Security Aspects of an Empirical Study into the Impact of Digital Transformation via Unified Communication and Collaboration Technologies on the Productivity and Innovation of a Global Automotive Enterprise

Anthony Bolton[1], Leila Goosen[2(✉)], and Elmarie Kritzinger[1]

[1] University of South Africa, Johannesburg 1710, South Africa
49039210@mylife.unisa.ac.za
[2] University of South Africa, Pretoria 0003, South Africa
GooseL@unisa.ac.za

Abstract. The purpose of this paper is to focus on the security aspects of digital transformation through Unified Communication and Collaboration (UC&C) technologies impacting productivity and innovation within a global automotive enterprise. The rationale for the study came from a desire to address the challenge of integrating the complex technology landscape of the Internet of Things in the daily lives of people. This study explored the impact of digitization transformation on people in the context of the automotive industry. A framework for digital transformation via UC&C technologies was designed at a large automotive enterprise. Research leveraged qualitative and quantitative methods, following the implementation of the framework and digital transformation. Observational data combined with data from quantitative enterprise metrics to support analysis. Critical realist interpretation of results suggested that digitally transformed UC&C technologies are changing employees' work practices. The study concludes that digital transformation via UC&C technologies impact productivity and innovation within a global automotive enterprise.

Keywords: Digital transformation · Global automotive enterprise · Impact · Innovation · Productivity · Unified Communication & Collaboration technologies

1 Introduction

Against the background of the current state and future directions in terms of the *security* of the Internet of Things (IoT), automotive enterprises are characterised by the complex global nature of their enterprise operations, with the increasing technical complexity of the Internet of Things influencing manufacturing and vehicle systems [1]. Large automotive Original Equipment Manufacturers (OEM), such as General Motors (GM), face unique challenges in transforming their enterprises into the IoT and Industry 4.0 age, due to their scale and broad dependency on global supply chain and

H. Venter et al. (Eds.): ISSA 2019, CCIS 1166, pp. 99–113, 2020.
https://doi.org/10.1007/978-3-030-43276-8_8

product partnerships. Enterprises such as GM have a long history of industrial development (GM is a 109-year-old enterprise) and must contend with deeply rooted enterprise processes corporate culture. Shared challenges include transforming employee communication regarding increased efficiency, convenience and speed across a global workforce.

Multiple architectures, such as the Internet of Things Architecture (IoT-A) [2] and the Reference Model for Industrie 4.0 (RAMI4.0) [3], have emerged and developed in recent years. In their paper on the *security* and privacy of Internet of Things architectures and systems, however, Vasilomanolakis et al. [4] indicated that no ubiquitous industry standard, framework or reference architecture has been adopted. The lack of an industry-wide architecture increases the challenges associated with the broader horizontal digital transformation of the progressive enterprise. The absence of an industry standard framework for digital transformation can also lead to increased complexity and a lack of consistency in the experience of users. A robust transformation plan and deployment framework, tailored to an enterprise's specific business model, is required to avoid these issues. The requirement for structured planning, integrated into the business model of the target enterprise is increasingly essential where the digital transformation affects employee and customer communication. Digital communication is increasingly vital in Industry 4.0 and IoT enabled business models. Wolf [5] reminds us that digitalization has the propensity to transform industries and business models, rapidly affecting the entire enterprise involved. The transformation may be digital, but it is planned, led and executed by people.

In light of the afore-mentioned, the purpose of this paper is therefore to focus on the security aspects of digital transformation through UC&C technologies impacting productivity and innovation within a global automotive enterprise.

2 Enterprise Digital Transformation

2.1 Motivators for Enterprise Digital Transformation

In terms of motivators for enterprise digital transformation, and against the background of *security* for the digital world within an ethical framework, the Digital Enlightment Forum [6] pointed out the digital disruption is profoundly impacting industry and society. Enterprises that move ahead with digital transformation stand to disrupt industry, reaching new markets and customers almost immediately. Entry into expanded digital markets and customer bases in many cases can be achieved, while generating savings and optimizing gross profit margins [7]. Productivity impact can be introduced rapidly through combinatorial digital innovation. As the age of the fourth industrial revolution emerges, digital transformation will be a catalyst in defining and iterative redefining of the modern enterprise.

