential to assist with mitigation solutions to cyber-related challenges that are born out of insecure component integration processes. The organisational structure helps understand, address and develop processes for the sharing of knowledge that is necessary for secure component integration.

Human resources

The development needs and requirements of employees within the organisation is crucial, as it is within this remit, that staff are qualified, informed and motivated to fulfilling core functions related to the sharing of knowledge in component integration processes. If staff are not well informed, trained and confident, they may not feel qualified to share their knowledge, qualified to engage and, qualified to use new technology or processes that are designed to target and promote the sharing of knowledge. Human resources within the organisation are crucial in ensuring that tacit knowledge; which expresses skills, know-how and practical knowledge, and explicit knowledge; which consists of knowledge expressed in a tangible way possessed by the organisation’s employees, is not left untapped.

Communication

Communication is potentially the most crucial component, it refers to how information and knowledge is shared within the organisation, between different organisations, and between employees and relevant stakeholders. It identifies processes, strategies and relevant media (technological infrastructure) suitable for knowledge sharing (verbally, non-verbally or via other mechanisms) within an organisation and, between geographically dispersed organisations exposed to varying political, legal and regulatory knowledge sharing requirements. The communication component also encompasses ways to address and solve knowledge sharing challenges that arise and are identified by stakeholders involved in component integration processes.

Leadership

The leadership within an organisation plays a vital role in encouraging all forms of knowledge sharing. The sharing of knowledge related to component integration processes can be seen as a multifaceted and complex process that involves intricate human behaviour. Empowering leadership significantly influences individuals' knowledge sharing behaviour by affecting their attitude towards knowledge sharing. A variety of leadership behaviours have been studied, among which empowering leadership is found to improve conscious and voluntary knowledge sharing. The leadership in vehicle manufacturing organisations and organisations that focus on component development should be motivated dynamic individuals who work closely with employees involved in component design, development and integration. The leadership should have an understanding of resources that are needed to identify, develop and improve processes for knowledge sharing. Additionally, they should not only identify knowledge sharing needs for their organisation but also influence ways in which partner organisations and other stakeholders share knowledge.

Technological infrastructure

The technological infrastructure refers to the organisations' entire collection of hardware, software, networks, data centres, facilities and related equipment used within the organisation that assist and permit processes for knowledge acquisition, creation, storage, dissemination and application.

Regulatory requirements

Regulations, best practices and standards designed to assist vehicle manufacturers, component suppliers and developers are crucial for knowledge sharing. The organisation must demonstrate compliance with design and manufacturing standards such as the Society of Automobile Engineers (SAEJ3061), International Organisation for Standardisation (ISO26262). Component integration approaches must adhere to integration requirements set out within automotive best practices, standards and regulations, or order to capture and share knowledge that is deemed as current, compliant and usable.

Political and legal environment

The political and legal environment in which the OEM or component supplier operates in has a tremendous impact on the way knowledge can be shared. Political and legal environments can potentially create barriers that cause knowledge sharing to be slow, costly, and uncertain. Achieving effective knowledge sharing processes in component integration requires compliance with laws and legislative measures that are imposed and required by the host nation where the organisation resides. The legal and legislative requirements for different countries to which the organisation is exporting too, also need to be fulfilled for example, in the European Union (EU), legislation such as the General Data Protection Regulation (GDPR) which came into effect from 25 May 2018, plays a vital role as it sets out guidelines for information sharing; these guidelines affect knowledge sharing in the automotive domain to an extent.

Financial resources

Financial resources are greatly linked to how knowledge is shared. The development and creation of an appropriate infrastructure to facilitate knowledge sharing processes that remain current, usable and available requires support and resources from the financial team. Insufficient or the lack of adequate financial resources can impact on creating an effective knowledge sharing environment. Knowledge sharing processes that are not backed up by adequate financial resources are often doomed to fail before they begin due to the absence of appropriate infrastructure and sharing capabilities.

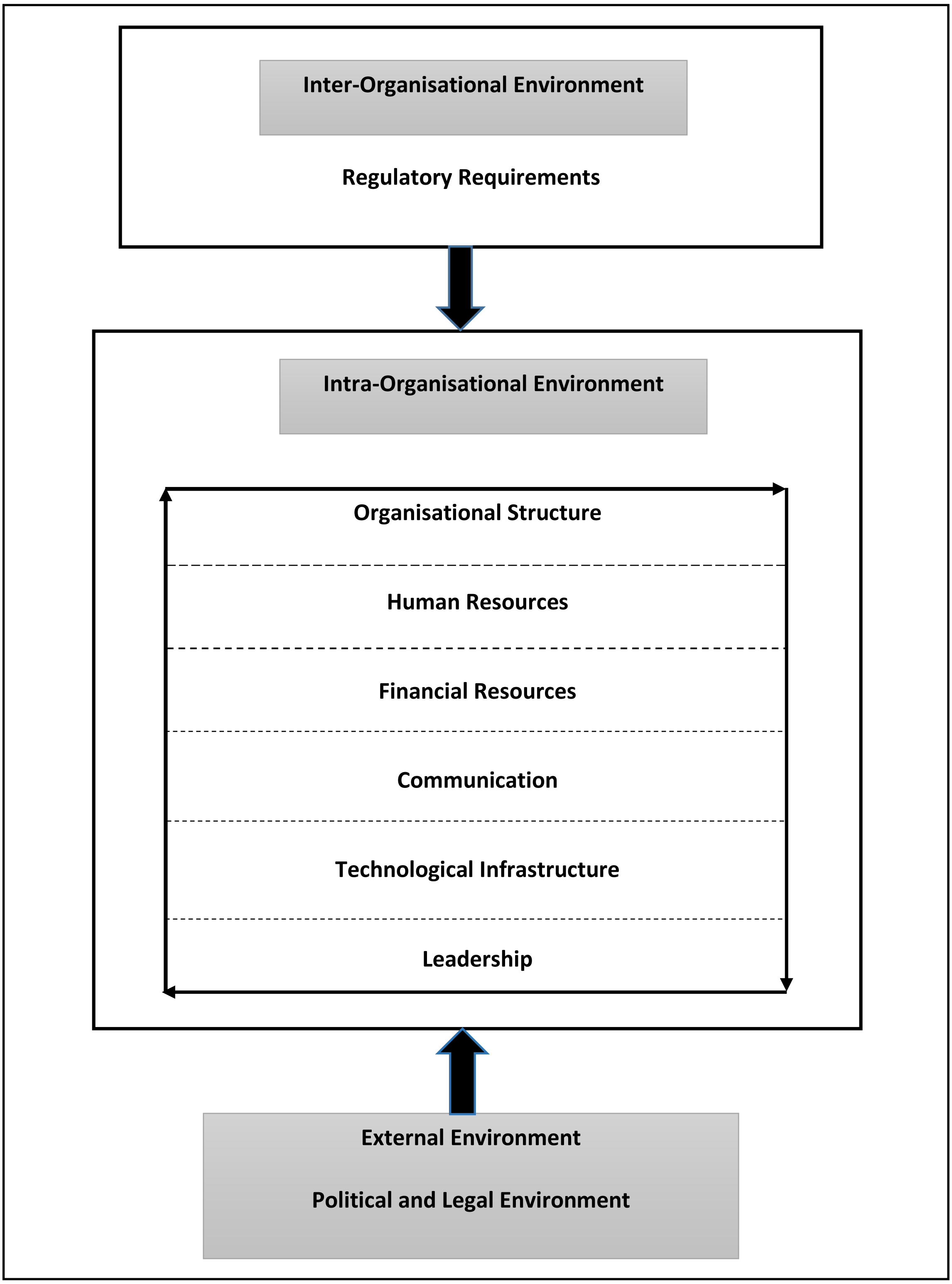

Figure 7. 3: Knowledge sharing components

The key component areas that have emerged from the research in the foregoing have been clustered and structured in Figure 7.3 above. The arrows in the framework highlight the horizontal and vertical interaction of each component, the framework is not generally intended to be sequential, but for illustrative convenience has been presented in this way. In Chapter 2, the factors which influence knowledge sharing in the automotive sector, in particular, the sharing of knowledge associated with component integration processes were identified. The researcher undertook an analysis of the factors highlighted in the literature and those highlighted by the study's participants. These are summarised in Table 7.1 below.

Table 7. 1: Knowledge-sharing factors grouped according to environment

Component	Factors that influence knowledge-sharing	Environment
Organisational structure	Management	Intra-organisational
Organisational structure	Organisational structure	Intra-organisational
Organisational structure	Organisational aim	Intra-organisational
Organisational structure	Knowledge sharing behaviours	Intra-organisational
Organisational structure	Project plan	Intra & inter-organisational
Organisational structure	Roles and internal structures	Intra-organisational
Human resources	Training	Intra-organisational
Human resources	Performance improvement	Intra-organisational
Human resources	Incentives and rewards	Intra-organisational
Human resources	Motivation	Intra-organisational
Human resources	Personal satisfaction	Intra-organisational
Human resources	Organisational commitment	Intra-organisational
Human resources	Knowledge sharing behaviours	Intra-organisational
Human resources	Teams	Intra-organisational
Human resources	Human resource policy	Intra-organisational
Financial resources	Financial management	Intra-organisational
Financial resources	Funding environment	Intra-organisational
Financial resources	Financial responsibility	Intra-organisational
Communication	Knowledge sharing opportunities	Intra-organisational
Communication	Knowledge sharing behaviours	Intra & inter-organisational
Communication	Social environment	Intra & inter-organisational
Leadership	Trust	Intra-organisational
Leadership	Leadership	Intra-organisational
Leadership	Organisational culture	Intra-organisational
Leadership	Power	Intra-organisational
Leadership	Knowledge sharing behaviours	Intra-organisational
Technological infrastructure	communication	Intra-organisational
Technological infrastructure	technology	Intra & inter-organisational
Technological infrastructure	Knowledge sharing processes	Intra & inter-organisational
Regulatory requirements	Regulation	Inter-organisational
Regulatory requirements	Automotive best practices	Inter-organisational
Regulatory requirements	Automotive and manufacturing standards	Inter-organisational
Regulatory requirements	Governing boards	Inter-organisational
Political and legal	Government climate	External environment
Political and legal	Political structures	External environment
Political and legal	Government policies	External environment
Political and legal	Industrial policies	External environment
Political and legal	Economic climate	External environment

The components which have a direct impact on the sharing of relevant knowledge concerning component integration processes, the main focus of this thesis, are illustrated in Figure 7.4 below. Organisational structure, human resources, communication and leadership all deal with the people aspect of knowledge sharing. Financial resources, communication processes and infrastructure which are enabled by technology need to be available to support people in knowledge sharing approaches within an organisation.

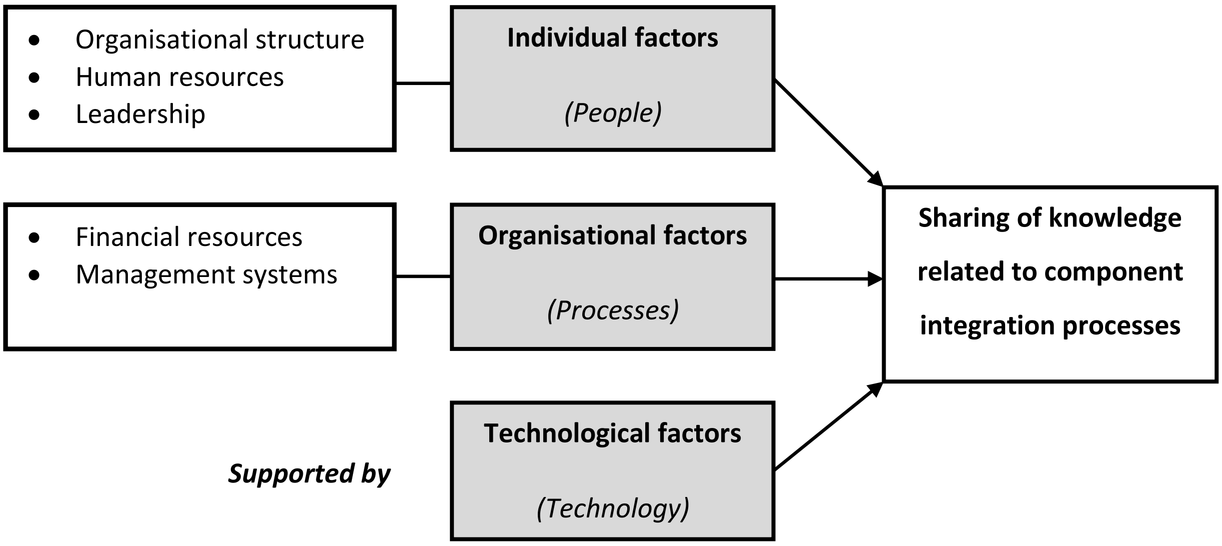

Figure 7. 4: Knowledge sharing factors

7.2.3 Identification of essential knowledge sharing factors

Practices, processes and activities for the sharing of knowledge in component integration procedures must be supported and encouraged through policy, structures, systems and actions. This corresponds to what the study's participants referred to as "elements" that influence the sharing of knowledge in component integration processes. According to the study's participants, elements are essential processes and activities that ensure that knowledge appropriate for integration is captured and shared. To increase the efficiency and effectiveness of the knowledge capture and share process, all of the elements described in the framework are essential. Without a deep understanding of these elements and how they interact, the effectiveness and sustainability of sharing knowledge for component integration is at risk, therefore, the following sections discuss each component and the relevant elements identified within each component. Justification for the inclusion of each component and the relevant elements can be found in Chapter 2 and Chapter 6.

Organisational structure

Organisational structure relates to the broad purpose and vision of the vehicle manufacturing or component manufacturing organisation. It also relates to how the different segments of the business are organised and how they relate to one another. The organisational structure encompasses policies, procedures, values and long-term planning to meet the purpose and vision of the organisation. The various factors which fall into this category identified through the literature review process, and through the data collection process are: management, organisational aim, knowledge sharing behaviours, roles and internal structures, and project plan.

The "*project plan"* defines the scope and objectives of the intended component integration task. An updated project plan should exist for each project, and it should include the roles and location of all staff engaged within the project. Most importantly, the project plan should be kept electronically and should be made available to all relevant stakeholders with an interest in the project. Management, roles and internal structures are grouped to form the element "*management"* which defines the roles and responsibility of the organisation. These roles and responsibilities are defined in the policies and procedures manual and used as the basis of task assignment. The organisational infrastructure which also includes the technology required to support the organisational structure relates to physical mechanisms to support *knowledge sharing behaviours*. The mission and vision statement which is initially defined when the organisation is established should be reviewed on an annual basis and should be visible to all employees.
The key elements which encompass all the elements in the organisational structure component, and greatly affect the sharing of knowledge in component integration processes are:

- Project plan
- Management
- Knowledge sharing behaviours

Table 7.2 below summaries the organisational structure component with its essential elements and core competencies that are relevant for the sharing of knowledge for component integration processes.

Table 7. 2: Elements for the organisational structure component

Core component	Knowledge sharing factor	Core competencies
1. Organisational structure	1.1 Project plan	A project plan that shows the following should be available: • The integration strategy to be employed within the project • The process of capturing and disseminating knowledge relating to component integration • List of associated projects • A list of the staff, their expertise and their location Changes or amendments to the project plan should be communicated to all relevant stakeholders
	1.2 Management	The organisation's managerial brass should play an important role in building knowledge sharing structures and processes. Ensuring that knowledge sharing processes remain relevant and usable is a task management should oversee
	1.3 Knowledge sharing behaviours	The organisational structure should include technology and physical mechanisms that support knowledge sharing behaviours

Human resources

In the context of this study, human resources within an organisation refers to the development needs of employees to ensure that they are qualified, informed, and motivated to fulfilling core functions related to the integration of components and the sharing of knowledge related to component integration processes. The various factors which fall into this category identified through the literature review process, and through the data collection process are: training, performance improvement, incentives and rewards, motivation, personal satisfaction, organisational commitment, knowledge sharing behaviours, team and human resource policies

It is essential for an organisation to have a *human resources policy* that supports the organisations' administrative functions, performance management, employee relations and resource planning. Each organisation engaging in component integration, and knowledge sharing tasks will potentially have a different organisational structure depending on its mission statement, objectives and aims, and so, develops an individual set of human resource policies. Nonetheless, the establishment of policy aids in demonstrating, both internally and externally, compliance with standards, corporate governance, regulation and legislative commitments. The establishment of policy also demonstrates how an organisation meets requirements for employee training, this ensures that it has qualified personal to fulfil the project requirements. Human resources policy can potentially build and/or support knowledge sharing behaviours within the organisation.

The training, performance improvement, and team factors are grouped to form the element *staff performance and development.* Staff development and training requirements should be evaluated on a project-by-project basis to ensure that staff have relevant and required skills. Following on from the evaluation process, relevant training should be provided. The motivation, personal satisfaction, organisational commitment, and incentives and rewards factors are grouped to form the *personal commitment and satisfaction* element. The *knowledge sharing behaviours* element is greatly influenced by the organisation's human resource policy, training and development initiatives. It is also influenced by team structures, incentives and rewards along with organisational commitment.

The key elements which encompass all the factors that affect the sharing of knowledge in component integration processes in the human resources component are:

- Human resources policy
- Staff performance and development
- Personal commitment and satisfaction
- Knowledge sharing behaviours

Table 7.3 below summaries the human resources component with its essential elements and core competencies that apply to the sharing of knowledge of relevance for component integration processes.

Table 7. 3: Elements of the human resources component

Core component	Knowledge sharing factor	Core competencies
2. Human Resources	2.1 Human resources policy	The organisation should have a policy that supports the organisation's administrative personal functions, performance management, employee relations and resource planning. The policy should address how the organisation complies with standards, corporate governance, regulation and legislative commitments with regards to knowledge sharing
	2.2 Staff performance and development	Staffs' performance is evaluated on a project-by-project basis to identify training and development requirements. Teams are formed and designed to contain diverse skillsets
	2.3 Personal commitment and satisfaction	The organisation must ensure staff are committed, motivated and satisfied through training and development opportunities, rewards and incentives, recognition of individual and/or team performance, career progression and empowerment
	2.4 Knowledge sharing behaviours	The organisation should have a well-established knowledge sharing culture. Employees should be well informed on the benefits of knowledge sharing, and the processes for knowledge capture and sharing

Financial resources

Financial resources refer to how the organisation's financial requirements are addressed. The study's participants highlight the importance of financial resources to support knowledge sharing and component integration. The various factors which fall into this category identified through the literature review process, and through the data collection process are: financial management, funding environment, and financial responsibility.

The *financial management* factor ensures that relevant and sufficient monitory support to acquire and install required infrastructure (technical and non-technical), that supports knowledge sharing within an organisation or within a collaborative project is available. Employees with adequate skills and knowledge should lead the financial resources team. The *funding environment* factor provides organisations with access to resources and funding provided by local governments, funding agencies and relevant stakeholders whose interests focus on improving and developing research in component integration, automotive cybersecurity and knowledge sharing approaches. The *financial responsibility* factor ensures that the organisation implements measures for regular internal and external financial reporting.

The key elements which encompass all the factors in this component are:

- Financial management
- Funding environment
- Financial responsibility

Table 7.4 below summaries the financial resources component with its essential elements and core competencies that are relevant for the sharing of knowledge related to component integration processes.

Table 7. 4: Elements of the financial resources' component

Core component	Knowledge sharing factor	Core competencies
3. Financial Resources	3.1 Financial management	The organisation must set up a financial budget for component integration and knowledge sharing processes. The budget must support training and staff development. The budget must have provision for the acquisition of infrastructure to support and maintain knowledge sharing processes
	3.2 Funding environment	The organisation should ensure it has access to resources and funding to support knowledge sharing processes and associated processes
	3.3 Financial responsibility	The organisation should ensure transparent, lawful and regular internal and external financial reporting. The project plan should state whether reporting will be conducted monthly, quarterly etc.

Communication

The communication component refers to how information and knowledge is shared within the organisation, between different organisations and, between employees, and with relevant stakeholders. It is a crucial component that also encompasses processes, strategies and technologies that support the sharing of knowledge. The various factors which fall into this category identified through the literature review process, and through the data collection process are: knowledge sharing opportunities, knowledge sharing behaviours, and social environment.

All three factors; knowledge sharing opportunities, knowledge sharing behaviour and social environment, within this category are grouped to form one element termed *communication mechanism*. While knowledge sharing opportunities are contained within the organisation, knowledge sharing behaviours and social interaction can occur within the organisation and between different organisations. It is crucial that the organisation has a clear communication mechanism, that is understood by all participants and relevant stakeholders involved in the knowledge sharing process. Changes in regulation, standards and/or procedures for knowledge sharing or component integration should be well communicated to all stakeholders.

The key element which encompasses all the factors in this component is:

- Communication mechanism

Table 7.5 below summaries the communication component with its essential element and core competency that is relevant for the sharing of knowledge for component integration processes.

Table 7. 5: Elements of the communication component

Core component	Knowledge sharing factor	Core competencies
4. Communication	4.1 Communication mechanism	The organisation should have clear communication mechanisms that create knowledge sharing opportunities, encourages knowledge sharing behaviour across intra and inter-organisational levels. Changes to procedures, processes, standards and, regulation concerning component integration knowledge sharing must be communicated to all relevant stakeholders

Leadership

The leadership within an organisation plays a vital role in encouraging all forms of knowledge sharing. As highlighted by the study's participants, the knowledge sharing culture starts with management and trickles down the organisational structure. The various factors which fall into this category identified through the literature review process, and through the data collection process are: trust, leadership, organisational culture, power and knowledge sharing behaviours.

The literature on social interaction and economic transactions (Chapter 2 section 2.3.3) define trust, power and supportive leadership as important factors that facilitate knowledge sharing. Employees are more willing to engage in cooperative behaviours such as knowledge sharing when the relationship, they have with their organisation is characterised by a high level of trust and support from leadership. These skills are important in knowledge sharing within an organisation for transparency and accountability. For example, the component manufacturing organisation must demonstrate fairly and transparently, how component integration information is shared with OEMs and other component suppliers. The trust, power and knowledge sharing behaviours factors have been grouped to form the element of *transparency and accountability*.

The leadership and organisational culture factors have been grouped to form the *organisational culture* element. As noted by some of the study's participants, the organisational structure plays a crucial role in the quality of knowledge shared. Leadership plays a crucial role in creating an organisational culture which supports and encourages knowledge sharing, navigating legal and regulatory challenges that impact knowledge sharing in component integration processes.

The key elements which encompass all the factors in this component are:

- Transparency and accountability
- Organisational culture

Table 7.6 below summaries the leadership component with its essential elements and core competencies that are relevant for the sharing of knowledge for component integration processes.

Table 7. 6: Elements of the leadership component

Core component	Knowledge sharing factor	Core competencies
5. Leadership	5.1 Transparency and accountability	The organisation should demonstrate fair, transparent and accountable knowledge sharing processes. Component integration knowledge must be made available to all relevant stakeholders. The organisation must demonstrate how its knowledge sharing processes address legal and regulatory requirements
	5.2 Organisational culture	The leadership should create an environment and culture that encourages and supports knowledge sharing

Technological infrastructure

This component refers to the entire media and, associated processes and procedures that an organisation employs to ensure it fulfils its knowledge sharing objectives. The technological infrastructure should aim to address current and future knowledge sharing requirements that exist within the organisation, and requirements that permit knowledge sharing with external organisations. This is to ensure that knowledge sharing in collaborative projects or joint ventures are catered for. The various factors which fall into this category identified through the literature review process, and through the data collection process are: communication, technology, and knowledge sharing processes. The communication and technology factors were grouped to form the *information technology* element. This element encompasses IT procedures that an organisation should have in place.

The data collection process highlighted additional elements required for effective knowledge sharing. The study's participants highlighted the need for a clear knowledge sharing strategy designed to address knowledge acquisition, creation, storage, and dissemination. Therefore, the organisation should also have an information management system that caters for and addresses knowledge sharing requirements and challenges introduced by non-disclosure agreements, design contracts, and other gagging orders that are so prominent in the automotive continuum. The information management system should also have provisions for documenting and packaging best practices and lessons learnt from each project executed internally or with external partners. These should be fed back to the knowledge sharing strategy to ensure that the quality and performance of the knowledge sharing strategy is monitored, adjusted and improved with each project completed.

The key elements which encompass all the factors in this component are:

- Information technology
- Knowledge sharing strategy
- Quality assurance system
- Information management system
- Training teams

Table 7.7 below summaries the technological infrastructure component with its essential elements and core competencies that apply to the sharing of knowledge of relevance for component integration processes.

Table 7. 7: Elements of the technological infrastructure component

Core component	Knowledge sharing factor	Core competencies
6. Technological Infrastructure	6.1 Information technology	IT procedures should include procedures for maintaining, replacing and updating equipment used for knowledge sharing. The procedures must be well communicated to all relevant stakeholders
	6.2 Knowledge sharing strategy	All organisations (OEMs and component suppliers) should have a clear process for the acquisition, creation, storage, and dissemination of integration knowledge that is well understood by all relevant stakeholders engaged in the project
	6.3 Quality assurance system	The organisation should have a well-established system for monitoring, assessing and improving the quality of the knowledge sharing process
	6.4 Information management system	The organisation should have an information management system that will address knowledge sharing requirements and challenges introduced by non-disclosure agreements, design contracts etc. Best practices and lessons learnt within each project should be documented in the knowledge sharing strategy
	6.5 Training teams	The training teams will monitor for changes in best practices, standards, requirements and lessons learnt from other projects. The training teams will train staff (internal and external) on new processes and procedures for quality and performance improvement

Regulatory requirements

Effective knowledge sharing related to component integration processes requires compliance with regulation, best practices and standards that are developed to improve component integration approaches. The organisation must demonstrate compliance with regulations, best practices and standards designed for the automotive industry. The various factors which fall into this category identified through the literature review process, and through the data collection process are: regulation, best practices, standards, and governing boards.

A vehicle manufacturing organisation or component manufacturing organisation will have relationships with external entities, for example, governing boards for organisations that provide funds for automotive research initiatives, government authorities, board members of governing organisations focused on creating best practices and standards etc. According to the study’s participants, a clearly defined strategy and operational plan for policy engagement and advocacy with other organisations and stakeholders are needed. The policy should include clear terms of engagement, a code of ethics and information on how the sharing of knowledge will be conducted on a project-by-project basis. Additionally, the organisation must demonstrate through policy, how it complies with industry best practices, regulation and standards. The relationship that the organisation has with organisations that are tasked with regulation, best practice and standards development should also be clearly defined.

The key elements which encompass all the factors in this component are:

- Partnerships with similar organisations
- Relationships with governing boards
- Regulation
- Standards
- Best practices

Table 7.8 below summaries the external environment component with its essential elements and core competencies that are relevant for the sharing of knowledge related to component integration processes.

Table 7. 8: Elements of the regulatory requirements component

Core component	Knowledge sharing factor	Core competencies
7. Regulatory Requirements	7.1 Partnerships with similar organisations	The organisation should have a clearly defined strategy and operational plan for policy engagements and advocacy with other similar organisations (an OEM's strategy for engagements should also cater for other OEMs)
	7.2 Relationships with governing boards	The organisation should have clearly defined terms of engagement with organisations that are focused on the creation of best practices, policy, standards, and funding opportunities available for knowledge sharing approaches. Such relationships are crucial for staying informed on changes that affect component integration knowledge sharing
	7.3 Regulation	The organisation will have to demonstrate compliance with regulations. The organisation must track and document changes to the knowledge sharing processes and component integration approaches to reflect changes introduced by changes in regulation
	7.4 Standards	The organisation will have to demonstrate compliance with standards created and developed by organisations such as ISO and SAE. The organisation must demonstrate how it complies with automotive standards
	7.5 Best practices	The organisation will have to demonstrate how it incorporates the industry's best practices concerning knowledge sharing and component integration

Political and legal environment

The political and legal environment in which the OEM or component supplier operates has a tremendous impact on the way knowledge can be shared. This component is potentially the most challenging factor to the sharing of knowledge related to component integration processes, as political and legal waters are hard to navigate due to the dispersed geographical nature of the automotive industry. As stated by some participants, political and legal requirements shift based on where the organisations sharing knowledge are located. The various factors which fall into this category identified through the literature review process, and through the data collection process are: the government, political structures, government policies, industrial policies, and the economic climate.

The dispersed geographical nature of the automotive industry affects how knowledge regarding component integration is shared. Political and legal structures differ for each country; thus, the organisation must remain well informed on any changes to a countries' political and legal structures that affect the sharing of knowledge for component integration processes. The political structures, economic climate factors are grouped to form the *laws and legal restrictions* element, while the government policies and industrial policies factors are grouped to form the *policies* element. The government policies and government factors were grouped to form the *relationships with government authorities'* element.

The key elements which encompass all the factors in this component are:

- Laws and legal restrictions
- Policies
- Relationship with government authorities

Table 7.9 below summaries the political, legal and regulatory component with its essential elements and core competencies that are relevant for the sharing of knowledge related to component integration processes.

Table 7. 9: Elements of the political and legal component

Core component	Knowledge sharing factor	Core competencies
8. Political and Legal	8.1 Laws and legal restrictions	The organisation should observe and adhere to laws and legal requirements that relate to the sharing of knowledge concerning component integration processes. The organisation should have procedures in place to document and track laws and legal requirements for all countries where the organisation conducts business
	8.2 Policies	The organisation should adhere to policies imposed by different countries where knowledge sharing will occur. The organisation should have procedures in place to document and track changes to policies
	8.3 Relationship with government authorities	The organisation should foster and maintain relationships with government authorities to ensure it remains informed on laws about knowledge sharing, and policy changes within the automotive domain that relate to component integration or knowledge sharing

The key areas that have emerged from the research in the preceding sections were clustered and structured in Figure 7.3 above. Figure 7.5 below brings together the identified knowledge sharing components and their associated elements. However, the initial framework presented in Figure 7.5 below does not fully reflect the dynamic interaction.

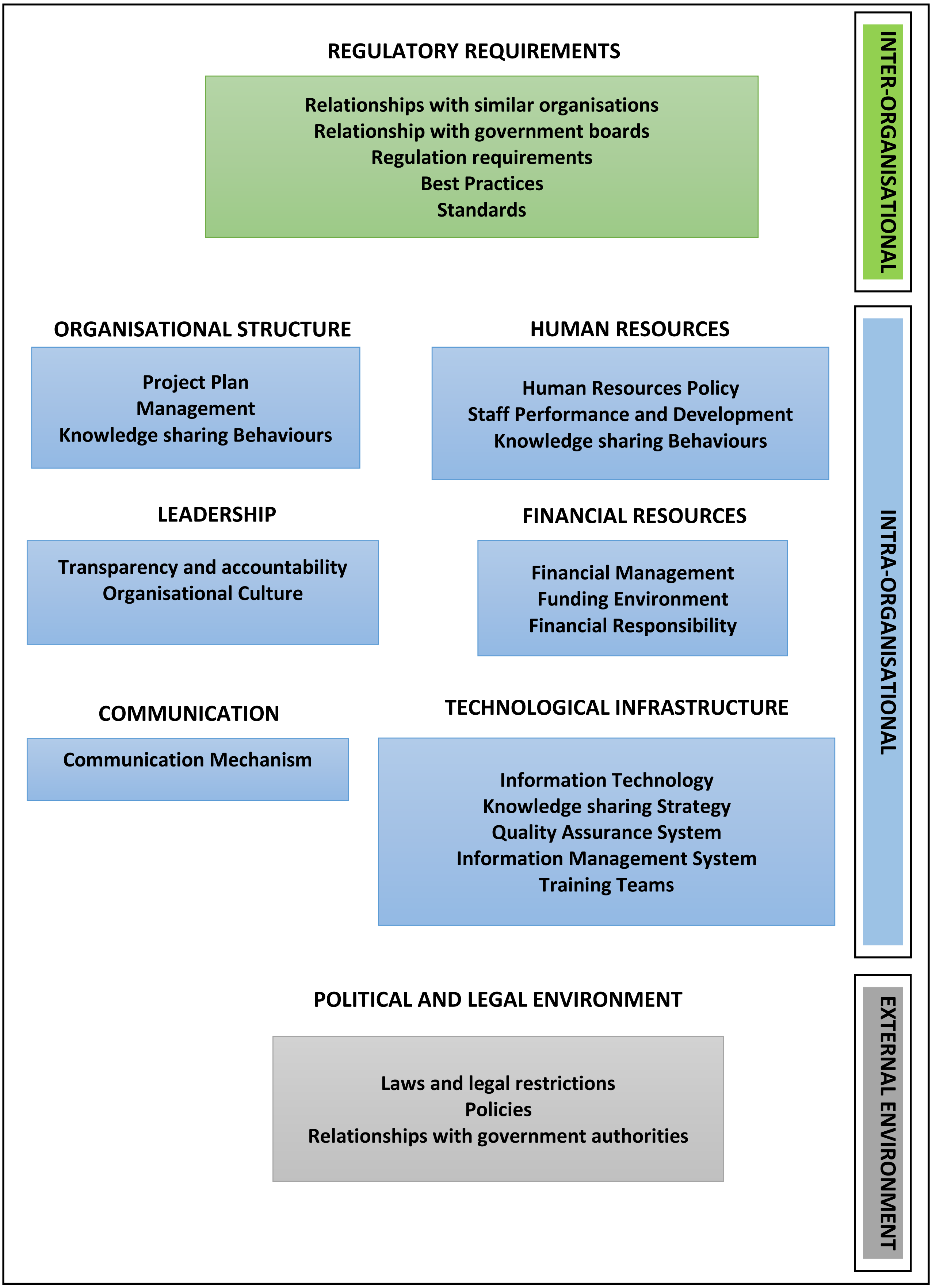

Figure 7. 5: The initial draft of the knowledge sharing framework

7.2.4 Identification of progress metrics and indicators

Indicators are the standard of measurement employed to monitor and assess whether each component in the framework and its associated core competence meet the standards for each knowledge sharing factor. Measuring each component to ensure it satisfies each knowledge sharing factor requires a systematic approach with metrics that assess efficiency, impact, effectiveness and fulfilment of requirements for the execution of knowledge sharing activities that relate to component integration processes. It also forms the basis for the identification and evaluation of value-adding activities and resources for; assessing and comparing knowledge sharing processes and, evaluating component integration processes for improving the security of connected vehicles. According to Grobler et al. (2011), measurements need not be hard and financial, they can be soft and non-financial. Indicators and measurements were added as highlighted by Table 7.10 below.

The conceptual framework presented in Figure 7.4 above addresses objective 6 and, potentially supports the sharing of knowledge of relevance for the digital security of connected vehicles. The knowledge sharing structure provides a comprehensive picture illustrating components and essential elements which form the foundations on which the sharing of effective knowledge for component integration is based. The figure also illustrates the environment in which the identified components and elements operate in. Section 7.3 discusses the eventual revision of the framework, thereby, addressing research question 5 "how can knowledge related to component integration processes be shared effectively between OEMs, the automotive supply chain, and amongst suppliers, for improved digital security of connected vehicles?" and subsequently addresses the final research objective "to expose the conceptual framework to critique before critically evaluating the final framework to demonstrate an original and significant contribution." This followed by section 7.4 which discusses the knowledge sharing process and methods for implementing the framework.

Summary

The framework has been developed to promote the sharing of knowledge of relevance for component integration processes. This framework aims to assist the automotive industry to overcome some of the limitations of existing techniques for knowledge sharing in the integration of components for connected vehicles as identified in the relevant literature. This new framework which is supported by theory and feedback from the study's participants presents a knowledge sharing infrastructure which further expands on the components and elements identified in the data collection process. It presents the core components of the organisation; the intra-organisational environment, the inter-organisational environment and the external environment, and the essential knowledge sharing factors by which the organisation that chooses to use the framework, can measure and identify knowledge sharing processes. The next section discusses and presents the revised and final framework after receiving feedback from personnel (senior management) employed by OEMs, automotive component manufacturing organisations, and knowledge experts from the automotive industry.

