sustainability

MDPI

Article

A Vulnerability Assessment Framework for Product-Service Systems Based on Variation Mode and Effect Analysis

Hanfei Wang [1,*], Yuya Mitake [2], Yusuke Tsutsui [3], Salman Alfarisi [1] and Yoshiki Shimomura [1]

[1] Faculty of Systems Design, Tokyo Metropolitan University, Tokyo 191-0065, Japan
[2] Human Augmentation Research Center, National Institute of Advanced Industrial Science and Technology, Chiba 277-0882, Japan; yuya-mitake@aist.go.jp
[3] Faculty of Computer Science and Systems Engineering, Okayama Prefectural University, Okayama 719-1197, Japan
* Correspondence: wang-hanfei@ed.tmu.ac.jp; Tel.: +81-80-4749-4966

Abstract: In recent decades, the product-service system (PSS) has been spotlighted due to its innovation and sustainability. As a novel business system, PSS provides additional value for products through the addition of service, which effectively upgrades the traditional manufacturing industry. For realizing a successful PSS, a robust and reliable operation stage is extremely important for users to stay satisfied and loyal. Thus, designers need to ensure that this system is not sensitive to any influential perturbation. Namely, they must achieve the desensitization of PSS to vulnerability. However, the current PSS design field still does not provide an effective method to assess the vulnerability in the whole life stage of PSS. This would lead to less time for the PSS provider to respond to various events. Furthermore, the tremendous loss could be caused due to the immaturity of the system. Therefore, this research has developed a vulnerability assessment framework based on variation mode and effect analysis (VMEA) for PSS. This developed framework has the ability to identify the potential noise factors and assess their severity based on multiple steps of analysis. This method has proved its effectiveness through an application example, and it is also expected to enable PSS researchers to design a robust PSS.

Keywords: product-service system; vulnerability assessment; noise factors; variation mode and effect analysis

Citation: Wang, H.; Mitake, Y.; Tsutsui, Y.; Alfarisi, S.; Shimomura, Y. A Vulnerability Assessment Framework for Product-Service Systems Based on Variation Mode and Effect Analysis. *Sustainability* **2023**, *15*, 5092. https://doi.org/10.3390/su15065092

Academic Editors: Golam Kabir, Muntasir Billah and Subhrajit Dutta

Received: 16 February 2023
Revised: 8 March 2023
Accepted: 10 March 2023
Published: 13 March 2023

1. Introduction

For recent decades, traditional manufacturing firms have been facing serious problems due to the surging cost of human resources and raw materials [1]. There are tremendous discussions about how to improve the value of the product and achieve sustainability [2]. Among various solutions, the product-service system (PSS), an integration of products and services, is considered a promising business mode [3]. As a novel system, PSS could provide further value through additional services. Furthermore, PSS could be classified into three types: product-oriented, use-oriented, and result-oriented PSSs. Tukker states that ownership is no longer extremely important since the product is shared for a specific period in use-oriented and result-oriented PSSs, which are sharing the products for customers. In these modes, the waste of material is reduced because manufacturers do not need to provide mass production [4,5]. For this reason, PSS is also regarded as a solution to a circular economy [6].

Despite the great potential, currently, the application of PSS in practice is not as successful as expected. Multiple literatures point out that PSS firms are not competent enough to avoid unwanted variations in PSS performance [7–10]. It is worrying that PSS might be a vulnerable system against various types of perturbations. According to Wang et al., there are six categories of PSS perturbation, namely behavioral, social, environmental, competence, resource, and organizational perturbations. Perturbations of the above categories

could lead to a sudden disruption or a long-term deviation of the performance of PSS [9,10]. Furthermore, it is worth noting that there is another dimension for considering the severity of an event, such as perturbation, which is the sensitivity of the system towards this event. Based on this consideration, Taguchi has proposed the concept of noise factor instead of perturbation, which is defined as any uncontrollable factor that leads to unwanted changes in the performance of products [11]. In the concept of robust design, the most critical task is to ensure the system's key characteristic is not sensitive to the existence of noise factors. For this reason, to achieve a robust and reliable PSS, it is extremely important for designers to identify and analyze the potential noise factors leading to variation [12]. However, current PSS researchers have not proposed any effective method or guideline to identify and analyze noise factors. The core reason for this dilemma could be explained by the limited data and low awareness relating to the identification of the noise factor. It is reported that in servitization, firms have a negative tendency not to document experiences learned from successes and failures [13]. In terms of noise factor analysis methods in the field of PSS design, currently, the major research focus is related to failure mode and effect analysis (FMEA) [14–16]. However, this method greatly emphasizes PSS failure, which is a type of disruption or interruption of functions. The perspective of deviation is overlooked. Furthermore, for the above papers, the consideration of sensitivity is lacking. The assessment of the influence of events is only based on the dimensions of possibility, detection, and severity.

Therefore, to enable PSS designers to assess the vulnerability of PSS, this paper has proposed a developed assessment framework based on a typical variation analysis method, namely variation mode and effect analysis (VMEA). VMEA is a well-known method for identifying noise factors in the field of robust design. This method could analyze noise factors based on screening out potential factors contributing to the deviation of the key product characteristics (KPC) [12,17,18].

However, it is worth noting that VMEA has not been modified to become a suitable tool for PSS vulnerability assessment. The challenge and difficulties of this research are explained below. First, PSS is a complex system which involves multiple stakeholders and a large amount of hardware and software components [19]. It is essential to find a solution to visualize the stakeholders' relationship and the condition of the key components before operating the assessment. Second, VMEA is designed for product design, which does not consider the existence of services. It is required to identify the key service characteristic (KSC). Thirdly, traditional VMEA does not provide a reliable method to find the cause of vulnerability, namely noise factors (NFs). There is a lack of a rational method to identify and analyze the actual NFs leading to different problems. Finally, traditional VMEA does not present a set of available mitigation strategies. For PSS, traditional risk mitigation measures are often ineffective and have side effects. Therefore, a new set of vulnerability mitigation strategies needs to be proposed.

To overcome the above difficulties, this paper has made some novel achievements in the following aspects. First, to visualize the stakeholders' relationship and key components, this framework has also utilized the knowledge from service engineering [20], including the flow model to visualize the stakeholders' relationships and use the view model to clarify the key components [20]. Second, to identify and analyze the KSC, this method adopts the concept of Receiver state parameter (RSP) and transforms it into related KPCs and KSCs. Thirdly, to analyze the cause and consequence, this study utilizes a cause–consequence analysis method [21]. To improve the rationality, six root causes have been selected based on the previous research [10]. Last but not least, a set of PSS vulnerability mitigation strategies has been proposed in this research. To verify the effectiveness of the proposed framework and the above novel improvements, an application has been used in the case of shared washing machines.

The paper is structured as follows: Section 2 introduces the research background. Section 3 explains the steps of the proposed method. Section 4 provides a case study to verify the effectiveness of this method. Section 5 discusses the practical meaning, theoretical importance, and future direction of this research. Section 6 offers a conclusion.

2. Literature Review

2.1. PSS and PSS Design

PSS is defined as an integration of products and services. It is considered a promising business mode which could satisfy the requirement of customers [3]. It is worth noting that PSS is not a simple integration of products and services. Indeed, a well-structured PSS should also consist of supporting networks and infrastructure, which could achieve the requirements of multiple stakeholders [22]. Based on the classification of Tukker, PSS could be classified into product-oriented, use-oriented, and result-oriented PSSs. Among the above categories of PSSs, the realizations of result-oriented and use-oriented PSSs have received tremendous attention due to their novelty and sustainability, which could improve the environmental performance of the traditional manufacturing industry [2,6,22,23]. It is not the first time for researchers to link environmental performance with PSS. Considering that PSS might require products to be used by various users and keep a contract of maintenance with customers for a long time, the life cycle of products is usually longer than the ones of traditional manufacturing [22–25]. In this mode, products and materials could be reused for several times and even used by multiple users [24].

However, this great transformation also results in troubles for designers and providers of PSS. On the one hand, for PSS providers, it is argued that the novelty of PSS is rejected by many staffs and managers. It is pointed out that involved stakeholders of PSS feel difficult to learn the knowledge of service providing and accept the orientation of sharing and renting [26–28]. On the other hand, for PSS designers, the problem is even more complex. Indeed, the current PSS field does not lack design methodologies. To enable this novel system to be designed in a productive way, there are multiple methodologies that provide solutions to integrate products and services, achieve sustainability, and fulfill further requirements of multiple stakeholders [2,29–36]. Some famous methods in the field of service engineering and system engineering, such as TRIZ, QFD, and Axiomatic design, have already been used for PSS design [37]. The above studies have obviously filled in the gap of methodology relating to modular design and customization [32–34], sustainable design [2,35], design of integrating products and services [29,36], and knowledge-based design [30,31]. In addition to the system design, there are also multiple researchers realizing that PSS requires further contribution in the issue related to life cycles [2,6,38–42]. Although there are a number of existing methodologies to build a PSS, it does not mean that the current design solution is perfect. Indeed, methodologies before 2012 have been criticized for lacking practice in the real industry [43]. Furthermore, for many specific aspects, the PSS design has exposed its vulnerability. Wang et al. have proposed a taxonomy of PSS perturbation, which points out that current PSSs are not robust and could be threatened by internal and external accidents [10]. For the above reasons, to achieve a feasible and robust PSS, further contributions are required in the fields of PSS management and PSS design.

