Proceedings of the Design Society, Volume 5: ICED25
https://doi.org/10.1017/pds.2025.10330

Towards an integrative approach for designing for cybersecurity in systems engineering

Megan A. Harris✉, Matthew L. Hale and Christine A. Toh

University of Nebraska at Omaha, USA

✉ megharris@unomaha.edu

ABSTRACT: Secure development is an ever-evolving field that has advanced quickly in recent years with initiatives like Secure Development Lifecycle (SDLC), Development Security Operations (DevSecOps), and Model-Based Security Engineering (MBSE). Despite the persistence of the security and design communities to include security in the design process, significant security breaches continue to occur. Our work reviews existing literature to determine the current state of the research at the intersection of these design and cybersecurity fields and ultimately proposes an integrative and systematic approach for developers to generate design principles that incorporate traceable security. This approach integrates security regulations and design principles and activities, encouraging compliance and security considerations at the earliest stages of the design thinking process.

KEYWORDS: systems engineering (SE), requirements, design process, design theory, design for cybersecurity

1. Introduction

Security is often an afterthought in software design—a problem that persists across small startups and large corporate environments (CISA, 2023). Under tight deadlines and market pressures, development teams frequently prioritize functionality and user experience over security. When protective features are bolted on late in the process rather than integrated from the start, it can create a host of problems: vulnerabilities emerging from design weaknesses become deeply embedded, costly code revisions are needed to fix them, and patchwork solutions (Tzavara & Vassiliadis, 2024; Chauhan & Shiaeles, 2023) may only partially address root issues. The fallout from this type of design oversight is not theorethical. High-profile incidents, such as exploiting the Log4j vulnerability (Ferreira et al., 2023), have demonstrated the severe impact of poor security planning during the early phases of the deisgn process, which can result in data breaches, data theft, financial losses, and damage to an organization’s reputation. Recognizing the need for a more proactive stance, the software engineering community has moved towards the incorporation of a ‘secure by design’ mindset into the systems/software development lifecycle (SDLC) resulting in approaches like DevSecOps (Development, Security, Operations) and model-based software/systems engineering (MBSE) to gain traction for the creation of systems with high assurance requirements. Security by design encourages designers, developers, and assessors to consider security as an integral element of every phase—from requirements gathering, design, implementation, testing, deployment, and maintenance—rather than as a tacked-on safeguard added as an afterthought (Shostack, 2014).

Being secure by design means that during each phase, specific security activities need to be performed to identify and mitigate risks. For example, threat modeling during the design phase helps to identify potential security threats, while DevSecOps embeds security requirements satisfaction checks into code reviews and automated continuous integration test cases that occur throughout the implementation, testing phases. These steps ensure that vulnerabilities are addressed before deployment (Kamal et al., 2020). SDLC also emphasizes continuous monitoring and improvement, ensuring that security measures evolve with emerging threats (McGraw, 2012).

However, these approaches are not without their challenges and limitations. While principles of security by design, such as least privilege, defense in depth, secure defaults, and regular auditing and monitoring, are powerful tools, they are abstract and lack context-specific gudiance that is needed to address system or application specific constraints. Secure by design is also not without cost. Approaches like MBSE can significantly increase development time, while DevSecOps can rely too heavily on automated tools, being able to articulate the right kinds of test cases, and/or demand significant and disruptive cultural changes within teams and companies. Without a more specific approach to security by design, organizations risk misapplying general principles, investing in ineffective defenses, or overstretching their security budgets.

This paper responds to these challenges by exploring the intersection of the cybersecurity and design research fields to uncover actionable themes that can better contextualize design principles. Our goal is to move beyond high-level strategies and provide a systematic approach for creating practical, context-sensitive design principles that can guide designers towards security by designing in a traceable way across every stage, particularly the early stages, of the system creation process.

1.1. Related work on design and cybersecurity

While these principles center on design, they have been implemented in cybersecurity contexts to enhance threat detection by improving how analysts perceive patterns and anomalies in data (Marriott, 2018), creating user-friendly security systems, ensuring that security measures are intuitive and accessible and reducing human error (NIST, 2021). Design principles have also been used to make security protocols more engaging and less intrusive, encouraging better adoption by users (Laurel, 2024) and to create clear and effective security warnings and dashboards, making it easier for users to understand and respond to threats (Seong et al., 2020). Despite these advancements in the use of design principles in cybersecurity, their use is ad hoc, unstandardized, is often in conflict with other design goals, and most importantly, are not integrated into organizational functions. This makes enforcement difficult. Formalization of when and how to use design principles to promote cybersecurity in all development processes is necessary.