Table 7. 10: Indicators and measurement for knowledge sharing infrastructure (the initial version)

Component	Knowledge sharing factor	Core competencies	Indicator	How it can be measured
INTRA-ORGANISATIONAL ENVIRONMENT				
1. Organisational structure	1.1 Project plan	A project plan that shows the following should be available: • The integration strategy to be employed within the project • The process of capturing and disseminating knowledge related to component integration processes • List of associated projects • A list of the staff, their expertise and their location Changes or amendments to the project plan should be communicated to all relevant stakeholders	A project plan that is reviewed and evaluated by all stakeholders A process and timeframe for reviewing the project is based on project timeline and duration An organisational chart that is regularly updated and consistently used	A project plan with an integration strategy and a knowledge sharing process that is available to all stakeholders An organisational chart that shows roles and responsibilities should be available to all stakeholders
	1.2 Management	The organisation's managerial brass should play an important role in building knowledge sharing structures and processes. Ensuring that knowledge sharing processes remain relevant and usable is a task management should oversee	Knowledge sharing initiatives that are supported by management A strategy for reviewing and updating knowledge sharing processes A strategy for reviewing and updating component integration processes	Management backed knowledge sharing structures and processes An updated strategy for reviewing and updating knowledge sharing and component integration processes on a project-by-project basis
	1.3 Knowledge sharing behaviours	The organisational structure should include technology and physical mechanisms that support knowledge sharing behaviours	Training programs for developing skills and competencies A strategy that identifies areas that require support and	A training program available to all employees. Employees should be aware of the existence of the training program

			infrastructure to support knowledge sharing	A strategy to review and update staff training programs in-line with project demands and requirements
2. Human Resources	2.1 Human resources policy	The organisation should have a policy that supports the organisation's administrative personal functions, performance management, employee relations and resource planning. The policy should address how the organisation complies with standards, corporate governance, regulation and legislative commitments about knowledge sharing	Human resource policy documents that are accessible electronically and manually Policy documents that demonstrate how the organisation complies with standards, corporate governance, regulation and legislative commitments concerning knowledge sharing and component integration	A regularly reviewed and updated human resources policy document that is accessible to all stakeholders
	2.2 Staff performance and development	Staffs' performance is evaluated on a project-by-project basis to identify training and development requirements. Teams are formed and designed to contain diverse skillsets	An annual appraisal system which defines the organisations' expectations and identifies staff personal and organisational development needs	An annual review of staff's performance and a development plan agreed with management and employees
	2.3 Personal commitment and satisfaction	The organisation must ensure staff are committed, motivated and satisfied through training and development opportunities, rewards and incentives, recognition of individual and/or team performance, career progression and empowerment	Training and development opportunities that are available to all employees A reward and incentives scheme designed to encourage and motivate knowledge sharing	A satisfaction survey conducted annually Staff should have access to management and leadership Training and development programs to ensure staff have the necessary skills to part-take in knowledge sharing and component integration processes

	2.4 Knowledge sharing behaviours	The organisation should have a well-established knowledge sharing culture. Employees should be well informed on the benefits of knowledge sharing, and the processes for knowledge capture and sharing	Human resources have programs and sessions to raise awareness on the benefits of knowledge sharing Human resources and management support and install structures that encourage knowledge sharing	A knowledge sharing strategy that is available to all stakeholders
3. Financial Resources	3.1 Financial management	The organisation must set up a financial budget for component integration and knowledge sharing processes. The budget must support training and staff development. The budget must have provisions for the acquisition of infrastructure to support and maintain knowledge sharing processes	The organisation has sufficient financial resources to develop, support and maintain knowledge sharing, and component integration processes	A regularly reviewed budget to fund staff training and development needs A budget for knowledge sharing and component integration infrastructure acquisition
	3.2 Funding environment	The organisation should ensure it has access to resources and funding to support knowledge sharing and associated processes	The organisation has access to resources that support knowledge sharing The organisation has a strategy to apply and access funding to support knowledge sharing approaches	A regularly reviewed strategy to apply for funding A regularly reviewed process that supports resource acquisition
	3.3 Financial responsibility	The organisation should ensure transparent, lawful and regular internal and external financial reporting. The project plan should state whether reporting will be conducted monthly, quarterly etc	Organisation has regular internal meetings for financial reporting with regard to knowledge sharing and component integration Organisation has regular external meetings with relevant stakeholders to discuss financial matters with regard to knowledge sharing	Regular internal and external meetings with relevant stakeholders to address financial issues that can potentially affect knowledge sharing

4. Communication	4.1 Communication mechanism	The organisation should have clear communication mechanisms that create knowledge sharing opportunities, encourages knowledge sharing behaviours across intra and inter-organisational levels. Changes to procedures, processes, standards and, regulation concerning the sharing of knowledge relating to component integration processes must be communicated to all relevant stakeholders	Usable, relevant and current communication channels are available to all stakeholders and are used consistently to share knowledge internally and externally	Current and technologically adequate communication channels are available to all stakeholders Funds to maintain, support and update communication channels are available Staff can access and use available communication channels Training is available to train staff on the use of communication channels Communication channels comply with regulation, standards and laws
5. Leadership	5.1 Transparency and accountability	The organisation should demonstrate fair, transparent and accountable knowledge sharing processes. Component integration knowledge must be made available to all relevant stakeholders. The organisation must demonstrate how its knowledge sharing processes address legal and regulatory requirements	Knowledge sharing processes are communicated fairly and transparently to all stakeholders Leadership communicates fairly and transparently current component integration processes to all stakeholders	Standardised data collection methods and infrastructure that adheres to standards, best practices, regulation and law exist A repository for information archiving and storage is available Stored information from past projects is available on request for all stakeholders Organisation has a well-defined communication process for staff (internal and

				external) to communicate with leadership in a fair and transparent manner
	5.2 Organisational culture	The leadership should create an environment and culture that encourages and supports knowledge sharing	Leadership supports and encourages knowledge sharing within the organisation Leadership supports and encourages knowledge sharing with relevant stakeholders in the external environment	Rewards and incentives for new and innovative knowledge sharing ideas Training on how to share knowledge effectively and efficiently using available resources within the organisation is available Processes to aid in knowledge sharing with external organisations are available to all staff members
6. Technological Infrastructure	6.1 Information technology	IT procedures should include procedures for maintaining, replacing and updating equipment used for knowledge sharing. The procedures must be well communicated to all relevant stakeholders	The organisation has IT procedures that are available electronically and physically IT procedures are communicated to all stakeholders	Training on how to comply with IT policies and procedures is available to stakeholders IT services and products are current and up-to-date Communication channels between the IT department and staff are available
	6.2 Knowledge sharing strategy	All organisations (OEMs and component suppliers) should have a clear process for the acquisition, creation, storage, and dissemination of knowledge relating to component integration that is well understood by all relevant stakeholders engaged in the project	The organisation has a clear strategy for the acquisition, creation, storage, and dissemination of knowledge relating to component integration that is well understood by all relevant	A clear and well-defined process for knowledge sharing A knowledge sharing strategy that clearly defines the tools (hardware and software) and best practices used for knowledge sharing

			stakeholders engaged in the project	
	6.3 Quality assurance system	The organisation should have a well-established system for monitoring, assessing and improving the quality of the knowledge sharing process	The organisation has a well-established system for assessing the quality of its knowledge sharing processes The organisation has a well-established system for assessing the quality of its component integration processes	A regularly reviewed and updated quality assurance system is available
	6.4 Information management system	The organisation should have an information management system that will address knowledge sharing requirements and challenges introduced by non-disclosure agreements, design contracts etc. Best practices and lessons learnt within each project should be documented in the knowledge sharing strategy	The organisation has an information management system focused on knowledge sharing The organisation has a strategy for addressing and complying with NDA's, Design contracts and other gagging orders The organisation has an information management system for document storage and archiving	An up-to-date process for addressing issues relating to NDA's, design contracts etc A regularly reviewed and updated management system for data archiving and storage An information management system that is current and regularly reviewed and updated
	6.5 Training teams	The training teams will monitor for changes in best practices, standards, requirements and lessons learnt from other projects. The training teams will train staff (internal and external) on new processes and procedures for quality and performance improvement	The organisation has teams tasked with staff training Staff training addresses processes and procedures that enhance and improve the quality of knowledge sharing and component integration processes	A well-documented training programme that is supported by well-informed training personnel Staff training program supported by management and leadership

			Training programs extend to the external environment	Financial resources to support, maintain and develop future training programs
INTER-ORGANISATION ENVRIONMENT				
7. Regulatory Requirements	7.1 Partnerships with similar organisations	The organisation should have a clearly defined strategy and operational plan for policy engagement and advocacy with other similar organisations (an OEM's strategy for engagements should also cater for other OEMs)	A clear communication strategy for policy engagement and advocacy with other organisations A clear plan for resource, asset and knowledge sharing	Regular meetings with representatives from other organisations involved in the collaborative project The organisation has resources, assets for knowledge sharing
	7.2 Relationships with governing boards	The organisation should have clearly defined terms of engagement with organisations that are focused on the creation of best practices, policy, standards, and funding opportunities available for knowledge sharing approaches. Such relationships are crucial for staying informed on changes that affect the sharing of knowledge relating to component integration processes	The organisation has clearly defined terms of engagement with various governing boards The organisation receives current and up-to-date information on best practices, policy, standards, and funding opportunities	The organisation conducts meetings with various governing boards The organisation has communication channels to receive the latest information related to best practices, standards, policy and funding opportunities
	7.3 Regulation	The organisation will have to demonstrate compliance with regulations. The organisation must track and document changes to the knowledge sharing processes and component integration approaches to reflect changes introduced by changes in regulation	The organisation has a strategy that demonstrates awareness and compliance with regulatory requirements that apply to knowledge sharing and component integration The organisation has a strategy to track changes to regulation that applies to knowledge sharing and component integration	Regulatory requirements are reviewed on a project-by-project basis Regulatory requirements are communicated to all stakeholders The organisation has a strategy for regulation compliance training

	7.4 Standards	The organisation will have to demonstrate compliance with standards created and developed by organisations such as ISO and SAE. The organisation must demonstrate how it complies with automotive standards	The organisation has a strategy that demonstrates awareness and compliance with standards that apply to knowledge sharing and component integration The organisation has a strategy to track changes in standards that apply to knowledge sharing and component integration	Relevant standards are reviewed on a project-by-project basis Relevant standards and their requirements are communicated to all stakeholders The organisation has a strategy for standards compliance training
	7.5 Best practices	The organisation will have to demonstrate how it incorporates the industry's best practices concerning knowledge sharing and component integration	The organisation has a strategy that demonstrates awareness and compliance with relevant best practices that apply to knowledge sharing and component integration The organisation has a strategy to track changes in Best Practices and their requirements that apply to knowledge sharing and component integration	Best Practices are reviewed on a project-by-project basis. Relevant Best Practices are communicated to all stakeholders. The organisation has a strategy for Best Practices compliance training
EXTERNAL ENVIRONMENT				
8. Political and Legal	8.1 Laws and legal restrictions	The organisation should observe and adhere to laws and legal requirements that relate to the sharing of knowledge relating to component integration processes. The organisation should have procedures in place to document and track laws and legal requirements for all countries where the organisation conducts business	The organisation is up to date with relevant laws and legal restrictions related to the sharing of knowledge relating to component integration information at provincial, national and international level	Regular meetings to inform and update staff on relevant laws and legal restrictions Staff are well informed on communication channels to use on the discovery of new laws or regulation

			The organisation has a strategy for tracking and documenting changes to relevant laws and legal restrictions	Training for law and legal requirements compliance
	8.2 Policies	The organisation should adhere to policies imposed by different countries where knowledge sharing will occur. The organisation should have procedures in place to document and track changes to policies	The organisation is up to date with relevant policies related to the sharing of knowledge relating to component integration information at provincial, national and international level The organisation has a strategy for tracking and documenting changes to relevant policies	Regular meetings to inform and update staff on relevant policies Staff are well informed on communication channels to use on the discovery of new policy that relates to knowledge sharing and component integration Training for policy requirements compliance
	8.3 Relationship with government authorities	The organisation should foster and maintain relationships with government authorities to ensure it remains informed on laws related to knowledge sharing, and policy changes within the automotive domain that relate to component integration or knowledge sharing	The organisation has a strong relationship with government authorities, and it well informed on changes to policy and law. The organisation has strong communication channels with the government authorities and has access to knowledge sharing resources made available by the government	Regular meetings with government authorities to get updates on policy, law and legal requirements that relate to knowledge sharing and component integration processes

7.3 The revised and final framework

This section critically discusses the changes made after presenting the framework to senior management employed by vehicle manufacturing organisations, automotive component manufacturing organisations, internationally recognised automotive knowledge experts, all of which have either agreed with the content or returned comments which resulted in changes to the framework. The revisions on the framework are an iterative process undertaken through critical reflection and exposure to critique and feedback received from the study's participants as discussed in Chapter 8. All changes identified in Chapter 8 have been incorporated into the revised framework presented in Figure 7.6 below.

Intellectual Property (IP)

Feedback received from the study's respondents highlighted that the framework needs to have a provision that caters for the protection of innovations and ideas that may result from the sharing of component integration-related knowledge and information. Since the framework advocates for identification, capture, storage and dissemination of knowledge, the framework must ensure that intellectual property (IP) protections, either in the form of copyrights, patents, design and trademarks, are used to protect all innovations. The researcher added this knowledge sharing factor under the *Political and legal environment* component after the evaluation process. The organisation should have a strategy for addressing IP rights on a provisional, national and international level. The strategy should include a process for the registration of copyrights, patents, design and trademarks. The organisation's strategy should also include a process to oversee the education of staff on the creation and protection of IP, and for providing legal advice on IP matters.

Non-discloser agreements (NDAs) and design contracts

Feedback received from the study's respondents highlighted the need for a legal team dedicated to addressing knowledge sharing challenges introduced by NDAs, design contracts, confidentiality agreements and other forms of gagging agreements that are a common feature within the domain. A new knowledge sharing factor was created in the external relationship environment, which is dedicated to gagging agreements that hinder knowledge sharing termed *Contract agreements*. The NDA, confidentiality agreements, and design contract core competencies were removed from the *Technological environment* component as a result. According to the study's participants, a majority of collaborative projects and joint ventures are heavily regulated by confidentiality agreements (NDAs, design contracts etc.), which pose significant challenges to the sharing of knowledge related to component integration processes. Organisations can navigate past challenges and obstacles that can potentially affect the sharing of knowledge in component integration processes by having a legal team or department dedicated to addressing such challenges. The team should be involved in contract negotiations, joint ventures and collaborative project negotiations for every project.

How can it be measured column?

The researcher removed the *How can it be measured* column from Table 7.8 above, after critical reflection from the researcher and feedback received from the study's participants. In Table 7.8 the *How can it be measured* factors were used to describe the measurement to be undertaken to ensure that an organisation has procedures in place to address identified knowledge sharing factors for each component. The reason for removing the column is; every vehicle manufacturing organisation or component manufacturing organisation is different and unique; therefore, each organisation will have to decide how to measure these knowledge sharing factors individually.

Social culture

A *Social culture* component was added to the external relationship environment based on the feedback provided by the study's participants and critical reflection from the researcher. The social environment in which the organisation operates in has a great impact on the way its staff view and perform knowledge sharing activities. The organisation needs to understand its social environment to fully appreciate and understand its staff's views and perceptions on the sharing of knowledge concerning component integration. According to the study's participants, by understanding its social environment, an organisation will be able to provide appropriate training and tailored personal development programs which in turn will improve staff knowledge on the benefits of sharing component-related knowledge. Staff motivation to participate in knowledge sharing activities will also be improved. As noted by the study's participants, and according to Menkel-Meadow (2011), although an independent component, social culture is greatly affected to an extent by political and legal activities within a community or country.

Financial resources changed to business processes

The study's participants advised that the *Financial resources* component should be changed to *Business processes* because financial resources are part of an organisation's business processes, which comprise of a collection of related structured activities including all activities highlighted in the financial resource's component. Feedback from the evaluators also suggests that the *Personal commitment and* *satisfaction* factor could also be considered to be an element of the *Business processes* component, therefore it was removed from the *Human resources* component.

The study's participants also advised that the organisation should have an overall *Integration strategy* as part of the *Business processes* component, as a result, an *Integration strategy* factor was added to the newly formed *Business processes* component.

Knowledge sharing behaviours changed to knowledge sharing culture

The *Knowledge sharing behaviours* factor in the *Organisational structure* component was changed to *knowledge sharing culture* as suggested by the study's participants. A knowledge sharing culture should exist within the organisation and should be supported by knowledge sharing behaviours that are encouraged through the *Human resource's* component.

All the changes identified and discussed in the foregoing have been incorporated into the revised framework illustrated in Figures 7.6, 7.7 and 7.8 below.

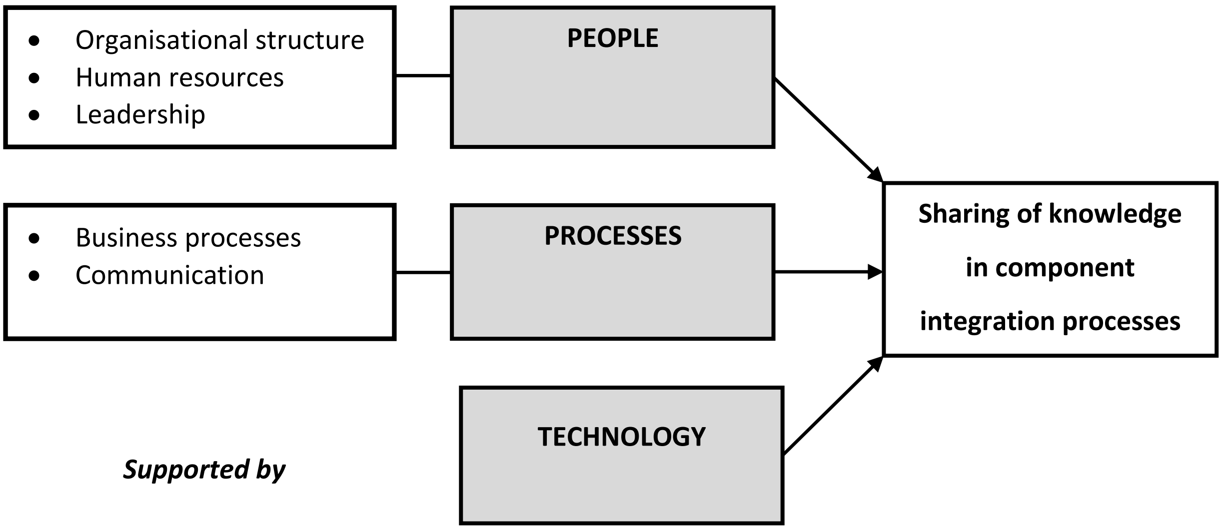

Figure 7. 6: Knowledge sharing factors

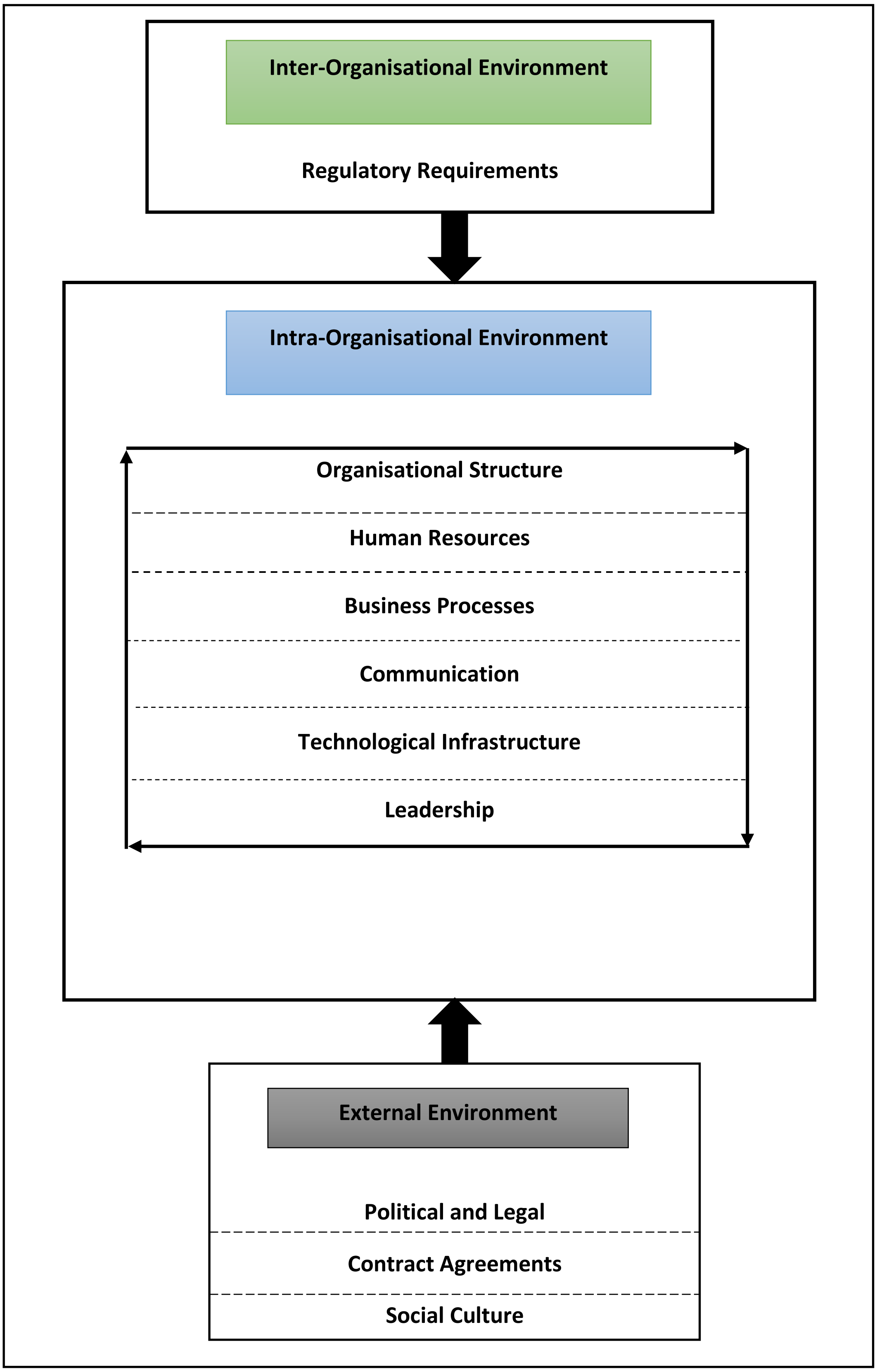

Figure 7. 7: The final evaluated knowledge sharing framework

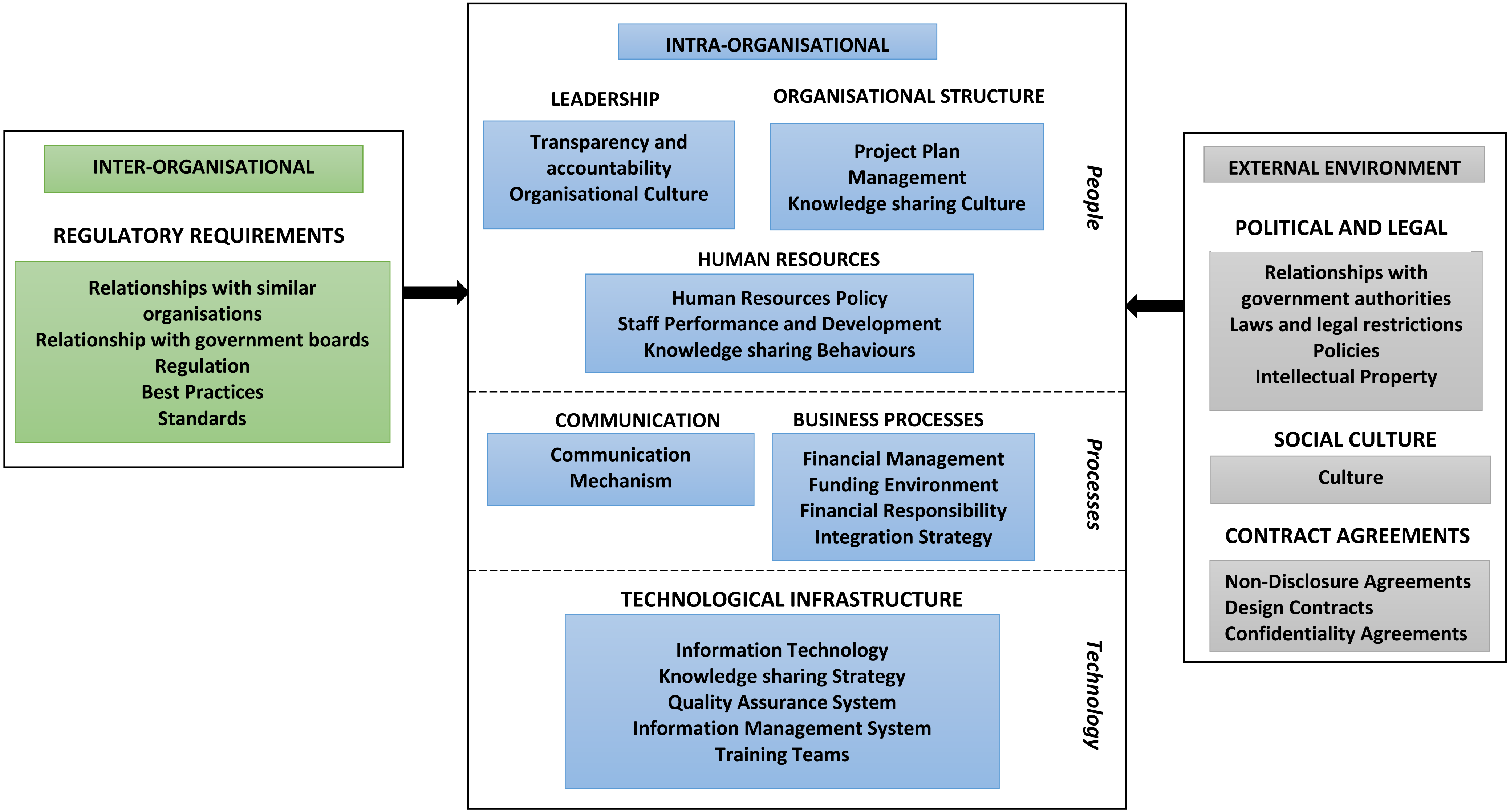

Figure 7. 8: The final evaluated framework and its knowledge sharing factors

Table 7. 11: The revised knowledge sharing infrastructure

Component	Knowledge sharing factor	Core competencies	Indicator
INTRA-ORGANISATIONAL ENVIRONMENT			
1. Organisational structure	1.1 Project plan	A project plan that shows the following should be available: • The integration strategy to be employed within the project • The process of capturing and disseminating knowledge relating to component integration processes • List of associated projects • A list of the staff, their expertise and their location Changes or amendments to the project plan should be communicated to all relevant stakeholders	A project plan that is reviewed and evaluated by all stakeholders The process and timeframe for reviewing the project is based on the project timeline and duration. An organisational chart that is regularly updated and consistently used
	1.2 Management	The organisation's managerial brass should play an important role in building knowledge sharing structures and processes. Ensuring that knowledge sharing processes remain relevant and usable is a task management should oversee	Knowledge sharing initiatives that are supported by management A strategy for reviewing and updating knowledge sharing processes A strategy for reviewing and updating component integration processes
	1.3 Knowledge sharing culture	The organisational structure should include technology and physical mechanisms that support knowledge sharing behaviours	Training programs for developing skills and competencies A strategy that identifies areas that require support and infrastructure to support knowledge sharing
2. Human Resources	2.1 Human resources policy	The organisation should have a policy that supports the organisation's administrative personal functions, performance management, employee relations and resource planning. The policy should address how the	Human resource policy documents that are accessible electronically and manually

		organisation complies with standards, corporate governance, regulation and legislative commitments concerning knowledge sharing	A policy document that demonstrates how the organisation complies with standards, corporate governance, regulation and legislative commitments concerning knowledge sharing and component integration
	2.2 Staff performance and development	Staffs' performance is evaluated on a project-by-project basis to identify training and development requirements. Teams are formed and designed to contain diverse skillsets	An annual appraisal system which defines the organisations' expectations and identifies staff personal and organisational development needs
	2.3 Knowledge sharing behaviours	The organisation should have a well-established knowledge sharing culture. Employees should be well informed on the benefits of knowledge sharing, and the processes for knowledge capture and sharing	Human resources have programs and sessions to raise awareness on the benefits of knowledge sharing Human resources and management support and install structures that encourage knowledge sharing
3. Business Processes	3.1 Financial management	The organisation must set up a financial budget for component integration and knowledge sharing processes. The budget must support training and staff development. The budget must have provisions for the acquisition of infrastructure to support and maintain knowledge sharing processes	The organisation has sufficient financial resources to develop, support and maintain knowledge sharing, and component integration processes
	3.2 Funding environment	The organisation should ensure it has access to resources and funding to support knowledge sharing processes and associated processes	The organisation has access to resources that support knowledge sharing The organisation has a strategy to apply and access funding to support knowledge sharing approaches
	3.3 Financial responsibility	The organisation should ensure transparent, lawful and regular internal and external financial reporting. The project plan should state whether reporting will be conducted monthly, quarterly etc.	Organisation has regular internal meetings for financial reporting concerning knowledge sharing and component integration Organisation has regular external meetings with relevant stakeholders to discuss financial matters with regard to knowledge sharing
	3.4 Integration strategy	The organisation should have an integration strategy which specifies clearly how to fulfil component integration requirements and processes that permit for the creation of a project-specific integration strategy	The organisation has an integration strategy that is regularly reviewed and updated

			The organisation has regular meetings with all relevant stakeholders to review the integration strategy on a project-by-project basis
4. Communication	4.1 Communication mechanism	The organisation should have clear communication mechanisms that create knowledge sharing opportunities, encourage knowledge sharing behaviours across intra and inter-organisational levels. Changes to procedures, processes, standards and, regulation with regards to component integration knowledge sharing must be communicated to all relevant stakeholders	Usable, relevant and current communication channels are available to all stakeholders and are used consistently to share knowledge internally and externally
5. Leadership	5.1 Transparency and accountability	The organisation should demonstrate fair, transparent and accountable knowledge sharing processes. Knowledge associated with component integration processes must be made available to all relevant stakeholders. The organisation must demonstrate how its knowledge sharing processes address legal and regulatory requirements	Knowledge sharing processes are communicated fairly and transparently to all stakeholders Leadership communicates fairly and transparently current component integration processes to all stakeholders
	5.2 Organisational culture	The leadership should create an environment and culture that encourages and supports knowledge sharing	Leadership supports and encourages knowledge sharing within the organisation Leadership supports and encourages knowledge sharing with relevant stakeholders in the external environment
6. Technological Infrastructure	6.1 Information technology	IT procedures should include procedures for maintaining, replacing and updating equipment used for knowledge sharing. The procedures must be well communicated to all relevant stakeholders	The organisation has IT procedures that are available electronically and physically IT procedures are communicated to all stakeholders
	6.2 Knowledge sharing strategy	All organisations (OEMs and component suppliers) should have a clear process for the acquisition, creation, storage, and dissemination of knowledge related to component integration processes that are well understood by all relevant stakeholders engaged in the project	The organisation has a clear strategy for the acquisition, creation, storage, and dissemination of knowledge related to component integration processes that are well understood by all relevant stakeholders engaged in the project

	6.3 Quality assurance system	The organisation should have a well-established system for monitoring, assessing and improving the quality of the knowledge sharing process	The organisation has a well-established system for assessing the quality of its knowledge sharing processes The organisation has a well-established system for assessing the quality of its component integration processes
	6.4 Information management system	The organisation should have an information management system that will address knowledge sharing requirements and challenges as they occur for each project	The organisation has an information management system focused on knowledge sharing The organisation has an information management system for document storage and archiving
	6.5 Training teams	The training teams will monitor for changes in best practices, standards, requirements and lessons learnt from other projects. The training teams will train staff (internal and external) on new processes and procedures for quality and performance improvement	The organisation has teams tasked with staff training Staff training addresses processes and procedures that enhance and improve the quality of knowledge sharing and component integration processes Training programs extend to the external environment
INTER-ORGANISATIONAL ENVIRONMENT			
7. Regulatory Requirements	7.1 Partnerships with similar organisations	The organisation should have a clearly defined strategy and operational plan for policy engagements and advocacy with other similar organisations (an OEM's strategy for engagements should also cater for other OEMs)	A clear communication strategy for policy engagement and advocacy with other organisations A clear plan for resource, asset and knowledge sharing
	7.2 Relationships with governing boards	The organisation should have clearly defined terms of engagement with organisations that are focused on the creation of best practices, policy, standards, and funding opportunities available for knowledge sharing approaches. Such relationships are crucial for staying informed on changes that affect the sharing of knowledge relevant for component integration	The organisation has clearly defined terms of engagement with various governing boards The organisation receives current and up-to-date information on best practices, policy, standards, and funding opportunities
	7.3 Regulation	The organisation will have to demonstrate compliance with regulations.	The organisation has a strategy that demonstrates awareness and compliance with regulatory requirements that apply to knowledge sharing and component integration

		The organisation must track and document changes to knowledge sharing processes and component integration approaches to reflect changes introduced by changes in regulation	The organisation has a strategy to track changes to regulation that applies to knowledge sharing and component integration
	7.4 Standards	The organisation will have to demonstrate compliance with standards created and developed by organisations such as ISO and SAE. The organisation must demonstrate how it complies with automotive standards	The organisation has a strategy that demonstrates awareness and compliance with standards that apply to knowledge sharing and component integration The organisation has a strategy to track changes in standards that apply to knowledge sharing and component integration
	7.5 Best practices	The organisation will have to demonstrate how it incorporates the industry's best practices concerning knowledge sharing and component integration	The organisation has a strategy that demonstrates awareness and compliance with relevant best practices that apply to knowledge sharing and component integration The organisation has a strategy to track changes in Best Practices and their requirements that apply to knowledge sharing and component integration
EXTERNAL ENVIRONMENT			
8. Political and Legal	8.1 Laws and legal restrictions	The organisation should observe and adhere to laws and legal requirements that relate to the sharing of knowledge related to component integration processes The organisation should have procedures in place to document and track laws and legal requirements for all countries where the organisation conducts business	The organisation is up to date with relevant laws and legal restrictions related to knowledge sharing of component integration information at provincial, national and international level The organisation has a strategy for tracking and documenting changes to relevant laws and legal restrictions
	8.2 Policies	The organisation should adhere to policies imposed by different countries where knowledge sharing will occur. The organisation should have procedures in place to document and track changes to policies	The organisation is up to date with relevant policies related to knowledge sharing of component integration information at provincial, national and international level The organisation has a strategy for tracking and documenting changes to relevant policies

	8.3 Relationship with government authorities	The organisation should foster and maintain relationships with government authorities to ensure it remains informed on laws about knowledge sharing, and policy changes within the automotive domain that relate to component integration or knowledge sharing	The organisation has a strong relationship with government authorities, and it well informed on changes to policy and law. The organisation has strong communication channels with the government authorities and has access to knowledge sharing resources made available by the government
	8.4 Intellectual Property	The organisation should have a strategy or process designed to ensure that innovations and ideas that may result from the sharing of knowledge related to component integration are protected	The organisation has a well-defined process for identifying and protecting IP on a provisional, national and international levels The organisation consistently briefs its staff and relevant stakeholders on the importance of protecting IP The organisation has a dedicated team with legal expertise focused on identifying and protecting IP and providing IP related information to staff
9. Contract Agreements	9.1 Non-disclosure agreements	The organisation should have a strategy to address knowledge sharing challenges that are introduced by non-disclosure agreements for each project	The organisation has a dedicated team that is involved in contract negotiations for each collaborative project or joint venture All stakeholders are well advised on the contents of the Non-discloser agreement on a project-by-project basis Training is made available to all relevant stakeholders on how and which knowledge can be shared and, with whom without violating the terms of the NDA
	9.2 Design contracts	The organisation should have a strategy to address knowledge sharing challenges that are introduced by design contracts for each project	The organisation has a dedicated team that is involved in contract negotiations for each collaborative project or joint venture All stakeholders are well advised on the contents of the design contract on a project-by-project basis

			Training is made available to all relevant stakeholders on how and which knowledge can be shared and, with whom without violating the contract agreement
	9.3 Confidentiality agreements	The organisation should have a strategy to address knowledge sharing challenges introduced by confidentiality agreements for each project.	The organisation has a dedicated team that is involved in contract negotiations for each collaborative project or joint venture All stakeholders are well advised on the contents of the confidentiality agreement on a project-by-project basis Training is made available to all relevant stakeholders on how and which knowledge can be shared and, with whom without violating the terms of the confidentiality agreement
10. Social Culture	10.1 Culture	The organisation should have an understanding of cultural issues which impact on the specific environment where the organisation is situated and where its staff originate from	The organisation and staff are involved in collaborative problem solving The organisation constantly has meetings to discuss political issues that can potentially affect the organisation and existing projects Staff and all relevant stakeholders are well informed on available communication channels to discuss cultural issues

7.4 Implementation of the knowledge sharing framework

The framework for sharing knowledge provided above, which is designed to potentially assist the automotive industry to manufacture cyber-secure vehicles, provides a relatively comprehensive description of the components and factors to consider in studies and investigations that focus on the sharing of knowledge related to component integration processes for automotive cybersecurity. The framework acts as a starting point for future research that could potentially yield an improved and more detailed framework of knowledge sharing influences. The synthesised literature review equipped the framework with context-specific language (terms and concepts) for the study of knowledge sharing, a checklist for consideration for knowledge sharing practitioners to consider when generating varied research issues to explore, and a frame of reference for benchmarking knowledge sharing in component integration practices that the auto-industry can consider. The researcher will briefly highlight the framework applications in the next section.