2.2. The Concept of Vulnerability and the Vulnerability of PSS

The concept of vulnerability was created in the 1970s. Initially, this concept was not used for assessing the condition of the system, but for items, especially military vehicles. Early researchers tend to use this attribute to test the strength of an aircraft against external attack [44]. After the 1990s, with the development of understanding regarding vulnerability, the focus was upgraded from the single item into systems. The research about vulnerability had been developed into some social, biological, and economical systems. The most popular definition of vulnerability was developed by Turner et al., that vulnerability is the degree to which a system, subsystem, or system component is likely to experience harm due to exposure to a hazard, either a perturbation or stress/stressor [45]. After that, another famous study of Adger emphasized that vulnerability is highly related to the sensitivity of systems to harm. It was also spotlighted that there was a challenge of providing a recovery plan to mitigate the vulnerability [46]. In recent decades, the focus relating to vulnerability and reliability was increased. The failures, which were the result of the system vulnerability, were divided into software and hardware failures based

on whether each failure was related to tangible or intangible components [47]. It was proposed that the complex systems, especially industrial systems, might bear having strong relationships with multiple failures due to their own composition [48,49].

In the current PSS field, the studies directly relating to vulnerability are still in an initial stage. The PSS vulnerability was defined as 'the property of itself; its product, service process, maintenance, supplying and management that may weaken or limit its ability to endure threats and survive accidental events that originate both within and outside the system boundaries' [50]. However, since the studies of vulnerability and PSS vulnerability still have not achieved an agreement on a generic definition of events leading to vulnerability, it was found that disturbance, disruption, and stress are also used to describe such kinds of events [9]. Thus, to clarify the description of the events leading to the threat, Romero and Estrade used the term 'perturbation,' which was defined as any endogenous or exogenous event that modifies the stated PSS operational conditions [50]. This definition was also used by other studies in PSS [9,10]. Wang et al. proposed a taxonomy of PSS perturbation, which classified it into six categories: behavioral, social, environmental, competence, resource, and organizational perturbations. The research was based on reviewing papers with the keywords 'service paradox', 'operational risk', 'barrier', and 'perturbation', which avoided the dilemma that there was a limited number of papers with the keyword 'perturbation' [10]. This study has also shown some interesting findings, especially those relating to social and behavioral perturbations. Compared with the vulnerability of products, which requires a focus on the failure ratio and life of the product, designers of PSS usually need to consider further issues due to the existence of services and complex business environments. For social perturbations in PSS, the social attitude of stakeholders, especially customers, is considered as the cause of loss. The concept of product lifetime is given high-level importance, which points out that a product might be abandoned before the end of its actual life [51,52]. It was found that customers would reject purchasing the service and product or reduce their satisfaction if they encountered a service failure or recovery [53]. In the case of furniture renting in Europe, it was found that customers were reluctant to continue the contract as the products were considered out of fashion [54]. Interestingly, it was also pointed out that PSS business could form a stronger consumerism, which forces customers to discard the old product. The psychological obsolescence was exposed to be accelerated in some situations [55]. For behavioral perturbation, the behavior of the customer was considered the cause of the physical loss of the machine or product, which led to the PSS vulnerability. Given that the business modes of use-oriented and result-oriented PSSs are usually giving a large extent of freedom to users when they are using the product, it is questionable whether users can keep careful and responsible during the usage [7]. Due to the lack of effective monitoring means and management mechanisms, the risk of unethical behavior and speculative behavior is unavoidable in PSS [7,56]. Furthermore, PSS also exposed its vulnerability against the variation brought by accidental events. For example, the event of COVID-19 had been proven to have an obvious strike on the positive emotion toward the use-oriented PSS [57]. Considering many customized PSSs are pointed out to only serve personal customers [58], the loss caused by this variation could possibly lead to the further loss of a loyal customer, which is unacceptable for PSS providers, especially for customized PSS providers. Furthermore, it was also exposed that PSS would become financially vulnerable and physically vulnerable due to the difficulty of logistics [59].

2.3. Vulnerability Assessment Methods and Their Applications in PSS

Since the existence of vulnerability would lead to continuous damage to the system, since the 1990s, there have been tremendous papers discussing how to identify and mitigate the vulnerability in the fields of multiple systems [60–63]. The vulnerability assessment aims to provide an effective way to identify not only known but also unpredicted vulnerable issues of various systems [62]. Generally, a comprehensive vulnerability assessment framework should consist of the following functions: (i) identify the potential perturbations; (ii) analyze the severity of various perturbations; and (iii) provide a mitigation

strategy [60,62]. However, it was also pointed out that there was a huge challenge to assess the vulnerability, especially when designers were required to analyze unpredicted events. Their existence and influence were difficult to understand in a direct way. Furthermore, in mitigating vulnerability, it was also worrying that one solution would have a side effect, which could also lead to further vulnerabilities [62].

To date, although the PSS field has not provided a comprehensive vulnerability assessment framework, there are also some related studies that could contribute to parts of the vulnerability assessment framework. To reduce the software and hardware failures, Zhang et al. have proposed a set of criteria to assess the reliability and cost of use-oriented PSS based on the Marcov method [63]. The method of the failure mode and effect analysis (FMEA) [14,64,65] had already been applied to PSS design by researchers. This method could identify, analyze, and mitigate the potential failure of PSS based on a top-down logic. Meanwhile, the theory of inventive problem solving (TRIZ) [16], which is a powerful solution-generating tool, has also been applied in the PSS field. However, the mentioned definitions and approaches also had disadvantages in assessing the vulnerability of PSS. First, in terms of PSS failure analysis, the existing methods [14,64] had a strong focus on the failure mode, which means a disruption of the service or a malfunction of the machine. This focus led to an overlook in the deviation of the components' performance and the variation brought by catastrophic events [9]. The above PSS FMEA did not have effective functions to identify the cause of variation in the level of deviation. Furthermore, for some PSSs, the variation of performance is not caused by internal variation but by external variation. For example, advances in fashion and technology can make existing products unattractive, even if they do not have problems [54]. This was also overlooked by many PSS FMEA. Second, according to Reim et al. and Sakao et al., the traditional risk management strategies, namely risk reduction, risk transfer, and risk avoidance, are not as effective as expected in preventing unnecessary variation in PSS performance. Indeed, some PSSs, especially result-oriented and use-oriented PSSs, share ownership with customers. Given that they benefit from taking the risk of owning a product, the actions of risk avoidance or risk transfer are not feasible and beneficial for PSS providers [7,8]. For PSS FMEA, the solution to solve a failure was usually based on the opinions of experts or group discussions. Therefore, it is questionable whether variation brought by failure could be mitigated in a productive way by traditional risk management strategies. Given that mitigating variation directly is not an effective method, the robust design, which aims at desensitizing internal and external variation, namely noise factors, should be a hopeful way. However, to consider the robustness of PSS, the term of sensitivity, which is the degree of the key characteristics to be affected by the variation of noise factors [17], has been pointed to be overlooked by the field of PSS design for a long period [10]. To make matters worse, the current PSS industry does not form the habit of collecting noise factors [13], which leads researchers to lack the means of recognizing noise factors. There is a strong need to provide a comprehensive and logical PSS vulnerability assessment framework.

2.4. The Variation Mode and Effect Analysis (VMEA)

VMEA is a deductive and statistical method which aims at enabling designers to analyze unwanted variations in the engineering characteristic [66]. This method is a power analysis method that could focus on variation in the performance instead of focusing on a single mode like failure or disruption. To date, this method has already been utilized in the fields of maintenance management [67] and robust product design [68]. In the field of vulnerability analysis and robust design, this method is also used to analyze the influential factor that leads to vulnerability [12]. To ensure that the focused performance indicator is effective and meaningful, before conducting a VMEA, designers need to transfer the confusing customer need into the product characteristics (PCs). After that, PCs need to be discussed, and designers need to decide on those that represent crucial interests as key product characteristics (KPCs). A comprehensive VMEA is usually made up of four steps, as seen below.

2.4.1. KPC Causal Breakdown

After selecting one KPC, in usual situations, this KPC could be decomposed into several Sub-KPCs. The Sub-KPCs are the characteristics of the product, product components, and manufacturing process, which contribute to the actual value of the related KPC. The existence of Sub-KPCs should be observable and controllable [66]. Additionally, given that a vulnerable product could be affected by multiple factors that lead to unwanted change, VMEA uses a famous concept of robust design [12], namely noise factors, to define such kinds of factors. The noise factor is defined as any factor that cannot be handled and leads to the weakened performance of the product [11]. The noise factor could also be understood as a kind of sensitive perturbation. It is worth noting that the relationship between perturbation and noise is an affiliation relationship. That is, a perturbation can only be identified as noise if it has been discussed to be extremely sensitive, and noise must be a perturbation.

Furthermore, to visualize the relationship among the above concepts, a VMEA usually adopts a modified Ishikawa diagram (see Figure 1).

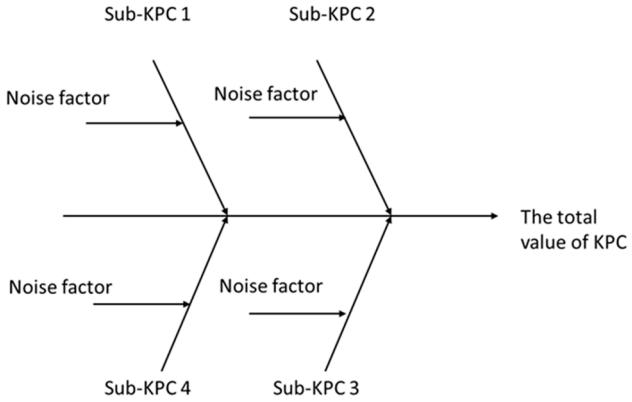

Figure 1. The modified Ishikawa diagram for VMEA.

2.4.2. Sensitivity Assessment

In this step, since KPC, Sub-KPC, and noise factors affect each other, it is crucial to understand the possibility that other factors will be affected when one of the factors is disturbed, namely sensitivity. Therefore, designers need to conduct an objective assessment of the sensitivity between KPCs and Sub-KPCs and between Sub-KPCs and noise factors, respectively [69]. For example, in a case of assessing the vulnerability of the shared bike, the usability of the bike is a crucial KPC. The customer adverse behavior, which has a high possibility to destroy the components of the bike, is given a degree of sensitivity of 9.

