Extending lifecycles of connected offerings

John Lindström and Karl Andersson
Cybersecurity, Department of Computer Science, Electrical and Space Engineering
Luleå University of Technology, 971 87 Luleå, Sweden

Abstract: The whitepaper provides an overview of how it is possible to extend the lifecycles of connected offerings comprising for instance hardware, software, a support-service system and long-term management of operation. These offerings may span from products, products with add-on or integrated services, solutions, product-service systems, industrial product-service systems, and functions, etc. The selection of business model for an offering has a large impact on how the provider and customer/user can maintain, update and support the offering and keep it operational with a high level of availability and cybersecurity. In addition, new ways of designing the sales agreements or contracts may also lead to an increased level of re-circularity, extension of lifecycles and less ecological impact. This requires that an offering's lifecycle is foreseen and planned for already at the initial conceptual, requirement engineering, and design phases, rather than trying to add this at a later stage at a much higher cost and effort. The **total cost of ownership** perspective is applied and compared to the **initial cost** perspective, which currently often is used.

The intended readers of the white paper are mainly the following roles within the European Union (EU): researchers, product owners, product managers, designers, enterprise/hardware/software architects, developers, and top managements.

Introduction

There are some foundational matters to consider for a business and its value chain (or value network) in order to understand how to organize to create, deliver and capture value for all the involved. If there is only a winning situation for one or a few of the parties involved, it is likely that the economic part of the lifecycle may be shortened considerably or stop. Further, the technical part of the lifecycle needs to match the expectations of the economic part or else that can impair or also stop the lifecycle too early (Lindström and Karlberg, 2017). Additionally, there are some circular economy principles to be aware of, which are formalized into the ISO 59004 standard, and can be summarized as follows: systems thinking, value creation, value sharing, resource availability focus, and resource traceability. However, nothing is 100% circular or preferred to be so (Lindahl and Dalhammar, 2022)!

Value-creating business models or concepts for the circular economy with connected offerings

The selection of an appropriate business model is key for extending lifecycles in a sustainable manner to enable necessary remote access, control and monitoring capabilities for both the provider and customer/users. Concerning connected offerings, this usually entails using business models or concepts that are further advanced and complex than a product or a product with simplistic optional add-on services. Examples of potential business models or concepts to consider are products with integrated

services, solutions, Product-Service Systems (PSS), Industrial Product-Services Systems (IPS^2), Functional/Total Care Products (FP) (White et al., 1999; Tomiyama, 2001; Mont, 2001; Meier et al., 2008; Alonzo-Rasgado et al., 2004; Roy et al., 2013). Thus, most of the basics are known but many of the concepts were a bit ahead of time due to the technical gaps – which now are being closed with affordable massive high performance computing and data storage services, scalable and flexible cloud services and data centers, high bandwidth 4G and 5G communications, edge services, improved cybersecurity and IoT security, and an in general improved and redundant communications infrastructure (Internet). All these aforementioned are more or less needed by the further advanced and complex business models or concepts to be attractive for both providers and customers/users in terms of **sustainable win-win situations**. What seems to be a major issue today is that customers/users need to look into these new types of connected offerings and ask that they are not provided as simple products or products with simplistic add-on services, but using further advanced and complex business models or concepts enabling a larger value co-creation while at the same time being additionally circular and allowing co-creation of value too (Rönnberg Sjödin et al., 2017).

