Asian Journal of Mathematics and Computer Research

Volume 31, Issue 4, Page 90-105, 2024; Article no.AJOMCOR.12559
ISSN: 2395-4205 (P), ISSN: 2395-4213 (O)

Digital Twin in Industrial Networks: A Cost-benefit Analysis in Operational Technology

Fabian Koke [a,b*], Tim Senn [a] and Raden Aswin Rahadi [b]

[a] School of Business, University of Applied Sciences and Arts Northwestern Switzerland FHNW, Switzerland.
[b] School of Business and Management, Institut Teknologi Bandung, Indonesia.

Authors' contributions

This work was carried out in collaboration among all authors. All authors read and approved the final manuscript.

Article Information

DOI: https://doi.org/10.56557/ajomcor/2024/v31i49004

Open Peer Review History:
This journal follows the Advanced Open Peer Review policy. Identity of the Reviewers, Editor(s) and additional Reviewers, peer review comments, different versions of the manuscript, comments of the editors, etc are available here: https://prh.ikprress.org/review-history/12559

Short Research Article

Received: 12/10/2024
Accepted: 14/12/2024
Published: 20/12/2024

Abstract

Security in Operational Technology (OT) networks faces different challenges when compared with traditional networks. In OT environments, availability and visibility are prioritized over data integrity, leading to unique cybersecurity concerns. The start-up *narrowin* offers a digital twin software solution with which companies can scan their existing network topology. With this visibility, they can optimize and monitor their infrastructure and ensure the availability of the OT network. However, despite the known benefits of digital twins, their adoption in the industry is limited.

This research aims to identify the underlying reasons for the limited adoption with a newly developed approach to understand customer requirements. Aligning the digital twin software with current market needs could foster wider adoption and therefore, reduce security risks in OT networks through increased visibility. A use-case-driven roadmap was developed to guide future software enhancements.

**Corresponding author: Email: fabian_koke@sbm-itb.ac.id, Fabian.koke@students.fhnw.ch;*

Cite as: *Koke, Fabian, Tim Senn, and Raden Aswin Rahadi. 2024. "Digital Twin in Industrial Networks: A Cost-Benefit Analysis in Operational Technology". Asian Journal of Mathematics and Computer Research 31 (4):90-105. https://doi.org/10.56557/ajomcor/2024/v31i49004.*

The research process consisted of interviews and workshops with experts active in OT-network environments. The insights of these interviews were used to identify product features, highlighting gaps in the current implementation of the digital twin. A comprehensive Cost-benefit analysis (CBA) evaluated product features for their market value. Finally, the interview findings and the CBA were combined to create a suitable persona, with which the current gaps of the digital twin can be targeted.
To conclude, the thesis provides insights on how customer specific challenges of a digital twin software can be addressed. The research contributes to the goal of enhancing cyber security and operational excellence in industrial environments.

Keywords: *Cost-benefit analysis; product management; operational technology; OT network topology; digital twin; cyber security in OT; industrial networks.*

1 Introduction

The most used definition comes from Gartner [1]: "Operational technology (OT) is hardware and software that detects or causes a change, through the direct monitoring and/or control of industrial equipment, assets, processes, and events."

According to Stouffer [2] the applications range from industrial control systems, building automation systems, transportation systems, physical access control systems, physical environment monitoring systems to physical environment measurement systems. OT systems are already in wide use, and trends like automatization and digitalization increases the demand further. As OT systems become increasingly connected to IT networks and the Internet, they face greater cybersecurity risks. The study of Schwab & Poujol [3] shows that:

- Three-quarters of the researched companies confirm that OT cyber security is a major concern
- A similar share states that it is likely to become a victim of a cyber security attack in the OT environment

Due to the pressure of optimization and the need of real-time insights, communication networks in companies are growing fast. However, security measures often fail to keep pace with the expansion of communication networks. One problem is the visibility in the network. Companies can only protect devices if they are aware of it. *narrowin*, a Swiss start-up, offers a software with which a visualization of the topology of the OT-network is possible through creating a digital twin. It allows companies to establish security measures and highlights weak points in the OT-network.

It has yet to be further analyzed which features and use cases customers find lacking. In addition, a suitable approach to identify said features is not defined. The research followed an iterative approach to develop a process for identifying customer requirements, combining feedback from industry experts with workshop results. These results were then evaluated using a cost-benefit analysis.

1.1 Research objective

The main research objective of this study is to identify a method by which customer requirements can be extracted and evaluated. The second main research objective is how customers of the topology digital twin software perceive the benefits of software features. The third main research objective is to compare the benefits with the costs. The resulting valuable product features are then summarized in a user profile, which helps *narrowin* in developing the software aligned with market needs.

The following process is planned:

- To determine how OT is used in the industrial industry.
- To investigate how Cyber security in OT works.
- To identify how OT users perceive the OT-network digital twin
- To research suitable product management methods to identify relevant product features, use cases and target groups in the OT environment.

- To conduct a cost-benefit analysis (CBA) for product features of the digital twin.
- To determine new user profiles based on previous information.

The study addressed the gap of a requirement identification process as well as a tool to prioritize the identified requirements according to the urgency of market specialists. *narrowin* could adapt their software to be better in line with customer requirements and therefore, increase cyber security of companies.

Finally, the study covers a relevant topic in times where OT equipment becomes a target for more sophisticated cyber security attacks, targeting infrastructure like power plants or government facilities [4]. The research provides an approach how an OT cyber security software can be improved and therefore, OT equipment is better protected against attacks.