Based on the recommendations made by the study's participants, Table 7.11 above provides a revised knowledge sharing infrastructure. The knowledge sharing factors and components may not be exhaustive, because each OEM or component manufacturer may identify additional knowledge sharing factors or components that are specific to their organisation that may require further consideration. Nonetheless, the framework can be employed to develop a checklist for knowledge sharing consideration. The columns on the right in the knowledge sharing infrastructure are designed to indicate how each factor can be addressed within and /or across various vehicle manufacturing organisations or component manufacturing organisations, depending on the scope of their project(s). The factors listed for each component are extracted from literature, the data collection process, and feedback from the study's evaluation process.

The knowledge sharing processes are derived from a review of the prior relevant literature of knowledge management theories, cybersecurity management theories, supply chain management theories and, theories that focus on vehicle manufacturing (Chapter 2). Among the frameworks and theories are many shared aims, these commonalities comprise of:

- The identification of a problem to be addressed
- The identification of knowledge relevant to the problem
- Selection of knowledge relevant to the problem
- Assessment of potential barriers to the use of identified knowledge
- Adaption and application of the identified knowledge to the problem

- Monitoring and evaluation of knowledge use
- Tailoring of the knowledge to suit the local context
- Sustaining and promoting the ongoing use of that knowledge

This research was undertaken to investigate and understand knowledge sharing challenges associated with component integration processes that lead to cyber-related challenges in connected vehicle development, and as part of this research, a process for knowledge sharing has been developed that comprises of five stages. Figure 7. 9 below illustrates the relations between the five stages.

Stage 1: Internal knowledge assessment

The first process involves assessing to understand the knowledge that already exists within the organisation. Component integration is not new to the automotive industry, some organisations may be in possession of integration knowledge from previous projects. The process also involves identifying knowledge gaps in terms of people, processes and technology.

Stage 2: External knowledge assessment

The second process involves identifying external sources of knowledge; both tacit and explicit, to address the knowledge gaps identified in the first process. Vehicle manufacturers and component manufacturers, at times, engage with other organisations in collaborative projects or joint ventures, this stage looks at how access can be gained to the knowledge source and the requirements to facilitate sharing of this knowledge.

Stage 3: Knowledge exploitation

This stage involves the application and exploitation of new knowledge to address the knowledge gaps identified in the first process. The process of tailoring the new knowledge to the project context is also conducted at this stage. The new knowledge includes component integration knowledge and new knowledge on how to access and share knowledge. This process also includes the identification of barriers that potentially affect the exploitation of new knowledge and ways to overcome the barriers.

Stage 4: Knowledge evaluation

This stage focuses on assessing whether the new knowledge addresses the knowledge gaps and, reviewing whether the new knowledge adds value to existing processes and people involved with the integration process.

Stage 5: Knowledge sustainability and re-use

This stage involves ensuring that new and existing relevant knowledge relating to the integration of components is shared appropriately within the organisation and externally with relevant stakeholders. With regard to this research, this stage is considered important, as it must ensure that the sharing of new knowledge adheres to NDAs and the various confidentiality agreements that exist within the automotive sector.

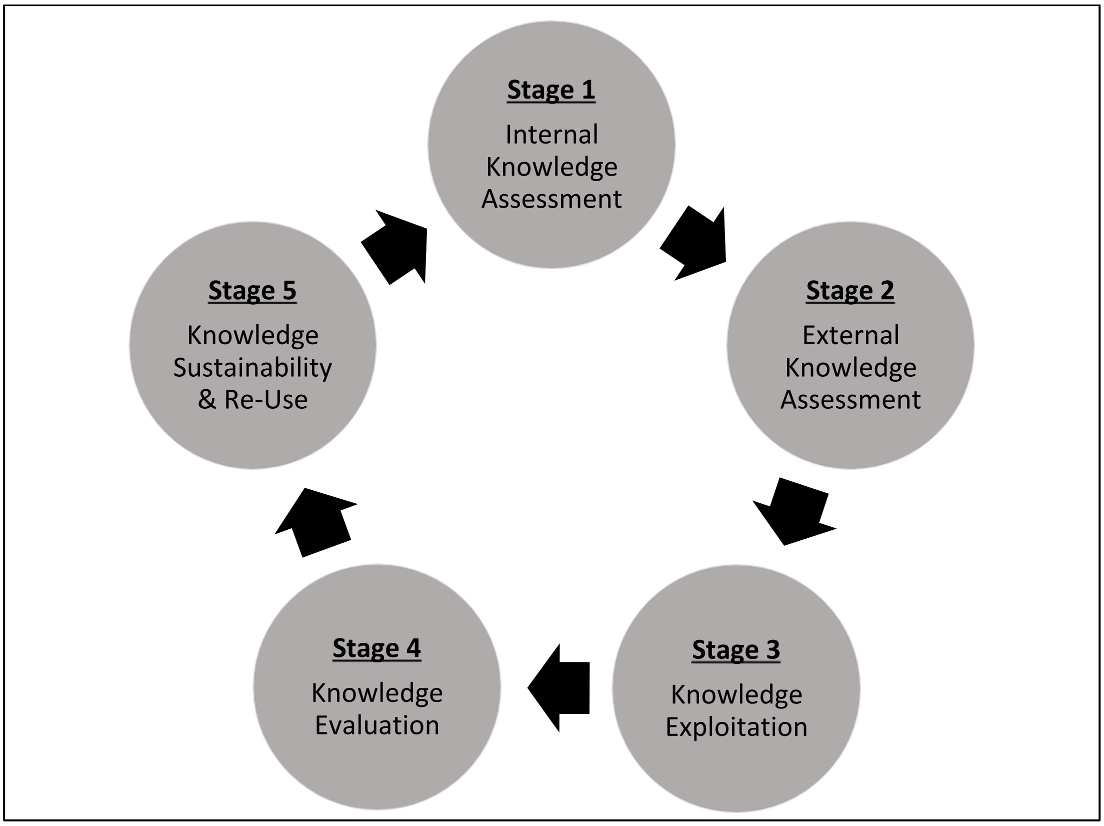

Figure 7. 9: The knowledge sharing process

7.4.1 Method of implementation

The following section will propose a method that an organisation (OEM or component manufacturer) can use to implement the proposed framework.

Stage 1: Internal knowledge assessment

The integration of components is not a new feature in the automotive industry, rather it is the type of components that have transformed. Vehicle manufacturers and component manufacturers are tasked with integrating ever more technologically complex components into systems and sub-systems that eventually make up the connected vehicle. To devise secure integration strategies, make good decisions regarding integration requirements and processes, OEMs and component manufacturers need to assess and analyse existing processes and resources within their respective organisations. Organisations need to analyse knowledge sharing processes that exist that permit the sharing of knowledge and information related to integration processes. Organisations need to identify knowledge gaps in their component integration processes and knowledge sharing processes on a project-by-project basis. They need to better identify where the knowledge gaps lie and who within the organisation can best address them. The approach to identify knowledge gaps on a project-by-project basis may seem repetitive, however, the difference in components and vehicles results in different integration challenges and requires different resources. The internal knowledge assessment should aim to address the following areas:

- Project aims
- The expertise of the people involved with the project (skills, education and experience obtained from training and other projects completed)
- Processes and procedures required for the project
- Tools and technology required to support the integration processes, knowledge sharing processes and procedures, and the people working on the project

The internal knowledge assessment stage assists in identifying where the knowledge resides within the organisation, by focusing on the people, processes and technology that already exists. The stage assists in identifying areas where resources are required, where they can be obtained from and, how they can be obtained. This stage also assists to set appropriate goals to the right people, procedures and technical support focused on addressing the project goal(s). The steps involved in this stage as illustrated by Figure 7.10 below are:

- *Process analysis* – for each specific project, what are the current processes and practices?
- *Value analysis* – according to the project's aims, what changes if any, can be added to current processes to achieve the project aims?
- *Knowledge Asset Identification* – what resources (internally and externally) are required to achieve the project aims?

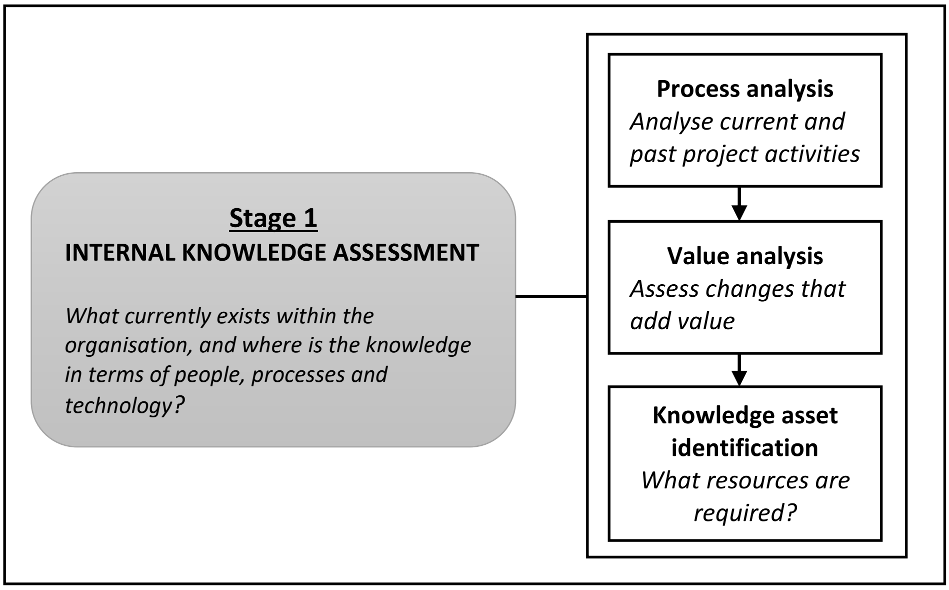

Figure 7. 10: Stage 1 – Internal knowledge assessment

Process analysis

A process analysis is used to identify existing component integration and knowledge sharing processes and practices. As noted earlier, component integration and knowledge sharing are not new to the automotive domain, most organisations may already have processes and practices that have been used previously. Therefore, it is important that an organisation carries out an analysis of current and previous processes and evaluates how these processes and procedures can be improved. The process analysis is not only important in avoiding using processes and procedures that have been deemed inappropriate, but it also assists in identifying processes or aspects thereof, that can be considered appropriate to the current project.

Value analysis

After the process analysis stage has been completed and existing processes have been identified, the organisation needs to establish what is required to ensure that the identified processes are capable of addressing the project aim(s). The organisation needs to establish what will add further value to the project. This stage also comprises identification of extra resources, either in the form of people or new technological infrastructure that could be acquired to further assist the existing processes to address the project aim(s).

Knowledge asset identification

On completion of the process analysis and value analysis, the organisation needs to establish and identify what knowledge assets are needed internally and externally. The organisation must identify tools to create, store, exploit and share knowledge relating to component integration processes. This stage should be performed on a project-by-project basis.

Stage 2: External knowledge identification

The data collection process revealed that an organisations' ability to improve its integration processes lies in its ability to form alliances. As stated by the study's participants, alliances formed via working groups, joint ventures and/or collaborative projects with the aim of encouraging mutual learning between organisations provides a platform for organisations to share knowledge. A vast amount of literature addresses the role of partnerships in the automotive industry, with a particular focus on supply chain integration (Lema et al. 2015), supplier parks (Marodin et al. 2016, Qamer & Hall 2018), and component outsourcing (Cabigiosu et al. 2013, Danese & Filippini 2013), but, notably, none on the sharing of knowledge related to component integration processes. The external knowledge identification process involves identifying external sources of knowledge; both tacit and explicit, to address component integration challenges, and knowledge sharing challenges in component integration approaches. The steps involved at this stage as illustrated in Figure 7.11 below are:

- Locate the relevant knowledge
- Negotiate access to the knowledge
- Identify knowledge access and knowledge sharing mechanisms

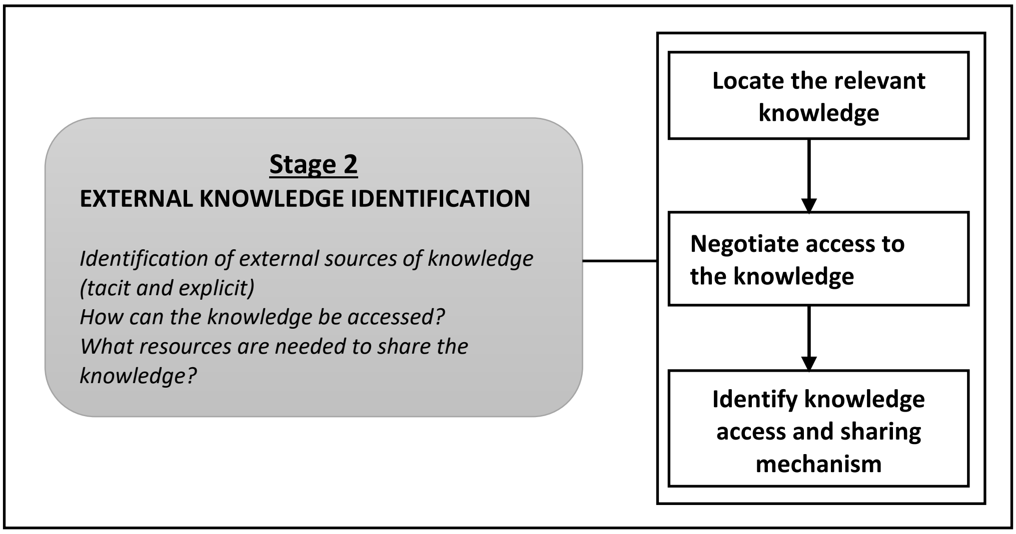

Figure 7. 11: Stage 2 – External knowledge identification

Locate relevant knowledge resources

Once the organisation has identified the knowledge gap, the knowledge sources must be identified. With component integration, the knowledge source in most cases is the manufacturer of the component. However, at times the knowledge source may comprise of more than a single supplier, this is mainly due to how modern digital components for connected vehicles are manufactured.

Access to the knowledge source

Once the knowledge source has been identified, the organisation will have to negotiate access to the knowledge source. The framework advocates for a well-defined strategy for gaining access to knowledge that is housed within the organisation, and for gaining access to an externally housed knowledge source. Externally housed knowledge sources can be accessed via contract negotiations, joint ventures, collaborative projects etc. with the component manufacturer.

Identifying knowledge access and sharing mechanisms

The last part of this stage involves the identification of knowledge sharing mechanisms. If it is agreed that the sharing mechanism will be technology-based, then the appropriate technology tools (hardware and software) need to be identified which will enable both parties to access and share knowledge. The framework advocates for a strategy that aims to ensure that the mechanisms remain current and relevant. Therefore, the sharing mechanisms must be reviewed and updated on a project-by-project basis. As noted by the study's participants during the data collection activity, the sharing and transfer of knowledge can be carried out by using people, via processes such as recruitment, secondment, working groups, statement of work (SOW), training sessions, knowledge sharing sessions, conferences etc.

Stage 3: Knowledge exploitation

This stage looks at how organisations can use the knowledge that exists within the organisation and, in externally housed knowledge sources. This stage also focuses on the steps that need to be taken to ensure that knowledge is used and shared effectively and efficiently so that components for connected vehicles can be integrated securely. This stage forms the building blocks for organisational learning. The steps involved at this stage as illustrated by Figure 7.12 below are:

- Adaptation of knowledge to the project context
- Assessment of barriers to ongoing knowledge use
- Implementation of appropriate interventions

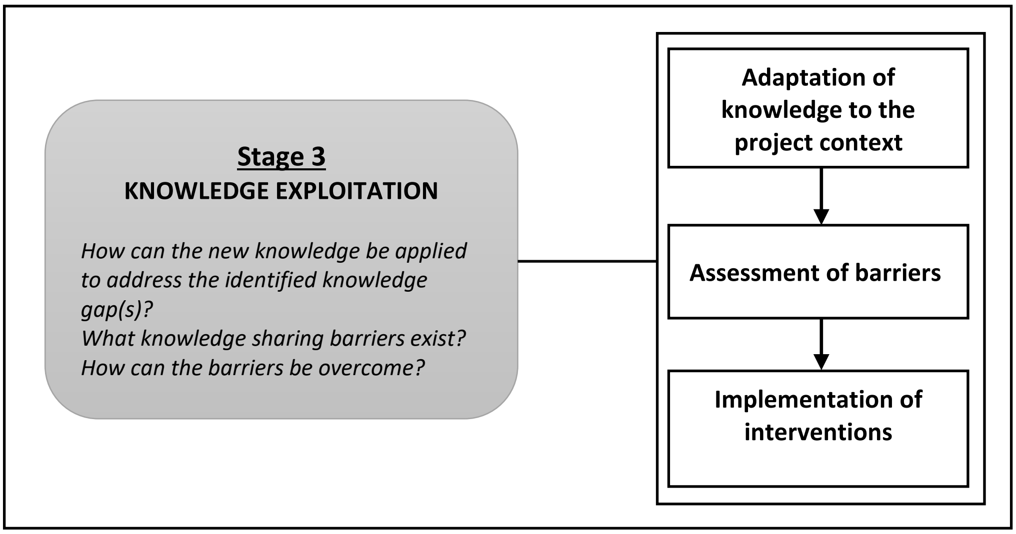

Figure 7. 12: Stage 3 – Knowledge exploitation

Adaptation of knowledge to the project context

The adaption of knowledge to a project context involves the processes all stakeholders go through as they make decisions on the appropriateness, value and usefulness of the knowledge with regard to the project aim(s) and available resources. The process also includes activities that are required to tailor the knowledge to suit the context of the project to be executed.

Assessment of barriers

This sub-stage involves the assessment of barriers that can potentially affect the sharing and re-use of knowledge. Upon identification of the potential barriers, the organisation should aim to develop relevant and appropriate intervention strategies to mitigate against the potential barriers. The main barriers that affect the sharing of knowledge associated with component integration processes within the automotive domain as noted by the study's participants are NDAs, design contracts, confidentiality agreements, trust, competition and the current structure of the automotive supply chain.

Implementation of appropriate interventions

This sub-stage involves decision making, planning and implementing measures to address the potential barriers to knowledge sharing. The framework advocates that measures to mitigate against identified barriers must be determined on a project-by-project basis. A possible solution to mitigate against potential barriers would be to create a 'roadmap' which makes it easier for vehicle manufacturers and component manufacturers to collaborate and share knowledge. Firstly, to navigate past the challenges imposed by NDAs, design contracts, and confidentiality agreements, the proposed framework proposes the use of a legal team to be part of the contract negotiation processes. Joint venture or collaborative work contracts should be designed to permit the sharing of knowledge related to component integration which can potentially protect connected vehicles from cyber-related threats. Secondly, organisations involved in the project must identify the knowledge medium and mechanisms for sharing knowledge. The framework advocates for transparency as a means to build trust, therefore all stakeholders must be granted access to the knowledge source.

Stage 4: Knowledge evaluation

The knowledge evaluation stage will provide a comprehensive overview of whether the knowledge source is adequate in addressing the project aim(s). Knowledge evaluation is a systematic determination of the acquired knowledge's worth and significance, using the criteria outlined in the framework. This stage assists organisations to determine if the knowledge is being used efficiently and effectively to address the project aim(s). If the degree of knowledge use is less than expected, then the organisation may need to revisit the knowledge assessment stages (stages 1 and 2). The evaluation of knowledge is also important in determining and assessing whether the interventions have been adequate to bring about the desired change, or whether more of the same or new interventions are required. The literature describes three types of knowledge use; conceptual, instrumental and strategic use. Conceptual or declarative use defines knowledge of, or understanding of concepts, principles and theories, instrumental use describes the changes in behaviour or practice, and strategic use relates to the manipulation of knowledge to attain specific goals. The steps involved at this stage as illustrated by Figure 7.13 below are:

- Monitor knowledge use (measure the conceptual, instrumental and strategic use of the new knowledge)
- Determine the impact of using the new knowledge

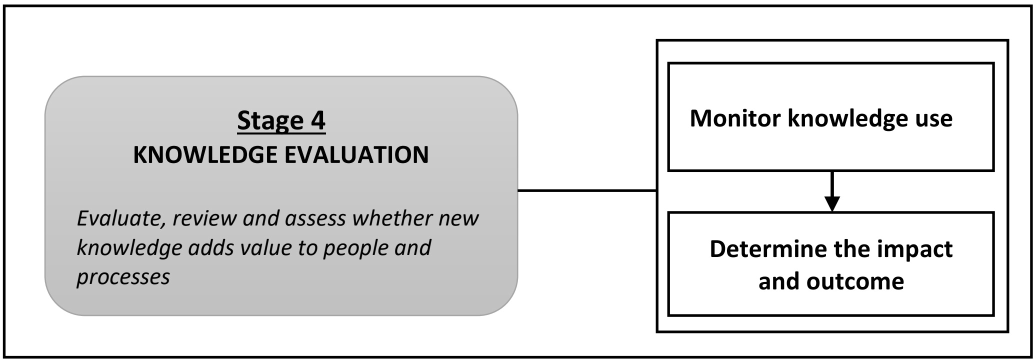

Figure 7. 13: Stage 4 – Knowledge evaluation

Monitoring knowledge use

The monitoring of new knowledge use at this stage focuses on measuring the conceptual use, instrumental use and, strategic use of the new knowledge. Component integration knowledge should address concepts, theories and principles in-line with relevant best practices, standards and regulations to achieve secure component integration through knowledge sharing.

Determine the impact of using the new knowledge

This sub-stage focuses on evaluating and determining the impact of using the new knowledge. It is designed to determine whether the application of the new knowledge assists in achieving the project aim(s). By evaluating the impact of knowledge use, the organisation can determine whether the knowledge source used is appropriate and, whether measures implemented to address knowledge sharing barriers are appropriate and adequate.

Stage 5: Knowledge sustainability and re-use

The knowledge sustainability and re-use stage focuses on sustaining the use of knowledge. Knowledge sustainability is still a relatively new aspect of knowledge sharing (Moore et al. 2017), nonetheless, vehicle manufacturers and component manufacturers need to ensure that knowledge sharing processes and activities are well documented and sustained for future re-use. The sharing of knowledge in component integration processes for automotive security is a necessity, but it is highly regulated by contract agreements. Knowledge sharing might occur during problem-solving in collaborative projects, however, these knowledge sharing activities are orchestrated in an unchartered and informal manner. Although this strategy may result in success at times, the reality is that most often the knowledge sharing is not sustained for future use and re-use, the knowledge is not recorded or shared with all relevant stakeholders. Furthermore, the medium employed to share knowledge is not maintained for future knowledge sharing activities. The steps involved at this stage as illustrated by Figure 7.14 below are:

- Identification of potential barriers that limit update of knowledge
- Identification of facilitators to on-going knowledge sustainability
- Formulate and implement mitigation processes to knowledge sustainability barriers

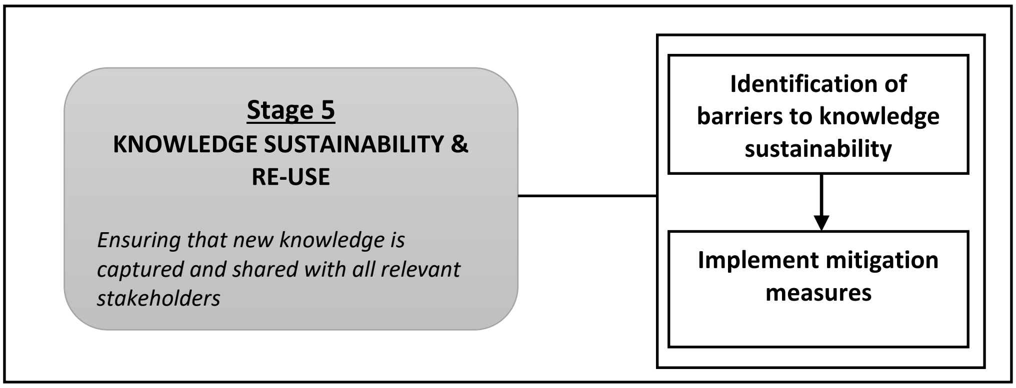

Figure 7. 14: Stage 5 – Knowledge sustainability and re-use

Identification of barriers to knowledge sustainability

This sub-stage focuses on identifying and assessing potential barriers to knowledge sustainability. This involves identifying the barriers on a project-by-project basis, designing and tailoring mitigation to the barriers, monitoring on-going knowledge use, and evaluating the impact of initial and sustained use of knowledge. The stage sets in motion an iterative process that cycles through all other stages.

Implementation of mitigation measures

This sub-stage focuses on the identification and implementation of mitigation measures to the identified knowledge sustainability barriers. Mitigation measures should cater to both inter-organisational and intra-organisational knowledge sustainability and knowledge use barriers.

The knowledge sharing framework is an attempt to provide consistency and simplicity for organisations involved in the design, development and integration of digital components for connected vehicles. Figure 7.15 below illustrates the knowledge sharing process that can be followed for the implementation of the framework. The framework is not intended to be sequential, but for illustration, it is presented as such.

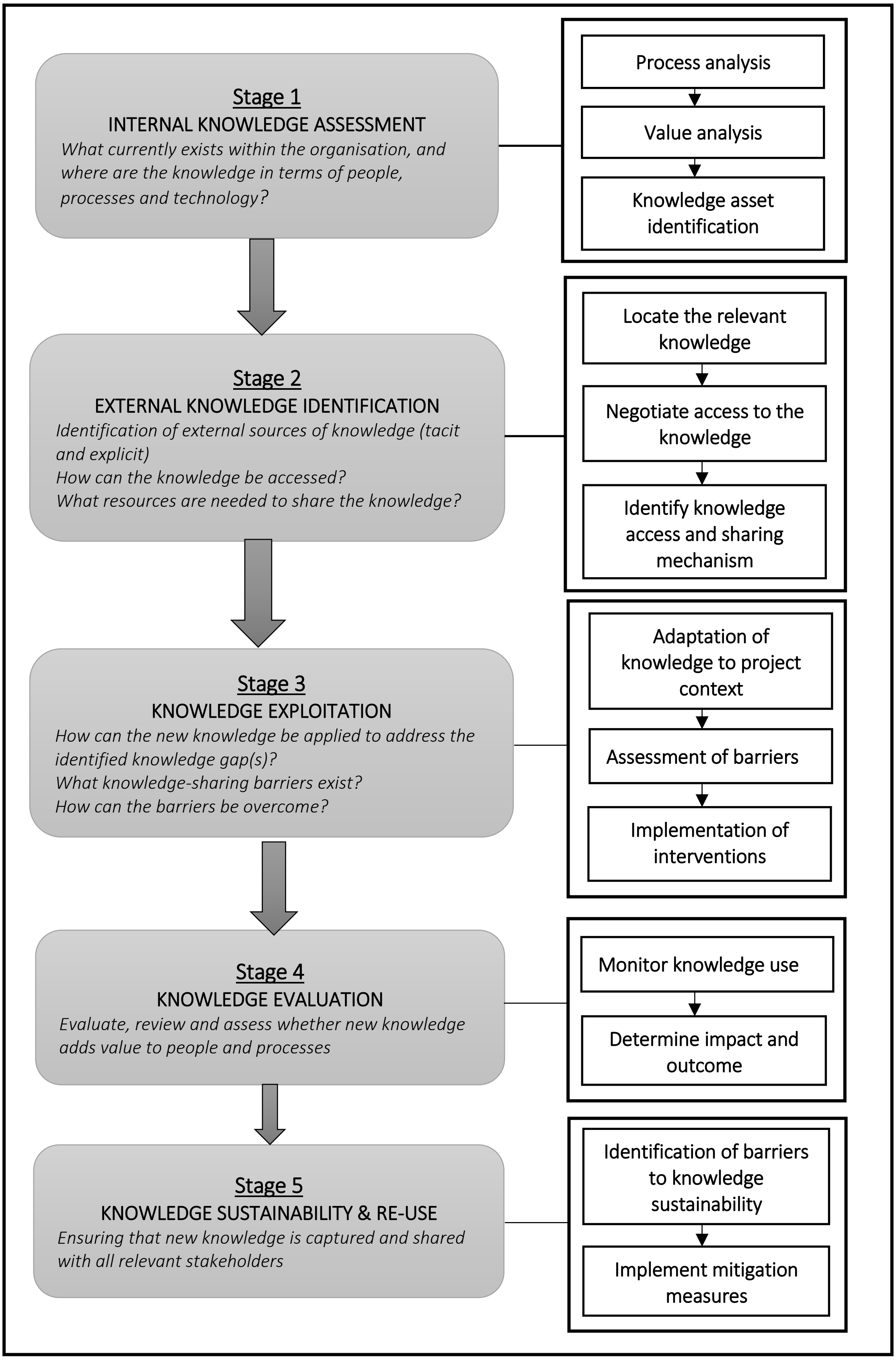

Figure 7. 15: Knowledge sharing processes with stages and sub-stages

The knowledge sharing framework is a highly iterative infrastructure that attempts to address the challenges of sharing knowledge in component integration processes. It provides a set of logical operational tasks that permit the integration of complex components and modules manufactured by a plethora of geographically dispersed organisations into a single functional cyber-resilient system. It achieves this by ensuring that information related to component integration is shared with all relevant stakeholders. However, as highlighted by Figure 7.16 below, its successful implementation requires consideration of 1) the final evaluated framework and its knowledge sharing factors (Figure 7.8); 2) the revised knowledge sharing infrastructure presented in Figure 7.11 and; 3) key strategic elements presented in the knowledge sharing processes in Figure 7.15.

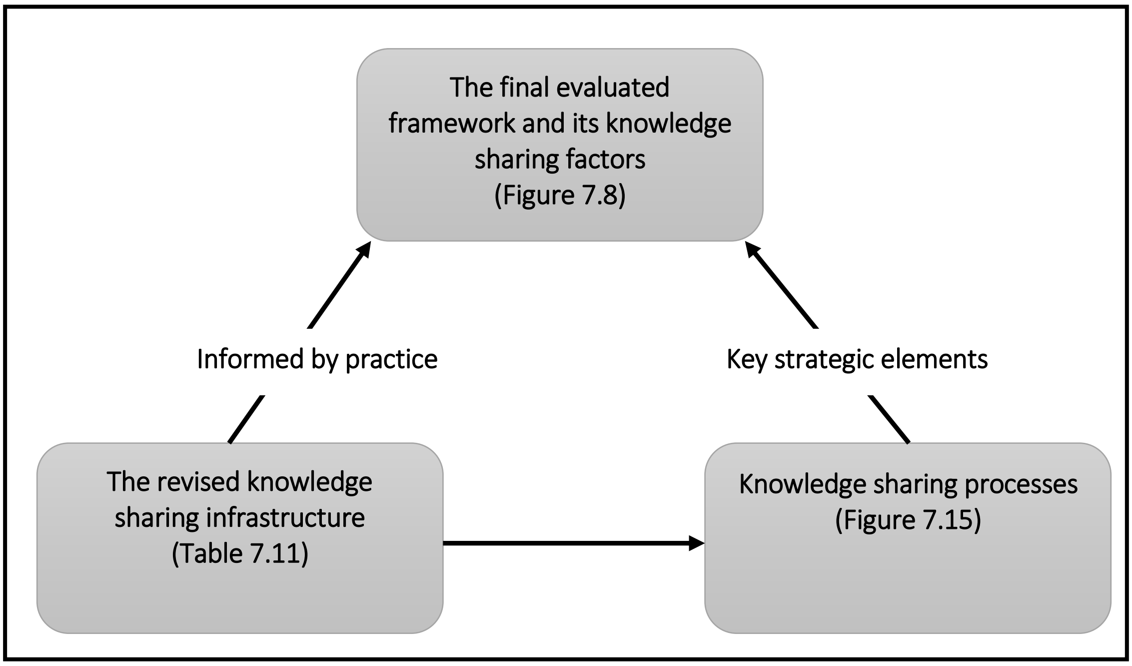

Figure 7. 16: Essential processes for the successful implementation of the knowledge sharing framework

7.5 Chapter conclusion

This chapter discussed the design and development of a knowledge sharing framework underpinning this research. The framework is designed to encourage vehicle manufacturers, component manufacturers and other relevant stakeholders that design and manufacture digital components for connected vehicles to understand how and why it is of utmost importance to share knowledge of relevance for component integration processes. The new framework offers a holistic and high-level strategic approach to knowledge sharing. Key factors generated from both empirical investigations and the outcomes of a literature synthesis were considered whilst devising the framework.

The main emphasis of the framework is on people, which derives from the view that knowledge resides within individuals who comprise the organisation. This, however, does not exclude other aspects of the organisation, and the framework reflects this through component and knowledge sharing factors that show the interdependency of knowledge sharing. A revised version of the framework was produced through critical reflection and reasoning, and feedback from the study's participants. It is recognised that the knowledge sharing factors may not be exhaustive, because organisations and project aims differ, and an organisation may identify additional factors that require further consideration according to their specific circumstances. All changes identified by the evaluation process have been incorporated into a revised framework presented in Figure 7.6, and the justification made clear, thereby ensuring a critically reflective and transparent process of development. The following chapter deals with the evaluation of the proposed knowledge sharing framework.

Chapter VIII

EVALUATION OF THE KNOWLEDGE SHARING FRAMEWORK

8.1 Introduction

The key limitations in current approaches for sharing knowledge for component integration processes in the automotive sector have been outlined in chapters 2 and 6 as a result of a review of relevant literature and feedback from industry professionals and knowledge experts. A new conceptual knowledge framework was formalised and presented in chapter 7.

This chapter addresses the final research objective and details the evaluation that has been undertaken to prove that the conceptual framework is fit for purpose. In the following sections, the results of the evaluation process are discussed and how the framework was revised to cater for the changes.

8.2 Evaluation strategy adopted

The objective of the evaluation process was to test the use of the conceptual knowledge sharing framework by presenting it to senior management personnel employed by component suppliers, OEMs and, knowledge experts in automotive manufacture. The key objective to be met was to identify any improvements to the generic framework.

To enhance reliability and validity, and to promote generalisability and credibility, the evaluation process included participants that were part of the initial data collection process (Chapter 4) and some who were not. The evaluation approach included triangulation, a useful means to pursue rigour, validity, reliability and justification of qualitative research (Darawsheh 2014, Morse 2015, Noble & Smith 2015, and Silverman 2015). Due to the dispersed geographic locations of the participants, the evaluation data was collected via a questionnaire sent via email to respondents, the email contained the framework, an explanation of how it functions and its intended purpose. Data collected via email has the advantage of enhancing response rates and, encouraging unbiased views, while potentially provoking a willingness to further participate and contribute to the research (Fan & Yan 2010). Additionally, data collected via email is less taxing on the researcher's time, effort and resources, and; offers a high degree of convenience for the respondents (Millar & Dillman 2011). A sample of the evaluation questionnaire and feedback is presented in Appendix 10.

8.2.1 Evaluation approach taken

The approach taken to evaluate the proposed framework was two-fold. Firstly, the evaluation process sought to elicit suggestions from the study's respondents as to how aspects of the generic framework might be improved. Secondly, evaluators were asked to comment on the comprehensiveness, clarity, conciseness and suitability of the framework within their organisation in assisting to address the sharing of relevant knowledge for component integration processes. These four conditions are very similar to the conditions used for theory evaluation. Comprehensiveness is similar to scope criteria, conciseness relates to parsimony, clarity and suitability relate to construct specification (Dhami 2016). According to Bulsara (2015), the evaluation process answers the posed questions from different perspectives and ensures that there are no gaps in the information or data collected. The evaluation approach addressed the following:

- The construct validity of the proposed framework by confirming whether the participants agree with the proposed integration processes contained in the framework.
- The level of understanding of the purpose and perceived value of the proposed framework.
- The usability and functionality of the proposed framework.
- Limitations and suggestions for improving the proposed framework.
- Suggestions on its potential adaptability into integration processes used within the automotive industry.
- Its ability to address knowledge sharing challenges in component integration processes.