Design and development of connected offerings for the circular economy

The design and development process must integrate several matters affecting the lifecycle - **starting from the very start until the very end of it!** To expect is also that changes, updates, or upgrades, will be necessary during the lifecycle for to keep the connected offering up-to-date and compliant to for instance various global legal, regulatory and standards requirements. An adequate level of cybersecurity over the lifecycle is and will be a key factor to be long-term competitive, sustainable, compliant with EU legal and regulatory requirements, and be able to efficiently manage many of the lifecycle aspects. Further, there is a need to be aware of design methods and lifecycle models for circularity (Bocken et al., 2016; Liu et al., 2020; Rojek et al., 2021), management of strained or stressed value chains/networks (cf. Zis, 2023) which occur due to for instance geo-political tensions and pandemics, and apply applicable design-for-Xs to accomplish durable connected offerings with long, sustainable and secure lifecycles (Lindström et al., 2024). In addition, there needs to be planning for how to handle the different phases of the lifecycle and manage these efficiently to uphold the necessary win-win situations. Remote fleet management functionality is a key for the efficiency as visits on site for all monitoring, service and support will take a lot of time and travelling – in particular, within rural areas or areas with heavy traffic and congestions. Wanted is to extend the use, or operations, phase as much as possible via durable design combined with supporting services, support and maintenance timely provided (Jacobson et al., 2023). To be able to do this, there is a need to be able to monitor connected offerings and their function plus wear and tear as well as analyze the use information/data to understand **how the offering is actually used and operated**. If there are signs of unexpected wear and tear or non-optimal usage, design changes or optimizations can be proposed as well as guidance on what usage patterns to change to avoid unnecessary stops or breakdowns (Lindström et al., 2024).

Logistics and its traceability/monitoring for safe and secure circularity

The logistics and its traceability/monitoring is required to manage both inbound, reverse and outbound logistics and **maintain the integrity** of the connected offerings and its parts or components etc. Depending on criticality of where and for what the connected offerings are aimed for, that may require to have safe and secure supply chains or networks. If so is needed, the connected offerings and its parts

or components need to be protected from tampering, unauthorized changes or additions regarding hardware, software or use of hostile/dishonest services, support or maintenance activities etc. which may disrupt or stop parts or the whole function of the connected offering (ENISA, 2023; Lindström, 2023). Some recent high profile supply chain attacks related to software were the Solarwinds (Orion) in 2019/2020 and Kaseya (VSA) in 2021 incidents as well as hardware-related were the electronic devices (pagers and walkie-talkies) attacks in Lebanon during 2024. However, most value chains or networks need a certain level of traceability/monitoring to uphold a level of safety and security for all parts that are transported, shipped, electronically downloaded or distributed, etc.

Extending lifecycles of connected offerings – some matters to consider while doing initial conceptualization, planning and design

To extend the lifecycle of connected offerings requires that quite a few matters are considered. If possible, as many as possible should start to be considered from as early on as possible. However, as it is impossible to know all about the future, many matters will emerge or change as time passes. Thus, it is important **to conceptualize, design, and plan for flexibility, changeability, and upgradeability at the same time as availability, with maintainability and reliability, of the connected offering is part of the equation too**. This section comprises some important additional matters and further it is important to remember that certain contexts may require additional ones as well.

Extending the lifecycles with associated costs and a need for new payment schemes

To extend the lifecycle of connected offerings **will not be free for anyone involved in the value chain or network**, and this goes for both the provider and customers/users. In addition, for instance the added requirements from the EU legal and regulatory developments, plus any additional global ones, will make the lifecycle quite a bit more expensive and complex than before and therefore the provider side needs to get compensated for that and consequently the prices will increase to cover this. Further, a lifecycle perspective is needed in the business modelling and the pricing strategy. Proposed is to employ a **total lifecycle cost strategy** versus staring only at the initial costs and a strive to cover these as early as possible. Foreseen is that there will be different payment schemes than for current products with potentially a higher initial payment combined with regular payments (which may be correlated to how much value that has been created for the customer/user). Thus, there is a need to develop the business contracts/agreements to cope with new schemes having regular monthly/annual payments and/or performance-based payment schemes as well. However, there is of course a risk related to this as it is hard to foresee and predict all that happens in the future in terms of cost increases, geo-political tensions or developments, and strained supply chains with resulting price surges due to shortages of parts and components. This will affect extending lifecycles in terms of planning, design, and operations with maintenance strategy. Further, the selected business model, or models, will impact this a lot too!