2 Literature Review

This literature review analyzes the existing theories in OT, in the IT/OT convergence, and shows an overview of the cyber security threats in OT. Data sources included well-established cybersecurity frameworks such as NIST, ISACA, and other expert institutions.

In order to identify a process of customer requirements different product management methods were identified and combined to be suitable for the research.

2.1 Operational Technology (OT)

OT is often compared with IT (Informational technology). While IT covers the backbone of the company, including email, finances, HR, other software, or the cloud, OT specifically defines hardware and software used to monitor and control the production procedure [5]. Applications range from the chemical sector to the communications sector, manufacturing, dams, food and agriculture, financial services, emergency services, or also government facilities [6]. Historically, these systems were operated separately from other networks and run on special proprietary protocols [7]. OT systems are nowadays often decades old and are slowly upgraded with connectivity due to business requirements of having live information about the production process, making them especially vulnerable. Often only a small number of staff can operate these machines [5].

The differences between IT and OT include specialized OT vendors such as Schneider Electric, Honeywell, Siemens, and Mitsubishi Electric. IT on the other hand relies on well-known equipment providers like Microsoft, Apple, or Samsung. The purpose of IT is to manage business applications, while OT maintains production with real-time and time critical responses. Uptime is of most importance, while in IT maintenance is plannable e.g. on weekends. Security in IT related to the CIA triad, focusing on customer and corporate data while in OT the availability and the equipment status is the highest concern. IT runs primarily on IP based and industry standardized wired applications, while OT consists of specialized control networks of proprietary manufacturers with mixed protocols. Meanwhile the lifetime of IT is around 3-5 years and often 10-20 years or higher in OT [8].

A phenomenon called “IT/OT convergence” is observed in the literature [9]. The convergence of OT and IT enables improved automation, optimization, and greater transparency across supply chain operations [10]. Through the implementation of IIoT sensors and actuators, it becomes possible to do remote control as well as increasing process efficiency [11]. Murray et al., [4] describe the convergence comprehensively: ranging from the difficulty in teams (low and agile hierarchy in IT, established controls in production and OT) to licensing products enterprise-wide in IT, while OT is often an ad-hoc deployment and on plant level. Together with the different aforementioned priorities (confidentiality vs availability) of IT and OT, this leads to problems among the technical employees, worsening OT security.

OT systems often cannot be upgraded with the latest firmware, leaving them vulnerable to security threats. This issue is frequently addressed through network architecture concepts, such as network segmentation and OT device isolation [6].

2.2 Cyber security in OT

In contrast to IT, which emphasizes the CIA triad (Confidentiality, Integrity, Availability), OT focuses more on safety, reliability, and availability (NCSC UK, 2017).

The vulnerabilities are according to Enisa [12]: Deficient physical security, inadequate authentication, improper encryption, unnecessary open ports, improper patch management capabilities, non-existing monitoring process, inexperienced employees, and the two wrong beliefs of security through obscurity (air-gapped) and that OT systems are isolated. These vulnerabilities can be exploited through various attack scenarios, such as targeting sensors, actuators, controllers, or exploiting protocol weaknesses. Luckily, there are several frameworks and guidelines supporting industry experts in ensuring cyber security. Enisa [12] mentions AGA 12, IEC 61968/61970/62351, IEEE P1711, ANSI/ISA99, NIST SP 800-82, and ISO 27000 as suitable frameworks.

NIST [6] has even a specialized guide called the Cybersecurity Framework. Lastly, the study shows relevant cases of OT cyber-attacks, mostly against energy power plants or industrial companies [13].

2.3 Product management methods

To analyze customer requirements, it is essential to understand the methodological tools and review the literature's definitions of 'benefit'. To identify how customers perceive value it is necessary to do market research [14]. It connects the customers in the market with the marketer and provides information [15].

Lutters et al. [16] provided an understanding that initially in a project, the requirements are not enough known. Even worse, often the requirements cannot be properly characterized because the users and the use cases are unknown.

The “user profile canvas” is a tool proposed by Lewrick & Link [17] to map the customer needs. It has the benefit of reducing the risk of realization through the involvement of stakeholders early in the process. The canvas consists of following blocks:

- Market & Trends
- Influencers
- Persona description
- Use Cases
- Pains, Gains and the Job
- Mood board

The benefit of this method is that everybody shares a shared understanding of the product vision through clear visualization. The customer benefits are structurally mapped, priorities defined and clear and a user-centric design is chosen.

To describe a persona the study of Guo et al. [18] was analyzed. According to the study a persona is a “fictional character that represents user archetypes”. It helps in a user-centric design and to prioritize the right customers. The components of a good persona are: Primary goal, background and motivation, Mindset, objectives / needs related to mindset and behavior to meet the objectives.

Guo et al. [18] also describe some traps, namely that personas describe a mentality or a behavior, not an actual person. A persona is distinct from market segmentation. When describing a persona, the focus should be on relevant information, clearly defining both attitude and behavior, and setting a specific target for the persona.

2.4 Cost-benefit analysis (CBA)

According to Mishan & Quah [19] and Aumayr [14] the purpose of a CBA is to create the groundwork for a future business decision. This decision could be if different projects should be continued or investments into new product should be done. The analysis can contain several options (projects or products) and can show numerically the best one.