2.2 Challenges to Digital Transformation

Enterprise Challenges Relating to Model, Vision, Culture and Security: As enterprises transform to digital business models, they become more susceptible to the impact of *cybersecurity* attacks and infiltration. Data, intellectual property, business process structure, private customer information, financial reserves and reputation are increasingly at risk through exposure to digital attacks, malware and cyber-crime.

A robust digital and *cybersecurity* strategy is required to replace physical forms of *security*. A recent global survey of IT and *security* professionals engaged in digital transformation, sponsored by Dell [8], highlighted that 98% of the enterprises surveyed were facing challenges securing digital transformation technologies and only 11% were confident about their digital transformation *security* plan. Table 1 depicts the top *security* challenges outlined by the latter white paper [8].

Table 1. Digital transformation security challenges.

1	Need to secure technologies without additional resources
2	Increased risk of security breach
3	Finding a balance between security and employee productivity
4	Reduced control over system access and data
5	Finding the right expertise to support new technologies
6	Security tools not keeping up with changing needs
7	Increased vulnerabilities due to siloed security tools

3 Internet of Things

3.1 Origins of the Internet of Things

Advanced Research Projects Agency Network (ARPANET). Against the background of the implementation, management, and *security* related to cloud computing, Rittinghouse and Ransome [9] explained that in terms of the history of the Advanced Research Projects Agency Network (ARPANET), the decision was taken that the network would be entirely decentralized. No single master computer on the network would act as a central processing point responsible for the sorting and routing of data packets from source to destination. This design resulted in a more complex architecture. However, it also increased resilience over a centralized design. Advanced Research Projects Agency (ARPA) computer sites would be linked together and share the routing of packets [9]. This decision led to the establishment of modern routing and switching techniques for packet switching, forwarding and routing. The project team decided that a dedicated computer would manage routing and switching functions on each local network called an Interface Message Processor (IMP).

In December of 1968, Bolt, Beranek and Newman (BBN) was awarded the contract to build ARPANET's first IMPs, the first of which was delivered in only nine months and installed on August 30, 1969, in the Network Measurements Centre of the University of California at Los Angeles [10]. The second ARPANET node and IMP was installed and connected to an early hypertext system at Stanford Research Institute (SRI) [9]. The third ARPANET node, located at the University of California at Santa Barbara, and the fourth node at the University of Utah, were installed and connected by

December 1969 [11]. The node at the University of Santa Barbara connected to an IBM 360/75, while the node at the University of Utah connected using the Tenex operating system.

3.2 Evolution of IoT and Cognitive Internet

The Combinatorial Effects of Mobile, Transmission Control Protocol (TCP)/ Internet Protocol (IP) and Sensor Technologies. Especially in terms of data *security* and privacy in the Internet of Things environment, Internet connectivity is required, irrespective of fixed (wired) or mobile (wireless) use-cases [12]. The integration of mobile and sensor technology plays an increasingly prevalent role in IoT functional use-cases and solutions. Sensors that are a part of solutions, such as connected vehicles, personal devices, autonomous systems and drones, require fast, reliable and efficient methods of mobile communication [13]. The concept of sensors connecting to other sensors is expanding and providing opportunities to develop a plethora of fixed-to-mobile, fixed-to-fixed and mobile-to-mobile solutions [14].

Content and Information Centric Networking and Communication. Because of the demands of the IoT and mass generation of contextual data and information, Context Centric Networking (CCN), as it develops from concept to reality, is likely to further transform the Internet at an infrastructure level with the addition of new developments in routing, packet forwarding, cipher and *security* technologies [15]. Key differentiators of the CCN approach versus traditional Internet networking and data transfer are the proposed features relating to in-network caching, multi-party communication via smart replication and interaction models that decouple senders and receivers of data and information.

Building on the IoT paradigm, the next section of this paper will focus on reviewing some of the literature surrounding the emergence of Industry 4.0, considered to be the fourth industrial revolution, and Unified Communications and Collaboration technologies, which provides a pathway for cyber-physical integration in a digital world.