Furthermore, as circumstances change, technological systems evolve and new threats emerge along with new methods for attacks (Carter et al., 2019). This requires additional flexibility and adaptability on the part of the designer to anticipate future threats and incorporate security measures that are adaptable to the evolving landscapes. Thus, balancing security with aesthetics and functionality is crucial, as overly restrictive measures can hinder the user experience in addition to the system's intended purpose. Thus, as Garfinkel & Lipford (2014, p. vi) stated, "only by simultaneously addressing both usability and security concerns will we be able to build systems that are truly secure."

The design of user interfaces (UIs) is crucial in balancing security and usability. Non-intuitive security features can lead to errors and frustration whereas a user-centred security design approach, integrating security seamlessly into user workflows and considering security at each design phase, can create user-friendly, robust systems. This proactive approach enhances application security and reduces long-term costs and risks. This study aims to develop design principles for incorporating cybersecurity considerations throughout the development process.

1.2. Design principles and heuristics

While the previous section highlighted the lack of systematic approaches for secure design early in development, substantial engineering design research has developed theories, frameworks, methods, and tools to support designers. In real-world, complex design engagements, practitioners often codify their knowledge into mental "rules of thumb," also known as guidelines, heuristics, and principles (Fu et al., 2016). These cognitive strategies guide decision-making during uncertain phases like problem formulation, framing, idea generation, and concept development. Existing research has shown that design heuristics significantly improve creativity and help overcome design fixation (Voss et al., 2014) during the ideation phase of the design process by encouraging designers of all experience levels (Yilmaz, Daly, et al., 2016) to consider a wide range of possibilities. They also support collaborative development by providing a framework for assessing ideas (Linsey et al., 2011) and have been incorporated into digital tools for real-time prompts and suggestions (Pinochet, 2017). Thus, these principles, heuristics, and guidelines are invaluable in real-world design contexts where interconnected systems (people, technology, organizations, and policy) need to be considered together.

The earliest and most notable example of formal guiding principles in the field of mechanical design is the Theory of Inventive Problem Solving (TRIZ) (Altshuller, 2002) developed to help designers address complex technical problems by identifying pairs of contradictory requirements (e.g., speed vs. weight). Innovative solutions were derived from decades of patent analysis and distilled into high-level principles, resolving contradictions across application areas. These principles help designers create solutions beyond mere compromises. Recent work has expanded this approach with heuristics applicable to various fields, not just mechanical design (Yilmaz et al., 2016). These heuristics improve design students' idea generation and problem space exploration, showcasing their educational utility, especially for designers lacking extensive experience (Yilmaz, 2010).

Beyond engineering design, many principles have been adopted in Human-Computer Interaction (HCI), like Gestalt psychology principles (Khamis et al., 2023). These principles have led to exploring the humanistic and therapeutic effects of visual organization (Moszkowicz, 2011) and graphic design (Khamis et al., 2023), for examples. Broader yet, are general guidelines adopted by practitioners in Human-Centered Design (HCD), where they prioritize user needs through empathy, iterative design, and user involvement (Norman, 2013). In visual design, foundational 'Principles of Design' like balance, contrast (Lidwell et al., 2010), emphasis, movement, consistency (Martin & Betrus, 2019), proportion, and rhythm ensure effective and aesthetically pleasing creations. These principles help both novices and experts understand underlying patterns, address complex design challenges, and establish a shared language for communication and critique among professionals. However, there is a notable lack of cybersecurity-related focus in design principles literature. Additionally, many principles are highly abstract, limiting their usefulness for specific contexts affected by industry norms, regulations, and system interdependence.