The process to create a CBA is described by Riegg Cellini & Edwin Kee [20]:

1. Set the framework.
2. Decision on which costs and benefits should be recognized.
3. Identify and categorize the costs and benefits.
4. Project costs and benefits over the life of the program (not applicable in this study).
5. Monetize costs, meaning putting a currency value on them.
6. Quantify the benefits, meaning putting a currency value on.
7. Discount costs and benefits for present values.
8. Compute the net present value.
9. Research the sensitivity analysis.
10. Summary

While costs are often easier to quantify (e.g., personnel, materials, and delivery), benefits are typically more challenging to measure. Applied to the OT network, the benefit would be the reduction of several man days, which are normally used to document the network topology manually. During operation, the digital twin creates the benefit of understanding how to maintain the OT devices effectively.

In the literature CBAs are often used in economics [19] or in infrastructure project for states, for example a for water management [21]. However, it was also used in the past by other research for companies and their business decisions.

2.5 Research gap

The growing importance of OT capabilities in the industrial network led to new benefits, but also new challenges. In the OT environment, the goals and the needs are differently organized in comparison to IT, namely the availability of the machinery. Due to the increased IIoT usage in OT environments the IT and OT worlds converge together. At the same time, networked devices and their topology plays an important role in cyber security. While there is much research done in OT environments and cyber security, the requirements for network topology and its transparency are not researched as much.

To further analyze the customer needs different product management methods were necessary. The importance of market research was highlighted. To tackle product features, a process to structurally capture different use cases and personas was researched. To compare the costs and benefits in an analysis, the process of the CBA and its key benefits and challenges are shown, and the application of a digital twin is critically reviewed.

Therefore, the identified research gap is that a suitable method of how to derive customer requirements of an OT digital twin can be applied and how the identified requirements can be evaluated.

3 Methodology

The previously described literature review provided a profound insight into existing knowledge and is considered secondary data.

The research model is based on the framework of the research onion as outlined by Saunders et al. [22]. It consists of a multilayered model, showing the sequential and connected nature of the research process. The study seeks to understand how people assign meaning to an objective, specifically how customers value certain features in a network digital twin. The inductive approach helps to build a theory from small data samples, to understand the phenomena and its characteristics. The research strategy was chosen to be a case study since it promised to answer the research questions most accurately. Therefore, the data type is qualitative and the method to understand the customers is a semi-structured interview. The goal was to not only find out what customers value but also to understand why, and how the software can address the problems they face. In a workshop following the interviews, qualitative data where afterwards translated into quantitative inputs for the CBA by assigning cost estimates to each product feature and mapping the perceived benefits based on the points allocated by participants. This allowed for a numerical comparison of the relative value of each feature.

3.1 Research process

To evaluate possible product features, an interview protocol was developed. This protocol aimed to identify possible problems and their root causes, where the OT digital twin software could offer support.

The participants included experts from different departments, ranging from network engineers and cybersecurity officials to head of IT infrastructure. They are working in different companies in different sectors like telecom, production, energy or transportation and had working experience between 12-40 years in the industry. The first part of the interviews focused on the own personal experience of the respondents, while the second part identified challenges in networking, OT, and cyber security. The third part was a live demonstration of the software by the researcher. This part prepared the respondents for the fourth phase, where they brainstormed new product features. The possible product features were written to sticky notes and glued to a workshop poster. In the final part, participants were given 20 points to distribute among the product features. They had full freedom to allocate the points according to their preferences.

The collected feedback was systematically analyzed using the post-processing method outlined by Kuckartz & Rädiker [23].

3.2 Reflection on the chosen methodology

Based on the results of the interviews and the workshop the outcomes were twofold: First, concrete product features were both brainstormed and evaluated based on expert feedback. Second, the process of "how to develop an OT digital twin software further" was adapted und refined in more detail, making it more robust and a usable tool in practice. One goal was to have a pragmatic approach, tested and grounded by industry professionals. Involving multiple industry experts in the development process enhanced credibility and ensured a more practical, real-life application.

To summarize the methodology, the study employed a combination of established methods, including semi-structured interviews and workshops, generating both qualitative and quantitative data. The cost-benefit analysis (CBA) integrated the quantitatively prioritized product features with qualitative feedback, providing a comprehensive approach to guide further development of the OT digital twin software. The practical application of this approach highlights the importance of OT network security in the industry and the potential benefit of this study.

4 Summary of Findings

Before the results of the process were deeper analyzed, several possible product features were rearranged due to one of two possible reasons: They were either very similar to features already mentioned in other interviews or did not require any technical changes to the OT software. Then all product features, which did not get any points by participants, were filtered out.

4.1 Evaluation of the results from a feature perspective

Product features only mentioned once were considered less important. The researcher described his observations and impressions during the interview for the other product features in the Fig. 1.

4.2 Evaluation of the results from a participant perspective

For each expert a detailed summary was described using the researchers' impressions. It was documented, what the biggest challenge for the respondent is, what background they have, and similarities between different participants were marked. One pattern was that participants 003 and 005 were particularly specific on what they needed the OT digital twin to do.

For the as-is product as well as possible product ideas feedback was summarized in Fig. 2.