2.4.3. Variation Size Assessment

In the actual product manufacturing environment, the deterioration performance of the product is caused by the existence of noise in the manufacturing process. However, designers sometimes think of the noise factor as a static existence, an uncontrollable adverse factor with a fixed impact. In fact, this is a wrong view. Noise factor could also become a dynamic factor in some cases, and this dynamic is a core source of product vulnerability. For example, during the woodworking process, the humidity of the air can cause the wood to deform. In this case, the humidity of the air is often difficult to maintain, and higher humidity results in worse product performance. Thus, in this step, designers need to assess the variation size of every noise factor based on the objective perspective.

2.4.4. Variation Risk Assessment and Prioritizing

Based on the evaluated weights of step 2 and step 3, designers need to analyze the severity of each noise factor for the related Sub-KPC. To achieve this target, VMEA requires designers to calculate a Variation Risk Priority Number (VRPN). This calculation could

quantify the influence of noise factors on Sub-KPCs, and the total VRPN of each Sub-KPC would also determine the vulnerability of the related KPC. The calculation formula is as follows:

$$VRPN_i = \omega_i \times V_j \times S_j$$

Here, ω_i is the importance of Sub-KPC i, V_j is the variation size of the noise factor j, and S_j is the sensitivity of each Sub-KPC towards noise factor j. Additionally, the total degree of the vulnerability of KPC_m could be calculated as below: $KPC_m = \sum_{i=0}^{n} KPC_i$. Based on the result of the final VRPN of each KPC, designers could distinguish which characteristic is more vulnerable.

2.5. Research Gap

In this research, the knowledge gaps to be filled exist on two sides, namely gaps in PSS vulnerability assessment and VMEA.

On the one hand, for the related methods that could contribute to PSS vulnerability assessment, most of them do not seem competent for vulnerability assessment. For FMEA-related methods [14,64], the existence of sensitivity and variation is not considered. Furthermore, PSS vulnerability focuses on the negative variation in the performance, which could be a deviation, disruption, or disaster [9]. PSS vulnerability assessment requires designers to identify any important variation, even if it is tiny.

On the other hand, for VMEA, there is also a gap because this method is not effective enough for PSS. Indeed, compared with the product vulnerability, the vulnerability of PSS is far more complex. According to Wang et al., the vulnerability of PSS could be affected by six categories of perturbations, namely behavioral, social, environmental, competence, resource, and organizational perturbations [10]. Among them, behavioral and social perturbation shows some unique features that might not appear in the traditional manufacturing field. Furthermore, given that the services are intangible, the characteristic of service is more difficult to be observed and controlled. The KPC is not enough for the context of PSS. Furthermore, in the normal VMEA, the step of mitigation, which requires analysts to provide solutions to mitigate the adverse impact of risky events, is usually lacked.

3. Methodology

To assess the vulnerability of PSS and fill in the knowledge gaps of Section 2.5, this paper has modified the VMEA for PSS. To develop the VMEA to become a feasible method for PSS vulnerability assessment, authors have made the following efforts. Firstly, to integrate the key characteristics of products and services, this research uses the concept of Receiver State Parameter (RSP) to present the key value of PSS, which is described as a state change of a customer in the field of service engineering [19,20]. According to Arai and Shimomura, this state should be observable and could be transformed into one or several functional parameters, which are parameters of functions [19]. In this way, designers do not need to struggle to integrate the key characteristics of products and services. Instead, RSP could enable designers to grasp the core value of PSS and transform it into functions. Secondly, to ensure that PSS designers could identify the potential noise factors threatening RSPs, the authors have improved the analysis process of the VMEA, which traditionally requires designers to identify factors based on expert interviews or brainstorming [18]. To improve the efficiency and effectiveness of the analysis, this paper has used a famous failure analysis method, namely fishbone analysis [21]. Given that the internal and external environments of PSS are complex, it is also essential to develop this method. For this reason, six root causes, including behavioral, social, environmental, competence, resource, and organizational perturbations, are provided based on the previous finding of a taxonomy of PSS perturbation [10]. Finally, a mitigation analysis method is proposed. The steps of the methodology are shown below (see Figure 2).

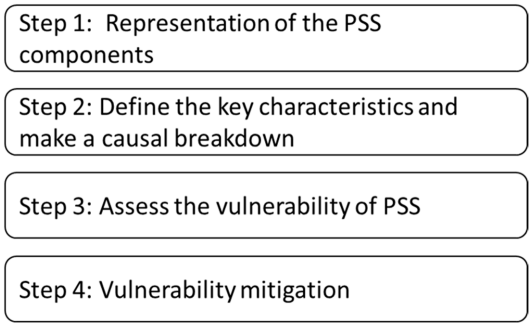

Figure 2. The steps of the methodology.

3.1. Representation of the PSS Components

In order to simplify the complexity of PSS, at this step, analysts need to show the products, services, and stakeholder relationships involved in PSS in a visual way. First, this step requires analysts to provide an understandable product drawing that points out the main tangible components of the product. Second, to make service components visible and represent their service objects, a flow model is adopted in this study. The flow model can represent the relationship among various stakeholders in PSS [20]. Between different stakeholders, analysts need to connect personas representing stakeholders with lines, on which service components are marked. In addition, arrows need to be used to indicate the provider and receiver of the service. The details for how to use this model are illustrated in Section 4.

3.2. Define the Key Characteristics and Make a Causal Breakdown

3.2.1. Define the RSP of the Targeted PSS

In order to assess the vulnerability of PSS, precise definitions of the engineering characteristics of PSS are necessary. In traditional manufacturing, because the product is tangible, the characteristic is understandable and observable. Furthermore, the designer is usually responsible for the products' subsequent sales and vulnerability assessment. The analysts have a high-level understanding of the engineering characteristic. Thus, the vulnerability assessment framework usually does not require analysts to define product characteristics again. However, for PSS, since manufacturers and suppliers are often two independent companies, in some cases, products and services are even designed separately. The person performing the vulnerability analysis may not be the designer of the product or service. In other words, they cannot grasp all the information in all situations. Therefore, analysts cannot directly obtain effective characteristic definitions. Additionally, existing descriptions of services can be ambiguous due to their intangible nature. The characteristics of PSS, namely service characteristics and product characteristics, need to be redefined using precise and effective language.

To identify the required characteristic, this paper regards each stakeholder as a receiver. A cross-functional team is required to identify the requirement of various stakeholders, and the requirement should be translated into the form of receiver state parameter (RSP), which could describe the functional requirement in an observable and controllable way. Considering that sometimes the data of customer requirements (CRs) and Stakeholder requirements (SRs), which are collected from the database of the firm, could be vague, it is essential to use RSPs instead of traditional CRs and SRs. After that, the cross-functional team needs to define the KPCs and KSCs based on every RSP. According to the classification of the RSP, any parameter with a positive influence is called 'value', while any parameter with a negative influence is called 'cost' [70].

In this research, given that the RSP is provided in the stage of assessment, not in the stage of requirement analysis, the selection of RSP should consider whether this parameter is highly related to the vulnerability of PSS. For this reason, the selection of RSP should follow the following rules:

1. The selected RSP has a positive or negative impact on one or several stakeholders.
2. If the performance of the selected RSP deteriorates, one or more stakeholders may suffer significant losses at the economic, social, and environmental levels. The loss should be direct and observable.

At the end of this step, given that the research aim is to assess the vulnerability of PSS, it is not thereby suitable to assess the RSP separately. Instead, analysts need to weigh the importance of each RSP for the targeted PSS. To give the weight in a rational way, this research adopts a 10-point scale. The criteria are provided in Table 1.

Table 1. The criteria of weighing importance of RSP.

Weight	Criteria
0–2	There is a very low-level contribution that the RSP could contribute to the benefit of the stakeholders of the targeted PSS
3–4	There is a low-level contribution that the RSP could contribute to the benefit of the stakeholders of the targeted PSS
5–6	There is a moderate-level contribution that the RSP could contribute to the benefit of the stakeholders of the targeted PSS
7–8	There is a high-level contribution that the RSP could contribute to the benefit of the stakeholders of the targeted PSS
9–10	There is a very high-level contribution that the RSP could contribute to the benefit of the stakeholders of the targeted PSS

3.2.2. Dividing RSP into PChs and SChs

After that, given the information of 3.1, the details of components, stakeholder relationship, and RSP are clear for the analyst. In this step, analysts need to clarify how the current PSS responds to the required RSP, including service characteristics (SChs) and product characteristics (PChs). Thus, a causal breakdown is essential to be carried out. For the causal breakdown of RSPs, several factors need to be clarified, including each RSP and their related SChs and PCh.

To clarify the relationship between RSP and PChs and SChs, this step adopts a modification of the view model [20]. The view model is an effective model of service engineering, which could show functional relationships among requirements, functions, service actors, and artifacts. To show the existence of SChs and PChs, this paper adopts the explanation of Sakao et al., which divides RSP into SChs and PChs [70]. This breakdown is also utilized in the field of PSS design [71]. Based on this explanation, the modified view model is shown below (see Figure 3). In this model, designers need to identify the involved service actors and product components that are related to various service and product characteristics.

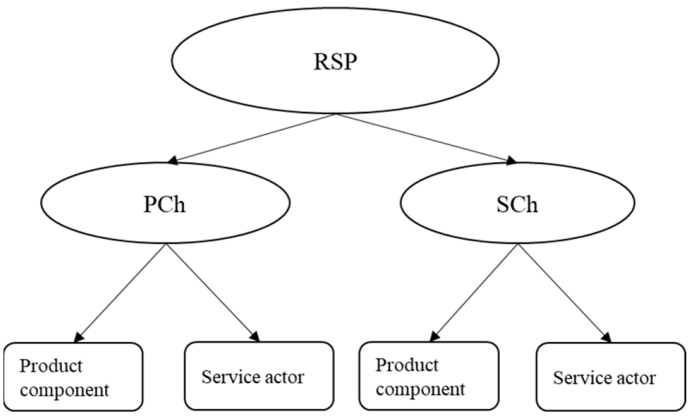

Figure 3. An example of the modified view model that is moderated from [20].