In cybersecurity, context-specific constraints challenge designers and developers to balance competing requirements and user needs while ensuring verifiable security properties. Recent interventions like the Design for Cybersecurity (DfC) Cards (Rao et al., 2021) help address these needs by prompting users to consider important cybersecurity requirements early in the design process. While a positive step, these cards do not link existing systems development practices (e.g., software architecture design, SecDevOps, CI/CD, platform engineering, software as a service, model-based software engineering (MBSE)) with established cybersecurity standards (e.g., NIST (US National Institute of Standards and Technology) SP 800-53, PSI DSS, HIPAA, GDPR, ISO 27001, NIST 800-172, etc.). This integration with real-world software engineering is crucial to bridge traceable security considerations with high-level design principles and ensure adoption in high-complexity contexts like cybersecurity and development operations in enterprise-scale applications. Other work in engineering design has developed preliminary user personas for developing cybersecurity requirements (Kim et al., 2019), which aid in guiding reasoning during the design process but lack specific principles for bridging the gap between security requirements and implementation in complex systems. To address these gaps, the current study proposes a systematic approach for developing traceable security design principles using existing cybersecurity standards and systems development practices. It distinguishes between "principles" (fundamental rules applicable across contexts) and "heuristics" (context-dependent directives for satisfactory solutions). These principles help designers integrate security considerations throughout the design process and enable systems architects to translate requirements into development outcomes, ensuring effective maintenance, management, and operations post-deployment.

1.3. Research goals

This study focuses on identifying key themes at the intersection of cybersecurity and design research and seeks to understand how these fields overlap as well as influence one another. By analysing patterns and trends in existing research, the study aims to **propose a systematic approach for developing design principles that can enhance cybersecurity measures from available information.**Therefore, the specific objectives of this paper are as follows:

1. Identify main challenges associated with implementing security considerations in the early systems design process.

2. Advance a formalized, systematic approach for developing practical, context-sensitive design principles to be used that can guide designers towards security by designing in a traceable way across the early stages of system creation

2. Objective 1: identifying the main challenges to incorporating traceable security considerations into the system design process

To address the first objective, online inquiry was conducted on the last 5 years of conference proceedings and peer-reviewed journal papers from publication databases relevant to both the fields of cyber security and design to identify the dominant themes: IEEE Xplore (IEEE), ACM Digital Library specifically for proceedings from CHI Conference Series (hereafter referred to as CHI), and Design Society. While the design process and activities are well-established, both the design and cyber security fields are rapidly evolving and thus, a search for research older than 5 years would not likely add to the contributions of the current study. The search query used for the IEEE and CHI databases was as follows: **(“cyber security” OR “cybersecurity” OR “cyber-security”) AND (“design process” OR “design activities” OR “design phases”)**. The search query for the Design Society publication database was: **“cybersecurity” OR “cyber-security.”**Papers were excluded from the review if they were not written in English or were only extended abstracts or presentations (i.e. not a full paper). The number of papers that resulted from this analysis is shown in Figure 1.

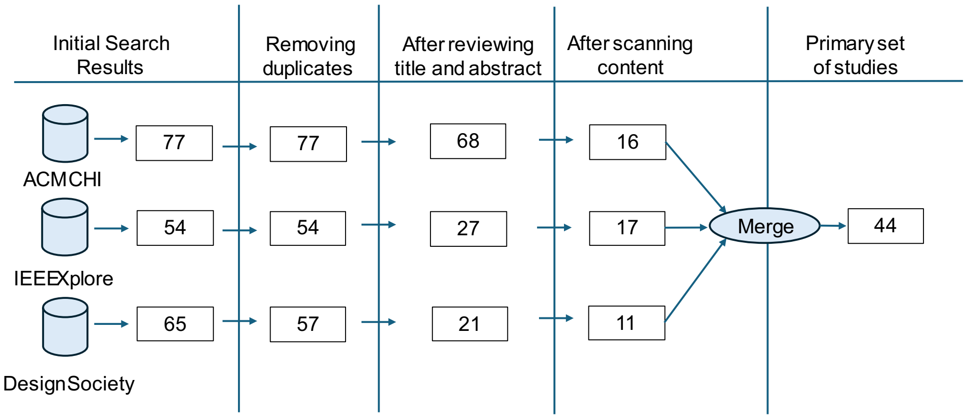

Figure 1. Number of papers that resulted from the search query along with the filtering process

Some duplicate papers resulted in the two searches from the Design Society database requiring elimination of said duplicates in the first step. Subsequent filtering included a title and abstract review and then content scanning before the final set of primary studies to be included in this study resulted. The following sections presents the themes that emerged from this analysis. Each theme highlights the specific challenges associated with attempts to integrate security considerations into the software engineering process.