Explorer and digital twin: Addition of other datasets	-No additional ideas from the respondents how to enrich the digital twin
Intelligence: Automized Checks, Recommendation for action, templates, scripts.	-Focus on automatization is well received among all participants
Configurations in Explorer (VLAN…), "SDN for OT Devices", Simplification through one login	-For network devices completely uninteresting -very difficult to implement -Participants would see value in it
Configuration test on consistency (what was when changed)	-provided by different tools
Traffic Overflow, How much traffic per port?	-Primarily interesting for networkers
Snapshot-comparison	-On the market and widely used -For some customer still useful
Anomaly check for security	-a major concern is that users get too many irrelevant alerts by other tools.
Anomaly check for patterns	-Participants note that they would like this feature to detect irregularities
Asset discovery and characterization	-Focus on OT end devices, not IT network components -Automated asset inventory with HW, SW, SN etc. is really needed -During the interviews it was made clear that this feature is highly demanded
Connection to an additional inventory system or data base, e.g. MAC addresses, Excel or Visio files, putting Systems together	-participants often had a clear idea what of their sub systems could be integrated or fed by *narrowin'* s solution -A concrete use case is to upload a picture of the position of a device
Vulnerability and topology check: Is the device even endangered? Alert prioritization	-Related to "anomaly detection for security", it seems that the alerting is a pain point
Connection to a vulnerability DB, automatic check of firmware for CVE	-Mentioned in nearly all interviews, it seems to be the most demanded feature -It helps with both availability and cyber security
Cloud integration and Azure Authentication	-Some use cases demand a cloud deployment strategy for the tool. Without cloud access, some companies cannot use the tool
AI Connection (e.g. Texts of CVE scanning.)	-AI was mentioned several times with one nice use case (CVE text scanning), but the researcher had apart from the use case the impression that interviewees mentioned it because AI is talked about everywhere
More vendors	-One of the biggest demands from participants and discussed in almost every interview. They want to have their OT devices covered.

Fig. 1. Summary of each product feature

4.3 Processing of the results

After the described rearrangements of product features, 27 possible ideas were left over. The next step was to map the 20 points per interview (6 Interviews, 120 points in total) to each product feature. These points mark the potential benefit for the customer, albeit only relative and not absolute. They are called "benefit points".

To calculate the development costs, a list of 27 product features was provided to *narrowin*. The list contained accurate descriptions and direct quotations from the interviews. *narrowin* calculated the necessary effort per product feature. The costs per hour in CHF were also communicated. With this data, it was possible to calculate the cost per product feature (pf):

$$costs\ per\ pf = effort\ (h) \times costs\ per\ h$$

With having both data sets, mapped benefit and calculated costs, it was possible to execute the cost-benefit analysis.

Participant 001 Telecom sector	- Biggest challenge is network and documentation - Not an OT but network expert - Demanded product features are network heavy. - Was skeptical throughout the interview. Often mentioned that the respondent "could only guess" - Very distributed product features since he works in telecom. Hard to adapt to the use case of *narrowin*. - Has the opinion that a lot of the existing features of *narrowin* is covered by other tools on the market - Had the same "distance" from the topic of OT as participant 004. Similarly, the chosen topics are comparable.
Participant 002 Production sector	- The challenge for him is cyber security. Availability seems to be surprisingly of lower importance (production sector) - Either OT does play a lesser role since production machines are running without connectivity or the production guys are running the OT - Absolute expert in both networking, IT and Cyber security - Very competent - Has a very mature solution already deployed - Driven by the latest developments of AI and cloud - Has the opinion that a lot of the existing features of *narrowin* is covered by other tools on the market - This respondent did stand out from the others due to his position and was not comparable. - Very distributed chosen product features. From the researcher's observation, this could show that no clear purpose of the *narrowin* tool is understood.
Participant 003 Energy sector	- Challenges are regulatory conform documentation and to a lesser degree cyber security - First very open and curious - Over the course of the interview, it became obvious that they had a clear idea how the product needs to look like. This behavior was like participant 005. - The workshop results do reflect the interview impression - Suggested, almost insisted several times to leave IT network components out. Focusing on OT is key. - Potential user of *narrowin'* s tool - Shows even interest to develop the tool together
Participant 004 Telecom sector	- Like participant 001, it is not an ideal "user" of *narrowin'* s tool. - The challenge for him is cyber security focused - Has knowledge of OT and OT markets. With this knowledge, the participant judged the success and potential of *narrowin* quite well - Was sometimes distracted - Sees energy sector as the main OT sector due to the business case described before
Participant 005 Transport sector	- Firstly, very defensive behavior, but started to develop interest on the topic - In the area of transportation availability and cyber security play the most important role - Very similar to participant 003, has a clear idea in mind how to use *narrowin*' s tool - Therefore, focused around one feature - Cyber security background
Participant 006 Transport sector	- Very big delay for the meeting - Interest was there, but one participant was too dominant and too detailed in the narrative - Difficult to make the software interesting for them since a very broad spectrum of features is demanded. - No clear focus visible. Visibility is a challenge, but also networks and availability

Fig. 2. Participants impression

4.4 Cost-benefit analysis

There were two approaches to the CBA: Firstly, a list of all product features. To relate cost and benefit to each other, the cost of a product features was divided by the benefit point of the product feature:

$$Costs\ per\ point = \frac{costs\ of\ pf}{benefit\ points\ of\ pf}$$

This creates a ranking that shows how much *narrowin* needs to spend in CHF per benefit point. There were three notable groups: The green group shows a very low cost per point with having to spend less than 1000 CHF per benefit point. The second group is set between 1000 CHF to 8000 CHF and is shown in blue. The third group has an unfavorable ratio of over 6000 CHF to spend per benefit point.

The second approach was a graphical one. The 27 product features were mapped in a graph with the axes "benefit score" and "costs". To interpret Fig. 3 it must be understood that the top right corner displays the "most valuable product" in the sense that it has the least cost, but the highest possible benefit for customers. This would be the product feature "Asset discovery and characterization". On the contrary, the bottom left corner displays features with the highest costs and the lowest benefit, which is "AI Connection".