Throughout the development phase, the initial and subsequent frameworks were evaluated against predefined criteria. Drawn from literature, these criteria were influenced by elements from the following:

- A set of best practices that relate to the sharing of knowledge as identified in the literature (Chapter 2)
- A set of knowledge sharing frameworks in the literature (Chapter 2).
- Component integration and knowledge sharing issues raised by the study's participants (Chapter 6).

The evaluation process consisted of two phases. In phase one, a questionnaire was designed and sent with the initial framework to the study's respondents to evaluate the framework in terms of comprehensiveness, clarity, conciseness and suitability. In the second phase, the initial framework was modified, refined and extended based on the responses provided by the study's participants. The reviewed framework and a questionnaire were then sent to the next round of evaluators for a response.

The processes undertaken to evaluate the framework are presented in Figure 8.1 below. The responses were collected, and a final framework produced (see Chapter 7, section 7.3).

This evaluation methodology serves dual purposes:

- It is a means for gathering expert perspectives and critiques of the framework as a basis for revision and improvement from personnel that engage with the phenomenon of sharing knowledge for component integration processes regularly.
- It creates an opportunity to obtain independent assessments of the proposed framework concerning the framework's comprehensiveness, clarity, conciseness and suitability.

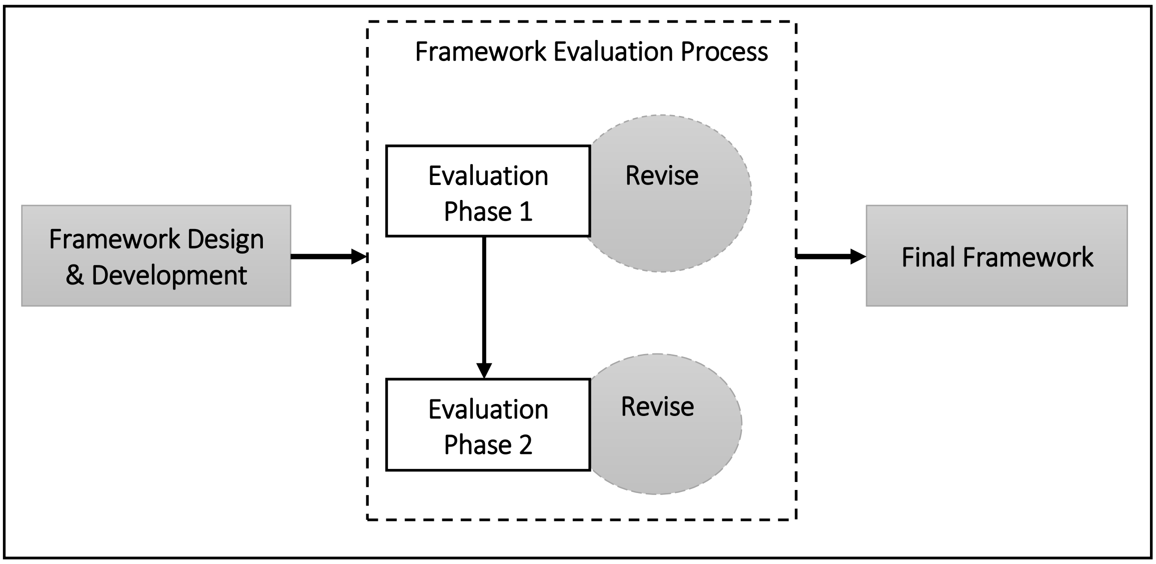

Figure 8. 1: The evaluation process

8.2.2 The evaluator selection process

The objective of the selection process was to identify a diverse group of individuals with expert knowledge about the phenomenon under investigation that correspond to the criteria outlined for inclusion in the study (Chapter 4, section 4.2.2). According to Flick (2014), selected individuals must be 'experts' in the field under investigation. This requirement introduces the first challenge in the selection process, which is, how to suitably define an "expert" in the context of knowledge sharing in component integration processes in the automotive domain. The use of "experts" is fundamental to reliability and according to Gobbens et al. (2010), an expert is an individual with a high level of knowledge or skill relating to a particular subject or activity. They have an intimate knowledge of the research area and are actively committed to a deeper understanding of the phenomenon under investigation.

A total of 10 candidates were identified and participated in the framework's evaluation process. According to Mason (2010), Dworkin (2012), and Baker et al. (2012), there are no guidelines, requirements or a clear understanding as to what constitutes as an ideal sample size. The participant's composition is more important than the number of participants (Marshall et al. 2013). Nonetheless, an increase in the number of participants is also imperative because it contributes to the reliability, validity and dependability of the results. Nworie (2011) suggests that the minimum acceptable sample size should not be lower than 4. The evaluation process comprised of four OEM employees, three employees of component manufacturing organisations and, three knowledge experts. Table 8.1 provides demographic characteristics and background information of the participants. The combination of such participants from different domains and roles, and possessing different skillsets provided rich information for evaluation, as supported by Flick (2014), who states that evaluation assessment will not be effective unless it comprises an appropriate balance of all the necessary expert knowledge. Given the participant's job roles and years of experience within the automotive domain, the feedback and knowledge provided from the evaluation survey; is accepted as and, is considered to be sufficient for analysis and recommendation.

Table 8. 1: Evaluator details

Phase 1	Job Title	Type of Organisation	Location	Experience
	Technology Manager	Component Manufacturer	Luxemburg	18 Years
	Manager	OEM	France	20 Years
	Director	OEM	Italy	19 Years
	Professor	University in the UK	United Kingdom	22 Years
Phase 2	Job Title	Type of Organisation	Location	Experience
	Executive Director	OEM	USA	39 years
	Director	OEM	Germany	26 Years
	Manager	Consultancy Firm	United Kingdom	15 Years
	Associate Professor	University in Germany	Germany	15 Years
	R&D Manager	Component Manufacturer	Germany	16 Years
	CEO	Component Manufacturer	Luxemburg	35 Years

Evaluation process – phase 1

The questionnaire used for evaluation in phase 1 was designed to ask the participants to rate and critique the initial framework in terms of comprehensiveness, clarity, conciseness and suitability. The questionnaire consisted of the following sections:

- Executive summary: providing a summary outlining the position, intention, purpose and goals for the framework. It also gives the reasons for the evaluation questionnaire.

- Abbreviations: this section provides definitions for the abbreviations used within the questionnaire.
- Phases and processes section: the section explains in brief, the purpose of each phase. The functions, processes and implementations that are executed at every phase within the framework.
- The proposed conceptual knowledge sharing framework.
- Process overview: explains in detail how the proposed framework functions, how it can be used, and how and what type of knowledge is gathered at each phase. It explains how the gathered knowledge is used in component integration processes.
- Questions and responses section: a number of questions regarding the framework's perceived value, usability and limitations are presented. The section also includes space where the participant can provide additional information not covered by the questions.
- Contact details: the section asks the respondent to provide their details including job title, company etc. for justification, rigour and validity.

The participants were requested to return the document containing their responses within two weeks. The author sent a reminder email 4 days before the due date reminding the participant to provide an evaluation of the framework. The responses were recorded, organised and analysed to identify suggestions to be considered for the framework revision and improvement, and for identifying suggestions that lie beyond the research boundaries (see Table 8.2).

Evaluation process – phase 2

In phase 2, the initial framework was reviewed and modified based on the feedback provided by the study's evaluators. Modifications to the initial framework involved extensive revisions by incorporating and developing new concepts stimulated by the evaluator's comments, detailing and further characterising the concepts existing in the initial framework. Fundamental modifications also included further justifying and clarifying the framework elements. The modified framework was then sent out to phase 2 evaluators for evaluation. Table 8.2 below further illustrates this process.

Similar to phase 1, participants were requested to return the document containing their responses within two weeks. The author sent a reminder email 4 days before the due date reminding the participant to provide an evaluation of the framework. Phase 2 responses were analysed in the same manner as phase 1 responses.

8.3 Response analysis

The purpose of the evaluation was two-fold. The first part of the evaluation document requested evaluators to provide specific comments for each component and its accompanying list of elements. The second part of the evaluation document asked for feedback on comprehensiveness, clarity, conciseness and suitability of the proposed framework. The proposed framework was exposed to critique to address the challenges of sharing relevant knowledge in component integration processes as highlighted by both empirical investigations and the outcomes of a literature synthesis. The results from this process allowed for further refinement of the framework.

Evaluation of the conceptual framework required direct experience from the automotive sector. This means that the specific data collection and data analysis methods in this study were driven by real organisations within the automotive domain and the researcher. The method of evaluation was the feedback from the questionnaires sent to senior management. The findings from these methods were collected and the conceptual model was refined to produce a 'final framework'. The 'final framework' captured the views of the evaluators and provided a more robust framework with the notion that the conceptual knowledge sharing framework is accepted as valid, useful and suitable by experts in the automotive domain.

Despite the value of qualitative data as a source of rich descriptions and explanations of processes, there are a number of well-known challenges associated with their analysis. In the context of this study, a challenge would be to provide evidence of the applicability of this framework for all component integration processes in different organisations, and by other individuals other than the researcher who implemented, assessed and refined the framework. Bryman (2012) and Glesne (2016) agree on the importance of aiming to achieve two key targets while analysing qualitative data. These are:

- Focusing on the most important aspects of the data.
- Transforming the data into something meaningful for the research and its target audience.

Following these viewpoints, the researcher focused on the important aspects of the data collected, making the necessary adjustments based on the evaluators' responses and transforming the framework into something meaningful for the research. Table 8.2 below summaries specific comments that emerged during the evaluation. In keeping with the concept of internal and external critique, the responses of the researcher to this feedback are also provided. The researcher's responses are intended to focus on the development and improvement of the framework, rather than any real evaluation of any organisation in the automotive sector. The reason for this is that it is the framework that is being evaluated to establish its fitness for purpose. To fairly evaluate an entire organisation within the automotive sector would require more time, resources, and research personnel to reach a fair balance and overview of the organisation.

Table 8. 2: Summary of critical reflection of responses from evaluators

Request	Evaluator comments and feedback	Critical reflection/response
Please consider the list of knowledge sharing factors associated with the component ***'organisational structure'*** (section 1.1 - 1.3 of the accompanying document). Can you suggest any other knowledge-sharing factors that the current framework does not consider?	• The framework and all accompanying documents consider information sharing from different perspectives, all equally useful to ensure that the information is communicated and delivered accordingly. While the framework clearly shows the structure and the "what should be done" to capture knowledge and to share the knowledge. Clarification on how any feedback from relevant stakeholders which could inform developments to refine the strategy is communicated. • The role that management plays in encouraging the creation of a knowledge culture, although clear, must be clarified further under the 'leadership' component. • The differences between organisational structure and business processes have some overlaps. Management should be involved in financial decisions that affect knowledge-sharing processes. • To promote and encourage knowledge-sharing, a culture of knowledge sharing should exist, therefore, I am more in favour of a knowledge sharing culture instead of behaviour.	• Noted and accepted. Relevant knowledge that is created and captured is included in the meeting agenda, where it will be discussed. The organisation will then update its project plan and its knowledge-sharing strategy. • Accepted and further clarified in the *'leadership'* component. • Noted, however, all financial requirements will be handled within the '*business processes'* component. Funding requirements and ensuring that all financial requirements are addressed transparently will be addressed in the '*business processes'* component. • Noted, the '*knowledge-sharing behaviour'* factor was changed to '*knowledge-sharing culture'*.
Please consider the list of knowledge sharing factors associated with the component ***'human resources'*** (section 2.1 – 2.4). Can you suggest any other knowledge-sharing factors that the current framework does not consider?	• To improve this component, I will suggest the use of individual development plans as a means of identifying training opportunities and assessing personal satisfaction. • A reward system should be available to encourage knowledge creation and transfer.	• Accepted and an annual appraisal system included as an indicator. • Rewards and incentives are offered, please refer to the 'staff performance and development' knowledge-sharing factor.

	• Recruitment should also focus on recruiting personnel with relevant integration knowledge.	• Noted, nonetheless, it is also, important to point out that recruitment will always recruit candidates with the required skillset, who are willing to adhere to the organisations business processes and culture.
Please consider the list of knowledge sharing factors associated with the component ***'business processes'*** (section 3.1 - 3.4). Can you suggest any other knowledge-sharing factors that the current framework does not consider?	• The knowledge-sharing factors highlighted within this component are best described as business processes, as they cover processes that are crucial to running an organisation. • The organisation should have a strategy focused on contract agreements/negotiations etc. This is particularly important in addressing challenges relating to NDAs.	• Noted, the name of the component changed from '*financial resources'* to '*business processes*.' • Noted, a component named 'contract agreement; was created to address contract negotiations and agreements.
Please consider the list of knowledge sharing factors associated with the component ***'communication'*** (section 4.1). Can you suggest any other knowledge-sharing factors that the current framework does not consider?	• The framework considers inter and intra-organisational communication, consider how unreliable or inaccurate knowledge acquired from unreliable sources can be filtered. • The 'communication' component is very crucial to the success of the framework. • The communication channels need to be regularly updated to keep pace with technology and modern-day demands.	• Discussions are held with all relevant stakeholders within each project. Through discussions held within these project meetings, relevant information is identified and included in the knowledge sharing strategy or project plan. No information is used or retained without going through a project meeting. • Noted. • Noted and highlighted as an indicator.
Please consider the list of knowledge sharing factors associated with the component ***'leadership'*** (section 5.1 – 5.2). Can you suggest any other knowledge-sharing factors that the current framework does not consider?	• I think leadership can also be measured or assessed for how they make strategic information available not only to relevant stakeholders within a project but to the organisation as a whole. I would also expect the leadership to demonstrate how the organisation is utilising and sharing information at a strategic level. • This section should include training. Leadership is at most times excluded from training. The expectation is that they should provide the training.	• Noted and recognised. • Noted, training will be provided to all employees.

	• The framework should also consider personal leadership styles within the organisation and/or within a project.	• Noted and recognised.
Please consider the list of knowledge sharing factors associated with the component ***'technological infrastructure'*** (section 6.1 – 6.5). Can you suggest any other knowledge-sharing factors that the current framework does not consider?	• A risk assessment of all aspects of the organisation and its communication infrastructure to identify areas in need of quality improvement. • Does the technological infrastructure cover the organisations networking infrastructure? • It seems the component takes into consideration infrastructure that exists outside the organisation but is used when interacting with other organisations, so well thought approach.	• Noted. The comment is noted ad recognised as very important; however, it is up to each organisation to conduct risk assessments as they deem necessary, risk assessments lie outside the scope of the framework. • The '*technological infrastructure'* component covers all infrastructure required for communication and the sharing of knowledge. • Noted.
Please consider the list of knowledge sharing factors associated with the component ***'regulatory requirements'*** (section 7.1 – 7.5). Can you suggest any other knowledge-sharing factors that the current framework does not consider?	• The framework aligns with existing industry's best practices, standards and guidelines. There are several guidelines, regulations and standards in the making which will be introduced soon, how will the framework adopt new requirements that will result from these new standards and regulations? • Good to see that regulation is considered as it does play an important part in how knowledge is created and shared. How are the relationships with regulatory boards managed?	• Regulatory requirements will be reviewed regularly to identify and comply with new requirements. • To influence and shape regulation, standards and guidelines, the framework encourages the organisation to take part in meetings, research and activities that lead to the creation of regulatory requirements.
Please consider the list of knowledge sharing factors associated with the component ***'political and legal'*** (section 8.1 - 8.3). Can you suggest any other knowledge-sharing factors that the current framework does not consider?	• Political and legal changes can also be added to the project meetings and briefings that occur within the organisation, to update staff on immediate crucial changes. • Environmental challenges have come to the fore with a lot of attention being afforded to reducing global carbon emissions. Therefore, if the framework could include global ecological issues aiming at the satisfaction and good service role an organisation in the auto-domain could play.	• Noted and changed on the framework. • Noted for future research. No changes made to the framework.

Please consider the list of knowledge sharing factors associated with the component ***'contract agreements'*** (section 9.1 - 9.3). Can you suggest any other knowledge-sharing factors that the current framework does not consider?	• This is probably the trickiest hurdle to knowledge-sharing, and it is of great importance that it has been considered. Each project, each organisation will have its requirements, having a dedicated team that works to bring it all together, while ensuring that fair play is maintained will be the challenge. • The department that will oversee contract negotiations will need a global reach as contracts depend on the country, company, national and international laws. • The inclusion of all stakeholders and personnel with relevant legal expertise will be vital in thrashing out agreements that allow for knowledge to be shared.	• Component created as a result of feedback received from evaluators. • Noted and changed on the framework. • Noted and highlighted on the framework.
Please consider the list of knowledge sharing factors associated with the component ***'social culture'*** (section 10.1). Can you suggest any other knowledge-sharing factors that the current framework does not consider?	• This is an important component and it could have been developed further to include political pressures employees are exposed too, that may or may not affect their views on knowledge-sharing. • Religion could be considered.	• Component created as a result of feedback received from evaluators. • Noted and more indicators added.

8.4 Results

The evaluation process resulted in changes to certain components and elements of the framework. Knowledge sharing processes were also revised and modified to cater to recent and ever-increasing technological developments that occur in vehicle manufacturing and to improve the sharing of knowledge in the integration of components for connected vehicles. It is clear from the suggestions provided by the evaluators, each organisation that chooses to adopt the framework into their organisation will need to adjust the framework to align it with their organisation's component integration processes and knowledge sharing approaches. This may involve the addition of more components and elements, however, if the organisation opts to omit certain components or elements that influence the sharing of knowledge, justification of this should be sought; otherwise, significant gaps may appear that affect the functionality of the framework.

8.4.1 Overall average scores for each component

After taking into consideration the feedback received concerning the generic framework and associated process for knowledge sharing, this section discusses the analysis of the results that are intended to highlight the outcome of the evaluation process. This section is not intended to be a comprehensive analysis of the automotive industry, but to establish that the framework is usable and applicable to a relevant conclusion.

The following section presents the evaluation results in graphical form. The horizontal axis identifies the domain within which each question was asked. The vertical axis shows the number of evaluators, and the key to the right presents the scores ranging from 1 to 4. Table 8.3 below presents an example of the scoring process employed. The use of percentages (%) is employed for clarity and greater understanding of the graphical form used to represent the scores.

Table 8. 3: Example of score capture for each component

Importance of each component to your organisation and integration processes			
Very Important	Important	Moderately Important	Unimportant

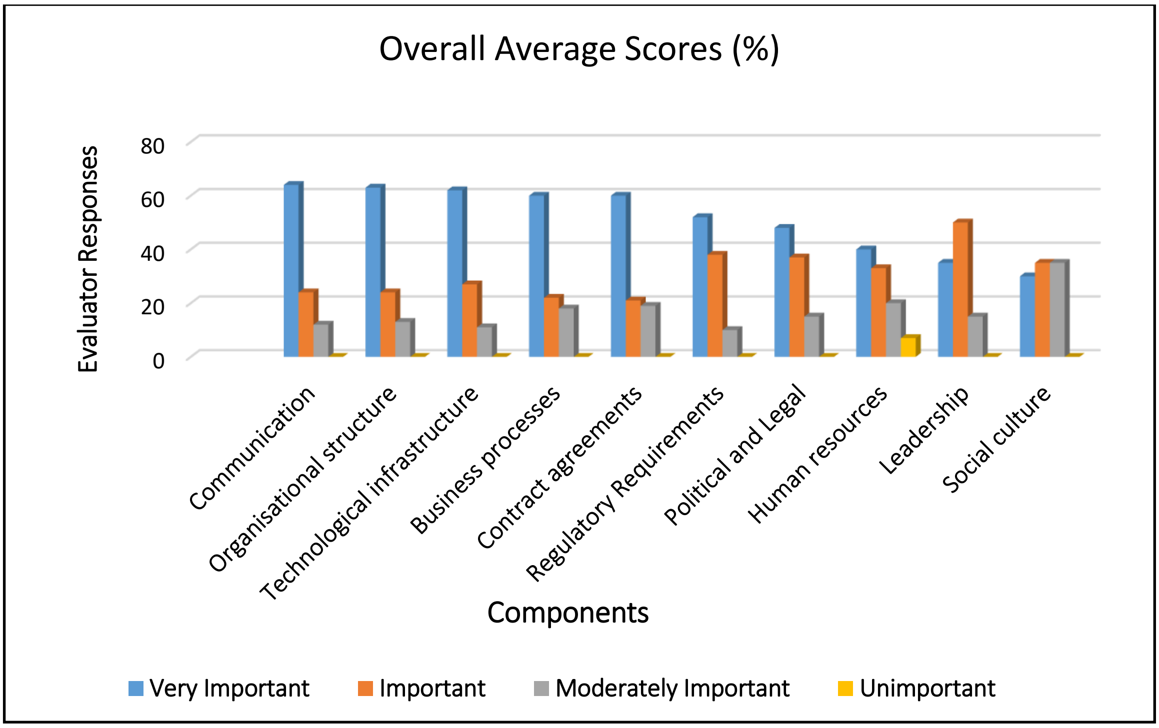

Figure 8. 2: Overall average scores

The "very important" components according to the evaluators are communication, organisational structure and technical infrastructure, both scoring above 60%. The Human resources component is the only component that obtained a score in the "unimportant" category. Table 8.4 below presents the components in order of "very important."

Table 8. 4: Overall scores from the study's evaluators

Component	Very Important	Important	Moderately Important	Unimportant
Communication	64	24	12	0
Organisational Structure	63	24	13	0
Technological Infrastructure	62	27	11	0
Business Processes	60	22	18	0
Contract Agreement	60	21	19	0
Regulatory Requirements	52	38	10	0
Political and Legal	48	37	15	0
Human Resources	40	33	20	7
Leadership	35	50	15	0
Social culture	30	35	35	0

Exploring individual components further, the following graphs present the overall scores for each component highlighting comparisons between OEM scores, component supplier scores and, scores from automotive knowledge experts.

Figure 8.3 below shows a comparison between the responses from OEMs, component suppliers and knowledge experts on the communication component.

1. Communication component

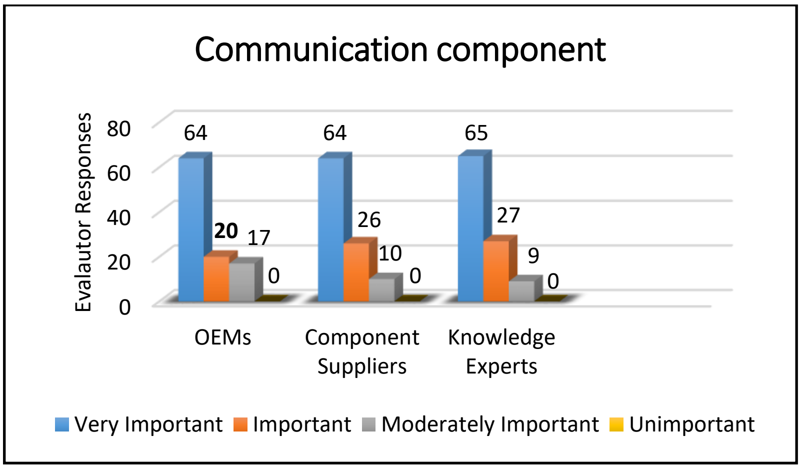

Figure 8. 3: Communication component

The results show that communication is regarded as '*very important*', evaluators from the component manufacturing organisations, knowledge experts and those employed by OEMs all scored more than 60%. All three sets of evaluators scored the communication component as *'very important, important or moderately important'*.

The results indicate the importance of communication and structures that encourage communication within an organisation. In the final version of the proposed framework, after reviewing comments from the evaluation process, the communication component accommodates for usable, current and relevant communication channels and processes that are in-line with the technological developments being experienced in the automotive industry. However, during the initial empirical investigations that the researcher took, communication was identified as lacking, especially within vehicle manufacturing organisations. The participants that participated in the data collection process highlighted trust, competition, and the automotive supply chain structure as challenges that affect communication within the domain. The researcher also regards the communication component and factors that encourage communication as very important for the sharing of knowledge associated with component integration processes.

2. Organisational structure component

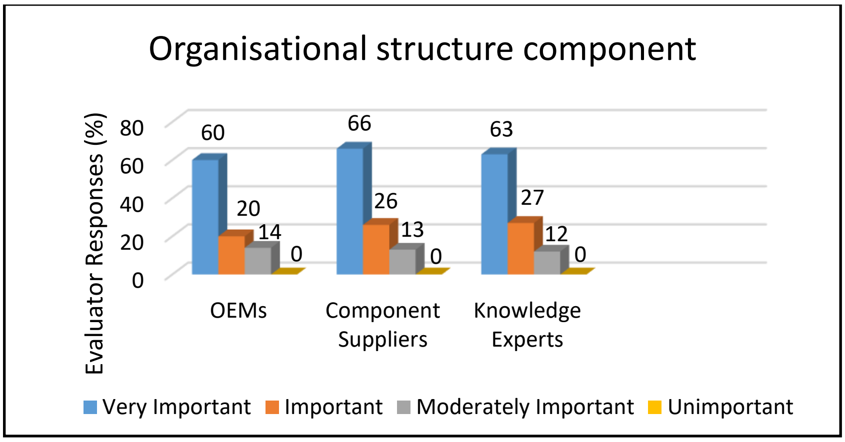

Figure 8. 4: Organisational structure component

All three sets of evaluators regard the organisational structure component as a *'very important'* component for the sharing of knowledge in component integration processes. Component suppliers regard the organisational structure component more important than OEMs and knowledge experts with 66% of component suppliers scoring the component as *'very important'* compared to the 60% of the OEMs and 63% of the knowledge experts. Nonetheless, all three sets of evaluators regard this component as *'very important, important or moderately important'*.

The results indicate that OEMs, component suppliers and knowledge experts realise that processes to share knowledge relevant for component integration are very dependent on the organisational structure of an organisation. For knowledge sharing processes to exist, prosper and effectively contribute to secure integration of components, the organisational structure should be capable of encouraging and creating a knowledge sharing culture. In the final version of the proposed framework, management is tasked with building knowledge sharing structures and establishing a knowledge sharing culture, please refer to Chapter 7, section 7.3 for further clarification.

3. Technological infrastructure component

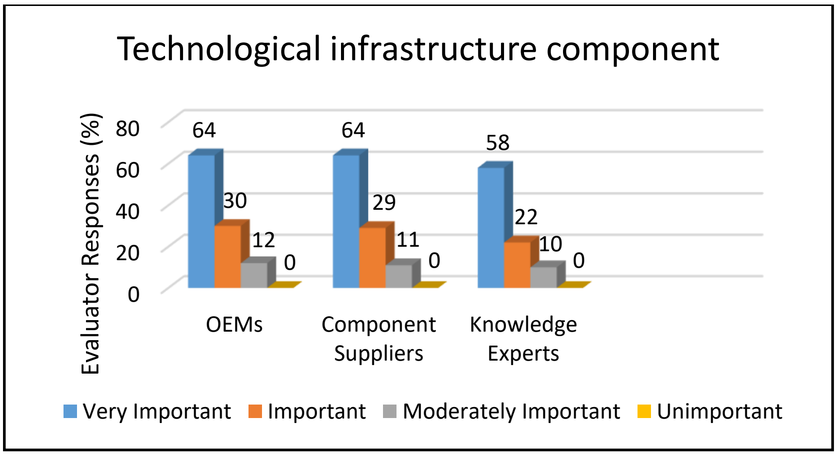

Figure 8. 5: Technical infrastructure component

Both OEM and component supplier evaluators regard the technical infrastructure component as *'very important'* for the sharing of knowledge for component integration processes. OEM and component supplier evaluators scored 64% each for the technical infrastructure component compared to the 58% scored by knowledge experts. In the final version of the proposed framework, after critical reflection stimulated by the feedback received during the evaluation process, the following factors for sharing knowledge were deemed necessary in improving the technical infrastructure component:

- Information technology
- Knowledge-sharing strategy
- Quality assurance systems
- Information management systems
- Training teams

4. Business processes component

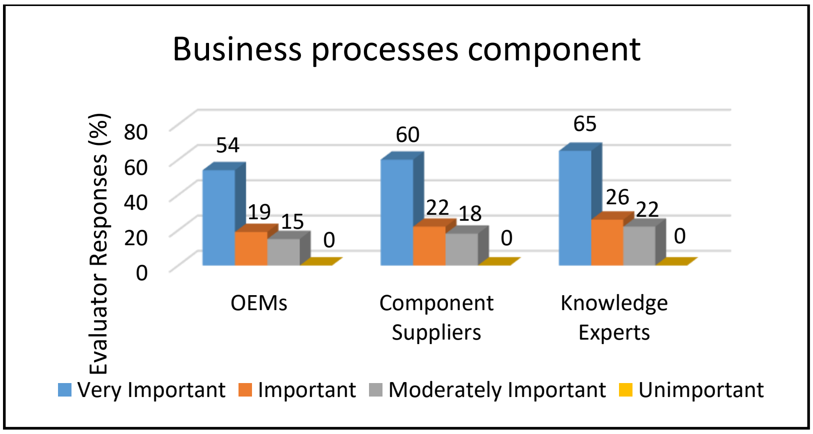

Figure 8. 6: Business processes component

Knowledge expert evaluators regard the business processes component as *'very important'*, scoring the component 65%, compared to 54% of the OEM evaluators and, 60% of the component supplier evaluators. The component was changed to business processes from financial resources based on the feedback provided by the evaluators, please refer to section to Chapter 7, section 7.3 for further clarification. Knowledge experts regard the business processes component as very important in sharing of component integration-related knowledge because it caters for personal commitment and satisfaction, an attribute that encourages individuals to create and share knowledge (Kim et al. 2010, Iglesias et al. 2011, and Matzler et al. 2011). When staff are happy, motivated and committed, they are more likely to share knowledge acquired and are more likely to engage in knowledge creation initiatives.

5. Contract agreement component

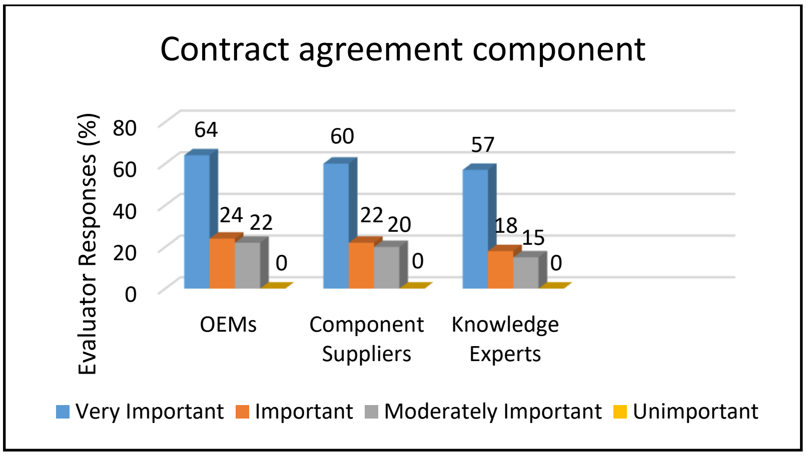

Figure 8. 7: Contract agreement component

OEMs and component suppliers are greatly affected by NDAs, design contracts, confidentiality agreements and other forms of gagging agreements. The scores, 64% provided by OEM evaluators and 60% provided by component supplier evaluators in the *'very important'* category, reflect the challenges OEMs and component suppliers face in the sharing of relevant knowledge which aids with component integration. The inclusion of the contract agreement component was stimulated by critical reflection and feedback received during the data collection phase and the evaluation phases, please refer to Chapter 7, section 7.3 for further clarification and justification for the component's inclusion in the proposed framework. From the discussions conducted during the data collection phase, the researcher thought the scores for the contract agreement would exceed the 70% score. This was a surprising result for the researcher. Nonetheless, the contracts agreement component is seen as very important by all three groups of evaluators.

6. Regulatory requirements component

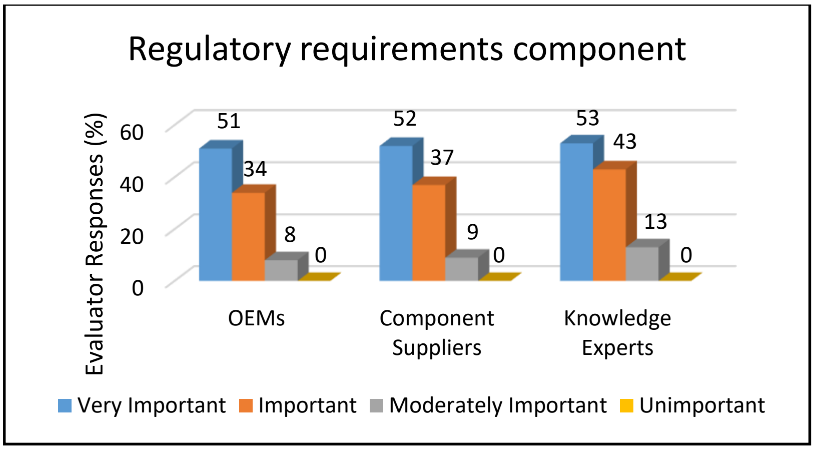

Figure 8. 8: Regulatory requirements component

All three sets of evaluators scored the regulatory requirements' component above 50% in the *'very important'* category, indicating the importance of regulatory compliance in processes for sharing knowledge associated with component integration processes. 43% of knowledge experts see this component as *'important'*, while 53% regard this component as *'very important'*. The researcher thought OEM and component supplier evaluators would regard this component as more important compared to knowledge experts. The review of relevant literature supported by the data collection phase highlighted knowledge sharing challenges that are a result of the lack of existing regulation or legislation for the sharing of knowledge, in particular, knowledge related to component integration processes (Macher et al. 2017), therefore the researcher thought OEMs and component suppliers would regard this component as critical for the sharing of relevant component integration-related knowledge. Existing standards, regulations and guidelines place an extra focus on the need to ensure data privacy in connected vehicles, instead of encouraging the sharing of knowledge of importance for secure component integration processes. Please refer to Chapter 2, section 2.7 for further clarification on automotive standards, regulation and best practices.

7. Political and legal component

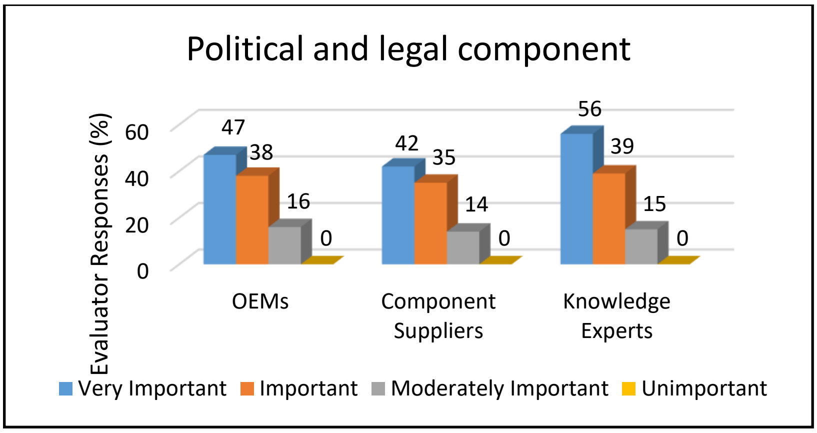

Figure 8. 9: Political and legal component

Knowledge expert evaluators scored the political and legal component 56% compared to the 47% of OEMs and 42% of component supplier evaluators in the *'very important'* category. The scores provided by the evaluators reflect an awareness of the political and legal challenges, and the difference in political and legal challenges faced by OEMs, component suppliers and knowledge experts. Another reason why knowledge experts regard this component as very important, maybe because, in most contract agreement negotiations, knowledge experts are tasked with addressing and ensuring the contract agreement terms are not in violation of political and legal laws. Nonetheless, the scores provided by OEM and component supplier evaluators indicate the importance of this component.