2.1. Theme 1: challenges of a security-first mindset during existing design workflows

The first major theme discovered from analysis of the literature focused on challenges with considering security early in the software design process. Designers have to balance competing interests such as functionality, scalability, resources, time to market, (Flechais et al., 2007) and security.

Researchers have also identified challenges in generalizing a security-first process in context-specific situations. For example, industry-specific challenges have been identified for space travel (Shahzad et al., 2024) and cyber-physical systems (CPS) (Carter et al., 2019). Space travel, for example, has the unique constraints of needing robust cyber resilience due to the isolation, high cost, and persistence of legacy systems (Shahzad et al., 2024). In the realm of CPS, challenges arise from the integration of computational and physical processes, requiring new abstractions to ensure safety and reliability

(Spiekermann, 2012). These challenges confirm the necessity for specialized approaches tailored to the distinct requirements of each industry, since general principles are often too abstract to be applied at the implementation stage.

While less explored in the literature, a few studies highlight challenges with implementing security-first principles to specific phases of design process. For example, work by Mathis et al (2022) identifies challenges specific to the prototyping phase, such as limited access to hardware and prototyping expertise. Similarly, McKenna et al. (2015) discusses challenges with effective visualizations of security solutions during the evaluation phase.

Analysis of existing work in this space reveals a lack of standardized methodologies for incorporating security into specific design phases, despite the existence of industry-standard guidelines such as NIST SP 800-53, PSI DSS, HIPAA, GDPR, ISO 27001, NIST 800-172, etc. (Knapp, 2009). Other challenges identified in the literature include the rapid pace of emerging technologies (Mckenna et al., 2015), communication barriers between security experts and design teams (Spiekermann, 2012), and the dynamic nature of security threats (Di Nocera et al., 2023).

These gaps compel the development of detailed, phase-, activity-, and industry-specific guidelines that can be easily integrated into existing design workflows for secure development that, at minimum, maintains, and at best, advances, user experience and functionality.

2.2. Theme 2: challenges with designing usable security

’Usable security,’ focuses on designing security systems that are both effective and user-friendly (Di Nocera et al., 2023; Wash & Rader, 2021; Faily et al., 2015; Fidas et al., 2010)), however, balancing these aspects is challenging as security often introduce complexity and inconvenience for users, while efforts to improve usability can sometimes weaken security protocols. This conflict is particularly evident in authentication, as strong password policies and multi-factor authentication (MFA), which enhance security and are even considered essential (Naqvi & Porras, 2020), can be cumbersome if not seamlessly integrated into the user experience (Colnago et al., 2018). Overly stringent security measures can disrupt users’ workflows, leading to poor practices like writing down passwords or using easily guessable ones, ultimately reducing overall security

Research in usable security addresses this challenge by ensuring that security measures are accessible and understandable to users, thus reducing the likelihood of security breaches due to user error. Psychological acceptability, introduced by Saltzer and Schroeder (1975), emphasizes that security mechanisms should not be so cumbersome that users are tempted to bypass them. Effective security interfaces should provide clear, concise information to help users understand risks and make informed decisions. Design strategies such as nudges, persuasive technologies, and gamification elements guide users toward more secure behaviours without restricting their freedom of choice (Egelman et al., 2016; Acquisti et al., 2013). By focusing on the human element, usable security aims to create systems that users can and will use correctly, enhancing overall system security (Di Nocera et al., 2023).

2.3. Theme 3: challenges with maintaining security in a brittle system

In the field of cybersecurity, humans are considered the weakest link in the security chain, yet this perspective oversimplifies the complexity of the issue as the real vulnerability lies in the interactions between humans and the software systems they rely on (Legrand, 2022). While humans can make mistakes, this ‘real vulnerability’ lies in how heavily systems depend on vigilant human input, making them susceptible to security breaches when deployed at scale—a characteristic we call “brittle” due to its inability to absorb human errors before breaking. This challenge is exacerbated by the cognitive limitations of human users, and the inherent complexity of modern enterprise systems. These systems have been designed primarily with the focus on functionality and performance neglecting the actual behaviours of users (Grobler et al., 2021). Don Norman, whose work has profoundly impacted user-centred design practice, makes an astute observation: “Suppose the fault really lies in the device, so that lots of people have the same problems. Because everyone perceives the fault to be his or her own, nobody wants to admit to having trouble. This creates a conspiracy of silence, where the feelings of guilt and helplessness among people are kept hidden,” (Norman, 2013, p. 61). This “conspiracy of silence” paired with the brittleness of the human-system interaction highlights the importance of designing systems that can accommodate human errors and do not induce shame when users’ natural behaviours are contradictory to the intended use of the system.