4 Industry 4.0

4.1 Challenges to Industry 4.0 Adoption

Challenges for adoption exist in a number of areas, including increased risk of *security*, counterfeiting, data analytics, machine to machine communication, cyber-physical integration and autonomous systems [16].

Security and Counterfeiting: The technology and process innovation that sits at the core of Industry 4.0 has the potential to act as a catalyst in the further enablement of counterfeiting of services and goods. With Industry 4.0 new processes, such as 3D printing and greater leverage of information, shared and contained in digital systems, can be both compromised and harnessed to rapidly duplicate services and products by illicit organisations. Highlights from the *Information Security* Solutions (Europe) 2015 conference, especially related to challenges in anti-counterfeiting, pointed out that protection measures, such as global trust infrastructure for the sharing of IoT data, approaches to robust authentication and verification methods will be required for industry 4.0 and manufacturing [17]. These countermeasures for the reliable transport of industrial data and information are likely, over time, to parallel the systems that are currently employed to protect critical financial transactions and information handled by the banking industry.

5 Research Design and Methodology

A sample group of 2,000 employees, chosen as representative across all GM business functions and regions, were invited to participate in the survey, while twenty-one employees agreed to participate in the interviews. The sample of interview participants again represented a broad mix of enterprise functions, with global and regional remit established within the scope of the study.

Table 2 represents data obtained regarding some of the questions posed to the interview participants, including each of their self-assessed technical proficiency, enterprise function at General Motors, type of function, tenure in role and years in industry. Participants ranged from novice users of technology through to highly experienced.

6 Empirical Research

6.1 Case Study Structure and Timeline

Scope and Timeline. Figure 1 provides a high-level timeline associated with the broader Enhanced Unified Communication and Collaboration (E-UC&C) technologies transformation deployment. Within the course of the GM case study, the limitations of a technology and user deployment strategy with an isolated focus on only UC&C core technology components were identified. In order to establish a fully integrated and scalable framework and technical architecture for UC&C technologies deployment, an enhanced framework, inclusive of dependent and adjacent technology systems (Network Transport, Quality of Service, Session Management, *Cybersecurity*, Telecom Expense Management & Operations), was developed.

6.2 Architectural Framework for Enhanced UC&C (E-UC&C)

Framework Primary Domain Modules (PDMs). The primary domain modules of the E-UC&C framework served as modular reference architectures for service governance, core technology services, service integration and service operation. These modules describe the sub-processes, stakeholders, interfaces and technologies, which were combined to deliver solutions aligned to the broader framework. Adherence to the framework facilitated high degrees of compatibility and re-use of common components, for example, Network Transport, Network Quality of Service, Voice and Video Session Management, Network and Voice *Security*, Video and Voice Transcoding, Change Management and Integrated Cross-Platform Monitoring.

Table 2. Interview participants' demographics.

Proficiency	Enterprise function	Function type	Years in role	Years in industry
Proficient	Facilities	Global	14 months	25
Fairly proficient/know enough	Design	Global	2	32
Proficient	Joint ventures	Regional	2	22
Highly proficient		Global	4	7
Know enough	Finance	Global	2	31
Expert	Manufacturing	Global	4	4
Expert	Sales & marketing	Global	3½	4
Highly proficient	Supply chain	Global	9 months	20
Expert	Real estate	Global	11	20
Highly proficient	Sales & marketing	Global	2	37
Proficient	Legal & HR	Global	3	28
Proficient	Finance & marketing	Global	3½	36
Proficient/know enough	Business operations	Global	1 month	13
Highly proficient	Share services IT	Global	2½	4
Proficient		Global	2	10
Highly proficient	Operations	Global	3 years and 9 months	3 and 9 months
Expert	Security	Global	2	4
Highly proficient	engineering & design	Global	2 weeks	4
Expert	Shared services IT	Global	3	4
Highly proficient	Human resources	Global	1 year 6 months	4
Know enough	Design/manufacturing	Regional	2 years 3 months	33½

6.3 Deployed Framework

Core Governance Domain. Please note that since the Core Governance Domain did not particularly relate to *security* issues, it is not discussed in any detail in this paper. Further details can, however, be accessed in Bolton, Goosen and Kritzinger [18].