3.2.3. Identifying the Noise Factor for Each PCh and SCh

To identify the noise factor that hinders the performance of the function in a logical and effective way, this paper adopts a fishbone analysis, which is an efficient analysis method to identify the cause based on the given root causes and a consequence [72]. Given that the effectiveness and rationality are decided by the choice of the root cause, this paper selects the taxonomy of Wang et al. [10], which classify the PSS perturbation into six categories, namely behavioral, social, environmental, competence, resource, and organizational perturbations. These perturbations are considered the root cause of PSS vulnerability. Thus, this paper creates a matrix based on fishbone analysis and the above taxonomy below (see Table 2). The definition of the above six root causes are presented below:

1. Behavioral perturbation: any event relating to the customer's adverse behavior that leads to product breakdown. Due to the lack of legal and contractual constraints, customer behavior may cause physical damage to PSS products or machines, thereby reducing availability and efficiency.
2. Social perturbation: any event relating to the adverse social attitude from various stakeholders, including customers, managers, staff, government, and the local community, that reduces the acceptance and satisfaction towards the targeted PSS. The adverse social attitude can be mainly divided into two types, namely insensitivity toward sharing or renting and resistance toward PSS novelty.
3. Environmental perturbation: any event relating to the lack of environmental prerequisites, which reduces the support from the legal environment, market, and micro-economy.
4. Competence perturbation: any event relating to the lack of the specific competence to overtake the basic function of PSS and the ability of service actors to maintain the system against accidental events, which weakens the performance of tasks and the availability of products.
5. Resource perturbation: any event relating to the shortage of resources, including investment, component, human resources, materials, and infrastructure, which could lead to disruption and even bankruptcy.
6. Organizational perturbation: any event relating to the structural problem that originates from the organization that reduces efficiency.

Table 2. The noise factor identification matrix.

Root Cause	**RSP 1**	
	PCh 1	**SCh 1**
Organization		
Society		
Resource		
Behavior		
Competence		
Environment		

3.3. Assess the Vulnerability of PSS

The vulnerability of PSS is determined by the total vulnerability of various components. Thus, to assess the vulnerability of PSS, it is crucial to understand the vulnerable condition of various major RSPs. First, given that various SChs and PChs have different importance for each RSP, analysts need to give a weight for each SCh and PCh. Therefore, the value relationship should follow the formula below:

$$V = \sum_{i=0,\ j=0}^{n} \left(\omega_{pi} \times V_{Pi} + \omega_{sj} \times V_{sj}\right)$$

Here, V is the total value of the RSP. V_{Pi} is the value of PCh i, while V_{sj} is the value of SCh j. ω_{pi} is the importance of the value of V_{Pi}. ω_{pj} is the importance of V_{sj}. The assessment of the weight should be based on the contribution of each SCh and PCh to improve the performance of related RSP. To normalize the value of importance, this study adopts a 10-point scale, which ranges the weight from '1: Extremely unimportant' to '10: Extremely important'. The criteria are shown below (see Table 3).

Table 3. The criteria of weighing importance of PCh and SCh.

Weight	Criteria
0–2	Extremely low contribution to the variation of the RSP performance that could be made by the impact of the product characteristic/service characteristic
3–4	Low contribution to the variation of the RSP performance that could be made by the impact of the product characteristic/service characteristic
5–6	Moderate contribution to the variation of the RSP performance that could be made by the impact of the product characteristic/service characteristic
7–8	High contribution to the variation of the RSP performance that could be made by the impact of the product characteristic/service characteristic
9–10	Extremely high contribution to the variation of the RSP performance that could be made by the impact of the product characteristic/service characteristic

After that, this paper adopts the prioritization calculation of VMEA, namely Variation Risk Priority Number (VRPN). The calculation formula of the VRPN of RSP i is as follows:

$$VRPN_i = \omega_i \times V_j \times S_j$$

Here, ω_i is the importance of PCh/SCh i, V_j is the variation size of the noise factor j, and S_j is the sensitivity of each PCh/SCh towards noise factor j. Additionally, the degree of the total vulnerability of PSS, $VRPN_m$, could be calculated as below:

$$VRPN_m = \sum_{i=0}^{n} (VRPN_i \times \omega_i).$$

Here, n is the number of RSPs, i is the code number of each RSP, and ω_i is the weight of RSP_i.

3.4. Vulnerability Mitigation

After conducting the calculation of VRPN, the vulnerable condition would become clear and observable. Thus, for vulnerable SChs and PChs, it is essential to take actions to mitigate the risk brought by noise factors. Based on the risk management strategy of PSS [7,73] and the mitigation strategy of the traditional vulnerability assessment framework [60], the vulnerability risk mitigation strategy could be classified into four types as below:

1. Risk avoidance: take actions to avoid the responsibility of the risk, which requires PSS providers to not provide PSS or not be responsible for the machine. This type of action is only adopted when the resource and contract support is poor for the current PSS.
2. Risk reduction: take actions to reduce the probability of the risk, which requires PSS providers to improve their technical ability including monitoring and data collecting. This type of strategy has a strict requirement on whether customers are willing to abide by the contract.
3. Risk sharing: take actions to share the risk with other stakeholders, including customers, manufacturers, insurance firms, and local government. This type of strategy also depends on the willingness of various stakeholders and their preference toward risk.
4. Risk retention: take no actions to solve the risk. Instead, let the user pay for the loss of the risk. This type of strategy has a high-level requirement on the relationship between providers and customers. The legal rules and customers' moral standards also play an important role in this context.

Furthermore, according to Reim et al., it is worth noting that risk management strategy is not suitable for PSS in all situations. Given that PSSs, especially use-oriented and result-oriented PSSs that benefit from the risk of owning a machine, solving a risk sometimes means that the social and economic value could be reduced. Thus, there is a probability for the existence of the side effect caused by the strategy [7]. To overcome this barrier, this framework requires each analyst to examine the side effect by discussing the following topics:

1. Will this action reduce the benefit or increase the cost?
2. Will this action be hindered by stakeholders?
3. Will this action lead to further risk of damaging the machine?
4. Will this action lead to the environmental risk, including pollution and waste?

If the above discussion has been agreed by the analyst, the mitigation is considered effective and safe.

4. Illustration of the Application Example

To verify the effectiveness of the proposed framework, this paper used an application example of the shared washing machine business. The information was collected from an online website, which had provided detailed data about the business mode, machine, and involved stakeholders [74,75]. The targeted firm A was a Japanese firm, which provided sharing washing services for the dormitories of firms and universities. In this business, the major product was a shared washing machine, which was used to clean the clothes for people who had no space or budget to own a washing machine. Furthermore, this firm also provided periodic maintenance, repair, and training services. In this case, the target company provides shared washing machine services to a Japanese nursing home. The customers of the case are old people who live in this nursing home.

The aim of this case study was to assess the vulnerability of this PSS and improve its performance based on the identified vulnerability. To conduct the assessment, a group of two PhD students and three researchers who had abundant knowledge in PSS were involved in this task. The steps of the vulnerability assessment are shown below.

4.1. Representation of the PSS Model

In this case study, the involved product is a washing machine. The main physical components of the washing machine include a U-shaped pipe that can transmit hot water, an internal rolling cylinder that can place clothes, an outer cylinder that weighs the internal cylinder, a detergent input pipe, a glass door for opening the rolling cylinder, a high-temperature heater, which is used to provide 85-degree sterilization, and a control board.

The stakeholders inside this PSS include a washing machine manufacturer, a washing machine provider, and a nursing home. The manufacturer is responsible for providing washing machines and provide a 3-year warranty. The provider provides washing machines for the customer that is the nursing home. The relationship is illustrated by a flow model (see Figure 4).

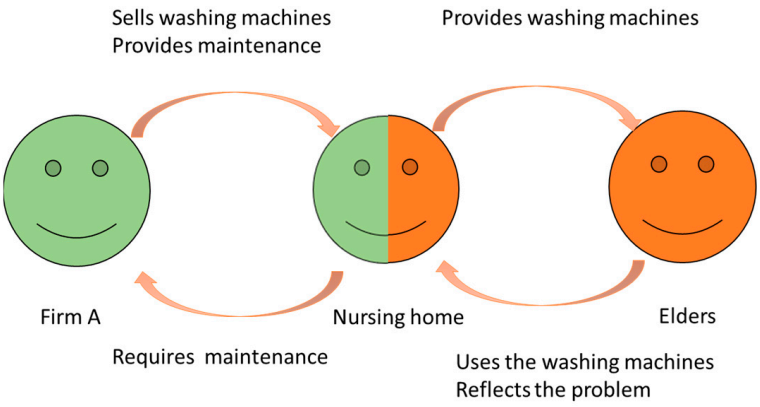

Figure 4. The flow model of the targeted case.

4.2. Define the Key Characteristics and Provide a Causal Breakdown

In this case, the analysts focused on the value propositions of elders, the nursing house, and firm A. Through a 2 h brainstorming, the analysts defined 2 RSPs.

RSP1 was defined as 'ensuring the washing machine is usable' based on the following considerations. For Firm A, the high failure rate of the machine would lead to a sharp increase in maintenance costs. For the elderly, the unavailability of the machine would reduce their satisfaction with the target PSS.

RSP2 was defined as 'ensuring the washing machine is sanitary', and the selection of this RSP was mainly based on the safety of the old users. For each use, it was crucial to ensure that the bacteria of the clothes could not stay alive in the machine and pollute the clothes of the next elder.

Based on the discussion, several PChs and SChs were defined for each RSP, as seen below (see Table 4). The created view model is shown below (see Figures 5 and 6).

Table 4. The PChs and SChs of each RSP.