The need for UCD to develop security tools that users are more likely to adopt and use appropriately (Norman, 2013) is often emphasized in the defining, ideating, prototyping, and testing phases with regards to determining user needs, identifying design opportunities, and iteratively evaluating ideas (Sanders & Stappers, 2014). As a result of UCD being used in a security context, adaptive security systems that tailor security measures based on user behaviour and context are gaining in popularity. These systems dynamically adjust security requirements based on the perceived risk and user actions, providing a balance between security and usability, further enhancing security without imposing unnecessary burdens on users (Ben-Asher & Gonzalez, 2015). UCD's emphasis on understanding users' needs and behaviours ensures that security measures are designed with the user in mind, making them more intuitive and less likely to be circumvented (Di Nocera et al., 2023). For example, during the defining phase, developers can gather comprehensive data about user needs and potential security threats. In the ideating phase, these insights can lead to innovative solutions that address security concerns while maintaining usability (Van Der Kleij, 2022). Prototyping allows for testing these solutions in real-world scenarios, ensuring they are practical and effective (Agboola et al., 2024). Finally, the testing phase provides an opportunity to refine these solutions based on user feedback, ensuring that the final product is both secure and user-friendly (Faily et al., 2015).

3. Objective 2: advance a formalized, systematic approach for developing traceable security design principles

While the overarching goal of this work is to advance the inclusion of security considerations early in design and development process, the primary contribution of this particular study is to **propose an integrative approach for developing principles that can advance security and development goals using existing models, frameworks, and processes from the systems development, cybersecurity, and design theory domains.** As mentioned in Section 2, existing research has discussed many challenges to considering security in the design process and has provided several resolutions including usable security and user-centred design in addition to the aforementioned SDLC, DevSecOps, and MBSE initiatives. However, these previous works have predominantly focused on isolated aspects of security and design (Grobler et al., 2021) be it industry-specific security initiatives (space, CPS, or maritime security, for examples) or specific phases of the design process (evaluation and prototyping) usually later in the process. This leaves a significant gap in integrating these disciplines in a formalized, structured, and actionable way, to complement these prior efforts of other initiatives including but not limited to the aforementioned SDLC, DevSecOps, and MBSE. Thus, there is a clear need for a holistic process that integrates design and cybersecurity to develop principles that developers can readily apply. Since existing frameworks in design theory, systems development, and cybersecurity have been developed in parallel, the overlap between these frameworks is explored for this study, see Figure 2. To illustrate the integration of traceable security design principles across these three domains, example frameworks and models from systems development, cybersecurity, and design theory are examined in parallel, as detailed below. Importantly, other industry-specific models can be substituted for any of the three examples described below, depending on the context of application and specific development workflow being investigated.

From the systems development domain, the Systems V-Model is one such framework which incorporates validation and verification tests into the entire development process (Mathur & Malik, 2010). The original model has been refined and updated several times with many variations still currently used in practice. Though there are more modern methods, we use the systems V-Model here as a primary example since it is the dominant method used in highly regulated industries such as aerospace, computer and robotics, and the automotive industry (2022). While robust, this approach does not explicitly integrate security standards that systems must adhere to, nor does it enable ethnographic analysis of users' real needs and interactions with complex systems.

From the cybersecurity domain, NIST issues standards that are enacted in a Risk Management Framework for Security Life Cycle in NIST 800-53 which aligns security standards with the systems development lifecycle. This is widely used by many organizations across sectors to manage information security and privacy risks. Specifically, United States government agencies, federal contractors, and large enterprises (Ross, 2007) often adopt this framework to ensure compliance with U.S. federal requirements and enhance their security posture. However, this framework is largely implemented at the verification