Operational Management Domain. The Operational Management Domain aligns to the horizontal processes that facilitate system operation, delivered via four integrated modules. The four primary domains specified governance and processes that facilitated tactical delivery and coordination of individual initiatives and programs. Ever-green processes designed for driving end user adoption and *security* compliance and assurance, and supporting end user service and infrastructure operations, were also specified.

In the preliminary framework, design *security* was inferred within the **Integrated Feature Domain**, broadly aligned with the individually specified technology modules.

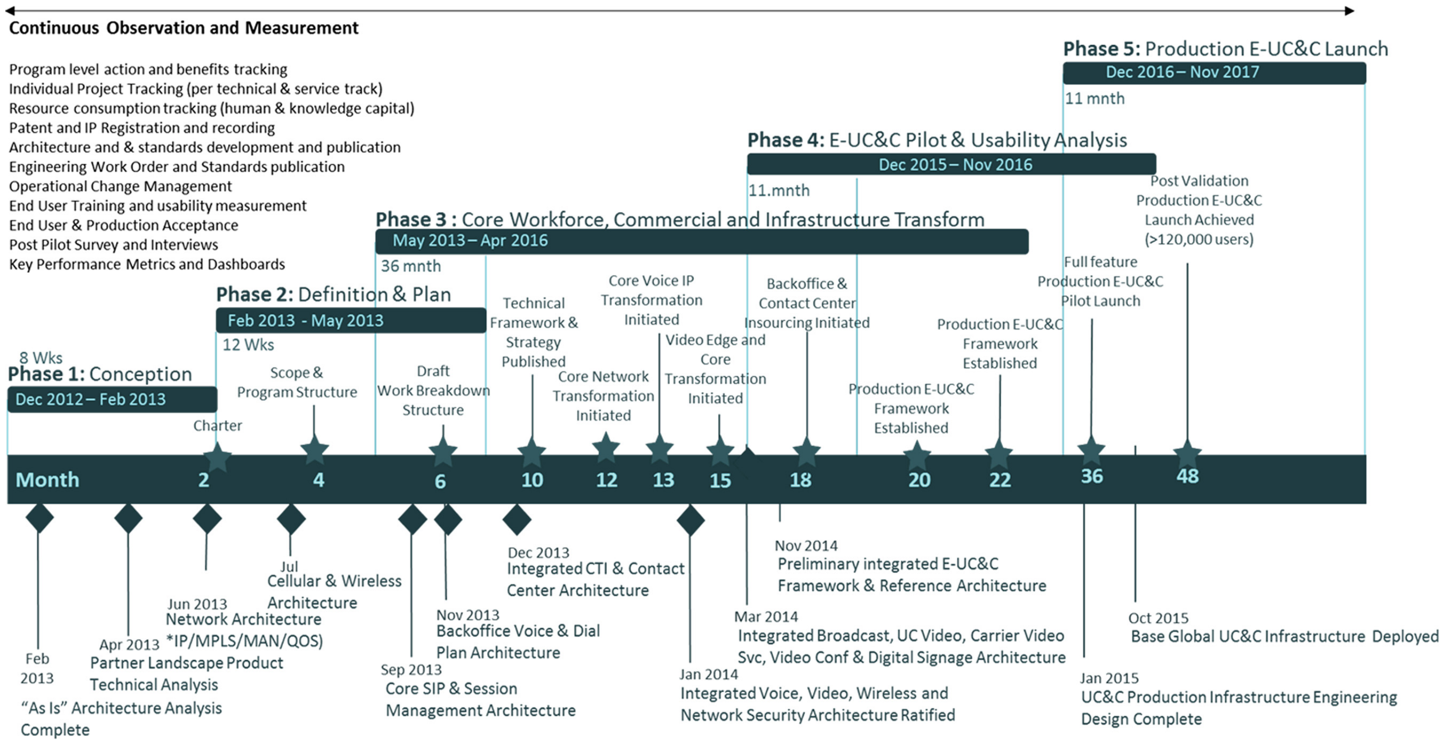

Fig. 1. High-level timeline and milestone summary – GM case study.