Maintenance planning, condition monitoring, and decision support for service and recycling

Concerning maintenance planning, condition monitoring and related decision-making for the later parts of the lifecycle, paramount is the design for availability, which can be seen as function of maintainability and reliability. If this is designed well, it can minimize the need for maintenance. This is, in particular, an advantage and cost saver if the connected offering will be deployed in hard-to-reach

places or rural areas. However, if there are contractual obligations (i.e., tough availability levels and/or service level agreements) there needs to be planning and monitoring of the connected offering's function and condition with related support to make decisions for service, maintenance, upgrades or retirement/replacement. The smarter and optimized the operations with maintenance etc. can be planned and implemented, the lower cost and improved sustainability can be achieved over the lifecycle. To support the planning of the maintenance and related activities/services for the whole lifecycle, there are the **5R**'s, which can be combined with the elliptical lifecycles concept, Reuse, Repair, Re-manufacturing, Re-processing, and Recycling (Jacobsson et al., 2023; Lindahl and Dalhammar, 2022). Furthermore, the are **two more R's**, Re-purposing and Re-conditioning, which can be added to this planning and later design efforts of the connected offering's parts or components, such as, hardware, software, services, and support, etc. (Psarommatis and May, 2022; Lindström et al., 2024). To be able to pull this off, there is a need to get out data and a possibility to also from a distance provide support and some services. A common tool to do that is to have **fleet management functionality** combined with **secure remote access solutions** (Lindström, 2023). A common related problem is how to get access through a customer's/user's IT/OT-environments to reach the connected offering.

Sustainable connected offerings enabled for more than the primary lifecycle with reuse and remanufacturing of components or parts as well as re-purposing for new use at new customers/users

The design of the lifecycle should preferably further support re-manufacturing of parts and the offering be designed for availability, re-cyclability and disassembly, etc., to support one or more lifecycles after the primary one (where re-purposing supported by re-conditioning may be applicable for the continuation in a new chapter of the lifecycle at a new customer/user). In addition, components and raw materials should be re-used as part of the lifecycle in a reverse logistics flow as well (Lindström et al., 2024). To have another or two additional lifecycles following the primary one requires that worn and torn hardware can be replaced or re-manufactured in combination with a general re-condition of the whole offering in terms of software updates/upgrades, addition of new add-on services, and support/maintenance improvements as well. Examples of such extensions of lifecycles beyond the primary one is a car driven in western Europe, whose second lifecycle continues in eastern Europe and finally may end with a third in Africa. This is sometimes mentioned as down-cycling.

Recent, emerging and upcoming EU legal and regulatory frameworks

Additional matters addressed will be the impact on design and planning of lifecycles from **recent, emerging and upcoming EU legal and regulatory frameworks** regarding product passports, cybersecurity and the strive for long and sustainable lifecycles requiring design allowing for upgrades, updates, extendibility of hardware/software/service architectures, and replacements with new versions of hardware components, etc. Due to the increasing number of sophisticated cyber/hybrid attacks, the European Commission has introduced a number of legal and regulatory requirements for the EU and many of its companies and organizations. The objective is to improve the level of resilience and robustness/ability to withstand cyberattacks as well as hybrid attacks. Commonly, cybersecurity has been well ahead of legal and regulatory requirements, but now most of EU has a large burden to catch up with the recent, emerging and upcoming requirements combined with those for sustainability and circular design. This goes in particular for providers of connected offerings but also the customers/users of such (c.f., Lindström et al, 2024; Psarommatis et al., 2024). For global operations

and providers of connected offerings, additional legal and regulatory requirements need to be factored in as well. A somewhat **slow harmonization and alignment of global legal and regulatory frameworks can be anticipated**. However, it seems like the EU together with the UK and Australia have most in common at the time and other large countries are lagging, either with intent, or because of fragmented government structures, or due to strong lobbying forces. Further, some totalitarian countries have a completely different ideology behind their legal and regulatory systems, and the concept is not to protect providers or customers/users, but to enable the government to control society and its actors. Being present in such countries will add complexity for providers of connected offerings and require special functionalities and configuration options!

There a shift in responsibility with an increase for the provider side, and quite a bit has moved from the customer/user side due the implementation of the EU's design concepts secure- or security-by-design, privacy-by-design, secure-by-default, zero trust, and the principles of least access rights or least privileges.