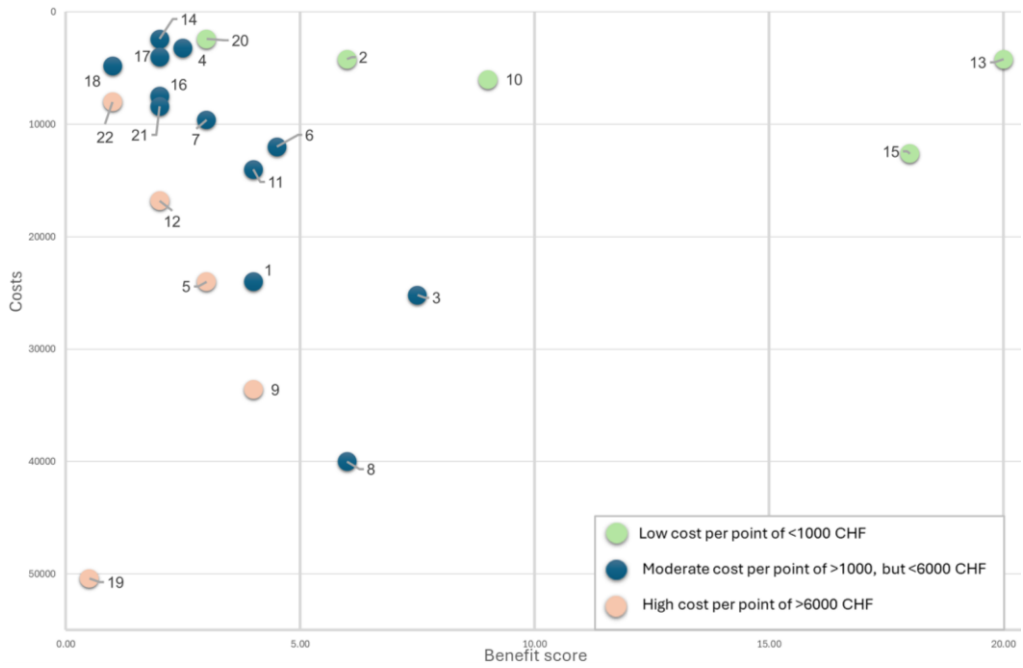

Fig. 3. Cost benefit analysis graphical

4.5 User profile canvas

Based on the qualitative data gathered through the interviews as well as the four most valuable product features, a user profile canvas was created. The persona was developed following recommendations from the literature review, primarily incorporating insights from participants 003 and 005. It is specifically targeted to fulfil as a potential customer for *narrowin*. The market trends, persona description, influencers and the job to be done are extracted from the first part of the interviews. The mood board uses the impressions from the researcher during the interviews as background information. The use cases, pains and gains are described with having the results from the interview as well as the workshop in mind.

The results can be found in Fig. 5.

Product Feature	#
SaaS solution, licensing /Pricing/Business model	1
Explorer and DT: Addition of other Datasets	2
Intelligence: Automized Checks	3
Configuration test on consistency	4
Automatic tools for deployment	5
Traffic Overflow, how much traffic per port?	6
KPI "availability"	7
Snapshot- comparison	8
Anomaly check for security	9
Anomaly check for patterns	10
Connection to an additional inventory system or data base	11
Compliance Scan	12
Asset discovery and characterization	13
Knowhow lost through changing staff	14
Connection to a CVSS DB	15
Vulnerability and topology check: Is the device even endangered?	16
MAC/NAS information feeding	17
Cloud integration and Azure Authentication	18
AI Connection (e.g. Texts of CVE scanning..)	19
Monitoring of WDM (Wavelength-division multiplexing))	20
More vendors	21
Facility management / Buildings: AC's, Heatings, Door Access	22