As the framework was deployed, the necessity for a dedicated module to provide focus on *security*, data loss protection and risk management were identified. The primary drivers for abstraction of the *security* requirements into a dedicated module in the final iteration of the production framework included:

- Enterprise drivers at a corporate level driving higher standards of policy specification and compliance associated with Data Retention and Loss Protection (DRLP) and *cybersecurity*.
- The need to bolster risk management, *cybersecurity* and data loss protection via defined *security* policy and auditable control processes.
- Identification of new sources of potential data loss risk and data retention strategies, because of the introduction of new digital communication services, such as Instant Messaging with integrated file and application sharing functionality.
- Identification that *security* and data risk and management definition within the Integrated Feature Domain modules tended to be focused on specific technology applications versus having a broad system-wide focus.
- The shift to a broader system-wide focused module within the production framework. The transformation of communication via a digital medium did not result in a 1:1 translation of old ways of communicating to a digital version. Messier [19] highlighted how the digitally transformed communication features of UC had increased the adoption of IP-based communication systems. Messier [19] also suggested that risk assessments were required to facilitate better decision making relating to technology selection and adoption. Architectures and solutions provided a broader integrated end state, which integrated chat with rich real-time video, file sharing, application sharing and voice communication. More data was stored electronically and digitally mediated. In Europe, Wong [20] argued that mandated *security* processes and policies were required to minimize data *security* breaches, as the level of electronically stored information created by the transition to digitally mediated technologies and communication increased.

Integrated Feature Domain. The Integrated Feature Domain contained the core technologies associated with features accessed and leveraged by end users within the scope of the communication solution. These features directly aligned with functionality that was embedded directly within technologies, such as the UC&C client (Skype for GM), video collaboration suites and integrated contact centre advisor applications. Technologies within the Integrated Feature Domain modules were specified at the application layer and applied in specific technologies for leverage by end users. For example, Instant Messaging and chat were delivered in multiple forms of standalone and embedded presentation to the end users, such as Contact Centre chat and Skype chat. However, these systems relied on shared services from the **Unified Services Domain** for integration and the provision of standard services, like routing, transport and *security* controls.

Figure 3 in [18] depicts a functional architecture proposed to articulate the primary technology service categories and specific technologies engaged in the delivery of a feature-rich, UC&C technologies digital transformation platform. This functional architecture built on the concepts and foundational UC&C technologies model proposed by Reimer and Taing [21], with the addition of modules and technologies associated with "security, service management and federated extensibility" [18, p. 6]. The enhanced functional architecture was leveraged as a basis for the core modules included in the GM framework. The framework was not restricted to the inclusion of specific technologies and had the flexibility to be adapted to expand or contract as the needs of the enterprise that it was applied to changed.

The adapted model also includes an expansion from the framework proposed by Rogers [22], through the inclusion of a module associated with data protection and *security* being added in consideration of recent Global Data Protection Regulation (GDPR) and *cybersecurity* priorities within industry.

Unified Services Domain. Specification and development of the Unified Services Domain structure were influenced by the distributed product realization environment [23] and eXtensible Distributed Product Realization framework proposed by Choi, Panchal, Allen, Rosen and Mistree [24]. Nakajima, Ishikawa and Tokunaga [25] highlighted the challenges of integrating complex enterprise networks and existing systems, such as corporate billing systems, with ubiquitous computing and communication systems. The challenges that Nakajima et al. [25] addressed in their proposed InterUbicomp framework showed significant parallels to the challenges encountered when developing an enterprise scale, digitally transformed, multi-modal and medium solution architecture. These challenges included heterogeneous service integration, context-aware embedded services, application specific networking, environmentally embedded devices, peer-to-peer communication, service survivability and *security*.

7 Results and Interpretation

The results from the current state assessment summarized in Fig. 2 were used as a reference asset for the development of the transformation architecture and resulting E-UC&C technologies framework reviewed in Sect. 6, as well as a transformation repository and architecture assessment process. Within each layer, the current state technical architectural components were summarized, along with pre-transformation limitations established from legacy baseline operational metrics and enterprise stakeholder feedback. Figure 2 presents the grid with the Instant Messaging and Textual Collaboration layer highlighted.

Fig. 2. Technology and service transformation grid.