Use of open-source software and open-design of hardware

A key factor regarding usage of open-source software and open-design of hardware in the connected offerings is that the contents of such are true, originators and contributors known, and without any extra malicious additions. This is very important as most connected offerings on the market today comprise open-source software and/or open-design hardware, which should require continuous monitoring and testing of such open-source software and open-design hardware. However, who really does that to the extent needed? Consequently, such questions need to be asked by the customer/user side to get verification that any open-source code or open-design hardware used are properly monitored and tested. Concerning open-source software, such **automatic testing** can partly be built into build systems or pipelines etc. used but additional monitoring of the contents, originators/contributors and deeper manual verification is likely to be needed in many cases over time. Regarding open-design hardware, any components or functionality that seems to not fit in should be investigated and **test suites used to test and verify that there is only the documented functionality and no more** (Lindström, 2023). A recent high profile open-source software attack in 2024 was the XZ Utils backdoor planted and aimed for the SSH server, part of many LINUX distributions, which likely could have led to disaster in the western world if not detected in time and stopped.

Digital twins and simulations

The further complex a connected offering is the more **benefits can be reaped from using digital twins and simulations**. The objectives are to test changes in functionality or configurations etc. in a virtual world before implementing them in the real world, find potential optimizations, find good start parameters/configurations to use after changes, and needs for design changes.

To design and craft digital twins require knowledge about the physical process and/or context where the connected offering operates as well as adequate knowledge on modelling, development of a digital twin and simulator, and most often also advanced mathematics. To be able to simulate provides many advantages and in particular a lot of time can be saved after changes as the time to get productive can be significantly shortened. Having many parts or components to model can be complex, and if possible abstraction layers and simplifications are necessary as a model, which is the base for it all, needs to be updated over time as the connected offering and the physical process and/or surrounding context

change. The further precise outcome of the simulations, the more effort usually needs to be spent on keeping the model, digital twin and simulator up to date. If it is possible, it should be investigated if the **model can be automatically updated** by an update function which can ingest drawings, specifications, and relevant information about the physical processes and the operational contexts (Birk et al., 2022).

Use and integration of artificial intelligence (AI) and machine learning (ML) into connected offerings

It is further necessary to investigate what to use AI and ML for as well as how to get the biggest bangs for the bucks! The use of AI and ML should be critically considered for new connected offerings and older connected offerings should be reviewed to learn what additional value AI and ML can create. However, bringing in AI and ML can cause both safety and cybersecurity concerns depending on what types of data and information that are to be used and processed. Particularly, if personal or sensitive data is to be used, privacy and authorization to mix data from different sources must be ensured. Further, trust and confidence levels of output must be considered and verified, i.e., accurateness and correctness, and if these are low it must be evaluated what the expected confidence level implicates for what outcomes that can be used for decision-support or when humans need to be in the loop as well to improve the confidence level. In addition, pertaining to use of AI and cybersecurity, the bad guys will use AI to automatize attacks to hack, impair availability or functionality, or steal data, etc., from connected offerings, AI also needs to be used to protect the connected offerings. However, this requires wider use of AI and ML than only the connected offering as the whole operational IT or OT environments, with networks and network segments, also need to be protected. AI and ML should further be used to find improvements and optimizations for connected offerings, plus any new ideas and opportunities for add-on services or completely new offerings. AI and ML-based decision-support using data collected from connected offerings is a low hanging fruit, as long as the quality of the collected data and meta-data is good enough to base decisions on with the wanted/required level of confidence (Lindström et al., 2025).

Cloud services/applications and risky dependability to big tech cloud platforms

Providers and customers/users of connected offerings need to consider what cloud services/applications, which may include AI services as well, that are key for the connected offerings to function. What happens if geo-political tensions, legal claims from the US government (e.g., US Cloud Act), or changes in privacy laws and regulations, either makes it **too dangerous or impossible to use or there is a risk that data is leaked?** Further, can providers of cloud services/applications as well as customers/users of such get the data out and transfer these to another cloud platform provider and migrate over and continue to operate without too much fuzz and problems? This should be investigated and plans made ready if there are signs of disturbance or other matters to worry about related to this. From a cloud service/application provider perspective, if there is a need to move away from for instance Microsoft Azure, Amazon AWS, Google Cloud, Tencent Cloud, or similar big tech cloud platforms, the services/applications should be developed to be **agnostic to the underlying cloud platform**.