Fig. 4. Legend for CBA graphical

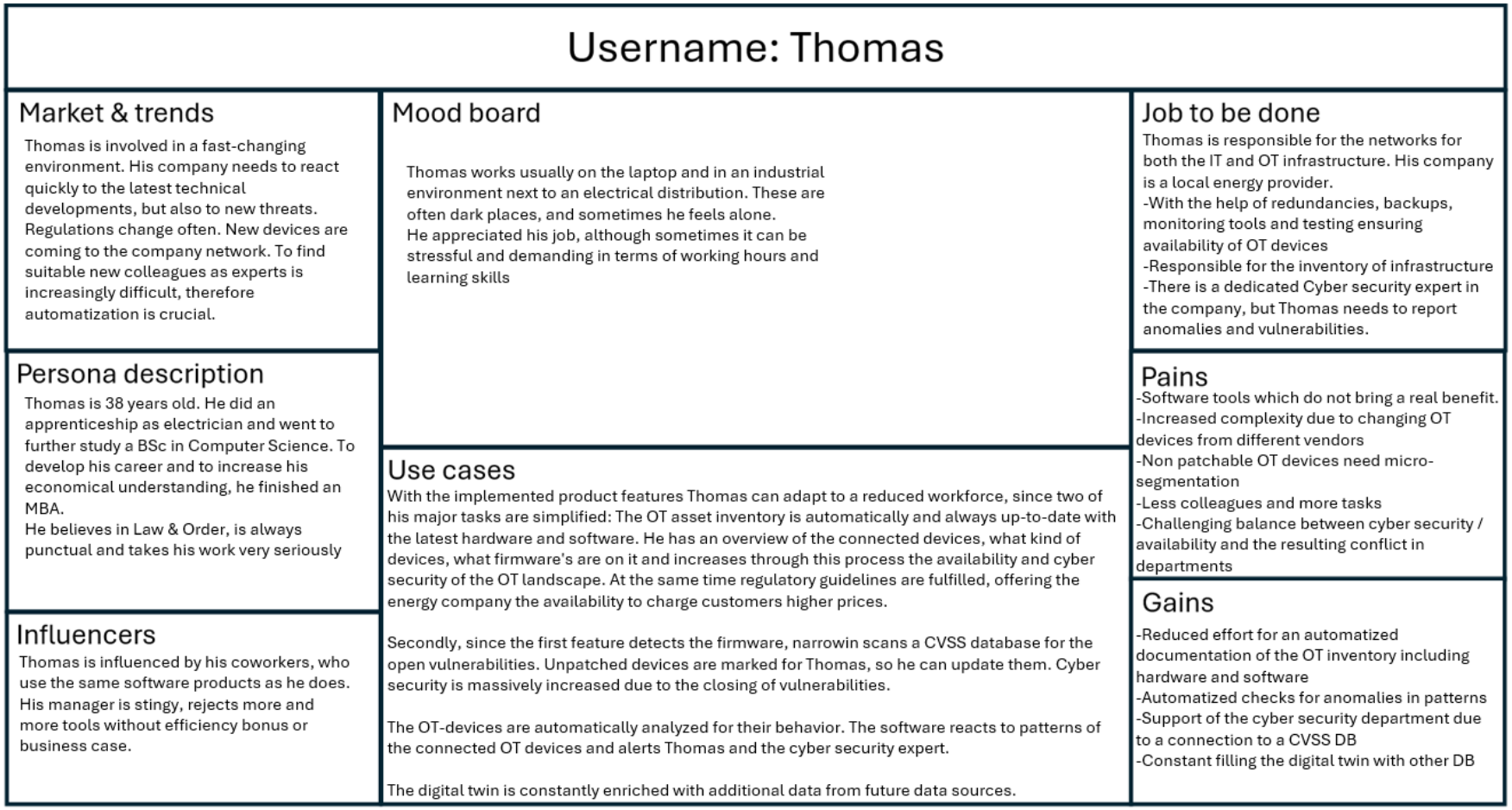

Fig. 5. User profile canvas

5 Results and Discussion

5.1 Identifying challenges in availability and cyber security in an OT network

In the literature review the differences between IT and OT were pointed out, and with this the OT challenges were named. A key technical challenge in OT is that performance must be real-time and time-critical, with minimal tolerance for delays. Availability must be ensured, and it is considered the highest target; an unexpected downtime is not an option. The life expectancy of the equipment is 10-20 years massively longer and creates the challenge of patching old devices or alternatively, reduce the security threat through micro-segmentation. In general, the lack of security of OT devices is challenging. IT departments and OT departments' silo thinking is also described as difficult. NIST [6] and Stouffer [2] emphasizes the difficulty of documenting the network architecture as well as the OT device landscape. Some are not IP-based, others are isolated with the aforementioned micro-segmentation. Another challenge are the open vulnerabilities described by Enisa [12].

A comparison between the literature review results and the interview extracted challenges confirms that the research successfully identified the challenges of OT networks. In the following examples the interview findings confirmed the literature review results:

- OT is often treated as an isolated system in a IT world. Many OT devices are decades old and were not designed with having connectivity in mind.
- Small number of experts in the company, but also on the market is described by both methods as a problem. Due to employee turnover, historical knowledge of OT devices is often not documented.
- The described regulations and guidelines (NIST, IEC62264, IEC27001) are confirmed by some participants as in use and sometimes regulatorily binding.

However, while is literature review tends to be more comprehensive, the interview responses are very concrete in the problem description and might not be representative for the entire market.

5.2 Process of customer requirement extraction

The developed process is a comprehensive approach to identify customer requirement. Starting with potential customers, which have specific requirements, an interview is conducted, and the background of participants is documented. In a later stage a persona is created based on this data.

The second phase is brainstorming together with the participants. If necessary, the software or tools need a demonstration to give context to participants. The results are product features, which are directly based on the needs of customers.

Lastly, in a workshop the brainstormed features plus the backlog features of the software were evaluated for their benefits using a point-based system.

The vendor of the software is contacted and costs for each feature is calculated. In a cost-benefit analysis the benefits and costs are compared. A list of desirable features is the result. The persona is based on the background information of the interview as well as the weighted product features. Compared with the theoretical framework, the practical process is more adapted and therefore detailed. The process has described deeply how the work with the customer/participant looks like.

The process is graphically shown in Fig. 6.

5.3 CBA and user profile canvas

The cost-benefit analysis in Fig. 3 shows the result of all product features. All the costs are assessed. To make the outcome of the CBA usable for a company like *narrowin*, a persona with use cases was invented in Fig. 5. The persona is based on the interview background information as well as the described challenges from

participants and proposed use cases. The product features, which topped the CBA analysis and showed a preferable cost-benefit ratio, were chosen to fulfil the persona.