7.1 Impact on Productivity

Digitally Transformed Multi-channel Persona Capabilities Facilitated Through a Consolidated Software Client Impact the Perception of Increased Productivity in Individuals. Findings from the research indicated that digitally transformation established via UC&C technologies and systems facilitated opportunities for users to establish and maintain changing work practices and relationships with colleagues and enterprise partners. Relationship building was enhanced and enabled through the facility of a virtual team and peer engagement. The research data showed that users perceived the ability to flexibly escalate communication through different levels and modes of communication to assist in the building of relationships through rich information sharing in a virtual workspace. Findings within the study also displayed that the consolidated features within the UC&C client, combined with the easy to use and adopt interface, resulted in many users establishing increased enterprise efficiency and changing work practices.

A small number of users reported having some difficulty in easily using and adopting or changing work practices to the UC&C technologies; however, they still reported these technologies as having the potential to impact their productivity. After being introduced to the digital technologies and UC&C features, most users preferred to keep their 'new' technologies, leading to legacy reduction and elimination. Users described the digital technologies as increasing the convenience and speed of their communication processes through the UC&C client, as a result of finding access to all of the features in one technology. The convenience and speed benefits of having one technology to access multiple channels for communication, both within the office and remotely, when travelling or at home, is likely to be associated with end users' perception of impact on productivity. The more convenience and speed are involved in doing something and/or executing a task, the more productive users are when executing the task.

Digitally Transformed Social Presence and Real-Time Status Indicators Positively Impact the Perception of Increased Productivity in Individual and Team Performance. Findings indicated that the virtual persona and presence established by the end users had a positive effect on personal productivity, as it increased the opportunity to engage in real-time collaboration when needed. Feedback from end users further showed that digital presence indicators were useful in identifying other users or groups, who may be available for immediate ad-hoc communication and engagement.

Also, it is likely that the custom presence indicators helped to set a baseline expectation for the requesting party in establishing the probable timeframe for response. For example, when a user is in an ad-hoc or scheduled meeting, that user's presence and status will be set to busy, indicating that the user is already engaged in collaboration or work of some form. When a user is presenting using their laptop or PC, the presence indicator is set to presenting, and blocks instant messaging pop-ups for the requested user, setting the expectation that an immediate response is unlikely to occur. It is likely that users reporting their experience of the UC&C technologies as having the effect of removing the sense of distance with their peers and partners was tied to the presence indicators, as they get real-time status views of their colleagues' location and engagement status. This status developed an arguable perception of virtual presence.

Users can additionally place commentary on what their current or planned daily activities are in the 'what's happening today' field of the UC&C client, further establishing the digital presence and persona.

7.2 Impact on Innovation

Digitally Transformed UC&C Technologies Can Impact Engagement in Innovation Generating Activities Across the Global Automotive Enterprise Value Chain. Four factors relating to innovation was identified within the study, which are related to changing work practices, collaboration, creativity and generating savings.

Users reported that the digitally transformed UC&C technologies led to changing work practices and impacted their ability to engage in collaboration. Users also found that multi-channel features facilitated richer virtual engagements and supported creative engagement, even when users were remote from each other. In their creativity processes, the ability to engage in an ad-hoc collaboration, as needed, helped users capitalize when they had ideas, or needed problems and questions quickly addressed. Engagement, which increased enterprise efficiency through the digitally transformed UC&C technologies, also increased speed-to-action creative thoughts or tasks. It is reasonable to assume that the convenience and speed of engagement offered by the UC&C technologies helped to maintain convenience and speed in creative collaboration, tied to innovation generation, such as sharing and working through new ideas, or rapidly developing plans and proof of concepts.

The factor related to convenience and speed of the UC&C technologies is likely to align with the changing work practices that the users reported. Users' changing work practices reflected the capabilities of the UC&C technologies and digitally transformed methods. Easy to use and adopt technologies, combined with positive results from convenient and speedy engagement, in a context of desired- versus restricted-schedule, lead users to positively associate these technologies with supporting their innovation and creativity processes. Many users identified generating savings associated with leveraging the digitally transformed UC&C technologies within their changing work practices and this is likely due to users seeing the generation of innovation as an asset to the enterprise. Innovation leads to new products, or product enhancement, and ultimately higher margins and revenue. If the users can engage and drive more innovation through digitally transformed technologies, or speed up innovation generation, the enterprise will benefit financially.