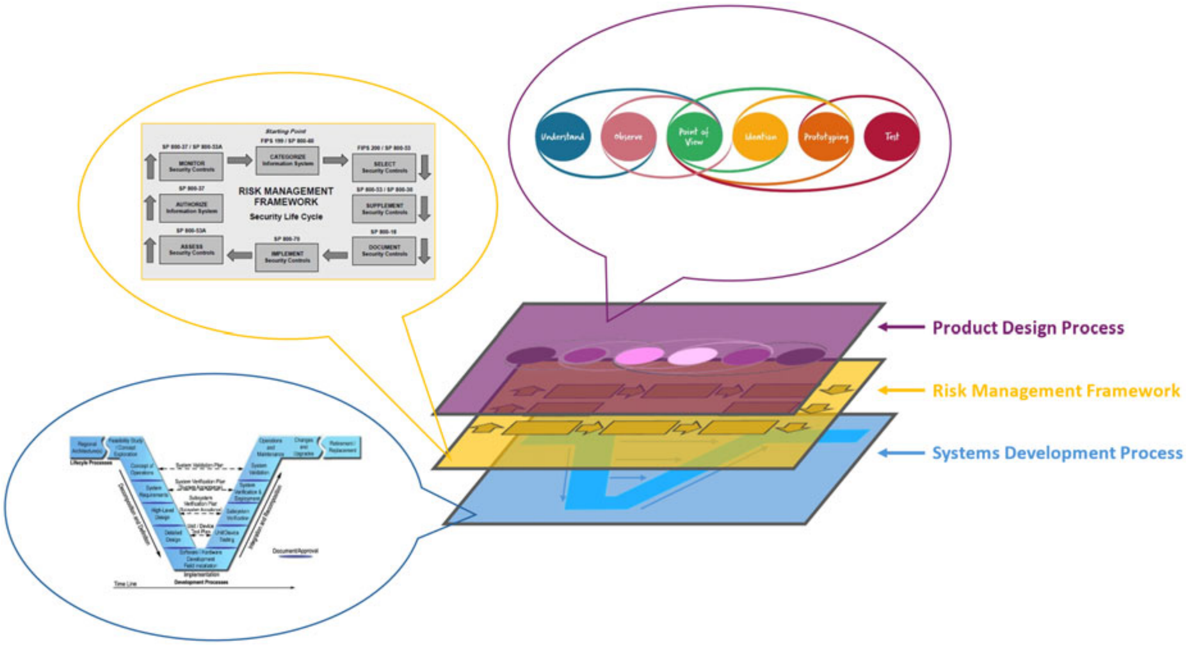

Figure 2. Integration of systems development, cybersecurity, and design theory domains

and maintenance stages of the systems development process, as opposed to the early phases of the design process, when security features are far less costly to implement.

Lastly, **from the design theory domain**, we use the Design Thinking Process (Hasso-Plattner Institute, 2018) popularized by the Stanford D-School, outlining design steps and iterative loops for developing a phenomenological understanding of users needs. This ethnographic approach captures behaviour nuances and uncovers latent user needs not expressed in surveys or focus groups, enhancing user-centred secure systems design. However, it hasn't seen widespread adoption in cybersecurity due to its lack of integration with industry-standard frameworks like NIST 800-53.

To address the weaknesses of these three frameworks, we propose an integrative approach that layers guides from systems development, cybersecurity, and design theory. The systems development model forms the foundation, guiding designers' and developers' work. The security framework is layered on top, indicating standards for each development phase. Finally, the design thinking process adds ethnographic methods and user needs interpretations. Figure 2 illustrates this layered approach.

It can be clear for those familiar with the systems development and design theory fields, to see how design thinking steps align with systems development steps, as shown in Figure 3. However, security standards for each step are often unclear. We propose a layered approach integrating all three domains to develop principles that help software developers incorporate security early in the design process for context-specific situations. These principles provide essential information for integrating security into the design process. Without early integration, users must compensate with additional measures. Addressing security needs from the outset can reduce or eliminate extra steps. Thus, developing detailed, phase-, activity-, and industry-specific guidelines ensures secure development while maintaining or enhancing user experience and functionality. These guidelines will be developed with the following steps, similar to the previously mentioned TRIZ principles:

1. An ethnographic approach entails integration of the design researcher into the requirements engineering and systems development field. This will be achieved through an internship with a small, US-based systems development firm.
2. In addition to integration in the field, observations of, and interviews with, employees at the firm will reveal gaps between the systems development process, cybersecurity standards, and the design thinking process.
3. As gaps are identified, the literature will be reviewed to determine if existing research as investigated the particular gaps and addressed them with innovative solutions.
4. The principles necessary to address these gaps will be accumulated from existing solutions and from the discussions with, and observations of, the software-development firm employees.