RSP	PCh	SCh
Ensuring the washing machine is usable	The availability of the washing machine The operability of the washing machine	The time to respond to a problem report The interval time between each usage
Ensuring the washing machine is sanitary	Manual sterilization function,	The interval time of regular disinfection

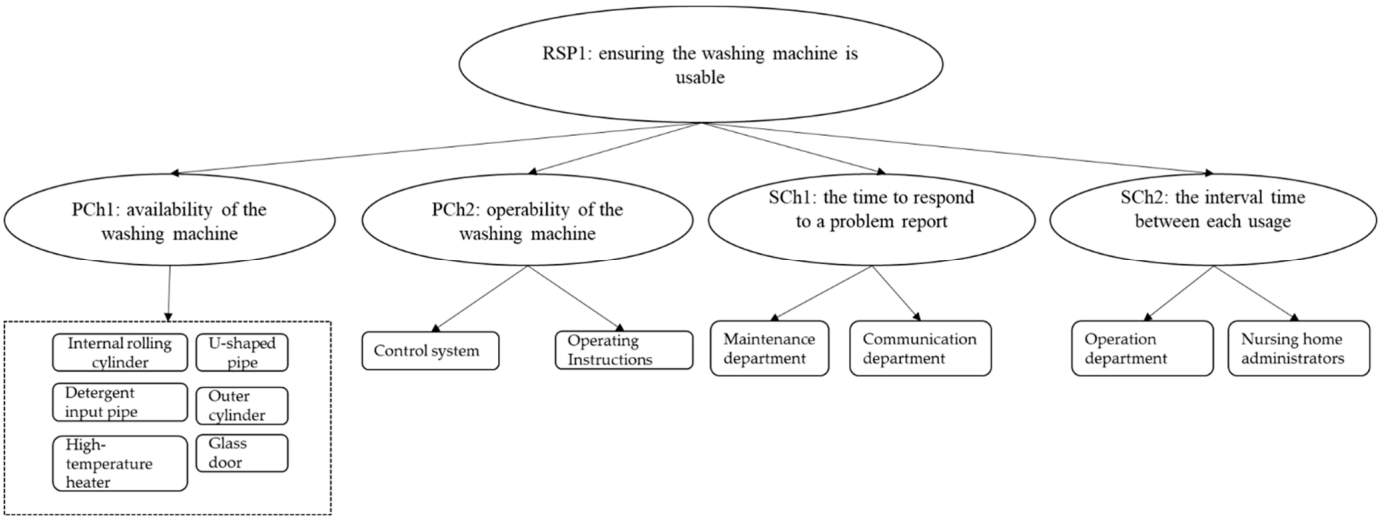

Figure 5. The created view model for RSP1.

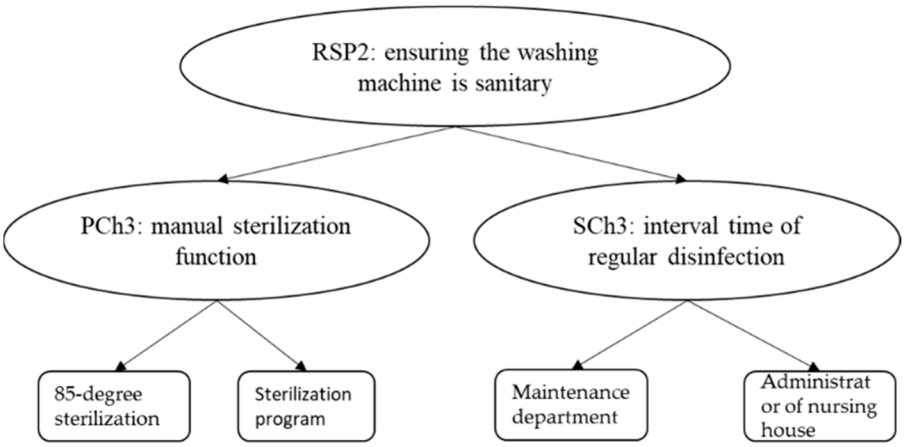

Figure 6. The created view model for RSP2.

After that, the analysts put the known PChs and SChs into the noise factor identification matrix by number. A total of 24 noise factors (NFs) were identified for 2 RSPs (see Tables 5 and 6).

Table 5. The noise factor identification matrix for RSP1.

Root Cause	RSP1			
	PCh1	PCh2	SCh1	SCh2
Organization			NF9: Lack of communication between the liaison department and maintenance department	
Society	NF1: Elderly people's resistance to technological products			NF13: poor understanding of sharing mode of elders
Resource	NF2: Power shortage NF3: aging components	NF7: electronic component failure	NF10: Lack of replacement parts	
Behavior	NF4: Careless customer behavior NF5: Adverse customer behavior		NF11: Frequent vandalism	NF14: Elders refuse to take out clothes timely
Competence	NF6: Mismanagement	NF8: Lack of experience in instructing old users	NF12: Lack of training on serving elders	NF15: Lack of co-operation with nursing administrators
Environment				NF16: Lack of policy about timely taking out

Table 6. The noise factor identification matrix for RSP2.

Root Cause	RSP2	
	PCh3	SCh3
Organization		NF22: Poor communication between administrator and maintenance department
Society		
Resource	NF17: Heater aging NF18: Bacteria in water pipes	NF23: Lack of effective fungicides
Behavior	NF19: The user has not used the sterilization function NF20: Patient using washing machine	
Competence		NF24: Insufficient anti-bactericidal Experience
Environment	NF21: The appearance of a new flu	

4.3. Vulnerability Assessment

This step first required analysts to give weight to each RSP. Based on the discussion, the RSP1 was considered to be extremely crucial for the stakeholders of the targeted PSS. For firm A, the usability of the machine determined the cost of repair and satisfaction of customers. For users (elders), the usability of the machine decided whether they could use the desired service (washing clothes) on time. Thereby, the importance of RSP1 was weighted as 10. For RSP2, although the hygiene issue played an important role in the satisfaction of customers, there was a low burden in the economic and environmental aspects. For this reason, the weight of RSP2 was 6, which was lower than RSP1.

After that, analysts were required to give weight to each PCh and SCh based on their importance for the targeted RSP. The PChs and SChs' impact on RSP should be assessed and weighted based on the probability that the specific PCh or SCh would contribute with a considerable number of variation to the targeted RSP, leading to a great impact on the benefit of stakeholders in the economic, social, and environmental aspects. The given weight was based on a 10-point scale ranging from '1: Extremely unimportant' to '10: Extremely important'. To weigh the importance of the involved characteristics, a brainstorming session was operated.

For RSP1, PCh1, namely the availability of the washing machine, determines to the greatest extent whether the target product could be used at the physical level. Therefore, PCh1 was evaluated as 10. PCh2, namely the operability of the washing machine, determines whether the washing machine could be easily used by the elderly. Considering the overall difficulty of operation of the washing machine was moderate, this characteristic was rated as 5. The time to respond to a problem report was considered to be an important factor in determining whether the product could be repaired in a timely manner. All washing machines must be repaired before the next use. A delay in the repair would lead to a high-level reduction on the satisfaction of the nursing house and elders. Therefore, SCh1 was evaluated as 6. The interval time between each usage determines whether the washing machine can quickly serve the next customer after one laundry service. If the interval were too long, customer dissatisfaction would increase, and the efficiency of the machine would decrease. Considering that the above negative impact will slightly reduce the economic benefit and social value of the target PSS, SCh2 was evaluated as 3.

The results are shown below (see Tables 7 and 8).

Table 7. The weight of each RSP.

Code of RSP	Importance
RSP1	10
RSP2	6

Table 8. The weight of each PCh and SCh.

Code of Characteristics	Weight
PCh1 (RSP1)	10
PCh2 (RSP1)	5
PCh3 (RSP2)	8
SCh1 (RSP1)	6
SCh2 (RSP1)	3
SCh3 (RSP2)	3

After that, this paper adopts the prioritization calculation of VMEA, namely Variation Risk Priority Number (VRPN). The calculation formula of RSP i is as follows:

$$VRPN_i = \omega_i \times V_j \times S_j$$

Here, ω_i is the importance of PCh/SCh i, V_j is the variation size of the noise factor j, and S_j is the sensitivity of each PCh/SCh towards noise factor j.

The results of the VRPN are shown in Table 9.

Table 9. The results of the VRPN.

Code of RSP	The Weight of RSP	Code of Characteristics	The Weight of Characteristics	Code of Noise Factor	Variation of NF	Sensitivity of Characteristic to NF	VRPN of NF	VRPN of Each RSP	Total VRPN
RSP1	10	PCh1	10	NF1	2	6	1200	11,400	29,424
				NF2	8	1	800		
				NF3	8	6	4800		
				NF4	6	6	3600		
				NF5	8	2	1600		
		PCh2	5	NF6	2	2	400	1000	
				NF7	8	4	800		
				NF8	2	2	200		
				NF9	5	4	1200		
		SCh1	6	NF10	8	4	1920	5420	
				NF11	8	2	960		
				NF12	4	6	1440		
		SCh2	3	NF13	2	8	480	4260	
				NF14	8	4	960		
				NF15	5	6	900		
				NF16	8	8	1920		
RSP2	6	PCh3	8	NF17	8	3	1152	6576	
				NF18	6	2	576		
				NF19	5	2	480		
				NF20	8	6	2304		
				NF21	9	5	2040		
		SCh3	3	NF22	2	4	144	792	
				NF23	10	2	360		
				NF24	4	4	288		

4.4. Recommendation on Mitigation

In this step, the analysts examine the VRPN of each NF and provide mitigation countermeasures for some NFs with high impact scores. Based on this consideration, NF 1, 3, 4, 5, 9, 10, 12, 16, 17, 20, and 21 were identified as risky NFs that had obviously higher VRPN than others. Among these NFs, NF3, 4, 20, and 21 were considered factors that can bring high vulnerability due to their high VRPN value. Therefore, the above four factors must be provided with solutions. The other seven factors need to be mitigated as much as possible. According to Section 3.4, mitigation strategies are divided into four categories, namely risk avoidance, risk reduction, risk sharing, and risk retention. Beyond that, analysts discuss side effects in order to prevent mitigation strategies from introducing new vulnerabilities. The results are shown in Table 10.