7.3 Impact via Digital Transformation Through UC&C Technologies

Digital transformation achieved through UC&C technologies results in increased inclusion and engagement of individuals and teams across the global automotive enterprise. Evaluation of the end user survey and interviews supported a view that communication delivered through the digital transformation of technologies enhanced the ability of people and groups towards engagement and collaboration. Findings from the research data show that users reported a positive experience aligned with leverage of the multi-channel communication features associated with UC&C technologies. Through the use of these features, users reported that it was easier to engage and collaborate efficiently with virtual teams. Users described the ability to engage in ad-hoc meetings with peers and virtual teams and obtaining answers to questions quickly.

These observations contrast with the reduction and elimination of legacy communication methods that required face-to-face communication to facilitate information exchange at any level beyond audio conference or basic slide sharing using external technologies. Users also described positive attitudes relating to the ability to engage personally with peers and partners when working in remote locations. The new digitally transformed capabilities made it easier to include other parties in media-rich virtual meetings and facilitate their direct participation. Tracking of feature-use across regions and room-to-room telepresence engagements supported the view of increased cross region and function engagement, inferring a high level of inclusion of people in virtual meetings outside of their local workplace locations.

8 Discussion and Conclusion

The purpose of this paper was to focus on the *security* aspects related to digital transformation, implemented through UC&C technologies, which impact productivity and innovation within a global automotive enterprise. Some of these included e.g. the *security* challenges to enterprise digital transformation, the *security* of the Internet of Things, and challenges to Industry 4.0 adoption, including increased risks related to *security* and counterfeiting. The research design and methodology incorporated e.g. a survey of IT and *security* professionals.

In terms of the structure, scope and timeline of the case study used in the empirical research, the enhanced framework was inclusive of dependent and adjacent technology systems, including e.g. *cybersecurity*. Adherence to the architectural framework for E-UC&C and PDMs facilitated high degrees of compatibility and re-use of common components, for example, Network and Voice *Security*. With regard to the Operational Management Domain in the deployed framework, ever-green processes designed for e.g. driving end user adoption and *security* compliance and assurance were specified. In the preliminary framework, design *security* was inferred within the Integrated Feature Domain, broadly aligned with the individually specified technology modules. Several systems relied on shared services from the Unified Services Domain for integration and the provision of standard services, like routing, transport and *security* controls.

Finally, the transformation grid presented as part of the results and interpretation section focused on four core layers, including Transport and *Security*.

A theory of enhancement through the lens of a UC&C technologies model and meta-framework for digital transformation have been analysed. The meta-framework and theoretical transformation model align to an enhanced UC&C technologies architecture. An empirical study focusing on the effects of the proposed E-UC&C technologies meta-framework and theoretical model for digital transformation was carried out – this involved a multi-year single subject case study of the General Motors global automotive enterprise. General Motors incorporated the E-UC&C meta-framework and theoretical model in their corporate strategy for Industry 4.0. E-UC&C technologies were adopted and applied to guide digital transformation for employees within that initiative. Analysis of the employee adoption rates, feature-use and experiential observation strongly suggest that digital transformation, delivered through a holistic framework for E-UC&C technologies, can have a positive impact on employee productivity.

If applied through a holistic framework including UC&C technologies, digital transformation can also impact an enterprise's opportunities towards generating savings and innovation, as well as increased enterprise efficiency, contributing positively to market differentiation. Further research is suggested to evaluate the application of the meta-framework and associated theories of digital transformation through UC&C technologies to other industries and enterprises experiencing business model digitization.