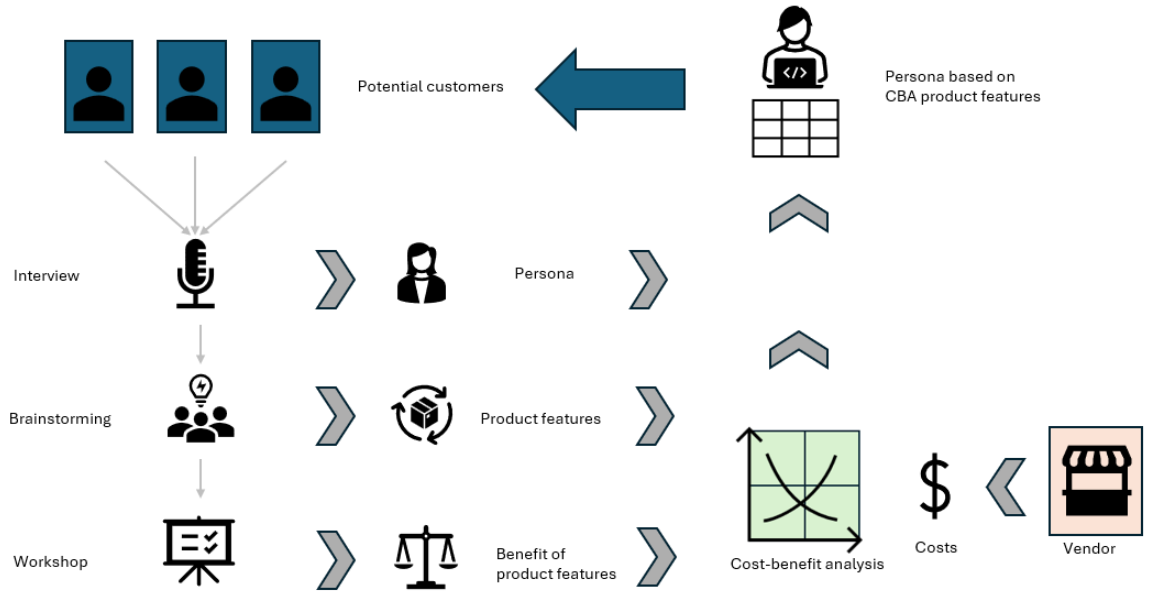

Fig. 6. Practical process of the research approach

6 Conclusions

The process of finding and evaluating customer requirements can be done in various ways. The chosen approach benefits from combining qualitative insights with quantitative evaluation.

However, there are also some limitations. For instance, the quantitative data collected is relative rather than absolute. In a more robust quantitative approach, participants would have been able to allocate an unrestricted number of benefit points, allowing for a more precise measure of feature importance. This would allow consideration of whether respondents have no interest in the tool.

However, the qualitative insights from the interviews help to compensate for the limitations in the quantitative analysis. For example, it tries to get a deep understanding of how respondents perceive possible product features, but a generalization out of this data is difficult to do. However, the quantitative part is more superficial, allowing for quick conclusions but failing to capture the deeper challenges faced by customers.

Additionally, the comparisons between product features are only limited in fairness. Sometimes a product feature was named often, leading to the tendency that it also receives points. To achieve a comprehensive evaluation of the product features, the process should be repeated with all features predefined on the workshop flipchart. According to the researcher's observation, the distribution of points was often done spontaneously by participants, who had the tendency to over reflect on the challenges they faced at the time of the interview. A repetition of the interview could verify this. Additionally, as highlighted in the recommendations, the low number of participants can have the effect that one participant influences the result drastically. However, the summary of all benefit points indicate that some product features are in demand across all participants more than others.

Another weakness in the study design is that the most valuable product features not always align. For instance, the product feature "monitoring of WDM" has a high value per benefit point but was selected only by one participant, making it difficult to integrate into the user profile canvas.

7 Recommendations

For *narrowin* it is suggested to follow the outcome of the study. There are two ways: Firstly, follow the study results and develop the software with the suggested user profile Thomas in mind. This approach will adequately address the needs of two major participant groups, while also appealing to other participants who could become customers in the future as additional product features are developed.

The second recommended approach is to replicate the process, but with a focus on a single customer rather than six participants. The reason behind this is that *narrowin* is still a start-up, development resources are scarce, and focusing on only one customer could lead to a faster return on investment. In addition, only the product features of this one customer are used in the cost-benefit analysis, but the relations can still be evaluated. The benefit of this method is that once one customer is satisfied, *narrowin* can repeat the process with other participants to identify those whose needs closely align with the first customer. Therefore, the possibility is to scale the software to other similar customers.

This study delivers an approach to how customer requirements can be extracted and how the extracted product features can be evaluated. It is recommended to repeat this approach with a greater sample size to verify the results.

8 Limitations of the Study

Upon completion of the study, several questions remain unanswered. The results presented are only valid at the current moment and are subject to change as technology evolves. As future advancements occur, people's opinions and priorities will likely shift as well. What participants consider important today may become irrelevant tomorrow, particularly in the evolving field of OT cybersecurity, which, as noted in the literature review, has only recently gained significant attention. Therefore, it is expected that future interviews could yield different outcomes. As a result, the findings from the cost-benefit analysis (CBA) may quickly lose their validity.

It is not researched if participants are potential customers of *narrowin*, instead only the relative benefit for the respondents is shown. The overall benefit of the digital twin software could be negligible, and this would not be captured in the quantitative analysis. However, in the interview this is sometimes discussed.

Another point is that benefit points indicate the desire of customers for a product feature, but not their readiness to pay. While a higher perceived benefit may lead to greater willingness to pay, pricing considerations were not part of this study.

Only one user profile was created, and it was based on the most valuable product features. It is open, if from the existing CBA a better way to combine product features to reach full market potential is possible.

Disclaimer (Artificial intelligence)

Author(s) hereby declare that NO generative AI technologies such as Large Language Models (ChatGPT, COPILOT, etc) and text-to-image generators have been used during writing or editing of manuscripts.

Competing Interests

Authors have declared that no competing interests exist.