Table 10. The results of the mitigation analysis.

Code of NF	Mitigation Strategy				Potential Side Effect
	Risk Avoidance	Risk Reduction	Risk Sharing	Risk Retention	
NF1		Education on elders about using washing machine			
NF3		Monthly examination			Improved cost of human resource
NF4			Strengthen collaboration with nursing home administrators		
NF5		Set up monitoring system			High technical competence is required
NF9		Integration of maintenance and liaison departments			

Table 10. *Cont.*

Code of NF	Mitigation Strategy				Potential Side Effect
	Risk Avoidance	Risk Reduction	Risk Sharing	Risk Retention	
NF10		Spare parts for Nursing Homes			
NF12		Post a description of the main problem characteristics at the washing machine work site			
NF16	Ask administrators to guide the per-usage time				
NF17		Provide a periodic examination on the condition of heater			
NF20		Infected people are prohibited from using washing machines			
NF21	Ask administrators to take charge of managing epidemic patients				Further infection caused by the poor competence of administrators

5. Discussion

5.1. Effectiveness of the Proposed Method

In this application, analysts analyze the targeted shared washing machine system. Based on the result of the application, the effectiveness has been shown in the following steps.

First, this vulnerability assessment framework requires analysts to identify the key characteristic of PSS, which is the focused vulnerable element. According to the characteristics of shared washing machines and customers, namely the characteristics of nursing homes, one key RSP is identified, namely ensuring that the washing machine is reliable and safe. Based on this RSP, four product and service characteristics (PChs and SChs) are identified: PCh1: the availability of the washing machine; PCh2: the sanitation of the washing machine; SCh1: the time to respond to a problem report; and SCh2: the interval time between washing machines being used by each elderly person. In this way, the characteristics of PSS could represent the product and service components. Furthermore, this method allows designers and analysts to show the key characteristic in an observable and controllable way. This step has also shown that the theory of previous papers [20,36,74] that RSP could help PSS designers identify PChs and SChs is also effective in the aspect of PSS vulnerability assessment.

After that, using a modified noise identification matrix based on fishbone analysis, which uses six root causes of previous research, 20 potential noise factors (NFs) are identified. This method provides an effective and efficient solution for analysts to identify the consequence of the vulnerable issue based on six rational root causes that have been proven by previous research [10]. All of the selected root causes have shown effectiveness in enabling designers to identify NFs in an efficient and effective way. The feedback from the multi-functional group has expressed a high-level satisfaction with this reasoning method.

Thirdly, with the help of VRPN, analysts can quantify the potential impact of different noises. The dimensions of variation and sensitivity have been successfully assessed by the members of the discussion group. Since this study asked analysts to assess the relative importance of features, although some noise had a large impact on the range of features, the proportion of impacted features lowered the final score. This is due to the fact that the proportion of importance each feature occupies in RSP allows analysts to assess their true impact more objectively. Eleven NFs are identified as influential factors based on discussion.

Fourthly, to mitigate the vulnerability caused by 11 high-impact noise factors, this study uses a mitigation analysis form to allow analysts to discuss potential solutions within the scope of 4 defined strategies. All of the members of the group believe these strategies could contribute to the mitigation of the target problem. In addition, the consideration of side effects is raised, considering that mitigating PSS risks could lead to further new risks. Indeed, this consideration has been proven to be essential. As the result, three side effects are identified to be highly possible to appear if the planned actions are taken.

Furthermore, this framework has shown a great degree of simplicity and comprehension for beginners and those without sufficient knowledge of vulnerability analysis to conduct a quick and effective vulnerability assessment. During the application, although some participants were only introduced for a short course, they showed a high-level competence to conduct this framework. This framework is considered to be a highly instructive tool, with step-by-step instructions that can be easily understood by inexperienced individuals and facilitate their participation in further evaluations.

Overall, this framework provides an intuitive, understandable, and simplified vulnerability assessment framework for designers and managers who want to assess PSS vulnerabilities and mitigate risks. The existence of the VRPN provides designers and managers with a feasible method to quantify the vulnerability of different noises to target characteristics. Although some steps still need to be further optimized, this study undoubtedly shows the current designers and managers the dimensions and issues that need to be considered in assessing the vulnerability of PSS.

5.2. The Theoretical Implication of This Research

In this research, the theoretical development and novelty could be explained as below.

For the development of the research relating to PSS vulnerability, this research has proposed the first assessment method that is suitable for the PSS field. Before this research, the study on the vulnerability of PSS was still in the understanding stage, which focused on definitions [9,10,50]. Although there were some similar methods such as PSS FMEA [14,64], PSS FMEA could not consider the dimension of sensitivity and variation. Additionally, the PSS VMEA has a stronger ability to analyze the vulnerable issues related to intangible items like social trends and organizational structure. Furthermore, it is worth noting that VEMA starts from the top-down vulnerability analysis based on the key characteristics and the value orientation of stakeholders, rather than the interruption of a single function. The above aspects could not be performed by PSS FMEA. This method has also utilized the theoretical findings of previous papers [7–10] related to PSS vulnerability. For example, the knowledge about risk management and side effects of various strategies [7,8] has been applied to the mitigation strategy. The knowledge about the definition of vulnerability and the taxonomy of perturbation [9,10] has been utilized in part of the cause–consequence analysis for NF identification and analysis. For this reason, this study successfully integrates previous theoretical knowledge into this framework and advances the study of PSS vulnerability from the theoretical stage to the implementation and verification stage.

Furthermore, as discussed in Section 2.5, the traditional VMEA is a method that focuses on the product field. However, PSS is a system that requires manufacturing firms to consider service elements, which limits the usefulness of the traditional VMEA. Based on this consideration, the proposed framework has integrated some knowledge from PSS perturbation [9,10], PSS risk management [7], service engineering [20], and PSS characteristics [70,71]. For this reason, this framework requires PSS analysts to consider dividing RSP into PChs and SChs to show the characteristics of services. Additionally, the cause–consequence process is optimized through a fishbone analysis based on six identified root causes. Furthermore, the existence of side effects caused by the characteristics of PSS is considered in this framework. The above actions enable the VMEA to become effective for PSS design and vulnerability. This modification is also meaningful for the future development of the traditional VMEA, which provides a good example about how to make it suitable for systems that are not only made up of hardware components.

5.3. Limitations

Despite the contributions, this study also exists some limitations.

First, due to the lack of resources, the application example of this study uses online secondary data. Since the authors could not build an effective relationship with the manager of the targeted firm, namely Firm A, the effectiveness of the application could not be verified by Firm A. Instead, it was verified by several researchers and PhD students who come from different academic institutes. With continuous discussion, all the members agreed that this framework could be utilized to assess the vulnerability of PSS. However, to date, the proposed framework has only been tested in the case of Firm A, which is a B-to-C business. There is a high-level expectation that this framework could be verified in further real and complex PSS cases.

Second, in this study, RSP represents the value orientation of different stakeholders. However, according to existing research, in a PSS, the value demands of different stakeholders may be conflicting [76]. For example, local communities often demand low pollution as well as low noise. However, this requirement will undoubtedly increase the cost of the provider and the manufacturer. Conflicting value demands may lead to further vulnerability, which was not considered in this study.

Last but not least, although VRPN is an effective and simplified method, it is limited in two situations. On the one hand, VRPN is usually operated based on a hypothesis that noise factors or failure modes are independent, which could not have an influence on each other. The usage of VRPN is not suitable when the system is extremely complex and noise factors have a negative influence on each other. On the other hand, in order to quantify the proportion of parameters and features in VRPN, this study adopts ten points to evaluate them. Although this method can quantify different parameters in an intuitive and easy way, this mathematical expression can be vague and somewhat subjective. In future research, some more precise quantitative methods, such as AHP and DEMATEL, need to be further discussed and used. Furthermore, this mathematical method has a high-level requirement on the competence and experience of the members of the multi-functional group. The result of the VRPN would be unreliable if analysts could not find multiple experts who have abundant experience.

6. Conclusions and Future Direction

In this study, authors have developed a vulnerability assessment framework based on the variation mode and effect analysis (VMEA) for the field of PSS. To enable this framework to be effective for the PSS vulnerability assessment, authors have also utilized the concepts of RSP, PCh, SCh, fishbone analysis, and risk management strategy. To verify the effectiveness of the proposed framework, an application example of the shared washing machine business is used. The assessment shows that 11 noise factors could have a serious threat on the 2 identified RSPs. A series of strategies are provided to mitigate the adverse influence. It is found that the proposed modification and improvement are effective for the assessment of PSS vulnerability. Through the application, this framework has been found to be powerful in analyzing the vulnerability of PSS. Additionally, participants in the application agreed that this method is easy to understand. VRPN and RSP identification is considered suitable for use and understanding by some B2C PSS providers. The simplicity and comprehension of this method is also considered to facilitate the participation of some stakeholders who do not have sufficient professional knowledge in the vulnerability assessment, thereby increasing the reliability of the assessment. Compared with many complex assessment methods, this method allows participants to gain an intuitive understanding of the vulnerability status of the PSS and prepare for potential problems faster and more efficiently.

The proposed framework has also shown great meaningfulness and novelty for filling the research gap of the PSS vulnerability analysis and developing the traditional VMEA to become suitable for PSS assessment. Based on the results of this study, it can be concluded that this research is the first to focus on the sensitivity of noise factors and mitigate the PSS

vulnerability in the form of a framework. This framework utilizes a mathematical method called VRPN to calculate the degree of vulnerability. In addition, this study utilized the RSP concept to replace the traditional KPC in VMEA and decomposed RSP into PChs and SChs, which solves the problem that traditional VMEA cannot analyze service characteristics. Furthermore, this study provided six reasonable root causes for causal analysis based on previous research findings. Finally, this study proposed a new set of vulnerability mitigation strategies that simultaneously consider risk management and the side effects led by PSS characteristics. Overall, the research presented in this paper provides valuable insights and practical methods for improving PSS design and management. This study demonstrated that this method can improve the traditional VMEA and make it suitable for PSS vulnerability analysis.