References

1. Dahabiyeh, L.: The security of internet of things: current state and future directions. In: Themistocleous, M., Morabito, V. (eds.) EMCIS 2017. LNBIP, vol. 299, pp. 414–420. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-65930-5_33
2. Holler, J., Tsiatsis, V., Mulligan, C., Karnouskos, S., Boyle, D.: From Machine to Machine to the Internet of Things: Introduction to a New Age of Intelligence. Academic Press Inc, Orlando (2014)
3. Sendler, U.: The Internet of Things: Industrie 4.0 Unleashed. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-54904-9
4. Vasilomanolakis, E., Daubert, J., Luthra, M., Gazis, V., Wiesmaier, A., Kikras, P.: On the security and privacy of internet of things architectures and systems. In: International Workshop on Secure Internet of Things (SIoT) (2015)
5. Wolf, G.: New challenges of the digital transformation: the comeback of the vision-mission system. In: Klewes, J., Popp, D., Rost-Hein, M. (eds.) Out-thinking Organizational Communications. MP, pp. 113–128. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-41845-2_9
6. Digital Enlightment Forum: Security for the Digital World Within an Ethical Framework. IOS Press, Amsterdam (2016)
7. Brush, K.: The Power of One: You're The Boss. CreateSpace Independent Publishing Platform, Scotts Valley (2012)
8. Dimensional Research, Digital Transformation - A Survey of IT and Security Professionals. https://software.dell.com/whitepaper/global-survey-digital-transformation-security-survey8113164, last accessed 2016/10/21
9. Rittinghouse, J., Ransome, J.: Cloud Computing: Implementation, Management, and Security. CRC Press, Boca Raton (2016)
10. Poole, H., Lambert, L., Woodford, C., Moschovitis, C.: The Internet: a Historical Encyclopedia, vol. 1. ABC-Clio, Santa Barbara (2005)
11. Weber, S.: The Internet. Infobase Publishing, New York (2003)
12. Varadharajan, V., Bansal, S.: Data security and privacy in the internet of things (IoT) environment. In: Mahmood, Z. (ed.) Connectivity Frameworks for Smart Devices. CCN, pp. 261–281. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-33124-9_11
13. Mavromoustakis, C., Mastorakis, G., Batalla, J.: Internet of Things (IoT) in 5G Mobile Technologies. Springer, New York (2016). https://doi.org/10.1007/978-3-319-30913-2
14. Slama, D., Puhlmann, F., Morrish, J., Bhatnagar, R.: Enterprise IoT: Strategies and Best Practices for Connected Products and Services. O'Reilly Media, Sebastopol (2015)

15. Guimaraes, P., et al.: Experimenting content-centric networks in the future internet testbed environment. In: IEEE International Conference on Communications Workshops (ICC), pp. 1383–1387 (2013)
16. Kagermann, H., Anderl, R., Gausemeier, J., Schuh, G., Wahlster, W.: Industrie 4.0 in a Global Context: Strategies for Cooperating with International Partners. Herbert Utz Verlag, Munich (2016)
17. Thiel, C.: Industry 4.0 - challenges in anti-counterfeiting. In: Reimer, H. (ed.) ISSE 2015: Highlights of the Information Security Solutions Europe 2015 Conference, pp. 111–119. Springer, New York (2015). https://doi.org/10.1007/978-3-658-10934-9_10
18. Bolton, A., Goosen, L., Kritzinger, E.: Enterprise digitization enablement through unified communication and collaboration. In: Proceedings of the Annual Conference of the South African Institute of Computer Scientists and Information Technologists, Johannesburg (2016)
19. Messier, R.: Collaboration with Cloud Computing: Security, Social Media and Unified Communication. Elsevier, London (2014)
20. Wong, R.: Data Security Breaches and Privacy in Europe. Springer, London (2013)
21. Reimer, K., Taing, S.: Unified communications. Bus. Inf. Syst. Eng. **1**(4), 326–330 (2009)
22. Rogers, E.: Diffusion of Innovations, 4th edn. The Free Press, New York (2010)
23. Gerhard, J., Rosen, D., Allen, J., Mistree, F.: A distributed product realization environment for design and manufacturing. J. Comput. Inf. Sci. Eng. **1**(3), 235–244 (2001)
24. Choi, H.-J., Panchal, J., Allen, J., Rosen, D., Mistree, F.: Towards a standardized engineering framework for distributed, collaborative product realization. In: Proceedings of the ASME Design Engineering Technical Conference (DETC 2003), pp. 1–11 (2003)
25. Nakajima, T., Ishikawa, H., Tokunaga, E.: Technology challenges for building Internet-scale ubiquitous computing. In: Proceedings of the Seventh IEEE International Workshop on Object-Oriented Real-Time Dependable Systems (2002)