8. Human resources component

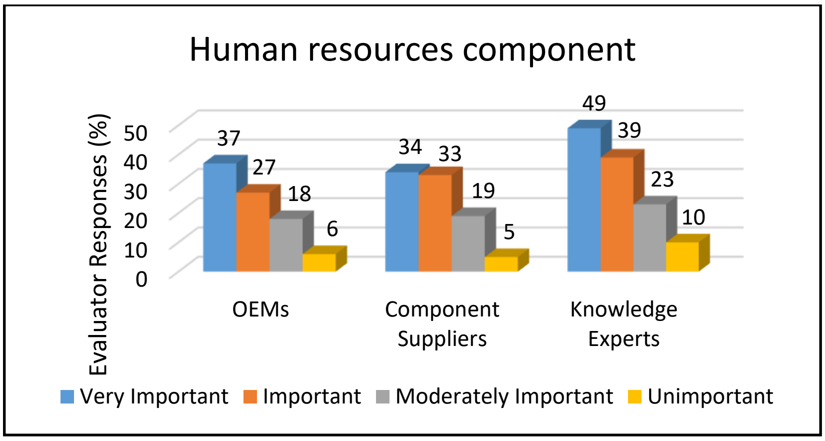

Figure 8. 10: Human resources component

The human resources component was the only component that received a score in the *'unimportant'* category. All three groups of evaluators scored the component below 50% in the *'very important'* section and, below 40% in the *'important'* category. The scores for this component surprised the researcher as human resources are tasked with addressing the needs and development requirements of employees. Human resources are a crucial attribute, as it is within this sphere of activity that employees within an organisation are motivated and encouraged to participate in processes for knowledge sharing. Knowledge experts scored the component the highest, a possible reason, maybe because knowledge experts are more aware of the importance of staff development to improve and encourage participation in knowledge sharing processes.

9. Leadership component

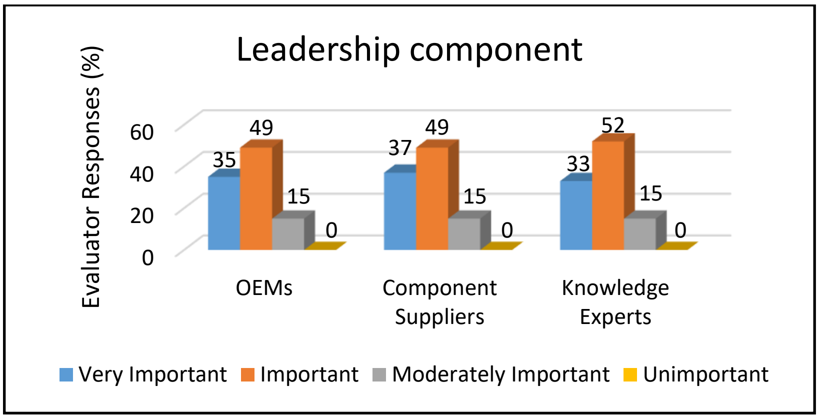

Figure 8. 11: Leadership component

Knowledge experts scored the leadership component above 50% compared OEM and component supplier evaluators who scored the component 49% each in the *'very important'* category, nonetheless, the distribution of scoring between the three groups is almost even. The sharing of knowledge emanates from the top of the organisational structure, this makes this component very crucial to the sharing of knowledge related to component integration processes.

10. Social culture component

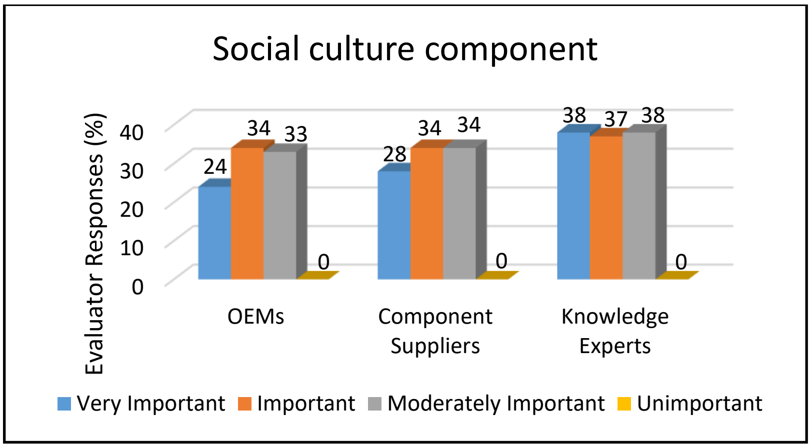

Figure 8. 12: Social culture component

The social culture component was not regarded as *'very important'*, OEM evaluators scored the component 24%, and component supplier evaluators rated it at 28%, while knowledge expert evaluators scored it at 38%. The scores for the *'important'* category for OEM and component suppliers were equal at 34%. Knowledge experts scored the component 37% in the *'important'* category. After critical reflection from the researcher and feedback received from the evaluators, the social culture component was added to the framework in the external relationship environment. The sharing of knowledge relevant for component integration processes can be improved if the organisation fully understands its social environment, appreciating and understanding its staff's views and perceptions to sharing of knowledge.

8.4.2 Overall feedback in terms of suitability, credibility and clarity

When asked whether the purpose of the framework was clear, a total of 96.4% of the evaluators thought the framework was clear. 97.3% of the evaluators from OEMS, 95.4% of the evaluators from component suppliers, and 96.4% of the evaluators from knowledge experts thought the framework was clear.

Table 8. 5: Specific comments from evaluators with regards to the framework's clarity

Evaluator	Evaluators' comments
OEM	The framework's knowledge sharing factors and the way they relate to their respective components are very well defined and explained. The relationship between the two has been well presented.
OEM	The core competencies section assists in defining and explaining what each knowledge sharing factor ought to or should address.
Component supplier	At a high level it addresses knowledge sharing challenges from key business functions, and it is very clear on the approach it adopts in addressing those challenges.
Knowledge expert	The knowledge sharing approach is sufficiently clear, its covers knowledge creation, capture and transfer to promote the purposes for which it was designed for.

When asked whether the purpose of the framework was suitable for automotive component integration, a total of 97% of the evaluators thought that the framework was suitable. 98% of the knowledge experts' evaluators thought the framework was suitable, while 97% of the evaluators from OEMs and 90% of evaluators from component suppliers thought the framework was suitable.

Table 8. 6: Specific comments from evaluators with regards to the framework's suitability

Evaluator	Evaluators' comments
OEM	The framework's integration processes are sufficient for integrating components for connected vehicles. It is a clear framework that is very easy to adapt to the already existing processes that we use. Could this be the solution that the industry has been waiting for?
OEM	The processes covered by the proposed framework are sufficient and suitable for the automotive industry. The processes not only address the technical but also business processes that are at times overlooked. Most frameworks tend to approach the integration challenge as a technical problem and attempt to address the challenges with technical solutions alone. This is where I think this framework has an advantage because it approaches the challenge from many yet different perspectives.
Component supplier	The processes are sufficient, the framework considers many segments of the business that are important for knowledge sharing. NDAs are considered that is why the framework is more than sufficient for us as component suppliers and for the OEMs that we work with.
Component supplier	This provides a good methodology for building a robust architecture with appropriate testing and integration processes. Its strength is knowledge sharing, this must be enforced and made mandatory, either by engaging with workgroups, governments, private sector etc. to break the culture of secrecy.
Knowledge expert	The processes are aligned with already existing best practices, standards and regulations (ISO26262, SAEJ3061), this consideration of such standards assists in ensuring that the processes are suitable for integration.
Knowledge expert	Because the framework caters for the protection of IP, it will be welcomed into the industry. One of the main challenges that have haunted the industry is the need to protect an organisation's innovations. Since the framework addresses this issue, I feel it is appropriate and will be adopted by some if not most organisations.

When asked whether the purpose of the framework was credible, a total of 96.4% of the evaluators thought the framework was credible. 97.3% of the evaluators from OEMS, 95.4% of the evaluators from component suppliers, and 96.4% of the evaluators from knowledge experts thought the framework was credible.

Table 8. 7: Specific comments from evaluators with regards to the framework's credibility

Evaluator	Evaluators' comments
OEM	The processes, the components and the knowledge sharing factors presented in the framework have the potential to address the challenges introduced by component integration approaches that we use within my organisation.
Component supplier	The framework was designed and developed through consultation with industrial and academic experts, and the use of academic articles. This provides the framework with a respectable level of integrity and dependability.
Knowledge expert	The framework considers both non-technical and the technical aspects required for effective knowledge sharing, something I consider lacking in most frameworks that already exist today. Based on my experience, I think this is a good approach which should be further developed to keep pace with the developments that are happening in the automotive industry.
Knowledge expert	The framework offers some form of guide on what needs to be taken into account to achieve secure component integration for the vehicles that the industry is now focused on manufacturing. The facts that it looks at areas where knowledge can be created and shared individually before bringing it all together offers a systematic approach that is necessary and helpful.

8.5 Summary of the evaluation process

The evaluation of the proposed framework was conducted in two phases. In phase 1, a questionnaire was designed and sent with the initial framework to the study's respondents to evaluate the framework in terms of clarity, credibility and suitability. In the second phase, the initial framework was modified, refined and extended based on the responses provided by the study's participants. The reviewed framework and questionnaire were then sent to the next round of evaluators for a response. The scoring method for each of the framework's components was kept to a simple scale to fully appreciate the level of importance each evaluator scored for each component. The major changes to the components and knowledge-sharing factors in the initial framework are:

- The inclusion of a new knowledge sharing factor in the external relationships' environment dedicated to contract agreements.
- The inclusion of a knowledge sharing factor under the '*political and legal environment*' dedicated to the protection of an organisation's intellectual property rights.
- A *'social culture'* component was added to the modified framework based on feedback provided by phase 1 evaluators.

The approach adopted in the analysis of responses gathered from the evaluators was a presentation and evaluation of results. This was not intended to be a comprehensive analysis of the automotive industry as a whole, but to establish that the proposed framework was useable to a relevant conclusion. During the analysis and evaluation of the results, it became evident that the proposed framework can be tailored to a company-specific context. There were no changes to the components, knowledge sharing factors and structure of the revised framework, confirming that the cycle of development and improvement, with previous critical review, had reached a reasonable point of saturation.

8.6 Chapter conclusion

This chapter has described how the proposed framework was evaluated. It has described in detail the evaluation approach and how the responses were analysed. The respondents; who are experts capable of forming acceptable technical, academic and scientific opinions on the proposed framework, provided feedback which can be accepted and considered as useful, sufficient and enhances the credibility of the framework. Based on the feedback, views and comments received from the evaluators, the framework has the potential to improve the sharing of relevant knowledge for the integration of components for connected vehicles.

However, the effectiveness of the proposed knowledge-sharing framework will differ between organisations. These differences are attributed to the difference in personnel, differences in organisational structures (Dark et al. 2015, Axelrod et al. 2014, Trim & Lee 2014), and differences in technology. Therefore, the proposed framework can be considered as an important support function without which most component integration-related knowledge sharing practices would either be non-existent or less effective. The next chapter presents a discussion on the study’s key contributions, outlining the study’s limitations, as well as discussing avenues for future research.

Chapter IX

CONCLUSIONS AND RECOMMENDATIONS

9.1 Introduction

Previous chapters have identified key factors that influence the sharing of knowledge in component integration processes and, proposed a knowledge sharing infrastructure that considers knowledge sharing in inter-organisational, intra-organisational and external environments. This chapter first returns to the main impetus for the research and briefly summarises the key findings, so as to provide the context within which the study's main implications can be considered. Following on from this discussion, the main contributions of the study are presented. It also evaluates the research against the original objectives and concludes by reflecting upon the study's limitations. The chapter also identifies potential avenues for further research.

For much of the 21st century, the idea that the automotive industry could develop intelligent vehicles capable of connecting to the internet has been an aspiration rather than a reality, and the idea of autonomous vehicles seemed futuristic rather than a realistic possibility in the short or medium term. Traditionally, the vehicle had been seen as an extension of a person's ambulatory system, docile to the driver's commands. However, the recent proliferation of computable devices, and the advances in ICTs, vehicle controls and embedded systems, has seen the automotive industry experiencing possibly its greatest technological transformation to-date. In the wake of these innovative advances, the auto-industry has responded by developing connected vehicles and is now on the verge of providing fully autonomous vehicles. Connected vehicles and AVs can be seen as two separate but overlapping technologies. AVs or "driverless vehicles" reduce the need for input from human operators, while connected vehicles interface with the internet, transport and road infrastructure and other intelligent vehicles to facilitate information sharing.

While all AVs are in some sense "connected", not all connected vehicles are automated. The manufacturing of connected vehicles capable of absorbing information from the environment and other vehicles and then feeding it to drivers and the infrastructure to assist with safe navigation, pollution control and traffic management, is an expensive, competitive complex task that demands an effective sharing of knowledge between vehicle manufacturers and component suppliers as well as between suppliers themselves. The modern connected vehicle, which has now become more than a mode of transportation, is built with digital components that are manufactured by a plethora of globally dispersed component suppliers.

9.2 Main findings

First, consistent with prior research on knowledge sharing in the automotive industry, the findings demonstrate that the automotive industry is an industry that relies on and encourages knowledge sharing. Before the introduction of electromechanical constructs in vehicle manufacturing, the automotive industry relied on knowledge sharing for fostering high involvement relationships with suppliers within the supply chain, and for developing and manufacturing mechanical constructs. Studies in the European, Chinese and Japanese auto-industries and elsewhere provide evidence of the existence of knowledge sharing practices and highlight how knowledge is used to improve vehicle manufacturing.

The study shows that the introduction of computable technologies that permit vehicles to connect and communicate to internal and external environments introduced a new breed of entrants into the automotive supply chain, and transformed vehicle manufacturers' core business activities, thereby introducing challenges to knowledge sharing approaches. One possible explanation for these results may be the globalisation and delocalisation of component suppliers to countries with potentially lower production costs. The potential delocalisation impacts on supply chain knowledge sharing approaches have not received the attention they demand or merit, such impacts are not well identified and discussed within the context of component integration, this possible explanation indicates a potentially interesting direction for future research.

Second, the findings indicate that there is a lack of mechanisms to enable and promote the sharing of knowledge, in particular, knowledge related to component integration practices. The success of the automotive industry relies on the security of the digital ecosystem where connected vehicles operate, which in turn, depends on the sharing of relevant knowledge that improves the security of connected vehicles between different stakeholders of the auto-ecosystem. The study's findings show that knowledge sharing approaches for component integration processes in use by the automotive industry have been evolved from traditional knowledge management and knowledge transfer mechanisms that have long existed within the sector. However, these knowledge sharing approaches of old have failed to encourage the sharing of knowledge related to component integration knowledge processes. There have been several attempts by the industry to create alliances, however, as noted by Choucri et al.

(2016) and Bryans (2017), the lack of economic incentives to participate and share knowledge, and the effectiveness of the information being shared has failed to encourage participation. Nevertheless, cybersecurity challenges that are born out of insecure integration approaches are new to the automotive industry and, beyond the available approaches highlighted by the study's respondents, the development of mechanisms that permit the sharing of such knowledge in the automotive industry remains a relatively under-researched area. Additionally, cybersecurity is predominately viewed as a technical problem that requires technical solutions. As discussed in Chapter 2, the bulk of extant literature focuses on the technical aspects of cybersecurity impacts. The concepts and practices of sharing cyber-related knowledge to improve the security of connected vehicles are still very much in their infancy and not prominent in the existing discourse. Knowledge sharing efforts assist OEMs and component suppliers not only to respond more quickly with focused remedies but also to design, develop and integrate components into secure systems. The view that security challenges in the automotive industry can only be addressed by technical solutions requires further considerations as to why such perceptions exist.

Third, the findings revealed that the automotive industry is still committed to existing traditional innovation values and ideas that place safety ahead of security. A culture of security is yet to fully embed itself within vehicle and component design and integration processes. The study's findings indicate that vehicle and component manufacturers treat security as a design extraneous in the same way that they treat quality, functionality, comfort and performance requirements. A possible explanation for this lack of security culture could possibly be narrowed down to the level of competition that exists within the domain. Despite being involved in so many revolutions at once; the electric vehicle (EV) revolution, the digital and autonomous vehicle revolution, the new mobility revolution, the industry 4.0 revolution, the main objective for automotive manufacturers is still to manufacture and sell vehicles. The value of the connected vehicle market is estimated at €42bn per annum and predicted to triple to €122.6 billion by 2021, vehicle manufacturers and suppliers compete on being the first to bring a new product to market. Nonetheless, the competitive nature of the industry could have been the reason for some of the changes that have occurred in the automotive supply chain such as delocalization, globalization and an increase in component outsourcing.

Fourth, the study's findings highlight an over-reliance on component manufacturers to provide, create and share knowledge and solutions. As highlighted in Chapter 6, a majority of polled participants employed by vehicle manufacturing organisations were not familiar with knowledge sharing processes utilised by their organisation. Consistent with the literature on manufacturer-supplier co-development approaches, the results highlight a lack of skilled personnel in vehicle manufacturing organisations capable of providing the required knowledge sharing solutions. Another possible explanation for these results may be the current structure of the automotive supply chain. With OEMs and suppliers geographically dispersed, OEMs are no longer capable of exerting the appropriate level of involvement in the supplier's design decisions and component integration processes. Manufacturer intrusiveness represents the level of detail and the amount of coordination the manufacturer employs in defining the design of the respective artefact. The level of intrusiveness influences the level of knowledge the OEM has about the component and the best integration processes required for the component, which in turn, leads to insights on how vulnerabilities may arise and what mitigation measures may be required to address the related cybersecurity threats. Moreover, this challenge of OEM intrusiveness is further compounded by the fact that globally dispersed component suppliers in a bid to remain relevant, jealously guard intellectual capital despite limited access to knowledge of the vehicle's architecture within which their components will reside. The possible over-reliance on component suppliers for solutions is an area that indicates a potentially interesting direction for future research.

Fifth, the study's findings highlight knowledge sharing challenges that result from a lack of trust between OEMs, between suppliers and between OEMs and suppliers. This lack of trust has seen excessive use of NDAs, design contracts and confidentiality agreement contracts in joint projects or with third party contractors. This lack of trust can be attributed to a number of factors, such as the competitive nature of the industry, and the need to protect IP and design documents. The list comprises of a number of justifications; however, it does provide significant scope for further research and investigation.

Sixth, the study's findings highlight a lack of component integration knowledge, particularly with OEMs. Although, recently there has been some effort to create and share knowledge through working groups, alliances, conferences and, collaborations. Most OEMs do not hold the technical knowledge about the components or cyber-solutions that they integrate into their architecture. These results could possibly be attributed to three explanations. First, the level of competition within the auto-domain has forced OEMs to outsource required solutions, while they (OEMs) focus their attention on increasing vehicle sales. Although OEMs have enjoyed an increase in vehicle sales, suppliers have benefited by gaining a vast amount of knowledge and expertise. Second, consistent with some of the responses provided by the participants, top managers view security as a design imperative that delays vehicles to market. This explanation could be one of the reasons some OEMs ignore secure development practices (Chapter 6). Third, the current structure of the automotive supply chain promotes competition and does not encourage the sharing of knowledge related to component integration. This lack of knowledge has led OEMs to over-rely on component suppliers for solutions, yet they do not know if the solutions being provided will address the challenges they are facing. The lack of integration knowledge particularly by OEMs also presents an interesting area for further research as to why component suppliers are emerging as the gatekeepers of component integration knowledge.

Seventh, the industry views cybersecurity as an after-thought that delays production and increases development costs, thus security is considered less important compared to sales and safety. This perception towards cybersecurity has resulted in the use of NDAs, design contracts and confidentiality agreements which limit the creation and sharing of knowledge of relevance for component integration processes. With vehicle manufacturers and component suppliers competing to bring the next technologically advanced product to market, this focus on sales and safety makes the industry very competitive and indicates a potentially interesting direction for future research.

9.3 Summary of the research

This research thesis aimed to investigate and analyse knowledge sharing in component integration processes within the automotive industry as a potential factor for improving the security of modern connected vehicles. In fulfilment of this aim, the research was structured around seven objectives. Informed by these objectives, the empirical investigation was designed utilising a multi-method research approach to investigate knowledge sharing in the integration of components for connected vehicles, and to inform the design and development of a knowledge sharing framework. The researcher believes that the framework developed in Chapter 7 has fulfilled both the immediate and underlying intent of the research. The following sections show how the research questions were answered.

> RQ-1: *How has the structure of the automotive supply chain been affected by the design, development, and manufacture of increasingly connected vehicles?*

The research aimed to understand the current structure of the automotive supply chain and the changes that have occurred as a result of the trend towards connectedness in vehicles. The literature review included academic, government and industry reports, to help identify transformations in the automotive supply chain (Chapter 2, sub-section 2.4.3). The changes to the automotive supply chain not only include ICT driven transformations, trends in component out-sourcing or technological developments; in addition, the supply chain has transformed from the traditional tiered structure to a network of multiple businesses and relationships (Schniederjans & Schniederjans 2015). New roles have emerged and have been fulfilled by organisations focused on supplying technical and software engineering skills (Loukas 2015, Manello & Calabrese 2018). Although the new supply chain structure provides the industry with many benefits such as component out-sourcing, reduced production costs etc. it does not encourage the sharing of knowledge in component design, manufacture, and integration. These findings are reported and discussed in detail in Chapters 2, 6 and 8.

> ***RQ-2****: What type of knowledge does the automotive sector rely on, and how is it shared amongst the different stakeholders involved in component design, development and integration?*

This research question was approached through an exploratory study involving the use of semi-structured face-to-face interviews and online surveys. The findings are outlined and discussed in Chapters 6 and 8 of this thesis. The study identified eleven approaches employed to disseminate knowledge by OEMs, a majority of these approaches are also utilised in inter-departmental knowledge sharing sessions (Chapter 6 section 6.2.1). The study's findings also highlight a total of eight knowledge sharing approaches employed by component manufacturers (Chapter 6 section 6.3.1), while four approaches are used by knowledge experts within the auto-domain. Overall, the approaches identified by the study used by all respondents to disseminate knowledge in component design, development and integration are working groups, joint projects, secondment, recruitment, knowledge sharing sessions, best practices and industry standards, and training sessions.

> ***RQ-3****: How is cybersecurity knowledge adopted and applied in component design and development processes?*

Similar to research question 2, the third research question was answered through an exploratory study involving the use of semi-structured face-to-face interviews and online surveys. The study's results on knowledge sharing approaches revealed that current approaches to share cyber-related knowledge related to component integration processes are insufficient, constrained and are at times mainly confined to inter-departmental sharing. This, in turn, affects how integration knowledge is adopted and applied to approaches and processes for securing connected vehicles. Chapter 6 outlines the challenges that affect the adoption and application of knowledge related to component integration processes in connected vehicle manufacture. The study's findings reveal some similar challenges such as competition and trust, experienced by both OEMs and component suppliers in sharing cyber-related knowledge associated with the integration of components for the connected vehicle.

RQ4: *What standards, best practices and guidelines exist in the automotive industry to inform knowledge sharing in connected vehicle manufacture?*

Standards and best practices are designed to assist manufactures, suppliers and developers to demonstrate compliance with the standard or practice, it is a belief that when a product or component follows the standard or practice, particular properties are present and associated threats have been considered. With the help of a literature review, government and industry reports, the study's findings highlight the absence of industry standards or best practices that are designed to encourage the sharing of knowledge in component integration processes. The study's findings revealed that available standards and best practices attempt to address cybersecurity challenges from a technical perspective, nonetheless, provided solutions are at times frequently fragmented or incomplete. Additionally, not all available best practices and standards are directly applicable to the automotive industry. Chapters 2 and 6 discuss available automotive standards, best practices and guidelines.

RQ-5: *How can component related knowledge be shared effectively between OEMs, the automotive supply chain, and amongst suppliers, for improved digital security of connected vehicles?*

The research synthesised relevant literature examined and interpreted the outcomes of the semi-structured interviews and questionnaires to provide a comprehensive foundation for the design and development of a knowledge sharing framework. The proposed conceptual framework which was developed to promote the sharing of knowledge in automotive component integration processes and to assist the automotive industry to overcome some of the limitations of existing techniques for knowledge sharing in the integration of components for connected vehicles is outlined and explained in Chapter 7 of this thesis. The framework which can be tailored to a company-specific context is supported by theory and, brings together the best practices established in this thesis through the detailed literature review and, the primary evidence from the semi-structured interviews and the online surveys. Figure 7.7 (Chapter 7, section 7.3), provides the complete grammatical representation of the revised conceptual framework.

The evaluation of the framework was achieved by presenting the framework to respondents employed by component suppliers, OEMs, and knowledge experts in the automotive sector. The researcher developed a survey and collected data from 10 respondents. To minimise the threat of reliability and validity, and to increase the chances of generalisability, the evaluation process included participants that were part of the data collection process and those that were not. Furthermore, the evaluation approach was interwoven with the concept of triangulation, a useful approach to ensure for rigour, validity, reliability and justification of qualitative research (Darawsheh 2014, Morse 2015, Noble & Smith 2015, and Silverman 2015). The respondents, who were from different domains and roles and, possessed different skillsets provided rich information for evaluation.

9.4 Summary of key contributions of the research

The study contributes to both theoretical and practical bodies of knowledge which include: 1) contributions in advancing theoretical and methodological underpinnings of automotive and knowledge sharing research; 2) contributions in uncovering limitations to the sharing of knowledge related to component integration processes, thus highlighting new promising leads for further research; and 3) contributions in the form of a conceptual framework, which has the potential to assist the industry to manufacture cyber-secure connected vehicles. The proposed framework could potentially be extended to autonomous vehicle manufacture, a potentially interesting direction for future research. These contributions are detailed below.

Contributions to the automotive industry

First, the study makes contributions to the automotive sector in the form of a conceptual knowledge sharing framework. The proposed framework was designed and developed on the back of information and feedback gathered from automotive knowledge experts, vehicle manufacturers, automotive component suppliers and, an extensive review of the literature. The proposed framework is designed to improve, extend and incorporate component integration knowledge sharing processes; if adopted by industry, the proposed framework has the potential to affect policy and standards within the automotive domain. In addition, the proposed framework provides an opportunity for guidance in the development of new knowledge sharing collaborations as the industry edges towards autonomous vehicle manufacturing, and the analysis of existing collaboration and knowledge sharing approaches.

Second, the research has addressed an area where very little has been done, but which requires urgent attention. Existing approaches to knowledge sharing have been studied to understand their applicability in the automotive component integration context. It has been found that existing approaches are not capable of addressing knowledge sharing challenges in the integration of digital components for connected vehicles. The research successfully challenges existing knowledge sharing frameworks and shows why these frameworks do not apply to the context in which this research was carried. The research demonstrated that whilst there are frameworks that can support knowledge sharing, there are none that specifically assist the automotive industry in supporting the sharing of knowledge related to component integration processes. The proposed framework which derives its strengths from knowledge sharing within all relevant segments of the organisation was evaluated by personnel close to the phenomena under investigation. The feedback from the evaluation process demonstrates that the framework has the potential for addressing knowledge sharing challenges, component integration challenges and addressing some of the weaknesses that are found in existing strategies.

Third, as revealed by the literature review, knowledge is one of the most strategically significant resources of a firm, knowledge sharing is a unique, valuable and stable source that is central to developing and maintaining a competitive edge. As the automotive industry steadily edges towards autonomy, the sharing of knowledge of relevance for component integration will be key in ensuring for the manufacture of safe and secure autonomous vehicles and the related infrastructure that will support theses appliances. The safety and security of the next generation of vehicles if left unchecked has the potential to devastate societies and disrupt lives. At the moment there is only speculation and ideas on how autonomous vehicles will be secured, this research assists in provoking thought on how knowledge sharing could be employed as a potential solution, or as a starting point in implementing the required security measures. Therefore, the study's proposed knowledge capture and sharing approaches contribute to the manufacturing processes of the next generation of vehicles.

Contributions to the cybersecurity domain

First, the study makes theoretical contributions to the cybersecurity domain. As revealed by the literature review, most research in automotive cybersecurity centres on providing technical architectures of security solutions. By integrating the literature on knowledge sharing with the emerging stream of research on automotive cybersecurity, the researcher developed theory, drawing links between a number of phenomena and concepts documented previously (Chapter 2). Furthermore, by extending the boundaries of enquiry into domains not directly involved with vehicle manufacturing such as consultancy and academia, the researcher was able to discover valuable streams of knowledge which would have possibly remained unexplored had the enquiry been limited to a sample of organisations directly involved in vehicle manufacturing.

Second, automotive cybersecurity is a new phenomenon, and existing solutions are mainly concentrated on providing technical solutions. This study adopts a different yet relevant path that investigates the sharing of knowledge as a means to assist the automotive industry to address cyber-related challenges. By doing so, the study contributes a knowledge sharing solution to the challenges introduced by cybersecurity. The proposed solution has the potential to be applied and employed to address cybersecurity challenges across a wider range of applications, sectors, domains and industries.

Contributions to the knowledge management discipline

The study makes contributions to knowledge management by outlining and exploring limitations to the sharing of knowledge in component integration in the automotive sector. A systematic approach to capture, structure, store, manage and disseminate knowledge required to inform component integration processes is proposed in Chapter 7. Additionally, the proposed solution aims to address challenges that do not favour the sharing of knowledge from automotive knowledge experts, vehicle manufacturers, and automotive component suppliers. These stakeholders help to shape policy, inform best practices, create standards and regulations, and conduct training in the field of automotive cybersecurity. Thus, the study has shown that potential risks inherent in cyber-vulnerable connected or autonomous vehicles will require a unified industrial effort to provide solutions. This supports the argument for the study for knowledge sharing, not only in the automotive industry but also in other industries where computing technologies have transformed manufacturing processes and introduced cyber-related threats. This contribution to knowledge management does not only assist with informing management decisions, promote innovation and, increase production but also paves the way for further theoretical developments.

9.5 Limitations of the research

Although the study has achieved some useful results, the research has certain limitations that need to be taken into account when considering the research and its contributions.

1. *Limitation of interaction between researcher and study participants*

   The current supply chain structure of the automotive industry is designed to promote competition, increase product innovation, reduce costs and introduce new design opportunities. This structural design has resulted in a delocalised supply chain whereby vehicle manufacturers and component suppliers have sought refuge in countries that offer lower production costs among other benefits. However, the design, development and production of modern vehicles (AVs and CVs) is, on the one hand, affected by a desire for strong and often elusive cooperative OEM-supplier relationships, and, on the other, security from cyber-threats demands an effective sharing of component integration knowledge between vehicle manufacturers and component suppliers as well as between suppliers themselves. As revealed in Chapter 2 and 6, this structure compounds the challenge of knowledge sharing and the creation of component integration knowledge sharing approaches. Additionally, the structure introduced challenges to the study's data collection process. This limitation imposed by the supply chain structure, together with the geographical location of participants affected the research's timeframe, the number of face-to-face interviews completed, the number of respondents contacted, and the number of survey responses received.

2. *The practicalities of a knowledge sharing method implementation*

Knowledge sharing is best studied by observing the people affected by the phenomenon within a real-life context. To achieve this, the researcher needed to gain access to a wide range of sources of evidence that included company documents and artefacts and to conduct interviews while observing existing knowledge sharing approaches. The structure of the automotive supply chain, the geographical location of the researcher, coupled with the secretive nature of the industry; a result of competition and a lack of trust, imposed challenges to the study's data collection process and evaluation activity.

3. *Lack of personnel with the required skillset*

Another challenge revealed by the study was that the industry has a major shortage of people with the required skillset and knowledge. This limitation was evident in the data collection phase, whereby the researcher had pre-arranged meetings cancelled because the participant felt they were not qualified to hold discussions about the phenomenon under investigation. Some organisations that the researcher reached out to, did not have a team or personnel dedicated to automotive cybersecurity, in particular, challenges that result from insecure component integration processes. Dark et al. (2015) and Axelrod et al. (2014) attribute the lack of such knowledge to academic institutions and state that engineering programmes and security programmes are taught in different faculties and advocate for these programmes to be taught together. Therefore, the lack of component integration knowledge creation and sharing approaches within the industry can partly be attributed to the shortage of people with the required skillset. The automotive industry requires personnel with skills, knowledge and capabilities that permit the creation and sharing of knowledge in component design, manufacture and integration to potentially assist with mitigating cyber-related threats in connected vehicle manufacture. To overcome this limitation, the study employed semi-structured face-to-face interviews and surveys with the people close to the phenomena under investigation.

4. *Perception towards cybersecurity*

   A major limitation of this study is the perception towards cybersecurity in the automotive industry which has resulted in the use of NDAs, design contracts and confidentiality agreements. Due to the use of such gagging agreements, the study suffered from interview rejections and cancellations with respondents openly stating that they are not permitted by their employer to engage in cyber-related discussions. Furthermore, NDAs, design contracts and confidentiality agreements contributed to the low response rates that affected the study's online surveys (Chapter 4, 5 and 6). Although a security culture is not yet fully embedded in the auto-domain, the study was successful in collecting valuable and relevant data to assist with the development of a conceptual framework.

The limitations of this study have been systematically identified and, where possible, mitigation measures have been applied to reduce the effect of the limitations on the research findings and contributions. It is considered that they do not detract from the overall interpretation and significance of the findings but may serve as future research avenues.

9.6 Recommendations and directions for future research

The researcher has identified interesting and important research avenues that can be pursued based on the work outlined in this thesis. The following areas are highlighted for further research:

1. *Confirmation of the research findings*

   The research was conducted using data from individuals employed in different sections of the automotive industry. For future research, multiple organisations, possibly from different countries, could be used to test the framework for its perceived value, usability and limitations, so as to explore where other knowledge factors exist which were not identified within this research.

2. *The design and development of an assurance framework*

   Further research could consider the design and development of an assurance framework that defines how an organisation incorporates component integration knowledge sharing into its component manufacturing processes. As stated by some of the study's participants, currently there are no measures in place to check whether integration processes are captured and shared between relevant stakeholders. The potential assurance framework should also define how component integration knowledge is shared between all stakeholders, and the results should take the form of an assessment report, which contains the organisation's component integration knowledge rating. The rating could be extended to rate the organisation on component integration knowledge sharing approaches. The results must be shared with all relevant stakeholders in the automotive industry, and government departments tasked with ensuring vehicle security. The assurance framework will aim to provide meaningful additional assurance over and above that provided by the minimum mandatory regulatory requirements available today.

3. *The creation of regulation and legal frameworks to promote component integration knowledge sharing.*

   Future research could encourage the development of industry standards and best practices that address cybersecurity challenges, in particular, challenges born out of insecure component integration approaches is an interesting avenue for further research. The study's results highlight the lack of standards that address knowledge sharing and/or automotive cybersecurity, however, even though the study attempts to outline the pros and cons of available standards and best practices on knowledge sharing, the design and development of standards specific for automotive cybersecurity is outside of this study's focus, it is important that this is addressed by further research since currently available standards such as the SAEJ3061 and ISO 26262 are not directly applicable to automotive cybersecurity. Furthermore, with autonomous vehicles on the horizon, the automotive industry is in great need of standards and best practices that are dedicated to addressing automotive cybersecurity challenges. The standards will need to be aligned with the eagerly anticipated ISO/SAE21434 standard which is expected to be published in 2021.

4. *Regulation and legislation for promoting knowledge sharing*

   The inclusion of complex automated technology in vehicles is becoming an increasing concern and, it is important and essential that all relevant stakeholders concerned with vehicle manufacturing are provided with regulation and legislation that support the manufacturing of cyber-secure vehicles and vehicle components. The creation of regulation and legislation that provides a framework seeking to promote not only trust, legal and ethical behaviour, but to promote and encourage the sharing of cyber-related information i.e. component integration knowledge, is an interesting and important research avenue. The threats posed by automotive cybersecurity have the potential to stifle innovation and destroy economies. Governments and policymakers can benefit from research that aims to create regulation and legal frameworks that promote the sharing of component integration knowledge. Furthermore, regulation and legislation that address component integration knowledge sharing should not be confined to vehicle manufacturing alone, but it must extend to infrastructures that support, communicate and enable connected and autonomous driving.

9.7 Concluding remarks

Overall, this thesis revealed that knowledge sharing in component integration can be used to mitigate cybersecurity-related vulnerabilities in connected vehicles. The research which has spanned over four years has involved leading vehicle manufacturing organisations, leading global suppliers of vehicle components and technologies, and automotive knowledge experts with vast amounts of experience and knowledge. The study contributed significantly to the body of knowledge available in both the knowledge sharing domain and the cybersecurity domain. Additionally, the study has put the spotlight on the automotive industry to create a security culture by employing secure development practices with consideration for cybersecurity in the integration of components for connected vehicles. Furthermore, there have been specific benefits for all stakeholders, derived from their relationship with the PhD research reported such as access to the framework and its knowledge sharing processes.