Providers and customers/users of connected offerings, and, in particular, with operations and origin within the EU, need to consider sovereignty matters and how to **manage and prepare if there is a need to move**. To remember is that when a lot of actors want to move at the same time, will you be at the head, in the middle, or at the tail of the queue?

Connectivity and the wish to be connected or not…

A good question to have as part of the design is if there any means to connect the offering? Potentially, the connected offering may need to **have multiple options for how to connect to the Internet and be able to store data in a cloud service or data center as well as get back updates and remote support or maintenance** etc. (Lindström, 2023). However, a hard question to pose is: do all or only some customers/users wish to connect the offering and what to do with the ones who do not? A first question is, **should the connected offering be sold to those who do not intend to connect it** or should we have **another offering** with lower levels of functionality and promised support, maintenance and availability for those? The not connected ones will require regular on-site visits for all physical maintenance as well as software updating or upgrading, etc. This is a problem for many providers as having laggards with old versions of, in particular, software can create undefined outcomes when the multiple updating or upgrading occurs although applying all software updates, patches, upgrades, etc., in the recommended order. Use of cumulative software changes is often a good strategy, however then there must be a way to roll back if it does not work as expected. Therefore, backup of data etc. should be made before such activities are started by for instance the service engineer on site. The customer/user can of course do some of this updating, but what to do if serious problems occur and the connected offerings stop working?

Additional matters to consider

There are of course additional matters to consider when aiming to extend the lifecycles of connected offerings. These matters may depend on context, laws and regulations, foreseen and unforeseen usage and application of the connected offerings, as well as the users' behavior, competence and knowledge levels. It is likely very hard to in the beginning know about the future, so thus a **suitable architecture which enables flexibility for change, scalability (if and when needed), and adaptability, will be necessary to be successful and efficient over long lifecycles**. However, there are some known already today, such as the need to become quantum computing compliant and replace non-compliant encryption algorithms and keys as well as key and certificate management processes.

Summary with a future outlook

The design of connected offerings and planning for their lifecycles, to achieve sustainable win-win situations, is hard but for many companies it is necessary to be a **provider for the future**. Some mental blocks may need to be removed and a slow adaptation, rather than all at once, can be a moderate way to implement key matters into a connected offering's various parts, components, functions, or layers. As indicated in the white paper, there are quite a few matters to consider for achieving extended lifecycles of connected offerings, and this will for sure also cost and the costs be factored into the business model or models used as well as pricing strategy. Furter, customers need to be informed on that extending lifecycles with included cybersecurity and futureproofing of architecture and functionalities will cost more at the same time as the value creation and capturing must be improved to get a win-win situation. This will require new ideas, concepts, skills and competencies, and therefore both providers and customers need to advance and prepare for connected offerings with extended lifecycles.

Acknowledgements

The white paper is based on work experiences and research from the Faste Laboratory, Centre for Distance-Spanning Technologies, Centre for Critical Infrastructure and Societal Security, ProcessIT Innovations R&D Centre, and the Cybersecurity Node North project (European Union contract 20366918) at Luleå University of Technology, Sweden.

The writing of the white paper was funded by **Creaternity** at Luleå University of Technology, https://www.ltu.se/en/research/creaternity---sustainable-materials-in-a-connected-and-circular-economy/about-us

References

Alonso-Rasgado, T., Thompson, G., Elfstrom, B.-O. (2004). The Design of Functional (Total Care) Products, Journal of Engineering Design, 15/6: 515–540.

Birk, W., Hostettler, R., Razi, M., Atta, K., Tammia, R. (2022). Automatic generation and updating of process industrial digital twins for estimation and control - A review. Frontiers in Control Engineering, 3:954858.

Bocken, N.M.P., de Pauw, I., Bakker, C., van der Grinten, B. (2016). Product design and business model strategies for a circular economy. Journal of Industrial Production Engineering, 33, 308–320.

ENISA (2023). Good Practices for Supply Chain Cybersecurity. Available online: https://www.enisa.europa.eu/publications/good-practices-for-supply-chain-cybersecurity (last accessed on 12-November 2025).