References

[1] Gartner. Definition of Operational Technology (OT)—Gartner Information Technology Glossary. Gartner; 2023 [cited 2024 Dec 15].
Available:https://www.gartner.com/en/information-technology/glossary/operational-technology-ot.

[2] Stouffer K. Guide to operational technology (OT) security (NIST SP 800-82r3). National Institute of Standards and Technology; 2023.
DOI: 10.6028/NIST.SP.800-82r3.

[3] Schwab W, Poujol M. The state of industrial cybersecurity 2018 [Internet]. 2018 [cited 2024 Dec 15].
Available:https://afyonluoglu.org/PublicWebFiles/Reports-CS/2018%20Kaspersky%20The%20State%20of%20IndustrialCyberSecurity.pdf.

[4] Murray G, Johnstone MN, Valli C. The convergence of IT and OT in critical infrastructure [PDF]. Australian Information Security Management Conference; 2017 [cited 2024 Dec 15].
Available:https://doi.org/10.4225/75/5A84F7B595B4E.

[5] Kamal SZ, Al Mubarak SM, Scodova BD, Naik P, Flichy P, Coffin G. IT and OT convergence—Opportunities and challenges. SPE Intelligent Energy International Conference and Exhibition; 2016 Sep 6 [cited 2024 Dec 15].
Available:https://doi.org/10.2118/181087-MS.

[6] NIST. Risk management framework for information systems and organizations: A system life cycle approach for security and privacy (NIST SP 800-37r2). National Institute of Standards and Technology; 2018.
DOI: 10.6028/NIST.SP.800-37r2.

[7] Savin VD. Cyber-security in the new era of integrated operational—informational technology systems. Bus Excell Manag. 2021;11(1):68–79.
DOI: 10.24818/beman/2021.11.1-05.

[8] Lara P, Sánchez M, Villalobos J. OT modeling: The enterprise beyond IT. Bus Inf Syst Eng. 2019;61(4):399–411.
DOI: 10.1007/s12599-018-0543-3.

[9] Paes R, Mazur DC, Venne BK, Ostrzenski J. A guide to securing industrial control networks: Integrating IT and OT systems. IEEE Ind Appl Mag. 2020;26(2):47–53.
DOI: 10.1109/MIAS.2019.2943630.

[10] Boyes H, Hallaq B, Cunningham J, Watson T. The industrial internet of things (IIoT): An analysis framework. Comput Ind. 2018;101:1–12.
DOI: 10.1016/j.compind.2018.04.015.

[11] Pivoto DGS, De Almeida LFF, Da Rosa Righi R, Rodrigues JJPC, Lugli AB, Alberti AM. Cyber-physical systems architectures for industrial internet of things applications in Industry 4.0: A literature review. J Manuf Syst. 2021;58:176–192.
DOI: 10.1016/j.jmsy.2020.11.017.

[12] ENISA. Communication network dependencies for ICS/SCADA systems [Internet]. ENISA; 2017 [cited 2024 Dec 15].
Available:https://www.enisa.europa.eu/publications/ics-scada-dependencies.

[13] Gunduz MZ, Das R. Cyber-security on smart grid: Threats and potential solutions. Comput Networks. 2020;169:107094.
DOI: 10.1016/j.comnet.2019.107094.

[14] Aumayr KJ. Successful product management: Tool box for professional product management and product marketing. Wiesbaden: Springer Fachmedien Wiesbaden; 2023.
DOI: 10.1007/978-3-658-38276-6.

[15] Kotler P, Burton S, Deans K, Brown L, Armstrong G. Marketing. 12th ed. Sydney: Pearson Higher Education AU; 2015.

[16] Lutters E, van Houten FJAM, Bernard A, Mermoz E, Schutte CSL. Tools and techniques for product design. CIRP Ann. 2014;63(2):607–630.
DOI: 10.1016/j.cirp.2014.05.010.

[17] Lewrick M, Link P. Design thinking tools: Early insights accelerate marketers' success. Mark Rev St Gallen. 2015;32(1):40–51.
DOI: 10.1007/s11621-015-0507-7.

[18] Guo FY, Shamdasani S, Randall B. Creating effective personas for product design: Insights from a case study. In: Rau PLP, editor. Internationalization, Design and Global Development. Vol. 6775. Berlin Heidelberg: Springer. 2011;37–46.
DOI: 10.1007/978-3-642-21660-2_5.

[19] Mishan EJ, Quah E. Cost-benefit analysis. 5th ed. London: Routledge; 2007.

[20] Riegg Cellini S, Kee JE. Cost-effectiveness and cost-benefit analysis. In: Handbook of Practical Program Evaluation. 3rd ed. Hoboken: John Wiley & Sons. 2015;636–672.
DOI: 10.1002/9781119171386.ch24.

[21] Tapsuwan S, Peña-Arancibia JL, Lazarow N, Albisetti M, Zheng H, Rojas R, et al. A benefit cost analysis of strategic and operational management options for water management in hyper-arid southern Peru. Agric Water Manag. 2022;265:107518.
DOI: 10.1016/j.agwat.2022.107518.

[22] Saunders M, Lewis P, Thornhill A, Bristow A. Research methods for business students. In: Chapter 4: Understanding research philosophy and approaches to theory development. 6th ed. Pearson Education. 2019;128–171.

[23] Kuckartz U, Rädiker S. Qualitative Inhaltsanalyse: Methoden, Praxis, Computerunterstützung: Grundlagentexte Methoden. 5th ed. Beltz Juventa; 2022.

Peer-review history:
The peer review history for this paper can be accessed here (Please copy paste the total link in your browser address bar)
https://prh.ikprress.org/review-history/12559