For the Faculty of Business and Law (FBL), in particular the Centre for Business in Society (CBiS) at Coventry University, this has been an innovative project which has successfully uncovered an area with potential to open new avenues for research and collaboration with the automotive industry and other industries where computing technology have introduced cybersecurity challenges. For the automotive industry, the project which has the potential to affect policy, standards and training methods, has successfully highlighted the need for component integration knowledge sharing in vehicle manufacturing.

This research project has provided an exciting personal and professional opportunity for the researcher to explore and enhance his skills. He received important support from the Faculty of Business and Law, in particular the Centre for Business in Society (CBiS), and the University's Doctoral College to attend a summer school hosted by Bayerische Motoren Werke (BMW) in 2015, an international doctoral school in South Africa in support of the CARNiVAL project in 2016, and the 26th Gerpisa colloquium in Sao Paulo, Brazil in 2018 where he presented a conference paper titled "Supplier Delocalization: A Threat to Automotive Cybersecurity Knowledge sharing?". In 2019, the researcher attended the Association for Computing Machinery (ACM) Computer Science in Cars Symposium (CSCS2019), in Kaiserslautern, Germany where he presented a conference paper titled "Context-aware Anomaly Detector for Monitoring Cyber Attacks on Automotive CAN Bus". Due to this research and work conducted on knowledge sharing in the automotive industry, the researcher has begun a new phase in his career. He is now employed as a cybersecurity research scientist by a world-class automotive engineering and development consultancy organisation that provides product engineering, research, testing, certification services, and information to the automotive sector.

REFERENCES

Abdelhamid, S., Hassanein, H. S., and Takahara, G. (2015) 'Vehicle as a Resource (VaaR)'. *IEEE Network* 29 (1), 12-17.

AF Ragab, M., and Arisha, A. (2013) 'Knowledge Management and Measurement: A Critical Review'. *Journal of Knowledge Management,* Vol 17 (6), 873-901.

Akhavan, P., Ramezan, M., and Yazdi Moghaddam, J. (2013) 'Examining the Role of Ethics in Knowledge Management Process: Case Study: An Industrial Organization'. *Journal of Knowledge-Based Innovation in China* 5 (2), 129-145.

Al Saifi, S. A. (2015) 'Positioning Organisational Culture in Knowledge Management Research'. *Journal of Knowledge Management* 19 (2), 164-189.

Alguezaui, S., and Filieri, R. (2014) 'A Knowledge-Based View of the Extending Enterprise for Enhancing a Collaborative Innovation Advantage'. *International Journal of Agile Systems and Management* 7 (2), 116-131.

Allied Market Research (Global Opportunity Analysis and Industry Forecast, 2018 - 2025) *Connected Car Market Value by Technology: Global Opportunity Analysis and Industry Forecast, 2018 - 2025* [online] available from <https://www.alliedmarketresearch.com/connected-car-market> [Accessed March 2018].

Ambe, I. M., and Badenhorst-Weiss, J. A. (2011) 'An Automotive Supply Chain Model for a Demand-Driven Environment'. *Journal of Transport and Supply Chain Management* 5 (1), 1-22.

Ambe, I. M., and Badenhorst-Weiss, J. A. (2010) 'Strategic Supply Chain Framework for the Automotive Industry.Afr.J Bus. Manage. 4(10):2110-2120.

Amin, M., and Tariq, Z. (2015) 'Securing the Car: How Intrusive Manufacturer-Supplier Approaches Can Reduce Cybersecurity Vulnerabilities'. *Technology Innovation Management Review* 5 (1), p.21.

Araya, D., and Peters, M. A. (2010) *Education in the Creative Economy: Knowledge and Learning in the Age of Innovation*. Peter Lang.

Arduin, P.E., Negre, E. and Rosenthal-Sabroux, C (eds.) (2013) Towards a new tacit knowledge-based approach for decision process. *First international conference on Knowledge Management*, Information and Knowledge Systems (KMIKS 2013), Hammamet, Tunisia.

Argote, L. (2012) *Organizational Learning: Creating, Retaining and Transferring Knowledge*. Springer Science & Business Media, New York, NY.

Aris, I. B., Sahbusdin, R. K. Z., and Amin, A. F. M. (eds.) (2015) *Control Conference (ASCC), 2015 10th Asian*. 'Impacts of IoT and Big Data to Automotive Industry': IEEE.

Arnett, D. B., and Wittmann, C. M. (2014) 'Improving Marketing Success: The Role of Tacit Knowledge Exchange between Sales and Marketing'. *Journal of Business Research* 67 (3), 324-331.

Assante, M. J., and Tobey, D. H. (2011) 'Enhancing the Cybersecurity Workforce'. *IT Professional Magazine* 13 (1), 12.

Auto-ISAC (2016) *Automotive Information Sharing and Analysis Center Homepage* [online] available from <https://www.automotiveisac.com> [Accessed March 2018].

Axelrod, C.W. (2014) Bridging the Safety-security Software Gap. *WIT Transactions on Information and Communication Technologies*, *47*, pp.479-486.

Bacchiocchi, E., Florio, M., and Giunta, A. (2014) 'Internationalization and Industrial Districts: Evidence from the Italian Automotive Supply Chain'. *International Review of Applied Economics* 28 (1), 1-21.

Badampudi, D., Wohlin, C., and Petersen, K. (2016) 'Software Component Decision-Making: In-House, OSS, COTS or Outsourcing-A Systematic Literature Review'. *Journal of Systems and Software* 121, 105-124.

Baheti, R., and Gill, H. (2011) 'Cyber-Physical Systems'. *The Impact of Control Technology* 12, 161-166.

Baker, S. E., Edwards, R., and Doidge, M. (2012) 'How Many Qualitative Interviews is enough? Expert Voices and Early Career Reflections on Sampling and Cases in Qualitative Research, National Centre for Research Methods. Economic and Social Research Council (ESRC), Swindon, UK.

Barzilay, M. (2013) 'A Simple Definition of Cybersecurity'. disponível em: http://www.isaca.org/KnowledgeCenter/Blog/Lists/Posts/Post.aspx?ID=296, consultado a 23 de Outubro de 2015.

Bashouri, J., and Duncan, G. W. (2014) 'Communities of Practice: Linking Knowledge Management and Strategy in Creative Firms'. *Journal of Business Strategy* 35 (6), 49-57.

Baylon, C. (2014) '*Challenges at the intersection of cyber security and space security: country and international institution perspectives*.' Chatham House, The Royal Institute of International Affairs.

Bayuk, J. L., Healey, J., Rohmeyer, P., Sachs, M. H., Schmidt, J., and Weiss, J. (2012) *Cyber Security Policy Guidebook*. Wiley Online Library.

Bazeley, P. (2013) *Qualitative Data Analysis: Practical Strategies*. Sage Publications Limited, Los Angeles.

Bell, E., Bryman, A., and Harley, B. (2018) *Business Research Methods*. Oxford University Press.

Bernard, H. R., Wutich, A., and Ryan, G. W. (2016) *Analyzing Qualitative Data: Systematic Approaches*. Sage Publications, Washington.

Birch, J., Rivett, R., Habli, I., Bradshaw, B., Botham, J., Higham, D., Jesty, P., Monkhouse, H., and Palin, R. (eds.) (2013) *International Conference on Computer Safety, Reliability, and Security*. 'Safety Cases and their Role in ISO 26262 Functional Safety Assessment': Springer

Blair, J., Czaja, R. F., and Blair, E. A. (2013) *Designing Surveys: A Guide to Decisions and Procedures*. Sage Publications, Los Angeles, USA.

Blau, P. (2017) *Exchange and Power in Social Life*. Routledge, Taylor and Francis Group, London.

Blome, C., Schoenherr, T., and Eckstein, D. (2014) The Impact of Knowledge Transfer and Complexity on Supply Chain Flexibility: A Knowledge-Based View'. *International Journal of Production Economics* 147, 307-316.

Bogers, M. (2011) The Open Innovation Paradox: Knowledge Sharing and Protection in R&D Collaborations'. *European Journal of Innovation Management* 14 (1), 93-117.

Bonjour, E., Deniaud, S., and Micaëlli, J. (2013) 'A Method for Jointly Drawing Up the Functional and Design Architectures of Complex Systems during the Preliminary System-Definition Phase'. *Journal of Engineering Design* 24 (4), 305-319.

Brannen, J. (2017) *Mixing Methods: Qualitative and Quantitative Research*. Routledge, Taylor and Francis Group, London.

Brinkmann, S. (2014) 'Interview'. in *Encyclopedia of Critical Psychology*. ed. by Anon: Springer, 1008-1010.

Brown, S., Gommers, J., and Serrano, O. (eds.) (2015) *Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security*. 'From Cyber Security Information Sharing to Threat Management': ACM.

Broy, M., Kirstan, S., Krcmar, H., and Schätz, B. (2014) 'What is the Benefit of a Model-Based Design of Embedded Software Systems in the Car Industry?'. in *Software Design and Development: Concepts, Methodologies, Tools, and Applications*. ed. by Anon: IGI Global, 310-334.

Bryans, J. W. (2017) The Internet of Automotive Things: Vulnerabilities, Risks and Policy Implications'. *Journal of Cyber Policy* 2 (2), 185-194.

Bryman, A. (2017) 'Quantitative and Qualitative Research: Further Reflections on their Integration'. in *Mixing Methods: Qualitative and Quantitative Research*. ed. by Anon: Routledge, 57-78.

Bryman, A., (2016) *Social Research Methods*. Oxford University Press, USA.

Bryman, A., (2015) *Social Research Methods*. Oxford University Press, USA.

Bryman, A., and Bell, E. (2015) *Business Research Methods*. Oxford University Press, USA.

Bulsara, C. (2015) 'Using a Mixed Methods Approach to Enhance and Validate Your Research'. *Brightwater Group Research Centre*, 1-82.

Burgess, J. P. (2010) *Handbook of New Security Studies*. Routledge, Taylor and Francis Group, London.

Burgess, R. L., and Huston, T. L. (2013) *Social Exchange in Developing Relationships*. Elsevier.

Cabigiosu, A., Zirpoli, F., and Camuffo, A. (2013) 'Modularity, Interfaces Definition and the Integration of External Sources of Innovation in the Automotive Industry'. *Research Policy* 42 (3), 662-675.

Caldwell, T. (2013) 'Plugging the Cyber-Security Skills Gap'. *Computer Fraud & Security* 2013 (7), 5-10.

Cao, Y. and Xiang, Y. (2012) 'The Impact of Knowledge Governance on Knowledge Sharing'. *Management Decision* 50 (4), 591-610.

Carmeli, A., Gelbard, R., and Reiter-Palmon, R. (2013) 'Leadership, Creative problem-solving Capacity, and Creative Performance: The Importance of Knowledge Sharing'. *Human Resource Management* 52 (1), 95-121.

Cârstea, V. (2013) 'Delocalization-the Automotive Industry's Answer to Cost Reduction'. *Romanian Economic and Business Review*, 180.

Casimir, G., Lee, K., and Loon, M. (2012) 'Knowledge Sharing: Influences of Trust, Commitment and Cost'. *Journal of Knowledge Management* 16 (5), 740-753.

Cebula, J.L., and Young, L.R. (2010) *A taxonomy of operational cyber security risks* (No. CMU/SEI-2010-TN-028). CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST.

Charmaz, K. (2014) *Constructing Grounded Theory*. Sage Publications, London.

Cheah, M., Shaikh, S. A., Haas, O., and Ruddle, A. (2017) 'Towards a Systematic Security Evaluation of the Automotive Bluetooth Interface'. *Vehicular Communications* 9, 8-18.

Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S., Koscher, K., Czeskis, A., Roesner, F., and Kohno, T. (eds.) (2011) *USENIX Security Symposium (Vol. 4)*. 'Comprehensive Experimental Analyses of Automotive Attack Surfaces. San Francisco.

Chiarini, A., and Vagnoni, E. (2015) 'World-Class Manufacturing by Fiat. Comparison with Toyota Production System from a Strategic Management, Management Accounting, Operations Management and Performance Measurement Dimension'. *International Journal of Production Research* 53 (2), 590-606.

Choucri, N., Madnick, S., and Koepke, P. (2016) 'Institutions for Cyber Security: International Responses and Data Sharing Initiatives'. *Cambridge, MA: Massachusetts Institute of Technology*

Christensen, L. B., Johnson, B., Turner, L. A., and Christensen, L. B. (2011) 'Research Methods, Design, and Analysis', Pearson UK.

Christopher, M. (2016) *Logistics & Supply Chain Management*. Pearson UK.

Chung, T. W. (2016) 'A Study on Logistics Cluster Competitiveness among Asia Main Countries using the Porter's Diamond Model'. *The Asian Journal of Shipping and Logistics* 32 (4), 257-264.

Ciravegna, L., Romano, P., and Pilkington, A. (2013) 'Outsourcing Practices in Automotive Supply Networks: An Exploratory Study of Full-Service Vehicle Suppliers'. *International Journal of Production Research* 51 (8), 2478-2490.

Clark, D., Berson, T., and Lin, H. (2014) *At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues*. Washington DC: National Academics Press.

Clarke, R. A., and Knake, R. (2012) 'Cyber War: The Next Threat to National Security and what to do about it, Reprint Edition. Ed'. *Ecco, New York.*

Collins, K. F., Muthusamy, S. K., and Carr, A. (2015) 'Toyota Production System for Healthcare Organisations: Prospects and Implementation Challenges'. *Total Quality Management & Business Excellence* 26 (7-8), 905-918.

Colquitt, J., Dowsett, D., Gami, A., Equities, I. F., Jaysane-Darr, E., Partner, I. P. C., Manley, C., Equity, F., Shad, R., and Income, I. F. (2017) 'Driverless Cars: How Innovation Paves the Road to Investment Opportunity'. The Invesco White Paper.

Connelly, C. E., Zweig, D., Webster, J., and Trougakos, J. P. (2012) 'Knowledge Hiding in Organizations'. *Journal of Organizational Behavior* 33 (1), 64-88.

Cook, K. S., Cheshire, C., Rice, E. R., and Nakagawa, S. (2013) 'Social Exchange Theory'. *Handbook of Social Psychology*. ed. by Anon: Springer, 61-88.

Corbin, J., Strauss, A., and Strauss, A. L. (2014) *Basics of Qualitative Research*. Sage, Washington D.C.

Cornish, P., Livingstone, D., Clemente, D., and Yorke, C. (2010) *On Cyber Warfare*.: Chatham House London.

Corredoira, R. A., and McDermott, G. A. (2014) 'Adaptation, Bridging and Firm Upgrading: How Non-Market Institutions and MNCs Facilitate Knowledge Recombination in Emerging Markets'. *Journal of International Business Studies* 45 (6), 699-722.

Cousins, P. D., Lawson, B., Petersen, K. J., and Handfield, R. B. (2011) 'Breakthrough Scanning, Supplier Knowledge Exchange, and New Product Development Performance'. *Journal of Product Innovation Management* 28 (6), 930-942.

Craigen, D., Diakun-Thibault, N., and Purse, R. (2014) 'Defining Cybersecurity'. *Technology Innovation Management Review* 4 (10): 13-21.

Creswell, J. W., and Clark, V. L. P. (2017) *Designing and Conducting Mixed Methods Research*. Sage Publications London.

Creswell, J. W. (2013) *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. Sage Publications London.

Creswell, J. W., Klassen, A. C., Plano Clark, V. L., and Smith, K. C. (2011) 'Best Practices for Mixed Methods Research in the Health Sciences'. *Bethesda (Maryland): National Institutes of Health* 2013, 541-545.

Dalkir, K. (2013) *Knowledge Management in Theory and Practice*. Elsevier Butterworth-Heinemann., Burlington.

Danese, P., and Filippini, R. (2013) 'Direct and Mediated Effects of Product Modularity on Development Time and Product Performance'. *IEEE Transactions on Engineering Management* 60 (2), 260-271.

Darawsheh, W. (2014) 'Reflexivity in Research: Promoting Rigour, Reliability and Validity in Qualitative Research'. *International Journal of Therapy and Rehabilitation* 21 (12), 560-568.

Dardick, G. S. (2010) Cyber forensics assurance. *In 8th Australian Digital Forensics Conference* (pp. 57–64). School of Computer and Information Science, Edith Cowan University, Perth, Western Australia

Dark, M., Bishop, M., Linger, R., and Goldrich, L. (2015) *Realism in Teaching Cybersecurity Research: The Agile Research Process*. Springer New York LLC.

Deibert, R. (2012) 'Cybersecurity: The New Frontier'. *Foreign Policy*, Topic 4: 45-58.

Denzin, N. K. (2012). Triangulation 2.0. *Journal of Mixed Methods Research*, 6(2), 80-88. doi:10.1177/1558689812437186.

DeWalt, K. M., and DeWalt, B. R. (2011) *Participant Observation: A Guide for Fieldworkers*. Rowman Altamira.

Di Gangi, P. M., Wasko, M. M., and Tang, X. (2012) 'Would You Share? Examining Knowledge Type and Communication Channel for Knowledge Sharing within and Across the Organizational Boundary'. *International Journal of Knowledge Management (IJKM)* 8 (1), 1-21.

Di Natale, M., and Sangiovanni-Vincentelli, A. L. (2010) 'Moving from Federated to Integrated Architectures in Automotive: The Role of Standards, Methods and Tools'. *Proceedings of the IEEE* 98 (4), 603-620.

DiCicco-Bloom, B., and DiCicco-Bloom, B. (2016) 'The Benefits of Respectful Interactions: Fluid Alliancing and inter-occupational Information Sharing in Primary Care'. *Sociology of Health & Illness* 38 (6), 965-979.

Diewald, S., Möller, A., Roalter, L., and Kranz, M. (eds.) (2012) *Konferenz Mensch & Computer: 09/09/2012-12/09/2012*. 'DriveAssist: A V2X-Based Driver Assistance System for Android': Oldenburg Wissenschaftsverlag.

Doherty, N. F., Champion, D., and Wang, L. (2010) 'A Holistic Approach to Understanding the Changing Nature of Organisational Structure'. *Information Technology & People* 23 (2), 116-135.

Doody, O., and Noonan, M. (2013) 'Preparing and Conducting Interviews to Collect Data'. *Nurse Researcher* 20 (5), 28-32.

Ďurišová, J. (2011) 'Knowledge Life Cycle and its Application in Automotive Industry'. *Problems of Management in the 21st Century* 2, 45-53.

Durst, S., and Runar Edvardsson, I. (2012) Knowledge management in SMEs: a literature review. *Journal of Knowledge Management*, *16*(6), pp.879-903.

DW Rechberg, I., and Syed, J. (2014) 'Appropriation or Participation of the Individual in Knowledge Management'. *Management Decision* 52 (3), 426-445.

Dworkin, S. L. (2012). *Sample Size Policy for Qualitative Studies using in-Depth Interviews: Springer, 1319-1320.*

Eaves, S. (2014) 'Middle Management Knowledge by Possession and Position: A Panoptic Examination of Individual Knowledge Sharing Influences'. *The Electronic Journal of Knowledge Management* 12 (1), 67-82.

Edmondson, A. C. (2012) *Teaming: How Organizations Learn, Innovate, and Compete in the Knowledge Economy*. John Wiley & Sons.

Eisenberger, R., Karagonlar, G., Stinglhamber, F., Neves, P., Becker, T. E., Gonzalez-Morales, M. G., and Steiger-Mueller, M. (2010) 'Leader-member Exchange and Affective Organizational Commitment: The Contribution of Supervisor's Organizational Embodiment. *Journal of Applied Psychology* 95 (6), 1085.

Eizenberg, E., and Jabareen, Y. (2017) 'Social Sustainability: A New Conceptual Framework'. *Sustainability* 9 (1), 68.

Elo, S., Kääriäinen, M., Kanste, O., Pölkki, T., Utriainen, K., and Kyngäs, H. (2014) 'Qualitative Content Analysis: A Focus on Trustworthiness'. *SAGE Open* 4 (1), 2158244014522633.

Erdem, I., Kihlman, H., and Andersson, A. (eds.) (2015) *23rd International Conference for Production Research, ICPR 2015, Manila, Philippines, 2-6 August 2015*. 'Development of Affordable Reconfigurable Tooling in Car Manufacturing Cells–A Case Study'.

Erickson, F. (2012) 'Qualitative Research Methods for Science Education'. in *Second International Handbook of Science Education*. ed. by Anon: Springer, 1451-1469.

Ericson, C. A. (2015) *Hazard Analysis Techniques for System Safety*. John Wiley & Sons.

Esper, T. L., Ellinger, A. E., Stank, T. P., Flint, D. J., and Moon, M. (2010) 'Demand and Supply Integration: A Conceptual Framework of Value Creation through Knowledge Management'. *Journal of the Academy of Marketing Science* 38 (1), 5-18.

Etikan, I., Musa, S. A., and Alkassim, R. S. (2016) 'Comparison of Convenience Sampling and Purposive Sampling'. *American Journal of Theoretical and Applied Statistics* 5 (1), 1-4.

Evans, M., and Ali, N. (eds.) (2013) *International Conference on Intellectual Capital, Knowledge Management and Organisational Learning ICICKM 2013–Conference Proceedings*. 'Bridging Knowledge Management Life Cycle Theory and Practice'.

Falessi, N., Gavrila, R., Klejnstrup, M. R., and Moulinos, K. (2012) 'National Cyber Security Strategies: Practical Guide on Development and Execution'. *European Network and Information Security Agency (ENISA) Publication.*

Fan, W., and Yan, Z. (2010) 'Factors Affecting Response Rates of the Web Survey: A Systematic Review'. *Computers in Human Behavior* 26 (2), 132-139.

Faraj, S., Jarvenpaa, S. L., and Majchrzak, A. (2011) 'Knowledge Collaboration in Online Communities'. *Organization Science* 22 (5), 1224-1239.

Farcas, C., Farcas, E., Krueger, I. H., and Menarini, M. (2010) 'Addressing the Integration Challenge for Avionics and Automotive systems—From Components to Rich Services'. *Proceedings of the IEEE* 98 (4), 562-583.

Farwell, J. P. and Rohozinski, R. (2012) 'The New Reality of Cyber War'. *Survival* 54 (4), 107-120.

Ferber, M. P. and Harris, T. M. (2013) 'Critical Realism and Emergence in a Scaled Geography of Religion'. *Journal of Critical Realism* 12 (2), 183-201.

Fernández Fernández, J. L., and Sanjuán, A. B. (2010) 'The Presence of Business Ethics and CSR in the Higher Education Curricula for Executives: The Case of Spain'. *Journal of Business Ethics Education* 7, 25-38.

Fetters, M. D., Curry, L. A., and Creswell, J. W. (2013) 'Achieving Integration in Mixed Methods designs—principles and Practices'. *Health Services Research* 48 (6pt2), 2134-2156.

Filippini, R., and Forza, C. (2016) 'The Impact of the just-in-Time Approach on Production System Performance: A Survey of Italian Industry. A Review and Outlook'. in *A Journey through Manufacturing and Supply Chain Strategy Research*. ed. by Anon: Springer, 19-39.

Fink, A. (2015) *How to Conduct Surveys: A Step-by-Step Guide*. Sage Publications, London.

Fischer, E. A. (2014) Cybersecurity Issues and Challenges: In Brief, Available at: https://fas.org/sgp/crs/misc/R43831.pdf.

Flick, U. (2018) *Designing Qualitative Research*. Sage Publications, London.

Francis, J. J., Johnston, M., Robertson, C., Glidewell, L., Entwistle, V., Eccles, M. P., and Grimshaw, J. M. (2010) 'What is an Adequate Sample Size? Operationalising Data Saturation for Theory-Based Interview Studies'. *Psychology and Health* 25 (10), 1229-1245.

Fredrich, V., and Pesch, R. (2017). Partner selection and joint knowledge creation for business model innovation in alliances. In *Academy of Management Proceedings* (Vol. 2017, No. 1, p. 16171). Briarcliff Manor, NY 10510: Academy of Management.

Friend, J., and Caruthers, L. (2015) 'Transforming the School Reform Agenda: A Framework for Including Student Voice in Urban School Renewal.' *Journal of Urban Learning, Teaching, and Research* 11, 14-25.

Fuchs, C., and Schreier, M. (2011) 'Customer Empowerment in New Product Development'. *Journal of Product Innovation Management* 28 (1), 17-32.

Galletta, A. (2013) *Mastering the Semi-Structured Interview and Beyond: From Research Design to Analysis and Publication*. NYU Press.

Ganin, A. A., Quach, P., Panwar, M., Collier, Z. A., Keisler, J. M., Marchese, D., and Linkov, I. (2017) 'Multicriteria Decision Framework for Cybersecurity Risk Assessment and Management'. *Risk Analysis.*

Garcia-Perez, A. (2019) *Financial Integrity and Cybersecurity in Europe. Application Submitted to the European Commission in Response to the Call H2020-SU-DS-2018.*

Gasik, S. (2011) 'A Model of Project Knowledge Management'. *Project Management Journal* 42 (3), 23-44.

Gaur, A., and Kumar, M. (2018). A systematic approach to conducting review studies: An assessment of content analysis in 25 years of IB research. *Journal of World Business*, *53*(2), pp.280-289.

Gera, R. (2012) 'Bridging the Gap in Knowledge Transfer between Academia and Practitioners'. *International Journal of Educational Management* 26 (3), 252-273.

Gerla, M., Lee, E.K., Pau, G. and Lee, U. (2014) March. Internet of vehicles: From intelligent grid to autonomous cars and vehicular clouds. In *2014 IEEE world forum on internet of things (WF-IoT)* (pp. 241-246). IEEE.

Ghobadi, S., and D'Ambra, J. (2012) 'Knowledge Sharing in Cross-Functional Teams: A Coopetitive Model'. *Journal of Knowledge Management* 16 (2), 285-301.

Gholz, E., James, A.D., and Speller, T.H. (2018) The second face of systems integration: An empirical analysis of supply chains to complex product systems. *Research Policy*, *47*(8), pp.1478-1494.

Gibbs, J. L., Rozaidi, N. A., and Eisenberg, J. (2013) 'Overcoming the "ideology of Openness": Probing the Affordances of Social Media for Organizational Knowledge Sharing'. *Journal of Computer-Mediated Communication* 19 (1), 102-120.

Gilbert, L. S., Jackson, K., and di Gregorio, S. (2014) 'Tools for Analyzing Qualitative Data: The History and Relevance of Qualitative Data Analysis Software'. in *Handbook of Research on Educational Communications and Technology*. ed. by Anon: Springer, 221-236.

Giles, K., and Hagestad, W. (eds.) (2013) *2013 5th International Conference on Cyber Conflict (CYCON 2013)*. 'Divided by a Common Language: Cyber Definitions in Chinese, Russian and English': IEEE.

Glaser, B. G., and Strauss, A. L. (2017) *Discovery of Grounded Theory: Strategies for Qualitative Research*. Routledge, London.

Gobbens, R. J., Luijkx, K. G., Wijnen-Sponselee, M. T., and Schols, J. M. (2010) 'In Search of an Integral Conceptual Definition of Frailty: Opinions of Experts'. *Journal of the American Medical Directors Association* 11 (5), 338-343.

Goffin, K., and Koners, U. (2011) 'Tacit Knowledge, Lessons Learnt, and New Product Development'. *Journal of Product Innovation Management* 28 (2), 300-318.

Golinelli, G. M., Pastore, A., Gatti, M., Massaroni, E., and Vagnani, G. (2011) 'The Firm as a Viable System: Managing Inter-Organisational Relationships'. *Sinergie Italian Journal of Management* (58), 65-98.

Goodyear, M., Goerdel, H., Portillo, S., and Williams, L. (2010) 'Cybersecurity Management in the States: The Emerging Role of Chief Information Security Officers'. *Available at SSRN 2187412*

Greenhalgh, T. (2010) 'What is this Knowledge that we seek to "Exchange"?'. *The Milbank Quarterly* 88 (4), 492-499.

Grewe, A., Knieke, C., Körner, M., Rausch, A., Schindler, M., Strasser, A., and Vogel, M. (2017) 'Automotive Software Systems Evolution: Planning and Evolving Product Line Architectures'. *Special Track: Managed Adaptive Automotive Product Line Development (MAAPL), Along with ADAPTIVE*, 53-62.

Grobler, M., Van Vuuren, J., and Zaaiman, J. (eds.) (2011) *Proceedings of the 10th European Conference on Information Warfare and Security: The Institute of Cybernetics at the Tallinn University of Technology*. 'Evaluating Cyber Security Awareness in South Africa': Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia.

Guest, G., MacQueen, K. M., and Namey, E. E. (2011) *Applied Thematic Analysis*. Sage Publications, London.

Gursoy, D., Chi, C. G., and Dyer, P. (2010) 'Locals' Attitudes Toward Mass and Alternative Tourism: The Case of Sunshine Coast, Australia'. *Journal of Travel Research* 49 (3), 381-394.

Gutierrez, A. P., Candela, L. L., and Carver, L. (2012) 'The Structural Relationships between Organizational Commitment, Global Job Satisfaction, Developmental Experiences, Work Values, Organizational Support, and person-organization fit among nursing faculty'. *Journal of Advanced Nursing* 68 (7), 1601-1614.

Hammersley, M. (2017) 'Deconstructing the Qualitative-Quantitative Divide 1'. in *Mixing Methods: Qualitative and Quantitative Research*. ed. by Anon: Routledge, 39-55.

Harman, G. (2015) *Skepticism and the Definition of Knowledge*. Routledge, London

Harris, L. R., and Brown, G. T. (2010) 'Mixing Interview and Questionnaire Methods: Practical Problems in Aligning Data. Practical Assessment, Research, and Evaluation. 2010;15 (1):1–19.

Hartwig, M., and Granhag, P. (2015) 'Exploring the Nature and Origin of Beliefs about Deception: Implicit and Explicit Knowledge among Lay People and Presumed Experts'. *Detecting Deception: Current Challenges and Cognitive Approaches*, (pp. 125-154). Chichester: John Wiley & Sons

Harvey, W. S. (2011) 'Strategies for Conducting Elite Interviews'. *Qualitative Research* 11 (4), 431-441.

Hau, Y. S., Kim, B., Lee, H., and Kim, Y. (2013) 'The Effects of Individual Motivations and Social Capital on Employees' Tacit and Explicit Knowledge Sharing Intentions'. *International Journal of Information Management* 33 (2), 356-366.

He, H., Baruch, Y., and Lin, C. (2014) 'Modeling Team Knowledge Sharing and Team Flexibility: The Role of within-Team Competition'. *Human Relations* 67 (8), 947-978.

He, Y., Zhao, N., and Yin, H. (2018) 'Integrated Networking, Caching, and Computing for Connected Vehicles: A Deep Reinforcement Learning Approach'. *IEEE Transactions on Vehicular Technology* 67 (1), 44-55.

Henttonen, K., Kianto, A., and Ritala, P. (2016) 'Knowledge Sharing and Individual Work Performance: An Empirical Study of a Public Sector Organisation'. *Journal of Knowledge Management* 20 (4), 749-768.

Heywood, P. (2012). Anthropology and what there is: Reflections on Ontology'. *Cambridge Anthropology*, pp.143-151.

Hislop, D., Bosua, R., and Helms, R. (2018) *Knowledge Management in Organizations: A Critical Introduction*. Oxford University Press.

Ho, H., and Ganesan, S. (2013) 'Does Knowledge Base Compatibility Help or Hurt Knowledge Sharing between Suppliers in Coopetition? the Role of Customer Participation'. *Journal of Marketing* 77 (6), 91-107.

Holste, J. S., and Fields, D. (2010) 'Trust and Tacit Knowledge Sharing and use'. *Journal of Knowledge Management* 14 (1), 128-140.

Holt, A. (2010) 'Using the Telephone for Narrative Interviewing: A Research Note'. *Qualitative Research* 10 (1), 113-121.

Hung, S., Durcikova, A., Lai, H., and Lin, W. (2011) 'The Influence of Intrinsic and Extrinsic Motivation on Individuals' Knowledge Sharing Behavior'. *International Journal of Human-Computer Studies* 69 (6), 415-427.

Hur, W., Park, J., and Kim, M. (2010) 'The Role of Commitment on the Customer benefits–loyalty Relationship in Mobile Service Industry'. *The Service Industries Journal* 30 (14), 2293-2309.

Idrees, M.S., Schweppe, H., Roudier, Y., Wolf, M., Scheuermann, D. and Henniger, O. (2011) March. Secure automotive on-board protocols: a case of over-the-air firmware updates. In *International Workshop on Communication Technologies for Vehicles* (pp. 224-238). Springer, Berlin, Heidelberg.

Iglesias, O., Singh, J. J., and Batista-Foguet, J. M. (2011) 'The Role of Brand Experience and Affective Commitment in Determining Brand Loyalty'. *Journal of Brand Management* 18 (8), 570-582.

Ipe, M. (2003) 'Knowledge Sharing in Organizations: A Conceptual Framework'. *Human Resource Development Review* 2 (4), 337-359.

Irvine, A., Drew, P., and Sainsbury, R. (2013) ''Am I Not Answering Your Questions Properly? Clarification, Adequacy and Responsiveness in Semi-Structured Telephone and Face-to-Face Interviews'. *Qualitative Research* 13 (1), 87-106.

Jabeen, Q., Khan, F., Hayat, M. N., Khan, H., Jan, S. R., and Ullah, F. (2016) 'A Survey: Embedded Systems Supporting by Different Operating Systems'. *ArXiv Preprint arXiv:1610.07899.*

Jacob, S. A., and Furgerson, S. P. (2012) 'Writing Interview Protocols and Conducting Interviews: Tips for Students New to the Field of Qualitative Research'. *The Qualitative Report* 17 (42), 1-10.

Jacobides, M. G., MacDuffie, J. P., and Tae, C. J. (2016) 'Agency, Structure, and the Dominance of OEMs: Change and Stability in the Automotive Sector'. *Strategic Management Journal* 37 (9), 1942-1967.

Jain, S., Tyagi, M., Walia, R., and Mangla, S. (2015) 'Optimization of the Production System of Second Tier Suppliers'. *Proceedings of ICRBS* 2015.

Janich, P. (2018) *What is Information?* (Vol. 55). U of Minnesota Press.

Jean, R., Sinkovics, R. R., and Hiebaum, T. P. (2014) 'The Effects of Supplier Involvement and Knowledge Protection on Product Innovation in Customer–Supplier Relationships: A Study of Global Automotive Suppliers in China'. *Journal of Product Innovation Management* 31 (1), 98-113.

Jenkins, R. (2014) *Social Identity*. Routledge, London.

Jo, S. J., and Joo, B. (2011) 'Knowledge Sharing: The Influences of Learning Organization Culture, Organizational Commitment, and Organizational Citizenship Behaviors'. *Journal of Leadership & Organizational Studies* 18 (3), 353-364.

Julisch, K. (2013) 'Understanding and Overcoming Cyber Security Anti-Patterns'. *Computer Networks* 57 (10), 2206-2211.

Jürgens, U., and Krzywdzinski, M. (2013) 'Breaking Off from Local Bounds: Human Resource Management Practices of National Players in the BRIC Countries. *International Journal of Automotive Technology and Management*, ' 13(2), p.114.

Kaluza, A., Kleemann, S., Broch, F., Herrmann, C., and Vietor, T. (2016) 'Analyzing Decision-Making in Automotive Design Towards Life Cycle Engineering for Hybrid Lightweight Components'. *Procedia CIRP* 50, 825-830.

Kanellos, N. S. (2013) 'Exploring the Characteristics of Knowledge-Based Entrepreneurship in Greek High-Technology Sectors'. *Journal of Enterprising Culture* 13 (1), 69-88.

Kaplan, A. (2017) *The Conduct of Inquiry: Methodology for Behavioural Science*. Routledge, London.

Katsumata, P., Hemenway, J., and Gavins, W. (eds.) (2010) *Military Communications Conference, 2010-MILCOM 2010*. 'Cybersecurity Risk Management': IEEE.

Kaur, K., and Rampersad, G. (2018) 'Trust in Driverless Cars: Investigating Key Factors Influencing the Adoption of Driverless Cars'. *Journal of Engineering and Technology Management* 48, 87-96.

Khan, Z., Shenkar, O., and Lew, Y. K. (2015) 'Knowledge Transfer from International Joint Ventures to Local Suppliers in a Developing Economy'. *Journal of International Business Studies* 46 (6), 656-675.