However, this study also has several limitations. First, the information on the selected case comes from online data, which is secondary data. Secondly, this study has not proposed a clear and effective solution when there are two or multiple conflicting RSP. Thirdly, the mathematical model of this research, namely VRPN, has a poor performance when the identified NFs have a mutual influence on each other. Furthermore, although the sensitivity and variation scores as well as RSP and characteristics' weights are assessed according to existing criteria, these results may not be accurate due to limitations of subjective factors.

For the future direction, it is expected to use further case studies including B2B and B2C business to verify the effectiveness of this framework. There is a strong demand to manage the conflicting requirements of stakeholders based on the mathematical method or management means. Additionally, the usage of fuzzy math could be a promising solution to solve the problem relating to the calculation of VRPN. To further enhance and develop this framework, there should be more consideration about redesign. Indeed, risk management strategy sometimes has side effects and also cannot solve the problem effectively when analysts choose to use risk retention. Thus, it would be essential to replace, delete, and upgrade the components when they are related to vulnerable issues. One hopeful way to achieve redesign is the modular design. In order to allow PSS to be redesigned and improved at any time according to the source of vulnerability, a modular design is essential. Through modularity, PSS can easily delete, redesign, or upgrade vulnerable modules. However, so far, no research in the field of PSS has focused on how to use vulnerability analysis and robust design to provide a design scheme that can be continuously changed for modular PSS. A robust and upgradable PSS design is expected. Last but not least, although there is still no formal discussion about utilizing PSS VMEA to design a new PSS, it is highly possible that this method could contribute to the design of a reliable and robust PSS in the phase of design. In other words, by proposing RSPs during the design phase and translating them into key product and service characteristics, designers can take the potential noise seriously and prepare mitigation strategies before the implementation phase.

Author Contributions: Conceptualization, H.W.; methodology, H.W.; software, H.W.; validation, H.W., Y.M., Y.T., S.A. and Y.S.; formal analysis, H.W. and S.A.; data curation, H.W.; writing—original draft preparation, H.W.; writing—review and editing, H.W., Y.M., Y.T., S.A. and Y.S.; supervision, Y.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Oliva, R.; Kallenberg, R. Managing the transition from products to services. *Int. J. Serv. Ind. Manag.* **2003**, *14*, 160–172. [CrossRef]
2. Vezzoli, C.; Ceschin, F.; Diehl, J.C.; Kohtala, C. New design challenges to widely implement 'Sustainable Product–Service Systems'. *J. Clean. Prod.* **2015**, *97*, 1–12. [CrossRef]

3. Goedkoop, M.; van Halen, C.; te Riele, H.; Rommens, P. *Product Service Systems, Ecological and Economic Basics*; VROM: The Hague, The Netherlands, 1999.
4. Tukker, A. Eight types of product–service system: Eight ways to sustainability? Experiences from SusProNet. *Bus. Strategy Environ.* **2004**, *13*, 246–260. [CrossRef]
5. Haase, R.P.; Pigosso DC, A.; McAloone, T.C. Product/service-system origins and trajecto-ries: A systematic literature review of PSS definitions and their characteristics. *Pro-Cedia Cirp* **2017**, *64*, 157–162. [CrossRef]
6. Tukker, A. Product services for a resource-efficient and circular economy—A review. *J. Clean. Prod.* **2015**, *97*, 76–91. [CrossRef]
7. Reim, W.; Parida, V.; Sjödin, D.R. Risk management for product-service system operation. *Int. J. Oper. Prod. Manag.* **2016**, *36*, 665–686. [CrossRef]
8. Sakao, T.; Rönnbäck, A.Ö.; Sandström, G.Ö. Uncovering benefits and risks of integrated product service offerings—Using a case of technology encapsulation. *J. Syst. Sci. Syst. Eng.* **2013**, *22*, 421–439. [CrossRef]
9. Wang, H.; Mitake, Y.; Tsutsui, Y.; Alfarisi, S.; Shimomura, Y. An ontology for the vulnerability of Product-Service System. *Procedia CIRP* **2022**, *107*, 338–343. [CrossRef]
10. Wang, H.; Mitake, Y.; Tsutsui, Y.; Alfarisi, S.; Shimomura, Y. A Taxonomy of Product–Service System Perturbations through a Systematic Literature Review. *J. Risk Financ. Manag.* **2022**, *15*, 443. [CrossRef]
11. Taguchi, G. *System of Experimental Design; Engineering Methods to Optimize Quality and Minimize Costs*; UNIPUB/Kraus International Publications: New York, NY, USA, 1987; ISBN 978-0527916213.
12. Hasenkamp, T.; Arvidsson, M.; Gremyr, I. A review of practices for robust design methodology. *J. Eng. Des.* **2009**, *20*, 645–657. [CrossRef]
13. Martinez, V.; Neely, A.; Velu, C.; Leinster-Evans, S.; Bisessar, D. Exploring the journey to services. *Int. J. Prod. Econ.* **2017**, *192*, 66–80. [CrossRef]
14. Kimita, K.; Sakao, T.; Shimomura, Y. A failure analysis method for designing highly reliable product-service systems. *Res. Eng. Des.* **2018**, *29*, 143–160. [CrossRef]
15. Russo, D.; Birolini, V.; Ceresoli, R. Fit: A triz based failure identification tool for product-service systems. *Procedia CIRP* **2016**, *47*, 210–215. [CrossRef]
16. Song, W.; Zheng, J.; Niu, Z.; Wang, Q.; Tang, Y.; Zheng, P. Risk evaluation for industrial smart product-service systems: An integrated method considering failure mode correlations. *Adv. Eng. Inform.* **2022**, *54*, 101734. [CrossRef]
17. Chakhunashvili, A.; Johansson, P.M.; Bergman, B.L.S. Variation mode and effect analysis. In *Annual Symposium Reliability and Maintainability, 2004-RAMS*; IEEE: New York, NY, USA, 2004; pp. 364–369.
18. Cronholm, K. Design of experiment based on VMEA (Variation Mode and Effect Analysis). *Procedia Eng.* **2013**, *66*, 369–382. [CrossRef]
19. Arai, T.; Shimomura, Y. Proposal of service CAD system-a tool for service engineering. *CIRP Ann.* **2004**, *53*, 397–400. [CrossRef]
20. Shimomura, Y.; Tomiyama, T. Service modeling for service engineering. In *International Working Conference on the Design of Information Infrastructure Systems for Manufacturing*; Springer: Boston, MA, USA, 2002; pp. 31–38.
21. Phillips, J.; Simmonds, L. Using fishbone analysis to investigate problems. *Nurs. Times* **2013**, *109*, 18–20.
22. Mont, O.K. Clarifying the concept of product–service system. *J. Clean. Prod.* **2002**, *10*, 237–245. [CrossRef]
23. D'Agostin, A.; de Medeiros, J.F.; Vidor, G.; Zulpo, M.; Moretto, C.F. Drivers and barriers for the adoption of use-oriented product-service systems: A study with young consumers in medium and small cities. *Sustain. Prod. Consum.* **2020**, *21*, 92–103. [CrossRef]
24. Lindahl, M.; Sundin, E.; Sakao, T. Environmental and economic benefits of Integrated Product Service Offerings quantified with real business cases. *J. Clean. Prod.* **2014**, *64*, 288–296. [CrossRef]
25. Kühl, C.; Tjahjono, B.; Bourlakis, M.; Aktas, E. Implementation of Circular Economy principles in PSS operations. *Procedia CIRP* **2018**, *73*, 124–129. [CrossRef]
26. Coreynen, W.; Matthyssens, P.; Van Bockhaven, W. Boosting servitization through digitization: Pathways and dynamic resource configurations for manufacturers. *Ind. Mark. Manag.* **2017**, *60*, 42–53. [CrossRef]
27. Dmitrijeva, J.; Schroeder, A.; Bigdeli, A.Z.; Baines, T. Paradoxes in servitization: A processual perspective. *Ind. Mark. Manag.* **2022**, *101*, 141–152. [CrossRef]
28. Moro, S.; Cauchick-Miguel, P.A.; de Sousa Mendes, G.H. Product-service systems benefits and barriers: An overview of literature review papers. *Int. J. Ind. Eng. Manag.* **2020**, *11*, 61. [CrossRef]
29. Maussang, N.; Zwolinski, P.; Brissaud, D. Product-service system design methodology: From the PSS architecture design to the products specifications. *J. Eng. Des.* **2009**, *20*, 349–366. [CrossRef]
30. Muto, K.; Kimita, K.; Shimomura, Y. A guideline for product-service-systems design process. *Procedia CIRP* **2015**, *30*, 60–65. [CrossRef]
31. Akasaka, F.; Nemoto, Y.; Kimita, K.; Shimomura, Y. Development of a knowledge-based design support system for Product-Service Systems. *Comput. Ind.* **2012**, *63*, 309–318. [CrossRef]
32. Kimita, K.; Shimomura, Y. Design method for modular product-service system architecture. In Proceedings of the DESIGN 2012, the 12th International Design Conference, Dubrovnik, Croatia, 21–24 May 2012; pp. 979–988.
33. Song, W.; Sakao, T. A customization-oriented framework for design of sustainable product/service system. *J. Clean. Prod.* **2017**, *140*, 1672–1685. [CrossRef]