Jacobson, S., Wiklund, U., Hardell, J., Larsson, R. (2023). Tribology and the case for an Elliptical economy. In Proceedings of the 24th International Conference on Wear of Materials, Banff, AB, Canada, 16–20th April.

Lindahl, M., Dalhammar, C. (2022). The Circular Economy: Towards a New Business Paradigm with Support from Public Policy; Stockholm+50 background Paper Series; Stockholm Environment Institute: Stockholm, Sweden. Available online: https://www.sei.org/wp-content/uploads/2022/05/circular-economy-stockholm50backgroundpaper-corrected.pdf (last accessed on 8-November 2025).

Lindström, J. (Ed.) (2023). Handbook for Development of Cybersecure IoT-Products; Smarter Electronic Systems, IoT Sweden, and Swedish Electronics Trade Association: Stockholm, Sweden. Available online: https://www.smartareelektroniksystem.se/handbocker/ (last accessed on 11-November 2025).

Lindström, J., Karlberg, M. (2017). Outlining an overall Functional Product lifecycle – Combining and coordinating its economic and technical perspectives, CIRP Journal of Manufacturing Science and Technology, Volume 17, pp.1-9.

Lindström, J., Kyösti, P., Psarommatis, F., Andersson, K., Starck Enman, K. (2024). Extending Product Lifecycles—An Initial Model with New and Emerging Existential Design Aspects Required for Long and Extendable Lifecycles, Applied Sciences, 14, 5812.

Lindström, J., Kyösti, P., Birk, W., Lejon, E., Schneider, G., Andersson, A., Lindblad, O., Eliasson, J., Andersson, K. (2025). Interoperability requirements for Zero Defect Manufacturing within Industry4.0, Procedia CIRP, Volume 134, pp.532-537.

Liu, Y., Zhang, Y., Ren, S., Yang, M., Wang, Y., Huisingh, D. (2020). How can smart technologies contribute to sustainable product lifecycle management?, Journal of Cleaner Production, 249, 119423.

Meier, H., Roy, R., Seliger, G. (2008). Industrial Product-Service Systems – IPS2, CIRP Annals Manufacturing Technology, pp.1–24.

Mont, O. (2001). Introducing and Developing a Product-Service System (PSS) Concept in Sweden, The International Institute for Industrial Environmental Economics (IIIEE), Lund University, Sweden.

Psarommatis, F., Azamfierei, V., Lindström, J. D. (2024). Circular product design for allowing re-using and re-purposing of products and components: a conceptual framework for circularity, IFAC-PapersOnLine, Volume 58, Issue 8, Pages 306-311.

Psarommatis, F., May, G. (2022). Achieving global sustainability through sustainable product life cycle. In Proceedings of the International Conference on Advances in Production Management Systems, Gyeongju, Republic of Korea, 25–29th September, pp. 391–398.

Rojek, I., Mikołajewski, D., Dostatni, E. (2021). Digital Twins in Product Lifecycle for Sustainability in Manufacturing and Maintenance, Applied Sciences, 11, 31.

Roy, R., Shaw, A., Erkoyuncu, J.A., Redding, L. (2013). Through-Life Engineering Services, Measurement and Control, 46/6: 172–175.

Rönnberg Sjödin, D., Parida, V., Lindström, J. (2017). Barriers and conditions of open operation: a customer perspective on value co-creation for integrated product-service solutions, International Journal of Technology Marketing, Vol. 12, No. 1, pp.90-111.

Tomiyama, T. (2001). Service Engineering to Intensify Service Contents in Product Life Cycles. In Proceedings of EcoDesign 2001, 2nd Int. Symposium on Environment. Conscious Design and Inverse Manufacturing, 12–15th December, Tokyo, Japan.

White, A.L., Sloughton, M., Feng, L. (1999). Servicizing: The Quiet Transition to Extended Product Responsibility, Tellus Inst., Boston, USA.

Zis, T.P.V. (2024). The enhanced role of canals and route choice due to disruptions in maritime operations, Maritime Business Review, 9(2), pp.98-112.