Kim, H., Lee, M., Lee, H., and Kim, N. (2010) 'Corporate Social Responsibility and employee–company Identification'. *Journal of Business Ethics* 95 (4), 557-569.

Kim, Y., Choi, T. Y., Yan, T., and Dooley, K. (2011) 'Structural Investigation of Supply Networks: A Social Network Analysis Approach'. *Journal of Operations Management* 29 (3), 194-211.

Kimble, C., Grenier, C. and Goglio-Primard, K. (2010) Innovation and knowledge sharing across professional boundaries: Political interplay between boundary objects and brokers. *International Journal of Information Management*, *30*(5), pp.437-444.

King, N., Horrocks, C., and Brooks, J. (2018) *Interviews in Qualitative Research*. SAGE Publications Limited.

Kito, T., Brintrup, A., New, S., and Reed-Tsochas, F. (2014) 'The Structure of the Toyota Supply Network: An Empirical Analysis'. *Available at SSRN 2412512.*

Klimburg, A. (2015) '2012'. *National Cyber Security Framework Manual.*Tallinn*: NATO CCDCOE.*

Kochan, T. A., Lansbury, R. D., and MacDuffie, J. P. (2018) *After Lean Production: Evolving Employment Practices in the World Auto Industry*. Cornell University Press.

Koenig, M. E. (2012) 'What is KM? Knowledge Management Explained'. *KMWorld Magazine.*

Koscher, K., Czeskis, A., Roesner, F., Patel, S., Kohno, T., Checkoway, S., McCoy, D., Kantor, B., Anderson, D., and Shacham, H. (eds.) (2010) *Security and Privacy (SP), 2010 IEEE Symposium on*. 'Experimental Security Analysis of a Modern Automobile': IEEE.

Kotabe, M., Jiang, C. X., and Murray, J. Y. (2017) 'Examining the Complementary Effect of Political Networking Capability with Absorptive Capacity on the Innovative Performance of Emerging-Market Firms'. *Journal of Management* 43 (4), 1131-1156.

Koufteros, X. A., Rawski, G. E., and Rupak, R. (2010) 'Organizational Integration for Product Development: The Effects on Glitches, on-time Execution of Engineering Change Orders, and Market Success'. *Decision Sciences* 41 (1), 49-80.

Koulikov, M. (2011) 'Emerging Problems in Knowledge Sharing and the Three New Ethics of Knowledge Transfer'. *Knowledge Management & E-Learning: An International Journal* 3 (2), 237-250.

Kreiner, C. (ed.) (2017) *Computer Safety, Reliability, and Security: SAFECOMP 2017 Workshops, ASSURE, DECSoS, SASSUR, TELERISE, and TIPS, Trento, Italy, September 12, 2017, Proceedings*. 'Automotive SPICE, Safety and Cybersecurity Integration': Springer.

Krosnick, J. A. (2018) 'Questionnaire Design'. in *The Palgrave Handbook of Survey Research*. ed. by Anon: Springer, 439-455.

Kugele, S., Obergfell, P., Broy, M., Creighton, O., Traub, M., and Hopfensitz, W. (eds.) (2017) *Software Architecture (ICSA), 2017 IEEE International Conference on*. 'On Service-Orientation for Automotive Software': IEEE.

Kuo, T. (2013) 'How Expected Benefit and Trust Influence Knowledge Sharing'. *Industrial Management & Data Systems* 113 (4), 506-522.

Lam, A., and Lambermont-Ford, J. (2010) 'Knowledge Sharing in Organisational Contexts: A Motivation-Based Perspective'. *Journal of Knowledge Management* 14 (1), 51-66.

Lambe, P. (2014) *Organising Knowledge: Taxonomies, Knowledge and Organisational Effectiveness*. Elsevier.

Lawson, B., Krause, D., and Potter, A. (2015) 'Improving Supplier New Product Development Performance: The Role of Supplier Development'. *Journal of Product Innovation Management* 32 (5), 777-792.

Le Dain, M. A., and Merminod, V. (2014) 'A Knowledge Sharing Framework for Black, Grey and White Box Supplier Configurations in New Product Development'. *Technovation* 34 (11), 688-701.

Le Dain, M., Calvi, R., and Cheriti, S. (2010) 'Developing an Approach for Design-Or-Buy-Design Decision-Making'. *Journal of Purchasing and Supply Management* 16 (2), 77-87.

Lee, P., Gillespie, N., Mann, L., and Wearing, A. (2010) 'Leadership and Trust: Their Effect on Knowledge Sharing and Team Performance'. *Management Learning* 41 (4), 473-491.

Leenstra, H. (2017) 'Multi Actor Roadmap to Improve Cyber Security of Consumer used Connected Cars'. Openaccess.leidenuniv.nl.

Lehrer, K. (2018) *Theory of Knowledge*. Boulder: Westview Press.

Lema, R., Quadros, R., and Schmitz, H. (2015) 'Reorganising Global Value Chains and Building Innovation Capabilities in Brazil and India'. *Research Policy* 44 (7), 1376-1386.

Leminen, S., Westerlund, M., Rajahonka, M., and Siuruainen, R. (2012) 'Towards IOT Ecosystems and Business Models'. in *Internet of Things, Smart Spaces, and Next Generation Networking*. ed. by Anon: Springer, 15-26.

Leung, L. (2015) 'Validity, Reliability, and Generalizability in Qualitative Research'. *Journal of Family Medicine and Primary Care* 4 (3), 324-327.

Lewis, S. C., Zamith, R., and Hermida, A. (2013) 'Content Analysis in an Era of Big Data: A Hybrid Approach to Computational and Manual Methods'. *Journal of Broadcasting & Electronic Media* 57 (1), 34-52.

Li, Z., Ye, J., and Xia, C. (2014) 'The Approach to Accelerate Collaborative New Product Development Process through Managing Knowledge Sharing Behaviors'. *European Journal of Business and Management* 6 (2), 146-153.

Lilleoere, A., and Holme Hansen, E. (2011) 'Knowledge sharing Enablers and Barriers in Pharmaceutical Research and Development'. *Journal of Knowledge Management* 15 (1), 53-70.

Lin, N. (2017) 'Building a Network Theory of Social Capital'. in *Social Capital*. ed. by Anon: Routledge, London, 3-28.

Liu, S., Young, R. I., and Ding, L. (2011) 'An Integrated Decision Support System for Global Manufacturing Co-Ordination in the Automotive Industry'. *International Journal of Computer Integrated Manufacturing* 24 (4), 285-301.

Liu, T., Yuan, R. and Chang, H. (2012) October. Research on the Internet of Things in the Automotive Industry. In *2012 International Conference on Management of e-Commerce and e-Government* (pp. 230-233). IEEE.

Loebbecke, C., van Fenema, P. C., and Powell, P. (2016) 'Managing Inter-Organizational Knowledge Sharing'. *The Journal of Strategic Information Systems* 25 (1), 4-14.

López-Cuadrado, J. L., Colomo-Palacios, R., González-Carrasco, I., García-Crespo, Á., and Ruiz-Mezcua, B. (2012) 'SABUMO: Towards a Collaborative and Semantic Framework for Knowledge Sharing'. *Expert Systems with Applications* 39 (10), 8671-8680.

Lotfi, Z., Mukhtar, M., Sahran, S., and Zadeh, A. T. (2013) 'Information Sharing in Supply Chain Management'. *Procedia Technology* 11, 298-304.

Loukas, G. (2015) 'Cyber Physical Attacks on Implants and Vehicles'. in *CYBER-PHYSICAL ATTACKS: A Growing Invisible Threat.* ed. by AnonOxford, England: Elsevier, 82-102.

Lu, N., Cheng, N., Zhang, N., Shen, X., and Mark, J. W. (2014) 'Connected Vehicles: Solutions and Challenges'. *IEEE Internet of Things Journal* 1 (4), 289-299.

Ma, Z., Huang, Y., Wu, J., Dong, W., and Qi, L. (2014) 'What Matters for Knowledge Sharing in Collectivistic Cultures? Empirical Evidence from China'. *Journal of Knowledge Management* 18 (5), 1004-1019.

MacDuffie, J. P. (2013) 'Modularity-as-property, modularization-as-process, and ‘modularity'-as-frame: Lessons from Product Architecture Initiatives in the Global Automotive Industry'. *Global Strategy Journal* 3 (1), 8-40.

Macher, G., Much, A., Riel, A., Messnarz, R., and Kreiner, C. (eds.) (2017) *International Conference on Computer Safety, Reliability, and Security*. 'Automotive SPICE, Safety and Cybersecurity Integration': Springer.

Maduenyi, S., Oke, A. O., Fadeyi, O., and Ajagbe, A. M. (2015) 'Impact of Organisational Structure on Organisational Performance'.

Madzudzo, G., Morris, D., and Garcia-Perez, A. (2018) June. Supplier Delocalization: A Threat to Automotive Cybersecurity Knowledge Sharing?'. In June *Gerpisa The International Network of the Automobile*: Brazil, Sao Paulo.

Magzan, M. (2012) 'Mental Models for Leadership Effectiveness: Building Future Different than the Past'. *Journal of Engineering Management and Competitiveness (JEMC)* 2 (2), 57-63.

Mahutga, M. C. (2012) 'When do Value Chains Go Global? A Theory of the Spatialization of Global Value Chains'. *Global Networks* 12 (1), 1-21.

Manello, A., and Calabrese, G. (2018) The influence of reputation on supplier selection: An empirical study of the European automotive industry. *Journal of Purchasing and Supply Management*, *25*(1), pp.69-77.

Mann, S. (2016) *The Research Interview: Reflective Practice and Reflexivity in Researc*h. Houndmills, Basingstoke, Hampshire; New York: Palgrave Macmillan.

Marabelli, M., and Newell, S. (2012) 'Knowledge Risks in Organizational Networks: The Practice Perspective'. *The Journal of Strategic Information Systems* 21 (1), 18-30.

Marodin, G. A., Frank, A. G., Tortorella, G. L., and Saurin, T. A. (2016) 'Contextual Factors and Lean Production Implementation in the Brazilian Automotive Supply Chain'. *Supply Chain Management: An International Journal* 21 (4), 417-432.

Marshall, B., Cardon, P., Poddar, A., and Fontenot, R. (2013) 'Does Sample Size Matter in Qualitative Research? A Review of Qualitative Interviews in IS Research'. *Journal of Computer Information Systems* 54 (1), 11-22.

Marshall, C., and Rossman, G. B. (2014) *Designing Qualitative Research*. Sage Publications, London.

Mason, M., 2010, August. Sample size and saturation in PhD studies using qualitative interviews. In *Forum qualitative Sozialforschung/Forum: qualitative social research* (Vol. 11, No. 3).

Matzler, K., and Mueller, J. (2011) 'Antecedents of Knowledge sharing–Examining the Influence of Learning and Performance Orientation'. *Journal of Economic Psychology* 32 (3), 317-329.

McCarthy, C., and Harnett, K. (2014) *National Institute of Standards and Technology (NIST) Cybersecurity Risk Management Framework Applied to Modern Vehicles.*

McGuirk, P. M., and O'Neill, P. (2016) 'Using questionnaires in qualitative human geography". In *Qualitative research methods in human geography*, Edited by: Hay, I. 147–162. Oxford: Oxford University Press.

McIntosh, M. J., and Morse, J. M. (2015) 'Situating and Constructing Diversity in Semi-Structured Interviews'. *Global Qualitative Nursing Research* 2.

Menkel-Meadow, C. (2011) 'Why and how to Study Transnational Law'. *UC Irvine L.Rev.* 1, 97.

Merminod, V., Rowe, F., and Teeni, D. (2012) 'Knowledge Sharing and Maturation in Circles of Trust: The Case of New Product Development'.

Merriam, S. B., and Tisdell, E. J. (2015) *Qualitative Research: A Guide to Design and Implementation*. John Wiley & Sons.

Merriam-webster.com (2019) *Definition of KNOWLEDGE. (2019). Merriam-Webster.Com. Retrieved 5 March 2019, from Https://www.Merriam-Webster.com/dictionary/knowledge* [online] available from <https://www.merriam-webster.com/dictionary/knowledge> [Accessed March 2019]

Meszaros, J., and Buchalcevova, A. (2017) 'Introducing OSSF: A Framework for Online Service Cybersecurity Risk Management'. *Computers & Security* 65, 300-313.

Miles, M. B., Huberman, A. M., and Saldana, J. (2014) *Qualitative Data Analysis*: Sage Publications, London.

Miles, R. (2015) 'Complexity, Representation and Practice: Case Study as Method and Methodology'. *Issues in Educational Research* 25 (3), 309.

Millar, M. M., and Dillman, D. A. (2011) 'Improving Response to Web and Mixed-Mode Surveys'. *Public Opinion Quarterly* 75 (2), 249-269.

Moffett, S., Conn, S., Reid, A., and Hutchinson, K. (2014) September. From Data to Knowledge: KM Implementation in the UK Car Retail Industry. In *European Conference on Knowledge Management* (Vol. 2, p. 684). Academic Conferences International Limited.

Möller, D. P., Haas, R. E., and Akhilesh, K. (2017) Electronics, IT, and Cybersecurity' *16th Annual IEEE International Conference on Electro Information Technology, Lincoln, Nebraska, USA*, 118-121.

Monden, Y. (2011) *Toyota Production System: An Integrated Approach to just-in-Time*.: CRC Press.

Moore, J. E., Mascarenhas, A., Bain, J., and Straus, S. E. (2017) 'Developing a Comprehensive Definition of Sustainability'. *Implementation Science* 12 (1), 110

Moretti, F., van Vliet, L., Bensing, J., Deledda, G., Mazzi, M., Rimondini, M., Zimmermann, C., and Fletcher, I. (2011) 'A Standardized Approach to Qualitative Content Analysis of Focus Group Discussions from Different Countries'. *Patient Education and Counseling* 82 (3), 420-428.

Morin, A. J., Morizot, J., Boudrias, J., and Madore, I. (2011) 'A Multifoci Person-Centered Perspective on Workplace Affective Commitment: A Latent profile/factor Mixture Analysis'. *Organizational Research Methods* 14 (1), 58-90.

Morris, D., Madzudzo, G., and Garcia-Perez, A. (2018) 'Cybersecurity and the Auto Industry: The Growing Challenges Presented by Connected Cars'. *International Journal of Automotive Technology and Management* 18 (2), 105-118.

Morse, J. M. (2016) *Mixed Method Design: Principles and Procedures*. Routledge London.

Morse, J. M. (2015) 'Critical Analysis of Strategies for Determining Rigor in Qualitative Inquiry'. *Qualitative Health Research* 25 (9), 1212-1222.

Mössinger, J. (2010) Software in automotive systems. *IEEE software*, *27*(2), pp.92-94.

Motoyama, Y. (2016) *Global Companies, Local Innovations: Why the Engineering Aspects of Innovation Making Require Co-Location*.: Routledge.

Mundhenk, P., Steinhorst, S., Lukasiewycz, M., Fahmy, S.A. and Chakraborty, S. (2015) June. Security analysis of automotive architectures using probabilistic model checking. In *Proceedings of the 52nd Annual Design Automation Conference* (p. 38). ACM.

Munir, J. (2016) 'State-of-the-Art of Internet of Things Ontologies' Tech. Univ. Berlin, 2016.

Myers, M. D. (2019) *Qualitative Research in Business and Management*. Sage Publications Limited.

Nagy, S., Mills, J., Waters, D., and Birks, M. (2010) *Using Research in Healthcare Practice*. Lippincott, Williams and Wilkins, Broadway, NSW, Australia.

Nam Nguyen, H., and Mohamed, S. (2011) 'Leadership Behaviors, Organizational Culture and Knowledge Management Practices: An Empirical Investigation'. *Journal of Management Development* 30 (2), 206-221.

Natella, R., Cotroneo, D., Duraes, J. A., and Madeira, H. S. (2013) 'On Fault Representativeness of Software Fault Injection'. *IEEE Transactions on Software Engineering* 39 (1), 80-96.

Neches, R., and Madni, A. M. (2013) 'Towards Affordably Adaptable and Effective Systems'. *Systems Engineering* 16 (2), 224-234.

Nesheim, T., and Gressgård, L. J. (2014) 'Knowledge Sharing in a Complex Organization: Antecedents and Safety Effects'. *Safety Science* 62, 28-36.

Neuendorf, K. A. (2016) *The Content Analysis Guidebook*. Sage Publications, London.

Neuman, W. L. (2013) *Social Research Methods: Qualitative and Quantitative Approaches*. Pearson education.

NHTSA *Cybersecurity Best Practices for Modern Vehicles* [online] available from <https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/sae2017chatipoglu_0.pdf> [June 2017].

Nicolini, D. (2011) 'Practice as the Site of Knowing: Insights from the Field of Telemedicine'. *Organization Science* 22 (3), 602-620.

Nir, A., Ding, J., and Chou, C. (2012) 'Inter-Organizational Culture, Trust, Knowledge Sharing, Collaboration and Performance in Supply Chain of Maritime Industries: Examining the Linkages'. *African Journal of Business Management* 6 (19), 5927-5938.

NIST *Automotive Cybersecurity Framework* [online] available from <https://www.nist.gov/topics/cybersecurity> [Accessed September 2018].

Noble, H., and Smith, J. (2015) 'Issues of Validity and Reliability in Qualitative Research'. *Evidence-Based Nursing*, ebnurs-2015-102054.

Nonaka, I., and Toyama, R. (2015) The Knowledge-Creating Theory Revisited: Knowledge Creation as a Synthesizing Process'. in *The Essentials of Knowledge Management*. ed. by Anon: Springer, 95-110.

North, K., and Kumta, G. (2018) *Knowledge Management: Value Creation through Organizational Learning*. Springer.

Nworie, J. (2011) 'Using the Delphi Technique in Educational Technology Research'. *Techtrends* 55 (5), 24.

O'Cathain, A., Murphy, E., and Nicholl, J. (2010) 'Three Techniques for Integrating Data in Mixed Methods Studies'. *BMJ (Clinical Research Ed.)* 341, c4587.

Ofreneo, R. E. (2016) 'Auto and Car Parts Production: Can the Philippines Catch Up with Asia?'. *Asia Pacific Business Review* 22 (1), 48-64.

Omotayo, F. O. (2015) 'Knowledge Management as an Important Tool in Organisational Management: A Review of Literature'. *Library Philosophy and Practice* 1 (2015), 1-23.

O'Neill, M., Savage, B., Booth, S., and Lamb, J. (2018) 'Support for Novice Researchers using Digital Tools (Nvivo and Qualtrics).

Onishi, H. (2012) June. Paradigm change of vehicle cyber security. In *2012 4th International Conference on Cyber Conflict (CYCON 2012)* Tallinn, (pp. 1-11). IEEE.

Panahi, S., Watson, J., and Partridge, H. (2013) 'Towards Tacit Knowledge Sharing Over Social Web Tools'. *Journal of Knowledge Management* 17 (3), 379-397.

Parkinson, S., Ward, P., Wilson, K., and Miller, J. (2017) 'Cyber Threats Facing Autonomous and Connected Vehicles: Future Challenges'. *IEEE Transactions on Intelligent Transportation Systems* 18 (11), 2898-2915.

Patel, K. K., and Patel, S. M. (2016) 'Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges'. *International Journal of Engineering Science and Computing* 6 (5).

Paulin, D., and Suneson, K. (2015) 'Knowledge Transfer, Knowledge Sharing and Knowledge barriers–three Blurry Terms in KM'. *Leading Issues in Knowledge Management, Volume Two* 2, 73-94.

Peng, H. (2013) 'Why and when do People Hide Knowledge?'. *Journal of Knowledge Management* 17 (3), 398-415.

Pfarrer, M. D., Pollock, T. G., and Rindova, V. P. (2010) 'A Tale of Two Assets: The Effects of Firm Reputation and Celebrity on Earnings Surprises and Investors' Reactions'. *Academy of Management Journal* 53 (5), 1131-1152.

Piran, F. A. S., Lacerda, D. P., Antunes, J. A. V., Viero, C. F., and Dresch, A. (2016) 'Modularization Strategy: Analysis of Published Articles on Production and Operations Management (1999 to 2013)'. *The International Journal of Advanced Manufacturing Technology* 86 (1-4), 507-519.

Pirkkalainen, H., and Pawlowski, J. (2013) 'Global Social Knowledge Management: From Barriers to the Selection of Social Tools'. *Electronic Journal of Knowledge Management* 11 (1).

Polanyi, M. (2012) Personal Knowledge. Routledge, Taylor Francis Group, London.

Polit, D. F., and Beck, C. T. (2010) 'Generalization in Quantitative and Qualitative Research: Myths and Strategies'. *International Journal of Nursing Studies* 47 (11), 1451-1458.

Pratap, S. (2014) 'Towards a Framework for Performing Outsourcing Capability'. *Strategic Outsourcing: An International Journal* 7 (3), 226-252.

Prieto Pastor, I. M., Perez Santana, M. P., and Martín Sierra, C. (2010) 'Managing Knowledge through Human Resource Practices: Empirical Examination on the Spanish Automotive Industry'. *The International Journal of Human Resource Management* 21 (13), 2452-2467.

Pritchard, D. (2013) *What is this Thing Called Knowledge?* Routledge, Taylor Francis Group, London.

PWC *Driving Cybersecurity Advances in an Interconnected World* [online] available from <https://www.pwc.ru/ru/automotive/publications/assets/global-state-of-information-security-automotive.pdf> [Accessed March 2018].

Qamar, A., Hall, M. A., and Collinson, S. (2018) 'Lean Versus Agile Production: Flexibility Trade-Offs within the Automotive Supply Chain'. *International Journal of Production Research*, 1-20.

Qualtrics *The Leading Research, Survey & Experience Software* [online] available from <https://www.qualtrics.com/uk/> [Accessed January 2018].

Raggad, B. G. (2010) *Information Security Management: Concepts and Practice*. CRC Press

Rasula, J., Vuksic, V. B., and Stemberger, M. I. (2012) 'The Impact of Knowledge Management on Organisational Performance'. *Economic and Business Review for Central and South-Eastern Europe* 14 (2), 147

Rightmer, J.A. (2012) *Supply chain management strategies in the US motor vehicle industry* (Doctoral dissertation, Lawrence Technological University).

Rinehart, J., Huxley, C., and Robertson, D. (2018) *Just another Car Factory: Lean Production and its Discontents*. Cornell University Press.

Ritchie, J., Lewis, J., Nicholls, C. M., and Ormston, R. (2013) *Qualitative Research Practice: A Guide for Social Science Students and Researchers*. Sage Publications.

Roberts, M. E., Stewart, B. M., Tingley, D., Lucas, C., Leder-Luis, J., Gadarian, S. K., Albertson, B., and Rand, D. G. (2014) 'Structural Topic Models for open-ended Survey Responses'. *American Journal of Political Science* 58 (4), 1064-1082.

Rodriguez, E., and Edwards, J. (2010) 'People, Technology, Processes and Risk Knowledge Sharing'. *Electronic Journal of Knowledge Management* 8 (1), 139-150.

Rook, L. (2013) 'Mental Models: A Robust Definition'. *The Learning Organization* 20 (1), 38-47.

Rowley, J. (2012) 'Conducting Research Interviews'. *Management Research Review* 35 (3/4), 260-271.

Rusinek, A., and Zaera, R. (2018) 'Material Definition to Design Vehicle Components, Application to Crashworthiness'. *Logistics and Transport* 38, 63-68.

SAEJ3061 *SAE International. 2016. J3061 -Cybersecurity Guidebook for Cyber-Physical Vehicle Systems. Technical Report.* [online] available from <http://standards.sae.org/wip/j3061/.> [Accessed September 2016].

Sagstetter, F., Lukasiewycz, M., Steinhorst, S., Wolf, M., Bouard, A., Harris, W.R., Jha, S., Peyrin, T., Poschmann, A. and Chakraborty, S. (2013) March. Security challenges in automotive hardware/software architecture design. In *Proceedings of the Conference on Design, Automation and Test in Europe* (pp. 458-463). EDA Consortium.

Saldaña, J. (2015) *The Coding Manual for Qualitative Researchers*. Sage Publications.

Santos, V. R., Soares, A. L., and Carvalho, J. Á. (2012) 'Knowledge Sharing Barriers in Complex Research and Development Projects: An Exploratory Study on the Perceptions of Project Managers'. *Knowledge and Process Management* 19 (1), 27-38.

Sarantakos, S. (2012) *Social Research*. Macmillan International Higher Education.

Saunders, B., Sim, J., Kingstone, T., Baker, S., Waterfield, J., Bartlam, B., Burroughs, H., and Jinks, C. (2018) 'Saturation in Qualitative Research: Exploring its Conceptualization and Operationalization'. *Quality & Quantity* 52 (4), 1893-1907.

Schatz, D., Bashroush, R., and Wall, J. (2017) 'Towards a More Representative Definition of Cyber Security'. *Journal of Digital Forensics, Security and Law* 12 (2), 8.

Schiliro, D. (2012) 'Knowledge-Based Economies and the Institutional Environment'. *Theoretical and Practical Research in Economic Fields (TPREF)* 3 (05), 42-50.

Schniederjans, M. J., Schniederjans, A. M., and Schniederjans, D. G. (2015) *Outsourcing and Insourcing in an International Context*. Routledge London.

Schreier, M. (2012) *Qualitative Content Analysis in Practice*. Sage Publications.

Schulze, A., Paul MacDuffie, J., and Täube, F. A. (2015) 'Introduction: Knowledge Generation and Innovation Diffusion in the Global Automotive Industry Change and Stability during Turbulent Times'. *Industrial and Corporate Change* 24 (3), 603-611.

Scott, G., and Garner, R. (2013) *Doing Qualitative Research: Designs, Methods, and Techniques*. Pearson Upper Saddle River.

Shan, S., Zhao, Q., and Hua, F. (2013) 'Impact of Quality Management Practices on the Knowledge Creation Process: The Chinese Aviation Firm Perspective'. *Computers & Industrial Engineering* 64 (1), 211-223.

Shankar, R., Mittal, N., Rabinowitz, S., Baveja, A., and Acharia, S. (2013) 'A Collaborative Framework to Minimise Knowledge Loss in New Product Development'. *International Journal of Production Research* 51 (7), 2049-2059.

Shankar, R., Acharia, S., and Baveja, A. (2009) 'Soft-System Knowledge Management Framework for New Product Development'. *Journal of Knowledge Management* 13 (1), 135-153.

Shih, S. C., Hsu, S. H., Zhu, Z., and Balasubramanian, S. K. (2012) 'Knowledge sharing—A Key Role in the Downstream Supply Chain'. *Information & Management* 49 (2), 70-80.

Silverman, D. (2016) *Qualitative Research*. Sage Publications, London.

Silverman, D. (2015) *Interpreting Qualitative Data*. Sage Publications, London.

Silverman, D. (2013) *A very Short, Fairly Interesting and Reasonably Cheap Book about Qualitative Research*.: Sage Publications, London.

Silverman, D. (2011) *Interpreting Qualitative Data: A Guide to the Principles of Qualitative Research*. Sage Publications Limited.

Simchi-Levi, D., Schmidt, W., Wei, Y., Zhang, P. Y., Combs, K., Ge, Y., Gusikhin, O., Sanders, M., and Zhang, D. (2015) 'Identifying Risks and Mitigating Disruptions in the Automotive Supply Chain'. *Interfaces* 45 (5), 375-390.

Sandhu, M., Kishore Jain, K., and Umi Kalthom bte Ahmad, Ir (2011) 'Knowledge Sharing among Public Sector Employees: Evidence from Malaysia'. *International Journal of Public Sector Management* 24 (3), 206-226.

Soliman, M., Riebisch, M., and Zdun, U. (eds.) (2015) *2015 12th Working IEEE/IFIP Conference on Software Architecture*. 'Enriching Architecture Knowledge with Technology Design Decisions': IEEE.

Stehr, N., and Grundmann, R. (2011) *Experts: The Knowledge and Power of Expertise*. Routledge, London.

Stemler, S. E. (2015) 'Content Analysis'. *Emerging Trends in the Social and Behavioral Sciences: An Interdisciplinary, Searchable, and Linkable Resource*, Wiley Online Library, 1-14.

Stubley, D. (2013) 'What is Cyber Security'. *Mode of Access* Http://www.7elements.Co.uk/resources/blog/what-is-Cyber-Security

Studnia, I., Nicomette, V., Alata, E., Deswarte, Y., Kaâniche, M., and Laarouchi, Y. (eds.) (2013) *Dependable Systems and Networks Workshop (DSN-W), 2013 43rd Annual IEEE/IFIP Conference on*. 'Survey on Security Threats and Protection Mechanisms in Embedded Automotive Networks': IEEE.

Sturgeon, T. J., and Van Biesebroeck, J. (2011) 'Global Value Chains in the Automotive Industry: An Enhanced Role for Developing Countries?'. *International Journal of Technological Learning, Innovation and Development* 4 (1-3), 181-205.

Subramanian, N., and Gunasekaran, A. (2015) 'Cleaner Supply Chain Management Practices for Twenty-First-Century Organizational Competitiveness: Practice-Performance Framework and Research Propositions'. *International Journal of Production Economics* 164, 216-233.

Sue, V. M., and Ritter, L. A. (2012) *Conducting Online Surveys*. Sage Publications Limited.

Suppiah, V., and Singh Sandhu, M. (2011) 'Organisational Culture's Influence on Tacit Knowledge sharing Behaviour'. *Journal of Knowledge Management* 15 (3), 462-477.

Swift, M., Balkin, D. B., and Matusik, S. F. (2010) 'Goal Orientations and the Motivation to Share Knowledge'. *Journal of Knowledge Management* 14 (3), 378-393.

Symon, G., and Cassell, C. (2012) 'Assessing Qualitative Research 12'. *Qualitative Organizational Research: Core Methods and Current Challenges*, 204.

Szmelter, A. (2016) 'Supplier Parks in Supply Logistics Strategies in the Automotive Industry'. *Zeszyty Naukowe Uniwersytetu Gdańskiego.Ekonomika Transportu i Logistyka* (58 Modelowanie procesów i systemów logistycznych, Cz. 15), 227-240.

Tanev, G., Tzolov, P., and Apiafi, R. (2015) 'A Value Blueprint Approach to Cybersecurity in Networked Medical Devices'. *Technology Innovation Management Review* 5 (6).

Tangaraja, G., Mohd Rasdi, R., Abu Samah, B., and Ismail, M. (2016) 'Knowledge Sharing is Knowledge Transfer: A Misconception in the Literature'. *Journal of Knowledge Management* 20 (4), 653-670.

TechCrunch (2016) The End of the Automotive Supply Chain [Online] available from <https://techcrunch.com/2016/09/15/the-end-of-the-automotive-supply-chain/> [September 2018].

Teece, D. J. (2013) 'Nonaka's Contribution to the Understanding of Knowledge Creation, Codification and Capture'. in *Towards Organizational Knowledge*. ed. by Anon: Springer, 17-23.

Terrell, S. R. (2012) 'Mixed-Methods Research Methodologies'. *The Qualitative Report* 17 (1), 254-280.

Thomas, E., and Magilvy, J. K. (2011) 'Qualitative Rigor or Research Validity in Qualitative Research'. *Journal for Specialists in Pediatric Nursing* 16 (2), 151-155.

Thomé, A. M. T., Scavarda, L. F., Pires, S. R., Ceryno, P., and Klingebiel, K. (2014) 'A Multi-Tier Study on Supply Chain Flexibility in the Automotive Industry'. *International Journal of Production Economics* 158, 91-105.

Thyme, K. E., Wiberg, B., Lundman, B., and Graneheim, U. H. (2013) 'Qualitative Content Analysis in Art Psychotherapy Research: Concepts, Procedures, and Measures to Reveal the Latent Meaning in Pictures and the Words Attached to the Pictures'. *The Arts in Psychotherapy* 40 (1), 101-107.

Titi Amayah, A. (2013) 'Determinants of Knowledge Sharing in a Public Sector Organization'. *Journal of Knowledge Management* 17 (3), 454-471.

Tocan, M. C. (2012) 'Knowledge Based Economy Assessment'. *Journal of Knowledge Management, Economics and Information Technology* 2 (5).

Tohidinia, Z., and Mosakhani, M. (2010) 'Knowledge Sharing Behaviour and its Predictors'. *Industrial Management & Data Systems* 110 (4), 611-631.

Tracy, S. J. (2010) 'Qualitative Quality: Eight "big-Tent" Criteria for Excellent Qualitative Research'. *Qualitative Inquiry* 16 (10), 837-851.

Trim, P., and Lee, Y. (2014) *Cyber Security Management: A Governance, Risk and Compliance Framework*. Surrey, England: Gower Publishing Limited.

Trkman, P., and Desouza, K. C. (2012) 'Knowledge Risks in Organizational Networks: An Exploratory Framework'. *The Journal of Strategic Information Systems* 21 (1), 1-17.

Trope, R. L., and Smedinghoff, T. J. (2018) 'Why Smart Car Safety Depends on Cybersecurity'. *Scitech Lawyer* 14 (4), 8-13.

Tuli, P., and Shankar, R. (2015) 'Collaborative and Lean New Product Development Approach: A Case Study in the Automotive Product Design'. *International Journal of Production Research* 53 (8), 2457-2471.

Uhlemann, E. (2015) 'Introducing Connected Vehicles [Connected Vehicles]'. *IEEE Vehicular Technology Magazine* 10 (1), 23-31.

Urbancova, H. (2013) 'Competitive Advantage Achievement through Innovation and Knowledge'. *Journal of Competitiveness* 5 (1).

Vaccaro, A., Parente, R. and Veloso, F.M. (2010) Knowledge management tools, inter-organizational relationships, innovation and firm performance. *Technological Forecasting and Social Change*, *77*(7), pp.1076-1089.

Vaismoradi, M., Turunen, H., and Bondas, T. (2013) 'Content Analysis and Thematic Analysis: Implications for Conducting a Qualitative Descriptive Study'. *Nursing & Health Sciences* 15 (3), 398-405.

Valio Dominguez Gonzalez, R., and Fernando Martins, M. (2014) 'Mapping the Organizational Factors that Support Knowledge Management in the Brazilian Automotive Industry'. *Journal of Knowledge Management* 18 (1), 152-176.

Van Gelder, M. M., Bretveld, R. W., and Roeleveld, N. (2010) 'Web-Based Questionnaires: The Future in Epidemiology?'. *American Journal of Epidemiology* 172 (11), 1292-1298.

Van Teijlingen, E., and Hundley, V. (2010) 'The Importance of Pilot Studies'. *Social Research Update* 35, 49-59.

Venkatesh, V., Brown, S. A., and Bala, H. (2013) 'Bridging the Qualitative-Quantitative Divide: Guidelines for Conducting Mixed Methods Research in Information Systems.'. *MIS Quarterly* 37 (1).

Vogl, S. (2013) 'Telephone Versus Face-to-Face Interviews: Mode Effect on Semistructured Interviews with Children'. *Sociological Methodology* 43 (1), 133-177.

Vogt, W. P., Gardner, D. C., Haeffele, L. M., and Vogt, E. R. (2014) *Selecting the Right Analyses for Your Data: Quantitative, Qualitative, and Mixed Methods*.: Guilford Publications.

Von Krogh, G., Nonaka, I., and Rechsteiner, L. (2012) 'Leadership in Organizational Knowledge Creation: A Review and Framework'. *Journal of Management Studies* 49 (1), 240-277

Von Solms, R., and Van Niekerk, J. (2013) 'From Information Security to Cyber Security'. *Computers & Security* 38, 97-102.

Vuori, V., and Okkonen, J. (2012) 'Knowledge Sharing Motivational Factors of using an Intra-Organizational Social Media Platform'. *Journal of Knowledge Management* 16 (4), 592-603

Vyas, K. C. (2011) *Toyota Production System* (Doctoral dissertation).

Wahyuni, D. (2012) The Research Design Maze: Understanding paradigms, cases, methods, and methodologies. Journal of Applied Management Accounting Research, 10 (1), 69-80.

Walls, A., Perkins, E., and Weiss, J. (2013) 'Definition: Cybersecurity'. *Retrieved from Gartner.Com Website: Https://www.Gartner.com/doc/2510116/def Inition-Cybersecurity.*

Wamala, F. (2011) 'ITU National Cybersecurity Strategy Guide'. *International Telecommunications Union* 11.