34. Sakao, T.; Song, W.; Matschewsky, J. Creating service modules for customising product/service systems by extending DSM. *CIRP Ann.* **2017**, *66*, 21–24. [CrossRef]
35. Vezzoli, C.; Ceschin, F.; Osanjo, L.; M'Rithaa, M.K.; Moalosi, R.; Nakazibwe, V.; Diehl, J.C. *Designing Sustainable Energy for All: Sustainable Product-Service System Design Applied to Distributed Renewable Energy*; Springer Nature: Berlin/Heidelberg, Germany, 2018.
36. Hara, T.; Arai, T.; Shimomura, Y. Integrated representation of function, service activity, and product behavior for service development. In Proceedings of the International Design Engineering Technical Conferences and Computers and Information in Engineering Conference, Brooklyn, NY, USA, 3–6 August 2008; pp. 67–76.
37. Cong, J.-C.; Chen, C.-H.; Zheng, P.; Li, X.; Wang, Z. A holistic relook at en-gineering design methodologies for smart product-service systems development (Nov.). *J. Clean. Prod.* **2020**, *272*, 122737. [CrossRef]
38. Kuo, T.C.; Wang, M.L. The optimisation of maintenance service levels to support the product service system. *Int. J. Prod. Res.* **2012**, *50*, 6691–6708. [CrossRef]
39. Wang, N.; Ren, S.; Liu, Y.; Yang, M.; Wang, J.; Huisingh, D. An active preventive maintenance approach of complex equipment based on a novel product-service system operation mode. *J. Clean. Prod.* **2020**, *277*, 123365. [CrossRef]
40. Garetti, M.; Rosa, P.; Terzi, S. Life cycle simulation for the design of product–service systems. *Comput. Ind.* **2012**, *63*, 361–369. [CrossRef]
41. Sundin, E. Life-cycle perspectives of product/service-systems: In design theory. In *Introduction to Product/Service-System Design*; Springer: London, UK, 2009; pp. 31–49.
42. Yang, L.; Xing, K.; Lee, S.H. A new conceptual life cycle model for Result-Oriented Product-Service System development. In Proceedings of the 2010 IEEE International Conference on Service Operations and Logistics, and Informatics, Qingdao, China, 15–17 July 2010; IEEE: New York, NY, USA, 2010; pp. 23–28.
43. Clayton, R.J.; Backhouse, C.J.; Dani, S. Evaluating existing approaches to product-service system design: A comparison with industrial practice. *J. Manuf. Technol. Manag.* **2012**, *23*, 272–298. [CrossRef]
44. Ball, R.E. *Aircraft Combat Survivability: Susceptibility and Reduction*; Lecture Notes; Department of Aeronautics, Naval Postgraduate School: Monterey, CA, USA, 1979.
45. Turner, B.L.; Kasperson, R.E.; Matson, P.A.; McCarthy, J.J.; Corell, R.W.; Christensen, L.; Eckley, N.; Kasperson, J.X.; Luers, A.; Martello, M.L.; et al. A framework for vulnerability analysis in sustainability science. *Proc. Natl. Acad. Sci. USA* **2003**, *100*, 8074–8079. [CrossRef]
46. Adger, W.N. Vulnerability. *Glob. Environ. Change* **2006**, *16*, 268–281. [CrossRef]
47. Qiu, Q.A.; Cui, L.R.; Kong, D.J. Availability and maintenance modeling for a two-component system with dependent failures over a finite time horizon. *Proc. Inst. Mech. Eng. O J. Risk Reliab.* **2019**, *233*, 200–210. [CrossRef]
48. Li, Y.F.; Liu, Y.; Huang, T.D.; Huang, H.Z.; Mi, J.H. Reliability assessment for systems suffering common cause failure based on Bayesian networks and proportional hazards model. *Qual. Reliab. Eng. Int.* **2020**, *36*, 2509–2520. [CrossRef]
49. Zhang, Y.G.; Yu, T.X.; Song, B.F. A reliability allocation method of mechanism considering system performance reliability. *Qual. Reliab. Eng. Int.* **2019**, *35*, 2240–2260. [CrossRef]
50. Estrada, A.; Romero, D. A system quality attributes ontology for product-service systems functional measurement based on a holistic approach. *Procedia CIRP* **2016**, *47*, 78–83. [CrossRef]
51. Umeda, Y.; Daimon, T.; Kondoh, S. Proposal of Decision Support Method for Life Cycle Strategy by Estimating Value and Physical Lifetimes—Case Study. In Proceedings of the 4th International Symposium on Environmentally Conscious Design and Inverse Manufacturing, Tokyo, Japan, 12–14 December 2005; pp. 606–613.
52. Cooper, T. Inadequate life? Evidence of consumer attitudes to product obsolescence. *J. Consum. Policy* **2004**, *27*, 421–449. [CrossRef]
53. Smith, A.K.; Bolton, R.N. An experimental investigation of customer reactions to service failure and recovery encounters: Paradox or peril? *J. Serv. Res.* **1998**, *1*, 65–81. [CrossRef]
54. Besch, K. Product-service systems for office furniture: Barriers and opportunities on the European market. *J. Clean. Prod.* **2005**, *13*, 1083–1094. [CrossRef]
55. Hou, C.; Jo, M.S.; Sarigöllü, E. Feelings of satiation as a mediator between a product's perceived value and replacement intentions. *J. Clean. Prod.* **2020**, *258*, 120637. [CrossRef]
56. Reim, W.; Sjödin, D.; Parida, V. Mitigating adverse customer behaviour for product-service system provision: An agency theory perspective. *Ind. Mark. Manag.* **2018**, *74*, 150–161. [CrossRef]
57. de Medeiros, J.F.; Marcon, A.; Ribeiro JL, D.; Quist, J.; D'Agostin, A. Consumer emotions and collaborative consumption: The effect of COVID-19 on the adoption of use-oriented product-service systems. *Sustain. Prod. Consum.* **2021**, *27*, 1569–1588. [CrossRef]
58. Hara, T.; Sakao, T.; Fukushima, R. Customization of product, service, and product/service system: What and how to design. *Mech. Eng. Rev.* **2019**, *6*, 18–00184. [CrossRef]
59. Munoz Lopez, N.; Santolaya Saenz, J.L.; Biedermann, A.; Serrano Tierz, A. Sustainability assessment of product–service systems using flows between systems approach. *Sustainability* **2020**, *12*, 3415. [CrossRef]
60. Asbjornslett, B.E. Assess the vulnerability of your production system. *Prod. Plan. Control* **1999**, *10*, 219–229. [CrossRef]
61. DeSmit, Z.; Elhabashy, A.E.; Wells, L.J.; Camelio, J.A. Cyber-physical vulnerability assessment in manufacturing systems. *Procedia Manuf.* **2016**, *5*, 1060–1074. [CrossRef]

62. Anton, P.S.; Anderson, R.H.; Mesic, R.; Scheiern, M. The Vulnerability Assessment & Mitigation Methodology. Rand National Defense Research Inst Santa Monica Ca. 2003. Available online: https://www.rand.org/content/dam/rand/pubs/monograph_reports/2005/MR1601.pdf (accessed on 9 March 2023).
63. Zhang, J.; Zhao, X.; Song, Y.; Qiu, Q. Joint optimization of maintenance and spares ordering policy for a use-oriented product-service system with multiple failure modes. *Appl. Stoch. Model. Bus. Ind.* **2021**, *37*, 1123–1142. [CrossRef]
64. Flax, L.K.; Jackson, R.W.; Stein, D.N. Community vulnerability assessment tool methodology. *Nat. Hazards Rev.* **2002**, *3*, 163–176. [CrossRef]
65. Mahl, T.; Köhler, C.; Arnold, D.; Lins, D.; Kuhlenkötter, B. PSS-FMEA: Towards an integrated FMEA method to support the development of product-service systems in SMEs. *Proc. Des. Soc.* **2021**, *1*, 2501–2510. [CrossRef]
66. Johansson, P.; Chakhunashvili, A.; Barone, S.; Bergman, B. Variation mode and effect analysis: A practical tool for quality improvement. *Qual. Reliab. Eng. Int.* **2006**, *22*, 865–876. [CrossRef]
67. Bellinello, M.M.; Michalski, M.A.; Melani, A.H.; Netto, A.C.; Murad, C.A.; Souza, G.F. PAL-VMEA: A Novel Method for Enhancing Decision-Making Consistency in Maintenance Management. *Appl. Sci.* **2020**, *10*, 8040. [CrossRef]
68. Goetz, S.; Hartung, J.; Schleich, B.; Wartzack, S. Robustness evaluation of product concepts based on function structures. In Proceedings of the Design Society: International Conference on Engineering Design, Delft University of Technology, Delft, The Netherlands, 5–8 August 2019; Cambridge University Press: Cambridge, UK, 2019; Volume 1, pp. 3521–3530.
69. Pavasson, J.; Karlberg, M. Variation mode and effect analysis compared to FTA and FMEA in product development. In Proceedings of the 19th AR2TS Advances in Risk and Reliability Technology Symposium, Stratford-upon-Avon, UK, 12–14 April 2011; pp. 252–260.
70. Sakao, T.; Birkhofer, H.; Panshef, V.; Dorsam, E. An effective and efficient method to design services: Empirical study for services by an investment-machine manufacturer. *Int. J. Internet Manuf. Serv.* **2009**, *2*, 95–110. [CrossRef]
71. Haber, N.; Fargnoli, M.; Sakao, T. Integrating QFD for product-service systems with the Kano model and fuzzy AHP. *Total Qual. Manag. Bus. Excell.* **2020**, *31*, 929–954. [CrossRef]
72. Ishikawa, K.; Loftus, J.H. *Introduction to Quality Control*; 3A Corporation: Tokyo, Japan, 1990.
73. Reim, W.; Parida, V.; Sjödin, D.R. Managing risks for product-service systems provision: Introducing a practical decision tool for risk management. In *Practices and Tools for Servitization*; Palgrave Macmillan: Cham, Switzerland, 2018; pp. 249–266.
74. Daiwa Corporation. Available online: https://www.daiwa-corp.com/ (accessed on 12 December 2022).
75. Example of Commercial Laundry Equipment Shipment. Available online: https://www.daiwa-corp.com/business/record.php/ (accessed on 12 December 2022).
76. Song, W. Requirement management for product-service systems: Status review and future trends. *Comput. Ind.* **2017**, *85*, 11–22. [CrossRef]