Wang, C., and Hu, Q. (2017) 'Knowledge Sharing in Supply Chain Networks: Effects of Collaborative Innovation Activities and Capability on Innovation Performance'. *Technovation.*

Wang, L., Wakikawa, R., Kuntz, R., Vuyyuru, R., and Zhang, L. (eds.) (2012) *2012 Proceedings IEEE INFOCOM Workshops*. 'Data Naming in Vehicle-to-Vehicle Communications': IEEE.

Wang, S., and Noe, R. A. (2010) 'Knowledge Sharing: A Review and Directions for Future Research'. *Human Resource Management Review* 20 (2), 115-131.

Weinberg, F. J. (2015) 'Epistemological Beliefs and Knowledge Sharing in Work Teams: A New Model and Research Questions'. *The Learning Organization* 22 (1), 40-57.

Wendling, M., Oliveira, M., and Carlos Gastaud Maçada, A. (2013) 'Knowledge Sharing Barriers in Global Teams'. *Journal of Systems and Information Technology* 15 (3), 239-253.

Westerlund, M., Craigen, D., Bailetti, T., and Agwae, U. (2018) 'A Three-Vector Approach to Blind Spots in Cybersecurity'. in *Encyclopedia of Information Science and Technology, Fourth Edition*. ed. by Anon: IGI Global, 1684-1693.

Wiig, K. (2012) *People-Focused Knowledge Management*.: Routledge, London.

Wilhelm, M., and Dolfsma, W. (2018) 'Managing Knowledge Boundaries for Open innovation–lessons from the Automotive Industry'. *International Journal of Operations & Production Management* 38 (1), 230-248.

Wisdom, J., and Creswell, J. W. (2013) 'Mixed Methods: Integrating Quantitative and Qualitative Data Collection and Analysis while Studying Patient-Centered Medical Home Models'. *Rockville: Agency for Healthcare Research and Quality.*

Witherspoon, C. L., Bergner, J., Cockrell, C., and Stone, D. N. (2013) 'Antecedents of Organizational Knowledge Sharing: A Meta-Analysis and Critique'. *Journal of Knowledge Management* 17 (2), 250-277.

Woo, C., Jung, J., Euitack, J., Lee, J., Kwon, J. and Kim, D. (2016) Internet of Things Platform and Services for Connected Cars. In *IoTBD* (pp. 469-478).

Wood, R. L. (2017) 'A Dynamic Curation Method for Manufacturing-Related Knowledge'. *International Journal of Production Research* 55 (3), 891-903.

Woolliscroft, P., Caganova, D., Cambal, M., Holecek, J., and Pucikova, L. (2013) 'Implications for Optimisation of the Automotive Supply Chain through Knowledge Management'. *Procedia CIRP* 7, 211-216.

Wynstra, F., Von Corswant, F., and Wetzels, M. (2010) 'In Chains? an Empirical Study of Antecedents of Supplier Product Development Activity in the Automotive Industry'. *Journal of Product Innovation Management* 27 (5), 625-639.

Xue, J., and Zhang, Z. (eds.) (2010) *2010 International Conference on Management and Service Science*. 'Research on the Relationship between Knowledge Management Infrastructure, Knowledge Sharing and Knowledge Management Performance': IEEE.

Tesla Invites Hackers for a Spin. (2014) The Wall Street Journal Blog. [online] available fromhttps://blogs.wsj.com/digits/2014/08/08/telsa-invites-hackers-for-a-spin/ [10 November 2018].

Yağdereli, E., Gemci, C., and Aktaş, A. Z. (2015) 'A Study on Cyber-Security of Autonomous and Unmanned Vehicles'. *The Journal of Defense Modeling and Simulation* 12 (4), 369-381.

Yeniyurt, S., Henke, J. W., and Yalcinkaya, G. (2014) 'A Longitudinal Analysis of Supplier Involvement in Buyers' New Product Development: Working Relations, Inter-Dependence, Co-Innovation, and Performance Outcomes'. *Journal of the Academy of Marketing Science* 42 (3), 291-308.

Yilmaz, K. (2013) 'Comparison of Quantitative and Qualitative Research Traditions: Epistemological, Theoretical, and Methodological Differences'. *European Journal of Education* 48 (2), 311-325.

Yin, R. K. (2011) *Applications of Case Study Research*.: Sage Publications, London.

Zaied, A. N. H., Hussein, G. S., and Hassan, M. M. (2012) 'The Role of Knowledge Management in Enhancing Organizational Performance'. *International Journal of Information Engineering and Electronic Business* 4 (5), 27.

Zhang, T., Antunes, H., and Aggarwal, S. (2014) 'Defending Connected Vehicles Against Malware: Challenges and a Solution Framework'. *IEEE Internet of Things Journal* 1 (1), 10-21.

Zieba, M. (2013) *Knowledge-intensive business services (KIBS) and their role in the knowledge-based economy* (No. 7/2013 (7)). GUT FME Working Paper Series A.

Zirpoli, F., and Becker, M. C. (2011) 'The Limits of Design and Engineering Outsourcing: Performance Integration and the Unfulfilled Promises of Modularity'. *Research and Development Management* 41 (1), 21-43.

APPENDIX

Appendix 1: List of keywords and combinations for the literature search

Keywords	Combinations		
	Variation	or	and
knowledge	knowledge	automotive knowledge	knowledge and automotive
knowledge management	management of knowledge	knowledge or management	knowledge and management
cybersecurity	cyber security	cyber-security	cyber
		cyber attack	cyber-attack
		cyber war	cyber-war
		cyber defence	cyber-defence
cyber security knowledge	cyber security knowledge	cyber security ***or*** knowledge	cyber security ***and*** knowledge
	automotive cyber security knowledge	automotive cyber security ***or*** knowledge	automotive cyber security ***and*** knowledge
	automotive cybersecurity knowledge	automotive cybersecurity ***or*** knowledge	automotive cybersecurity ***and*** knowledge
cybersecurity management	cyber security management	cybersecurity ***or*** management	cybersecurity ***and*** management
		cyber security ***or*** management	cyber security ***and*** management
automotive cybersecurity management	automotive cyber security management	automotive ***or*** cybersecurity management	automotive cybersecurity ***and*** management
		automotive ***or*** cyber security management	automotive cyber security ***and*** management
automotive cybersecurity knowledge management	automotive cyber security knowledge management	automotive cyber security ***or*** knowledge management	automotive cyber security ***and*** knowledge management
		automotive cybersecurity ***or*** knowledge management	automotive cybersecurity ***and*** knowledge management
		automotive ***or*** cyber security knowledge management	automotive ***and*** cyber security knowledge management
		automotive ***or*** cybersecurity	automotive ***and*** cybersecurity knowledge management

		knowledge management	
automotive cybersecurity knowledge sharing	automotive cyber security knowledge sharing	automotive cyber security ***or*** knowledge sharing	automotive cyber security ***and*** knowledge sharing
		automotive ***or*** cyber security knowledge sharing	automotive ***and*** cyber security knowledge sharing
		automotive ***or*** cybersecurity knowledge sharing	automotive ***and*** cybersecurity knowledge sharing
		automotive cyber security ***or*** knowledge sharing	automotive cyber security ***and*** knowledge sharing
automotive cybersecurity	automotive cyber security	automotive ***or*** cybersecurity	automotive ***and*** cybersecurity
		automotive ***or*** cyber security	automotive ***and*** cyber security
connected vehicle cybersecurity	connected vehicle cyber security	connected vehicle **or** cybersecurity	connected vehicle ***and*** cybersecurity
		connected vehicle **or** cyber security	connected vehicle and cyber security
connected vehicle cybersecurity	connected vehicle cyber security	connected vehicle **or** cybersecurity	connected vehicle **and** cybersecurity
	connected vehicle security	connected vehicle **or** cyber security	connected vehicle **and** cyber security
		connected vehicle **or** security	connected vehicle **and** security
connected vehicle cybersecurity knowledge sharing	connected vehicle cyber security knowledge sharing	connected vehicle **or** cybersecurity knowledge sharing	connected vehicle ***and*** cybersecurity knowledge sharing
		connected vehicle **or** cyber security knowledge sharing	connected vehicle ***and*** cyber security knowledge sharing
		connected vehicle cyber security ***or*** knowledge sharing	connected vehicle cyber security ***and*** knowledge sharing
cybersecurity knowledge sharing	cyber security knowledge sharing	cyber security **or** knowledge sharing	cyber security ***and*** knowledge sharing
		cybersecurity **or** knowledge sharing	cybersecurity ***and*** knowledge sharing
cybersecurity knowledge management	management of cyber security knowledge	cybersecurity **or** knowledge management	cybersecurity knowledge ***and*** management
		cyber security **or** knowledge management	cyber security knowledge ***and*** management
knowledge sharing framework	framework for knowledge sharing	knowledge sharing ***or*** framework	knowledge sharing ***and*** framework

knowledge transfer framework	framework for knowledge-transfer	knowledge-transfer ***or*** framework	knowledge-transfer ***and*** framework
knowledge management framework	framework for knowledge-management	knowledge management ***or*** framework	knowledge-management ***and*** framework
cybersecurity framework	framework for cybersecurity	framework ***or*** cybersecurity	framework ***and*** cybersecurity
cybersecurity knowledge sharing framework	framework for cybersecurity knowledge sharing	cybersecurity knowledge ***or*** framework	cybersecurity knowledge ***and*** framework
	cyber security knowledge sharing framework	cybersecurity knowledge sharing ***or*** framework	cybersecurity knowledge sharing ***and*** framework
cybersecurity management framework	framework for cybersecurity knowledge management	cybersecurity knowledge management or framework	cybersecurity knowledge management and framework
cybersecurity knowledge transfer framework	framework for cybersecurity knowledge transfer	cybersecurity knowledge transfer ***or*** framework	cybersecurity knowledge transfer ***and*** framework
cybersecurity knowledge management framework	framework for cybersecurity knowledge management	cybersecurity knowledge management ***or*** framework	cybersecurity knowledge management ***and*** framework
component integration framework	framework for component integration	component integration ***or*** framework	component integration ***and framework***
automotive component integration framework	framework for automotive component integration	automotive component integration ***or*** framework	automotive component integration ***and framework***
automotive component integration knowledge		automotive component ***or*** integration knowledge	automotive component **and** integration knowledge
		knowledge sharing ***or*** component integration framework	knowledge sharing ***and*** component integration framework

Appendix 2: Cybersecurity related definitions

Concept	Definition
Cybersecurity	"the 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" (ITU, 2014) "the preservation of confidentiality, integrity and availability of information in the Cyberspace" (ISO/IEC 27032:2012, 2012) "methods of using people, process and technology to prevent, detect and recover from damage to confidentiality, integrity and availability of information in cyberspace" (Bayuk, 2012: p. 3) "includes strategy, policy, and standards regarding the security of and operations in cyberspace, and encompasses the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure. The scope does not include other information and communications policy unrelated to national security or securing the infrastructure." (US Government, 2009: p. 2) "The desired state of an information system in which it can resist events from cyberspace likely to compromise the availability, integrity or confidentiality of the data stored, processed or transmitted and of the related services that these systems offer or make accessible" (French Government, 2011: p. 21) "actions (...) to reduce the risk and secure the benefits of a trusted digital environment for businesses and individuals" (UK Cabinet Office, 2011) "the desired objective of the IT security situation, in which the risks of global cyberspace have been reduced to an acceptable minimum. Hence, cyber security in Germany is the desired objective of the IT security situation, in which the risks of the German cyberspace have been reduced to an acceptable minimum. Cyber security (in Germany) is the sum of suitable and appropriate measures. Civilian cyber security focuses on all IT systems for civilian use in German cyber-space. Military cyber security focuses on all IT systems for military use in German cyberspace." (German Federal Ministry of the Interior, 2011)

	"the protection of cyberspace itself, the electronic information, the ICTs that support cyberspace, and the users of cyberspace in their personal, societal and national capacity, including any of their interests, either tangible or intangible, that are vulnerable to attacks originating in cyberspace" (von Solms and van Niekerk, 2013: p.99) "Measures relating to the confidentially, availability and integrity of information that is processed, stored and communicated by electronic or similar means" (Australian Government, 2009) "the defense or protection of the integrity, operations and confidentiality of computers and computer networks" (Lewis, 2005: p. 821)
Cyber-attacks	"Cyber-attacks include the unintentional or unauthorized access, use, manipulation, interruption or destruction (via electronic means) of electronic information and/or the electronic and physical infrastructure used to process, communicate and/or store that information. The severity of the cyber-attack determines the appropriate level of response and/or mitigation measures: i.e., cyber security" (Public Safety Canada, 2014)
National Cybersecurity	Comprises 3 dimensions of activity (governmental coordination, national cooperation and international collaboration), 5 mandates (military cyber, counter cyber-crime, intelligence /counter-intelligence, critical infrastructure protection / national crisis management and cyber diplomacy / internet governance) and 5 dilemmas (Klimburg, 2012: p. 29)
Cyber Defence	"The set of all technical and non-technical measures allowing a State to defend in cyberspace information systems that it considers to be critical" (French Government,2011: p. 21)
Cyber Warfare	"(…) actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption." (Clarke and Knake, 2012: p. 6)
Information Security	"preservation of confidentiality, integrity and availability of information. In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can be involved" (ISO/IEC 27000:2009, 2009) "the general security objectives comprise the following: availability; integrity, which may include authenticity and non-repudiation; and confidentiality" (ITU, 2014) "the protection of information and its critical elements, including the systems and hardware that use, store, and transmit that information" (Whitman and Mattord, 2009, p. 8, von Solms and van Niekerk, 2013: p. 98) "without the confidentiality, integrity, availability, non-repudiation, accountability, authenticity and reliability of information resources, information cannot be deemed secure" (von Solms and van Niekerk, 2013: p. 99)
Cyber Space	"Virtual space of all IT systems linked at data level on a global scale. The basis for cyberspace is the Internet as a universal and publicly accessible connection and transport network which can be complemented and

	further expanded by any number of additional data networks. IT systems in an isolated virtual space are not part of cyberspace" (German Federal Ministry of the Interior, 2011: p. 14) "The communication space created by the worldwide interconnection of automated digital data processing equipment" (French Government, 2011: p. 21) "Interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries. Common usage of the term also refers to the virtual environment of information and interactions between people" (US Government, 2009) "The hypothetical place in which communication over computer networks takes place" (Oxford Dictionaries, 2009: p. 223)

Category	Reliance
Brief Definition	Reliance on a particular stakeholder
Detailed Description	Automotive manufacturers or component suppliers relying on a stakeholder to provide all necessary knowledge to a project or problem solution.
Inclusion Criteria	Code will be applied to all incidents or occasions when a participant highlights a reliance on a particular stakeholder(s).
Exclusion Criteria	Code will not be used when it is the responsibility of the stakeholder to provide the required knowledge or solution.
Example	"Vehicle manufacturers rely too much on component suppliers for security solutions."
Category	**Integration**
Brief Definition	Combining two or more components
Detailed Description	The concatenation of different software, the combination of several automotive components into one whole, the unification of hardware components and automotive software.
Inclusion Criteria	Code to be applied when the unification of two or more components are mentioned.
Exclusion Criteria	Not to be used at the mention of single components (unintegrated components).
Example	"The integration of hardware components and software has resulted in internet access in vehicles."
Category	**Automotive Cybersecurity**
Brief Description	Security of connected vehicles.
Detailed Description	the protection of vehicular electronic systems, communication networks, control algorithms, software, users, and underlying data from malicious attacks, damage, unauthorized access, or manipulation.
Inclusion Criteria	The code is applied at the mention of vehicles that possess some form of connectivity and in-vehicle computer networks.
Exclusion Criteria	Not to be used when the vehicle is a full mechanical construct.
Example	"The vehicle has over 70 ECUs and built-in capabilities that allow the vehicle direct internet access."
Category	**Restriction**
Brief Description	Prohibited from sharing, disclosing of information.

Detailed Description	Disclosure prohibition from sharing, dissemination or talking about joint ventures or current projects.
Inclusion Criteria	The code is applied to code the use of non-disclosure agreements or design contracts used to gag individuals from disclosing information deemed private.
Exclusion Criteria	Not be used when a participant is not bound by a non-disclosure contract.
Category	Trust
Brief Description	Trust between organisations and employees within the same project/venture.
Detailed Description	It defines that existence or lack of trust, and the structures in place to encourage trust.
Inclusion Criteria	Code is used to code trust that may or may not exist between organisations or employees engaged in the same project.
Exclusion Criteria	Will not be used when there are structures in place that encourage knowledge sharing.
Category	New Technology
Brief Description	New technology or advancements for vehicles.
Detailed Description	Defines new technology or advancements both is software and hardware that are built for connected vehicles.
Inclusion Criteria	Code is applied when participants highlight that they are working on new technology.
Exclusion Criteria	Does not apply if the technology has been used by another manufacture or supplier for long periods.
Category	Out-Sourcing
Brief Description	Acquisition of components, products or knowledge from an external source.
Detailed Description	The sourcing of products, components, talent or knowledge for the connected vehicle manufacturer.
Inclusion Criteria	Code is applied when an organisation sources components, products, knowledge or talent form an external organisation for connected vehicle manufacturing.
Exclusion Criteria	Code will not be included when the designs or brought in from within the same organisation but in a different town or country.
Category	Consent
Brief Description	Permission or agreement.
Detailed Description	Permission to share private information or agreeing to the use of information for a particular purpose.
Inclusion Criteria	Code is used when permission for the use of private information is granted.

Exclusion Criteria	Code will not be used when consent/permission has been denied.
Category	Competition
Brief Description	Activity of gaining superiority over other suppliers.
Detailed Description	It is when OEMs or component suppliers withhold information in a bid to gain an advantage.
Inclusion Criteria	Will be used where information is used to gain an advantage or leverage in manufacturing processes or for out-sourcing.
Exclusion Criteria	Will be excluded if there is no advantage is gained or to be gained.
Category	Control
Brief Description	Influence, power or authority.
Detailed Description	When an organisation expert's authority or influence over a process, organisation or person.
Inclusion Criteria	Will be included when knowledge is used to gain influence or when used as a means of control.
Exclusion Criteria	When there is no influence or control gained from knowledge retention.
Category	Organisational Approach
Brief Description	An organisations plan, goals and methods.
Detailed Description	The way an organisation conducts its management processes.
Inclusion Criteria	Will be sued to code knowledge sharing inhibitors due to the way the organisation is managed.
Exclusion Criteria	Will not be used when the inhibitors are due to external influences.
Category	Cybersecurity Knowledge Sharing
Brief Description	Cyber-related knowledge or information.
Detailed Description	This is knowledge that can influence the security of a vehicle, component or product.
Inclusion Criteria	Code will be used to code cyber-related knowledge, information, component-specific knowledge or architectural knowledge.
Exclusion Criteria	If the information or knowledge does not relate to cybersecurity.
Category	Contract
Brief Description	An arrangement, agreement or undertaking.
Detailed Description	An arrangement agreed in collaboration work between organisations or departments.
Inclusion Criteria	This will be used to code design contracts or non-disclosure contracts employed in joint projects, ventures or collaboration.
Exclusion Criteria	Will be excluded were joint venture, projects or collaborations are conducted absent a contract.

Category	Prospective
Brief Description	Expectations or goals.
Detailed Description	Will be used code references to an organisation's future plans or expectations.
Inclusion Criteria	Code is included when a participant highlights that the organisation has plans to bring in new technology or knowledge sharing processes.
Exclusion Criteria	Will not be used to refer to existing plans already in process.

Appendix 4: Second cycle coding list

	Category	Description and Use
I.	Cybersecurity Knowledge (CSK) Sharing	The presence of cybersecurity knowledge (CSK) sharing and transfer mechanisms in use within the Automotive Industry. The category is used to group data that informs of the existence of CSK sharing mechanisms or the lack of such mechanisms.
II.	Competition	The effects of competition within the industry on CSK sharing. Used to group data that highlights how competition (development, innovation, sales etc.) affects CSK sharing.
III.	Reliance	The level of reliance placed on a stakeholder to provide a solution or design to a cyber-related problem The category is used to identify and group data that assists in understanding the extent and level of reliance that OEMs place on component manufacturers for cyber-related solutions
IV.	Trust	The role that trust plays in CSK sharing within the industry between different competitors. The category is used to identify and group data that assists in identifying the effects and the role that trust plays in CSK sharing.
V.	Contracts	The role of contracts in automotive CSK sharing The category is used to identify and group data that highlights different types and uses of contracts that either limit or enhance CSK sharing.
VI.	New Technologies	The extent to which new technologies and devices in vehicles enable data collection and sharing. Used to group data that highlights how new technologies either enable or restrict CSK sharing.
VII.	Organisational Approach	The role of organisational-related factors affecting CSK sharing. Used to group data that assists in understanding the extent to which organisations are enabling or barring CSK sharing.
VIII.	Out-sourcing	The role of out-sourcing and how it affects CSK sharing. Used to group data that assists in understanding the effects of out-sourcing on CSK sharing within the automotive industry.
1X.	Perspectives	Perspectives of personnel employed within the automotive industry on CSK sharing. The category is used to group data that assists in understanding employee perspectives on cybersecurity knowledge sharing.
X	CSK Inclusion	The role of CSK in design processes

		Used to group data that assists in understanding how CSK is included in vehicle manufacture and component development processes.

Appendix 5: Prior codes

CATEGORY	CODE	SUB-CODE
New Technologies	Internet Access	Connectivity
	V2X Communication	Communication
	In-built Capabilities	Evolution
	Digital modules	Digital modules
Vehicle Software	Software development	Software-dev
Automotive Industry	Automotive Industry	Automotive Industry
Integration	Integrated hardware	Hardware-int.
	Software Integration	Software-int.
	Component Integration	Component-int.
	Knowledge Integration	Knowledge-int.
	Integration activities	Integration activities
In-Vehicle Networks	Vehicle-to-Vehicle	V2V
	Vehicle-to-Infrastructure	V2I
	Vehicle-to-Devices	V2D
Knowledge Management	Knowledge Management	KM
	Knowledge Sharing	KS
	Task Partitioning	Task Partitioning
Original Equipment Manufacturer	OEM	OEM
	Vehicle manufacturer	OEM
	Vehicle Manufacturer	OEM
Out-Sourcing	Out-Sourcing	Out-Sourcing
	Component out-sourcing	Comp-outsourcing
	Knowledge out-sourcing	Know-outsourcing
	Internal out-sourcing	Internal out-sourcing
Engine Control Unit	ECU	ECU
Product Development	Product development	Innovation
	Component development	Innovation
Knowledge	Architectural knowledge	Architectural knowledge
	Component-specific knowledge	Component-specific knowledge
Suppliers	Component suppliers	Tier-1
		Tier-2
		Tier-3
	Shared supplier	Shared supplier
Vulnerability	Cybersecurity vulnerabilities	CS-Vulnerability
	Security vulnerabilities	Sec-Vulnerability
Safety	Safety	Safety
		Security
		Condition
Cyber threats	Cyber threats	Cyber threats
		Cyber-vulnerabilities
		Security
Hardware	Components	Products

	Part	system
	Assembly	Sub-system
		Sub-component
Threat	Threat Landscape	Threat landscape
		Threat scope
		Intent
		Action
		Security threats

CATEGORY	CODE	SUB-CODE
cybersecurity knowledge sharing	CSKS	CSKS
Knowledge Transfer	Knowledge Transfer	Knowledge transfer
		Knowledge dissemination
Miss-use	Miss-use	Miss-use
Tech-communication	Tech-communication	Tech-communication
Threat Analysis	Threat Analysis	Threat Analysis
		Risk Analysis
Shift-by-wire	Shift-by-wire	Shift-by-wire
Purpose	Purpose	Purpose
		Motivation
		Reason
		Justification
Control	Control	Control
		Influence
		Authority
		Power
Reliance	Reliance	Reliance
		Dependence
		Over-Reliance
Perspectives	Functional Perspective	Fun-perspective
	Technical Perspective	Tech-perspective
	Security Perspective	Sec-perspective
Solution	Solution	Solution
		New Design
		New Component
	Generic solution	Generic solution
		Pre-defined solution
Concept	Concept	Concept
		Notion
	Cybersecurity concept	Cyber-concept
	Security concept	Sec-concept
Skill	Skill	Skill
		Ability
		Expertise
		Competence
Re-factor	Re-factor	Re-factor
		Change
		Adjust
	Shoehorn	Shoehorn
Restriction	Restriction	Restriction
		Not permitted
		Not allowed
Test Track	Test Track	Test Track

		Proving ground
Contract	Contract	Contract
		Contractual responsibility
	Design by Contract	Design by Contract
	Non-Disclosure Agreement	NDA
Policy	Legislation	law
	Regulation	policy
	Guidelines	Best practices
		Guidelines
Knowledge	Component Specific	Component specific knowledge
	Architectural	Architectural knowledge
	Ability	Know-how
		Technical Knowledge
Safety	safety	Functional safety
		Operational safety

Appendix 7: Invitation emails

Research invitation email

Dear Sir/Madam

I am writing to request your support for my doctoral research project on the topic of Automotive Cybersecurity Management. The main aim of the research project is to investigate the sharing of knowledge concerning component integration processes within the automotive industry for improving security for modern connected vehicles. I am doctoral research student studying at Coventry University, my Director of Studies is Dr Alexeis Garcia-Perez (Associate Professor in Cyber Security Management) and my supervisor Professor David Morris from the Faculty of Business and Law. I am conducting a series of interviews and surveys with personnel with experience and involvement with the automotive industry such as yourself.

Please would you be able to spare between 20-30 minutes of your time to complete an online questionnaire? The questions are not related to your specific organisation in particular but about your perception of automotive cybersecurity challenges. The project has been reviewed and approved through the formal Research Ethics procedure at Coventry University. The data collected through the interview will be anonymised, encrypted and treated confidentially. You will have full access to the findings of the research.

Please let me know if any additional information is required. If you are willing to participate, I will send the questionnaire link via email along with a consent form and additional information relating to the research.

Yours Faithfully

Garikayi Madzudzo

Evaluation email

Dear Sir/Madam

I wrote to you sometime last year requesting your support regarding my doctoral research project on the project of Automotive Cybersecurity to which you provided valuable information that l have now used to create a knowledge sharing framework for connected vehicles. The framework takes into consideration all the information gathered during the research's data collection phase from automotive knowledge experts, component suppliers and OEMs, on the need for a coordinated cross-industry approach to component integration.

Could l kindly request your assistance once more in looking at the framework in the attached document and answering the questions at the end of the document at your earliest convenience? The questions are designed to get your overall impression, opinions, suggested improvements and recommendations on whether the framework is capable of assisting the automotive industry address cybersecurity challenges in connected vehicle manufacture via knowledge sharing during component integration.

The project has been reviewed and approved through the formal Research Ethics procedure at Coventry University, and your responses will be anonymised, encrypted and treated confidentially. And, as mentioned in my previous email, you will have full access to the research findings when the research concludes. Please let me know if any additional information is required and thank you in advance for your anticipated assistance.

Yours Faithfully

Garikayi Madzudzo

Appendix 8: Participant information sheet

Project Title: Automotive Cybersecurity Management

Purpose of the Project

The interview is part of a PhD research programme about automotive cybersecurity management. The main aim of the research project is to investigate component integration knowledge sharing approaches within the automotive industry for improving security for modern connected vehicles. The study also investigates how component integration strategies for connected vehicles are affected by knowledge sharing approaches within the auto-domain. The research participants include Original Equipment Manufacturers (OEMs), component manufacturers, and knowledge experts. The objective is to better understand component integration knowledge sharing approaches for connected vehicles within the automotive industry and how those approaches affect automotive cybersecurity strategies employed within the industry.

Why have I been selected?

The main participants of the study are personnel from the automotive industry. You have been selected because of your involvement with the automotive industry.

Do I have to take part?

Participation is voluntary, and it is your individual decision to take part in the study. No disadvantages will arise for you should you decide not to take part. If you decide to withdraw at any time during the study, you can contact either me or my Director of Studies using the details provided below. After withdrawal from the study, your data will be destroyed and will not be used in the study.

What do I have to do?

You will be asked to take part in a semi-structured interview, arranged at the premises of your organisation or any other public building, the location of which is mutually agreed. You will be asked questions about cybersecurity awareness, cybersecurity knowledge sharing, and component integration strategies employed by your organisation.

What are the risks associated with the study?

The interview does not include intimate questions or questions of private nature. The questions are designed to understand processes for sharing cybersecurity-related knowledge within the automotive industry. The questions are also designed to understand how cybersecurity knowledge sharing affects the integration of components for connected vehicles. The research is purely academic, and its core purpose is to contribute to the body of knowledge on automotive cybersecurity. Any personal or controversial information shared by you will remain confidential at all times. The research does not contain any unethical or violating information that will cause harm or discomfort to you or your organisation.

What will happen with the results of the study?

The results of the study will be used for the researcher's PhD thesis. At a later point, parts of the thesis may be published in peer-reviewed academic journals. The results of the study may also be presented at academic conferences.

Who is administering and funding the research?

The research is being conducted by Garikayi Madzudzo, a PhD student at the Centre for Business and Society (CBiS), within the Faculty of Business and Law at Coventry University. Funding is provided CBiS.

Who has reviewed the study?

The project has been reviewed and approved through the formal Research Ethics procedure at Coventry University. The study has also been reviewed by the project supervisors as well as the Faculty's Research Ethics Leader, as part of the University Applied Research Committee (UARC).

Data Protection and Confidentiality

Participants will remain under anonymity in all stages of the study. Information received from every participant will be stored securely on the university's servers. All references to individuals or companies will either be removed or will be given pseudonyms if data is to be included within the submitted study unless express permission has been given. All data will be deleted by 30/11/2020.

Contact Information

Researcher

Garikayi Madzudzo

Centre for Business in Society

Faculty of Business and Law

Coventry University

Director of Studies

Dr Alexeis Perez-Garcia

Associate Professor in Cybersecurity Management

Faculty of Business and Law

Coventry University

Content removed on data protection grounds

Thank you very much for your participation.

<u>Informed Consent Form</u>

Project Title: Automotive Cybersecurity Management

Please tick

1.	I confirm that I have read and understood the participant information sheet for the above-mentioned study.	
2.	I understand that my participation is voluntary, and that I am free to withdraw at any time without providing a reason.	
3.	I understand that the information that I provide will be used for the research purpose stated and for no other purpose	
4.	I understand that the information I provide will be treated in confidence	
	I voluntarily agree to participate in the research project.	
5.	I agree to the interview consultation being audio recorded	
6.	Select only **one** of the following: • I would like my name used and understand what I have said or written as part of this study will be used in reports, publications and other research outputs so that anything I have contributed to this project can be recognised.	
	• I do not want my name used in this project.	

Participant:

__________________________ ______________________________ __________________

Name of Participant   Signature   Date

Researcher:

__________________________ ______________________________ __________________

Name of Researcher   Signature   Date

Part 1: General Information

1. Please state your current Job title/position (Please tick one box)

   ☐ Senior Level Manager (CEO/Director/Executive/General Manager)

   ☐ Mid-Level Manager (Project Director/Project Manager/ Senior Manager)

   ☐ Cybersecurity Consultant

   ☐ Automotive Engineer

   ☐ Software Engineer

   ☐ Integration Engineer

   ☐ Cybersecurity System Specialist

   Other (Please specify): ______________________________

2. Please provide a brief description of your current job role.

   ☐

3. In which category does your organisation fall under (Please select all that apply)

   ☐ OEM (Original Equipment Manufacturer)

   ☐ Component Supplier – 1ST Tier

   ☐ Component Supplier – 2nd Tier

   ☐ Component Supplier (other Tiers)

☐ Automotive Software Company

Other (Please specify): ______________________________

4. Please indicate the length of time (in years) you have been working in the automotive industry. Please tick one box

   1-10 ☐ 11-20 ☐ 21-30 ☐ 31-40 ☐ 41-50 ☐ more than 50 ☐

5. Please indicate the length of time (in years) you have been working in your current role/job. Please tick one box

   1-10 ☐ 11-20 ☐ 21-30 ☐ 31-40 ☐ 41-50 ☐ more than 50 ☐

Part 2: Component Integration

***NB:** Component Integration refers to the act of bringing smaller components into a more comprehensive system or sub-system. Processes and information that assist with the integration of components securely is referred to as integration knowledge within the context of this research.*

6. Does your organisation out-source components for connected vehicles?

   a) Yes (Please state how many organisations you out-source from)

   b) No

7. Does your organisation manufacture components for connected vehicles for other organisations?

a) Yes (Please state how many organisations you manufacture components for)

b) No

8. Could you please describe the type of information your organisation provides with the components you manufacture to aid with component integration? i.e. component design documentation, performance specification test results, security test results etc.

9. For components that your organisation outsources, could you please describe the type of information other organisations provide to your organisation to aid with integration? i.e. component design documentation, performance specification test results, security test results etc.

10. In your opinion, what type(s) of component information that can potentially assist with secure integration should be shared by vehicle manufacturers and component suppliers?

Part 3: Knowledge sharing

N.B: Integration knowledge or component integration knowledge refers to information that can be used to potentially assist with integrating/combining different, often disparate components, subsystems to form a new component, sub-system or a system.

11. Are you aware of any processes for sharing information about components that assists with integration between your organisation and component suppliers that you out-source from?

b) No

11a. (If no) in your opinion what are the barriers to knowledge sharing between your organisation and component suppliers that you out-source from?

12. Does your organisation share integration knowledge with component suppliers?
    a) Yes (Please describe the type of information shared)

b) No (if no what are the barriers that do not permit the sharing of integration knowledge, please explain)

13. What knowledge sharing processes does your organisation employ in the integration of components that you out-source?
    Please explain

14. What knowledge sharing processes does your organisation employ with organisations that you manufacture components for?
    Please explain?

15. Can you please describe knowledge sharing processes that you think will encourage/promote sharing of knowledge in component integration?

16. Are there any restrictions or rules imposed by your organisation on employees regarding knowledge sharing in component integration? **Please explain**

17. In your opinion, does the geographical dispersed structure of the automotive supply chain encourage or discourage knowledge sharing?

18. The trend towards connected vehicles and autonomous vehicles has ushered in cybersecurity challenges into the automotive industry, do you think knowledge sharing might help address those challenges?

Part 4: Knowledge sharing Framework

The study aims to design and develop a knowledge sharing framework to assist with the sharing of knowledge/information that potential can aid with addressing cybersecurity challenges that are a result of component integration challenges born out of the lack of relevant and sufficient knowledge and knowledge sharing processes.

19. Which methods of knowledge sharing do you consider to be appropriate for the sharing of knowledge that promotes the cybersecurity of components (i.e. informal events, project briefings, databases, Best practices, regulation, experience workshops etc)

20. Which level in the organisation should be the knowledge sharing framework focus on? (i.e. organisational level, team level, managerial level, unit level etc)

21. In your opinion, could you please specify the types of knowledge/information that the framework should contain?

22. In your opinion, could you please specify the knowledge sharing processes that the framework should employ?

23. Is there anything that you would like to address that you feel the survey may have missed concerning knowledge sharing in component integration within your organisation?

If you have any comments concerning the overall readability of the questionnaires, format, appropriateness of the measures used, relevance of the questions, time taken to complete the survey or any other possible issues (if any) which might lead to improvements, then you are welcome to do so in the space provided below.

Thank you very much for taking part in this survey. We anticipate that, with your help, the results will assist greatly in cybersecurity knowledge sharing and secure component integration in the automotive industry. If you would like a summary of the results of the research, please enter your name and contact address below.

Name: ....

Address: ....

....

....

Appendix 10: Evaluation questionnaire and feedback

Summary of phase 1 evaluation document

In Round 1, Evaluators were provided with the knowledge sharing framework and a definition of each component.

They were

a. asked to rate the relevance of the following components to their organisation

- Organisational structure
- Human resources
- Communication
- Leadership
- Technological infrastructure
- Regulatory requirements
- Political and legal environment
- Financial resources

b. Indicate any other elements that the current framework does not consider.

c. Asked for their views on the purpose, importance, readiness and usability of the framework.

d. Asked for their views on the clarity, credibility and suitability of the framework.

Summary of phase 2 evaluation document

In phase 2, evaluators were provided with the knowledge sharing framework and a definition of each component.

They were

a. asked to rate the relevance of the following components to their organisation

- Organisational structure
- Human resources
- Business processes
- Communication
- Leadership
- Technological infrastructure
- Regulatory requirements
- Political and legal environment
- Contract agreements
- Social culture

b. Indicate any other elements that the current framework does not consider.

c. Asked for their views on the purpose, importance, readiness and usability of the framework.

d. Asked for their views on the clarity, credibility and suitability of the framework.