5. The principles should be implemented into the development process and evaluated for their impact in addressing the integration of design, development, and security.
6. An iterative approach will be taken with steps 1 through 5 until a comprehensive set of guidelines is developed to sufficiently include cybersecurity in the early phases of the design process.

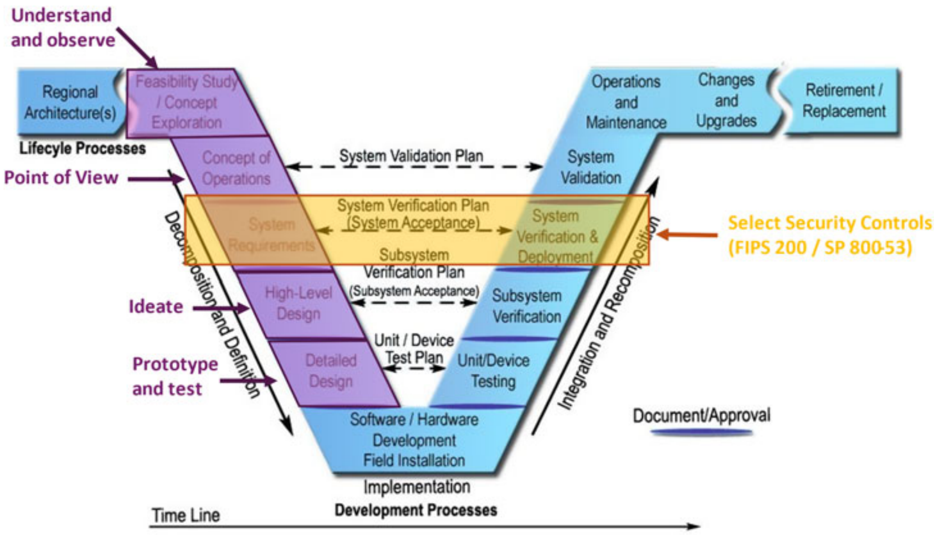

Figure 3. Layering design thinking phases & NIST standards over systems development process

4. Conclusion

Integrating design thinking into frameworks like the Systems V-model and NIST 800-53 enhances software security by embedding considerations early in development. This proactive approach helps identify vulnerabilities, ensuring intuitive, user-friendly measures that reduce circumvention. Adaptive security systems balance security and usability, evolving with user behaviour and emerging threats. Adopting User-Centered Design principles results in robust, secure, and user-friendly software, fostering security awareness and equipping designers with guidelines for a resilient digital landscape.

References

Acquisti, A., Adjerid, I., & Brandimarte, L. (2013). Gone in 15 Seconds: The Limits of Privacy Transparency and Control. *IEEE Security & Privacy*, 11(4), 72-74. IEEE Security & Privacy. https://doi.org/10.1109/MSP.2013.86

Agboola, T. O., Adegede, J., & Jacob, J. G. (2024). Balancing Usability and Security in Secure System Design: A Comprehensive Study on Principles, Implementation, and Impact on Usability. *International Journal of Computing Sciences Research*, 8, 2995-3009.

Altshuller, G. (2002). 40 Principles: TRIZ Keys to Technical Innovation. *Technical Innovation Center, Inc.*

Anthony. (2022, March 7). Everything you need to know about the systems engineering V-Model - Engineering Cheat Sheet. *Program Management | Systems Integration*. https://engineeringcheatsheet.com/systems-integration/describe-10-characteristics-of-the-automotive-product-development-process-illustrated-in-the-systems-engineering-v-model/

Ben-Asher, N., & Gonzalez, C. (2015). Effects of cyber security knowledge on attack detection. *Computers in Human Behavior*, 48, 51-61. https://doi.org/10.1016/j.chb.2015.01.039

Carter, B., Adams, S., Bakirtzis, G., Sherburne, T., Beling, P., Horowitz, B., & Fleming, C. (2019). A Preliminary Design-Phase Security Methodology for Cyber-Physical Systems. *Systems*, 7(2), Article 2. https://doi.org/10.3390/systems7020021

Chauhan, M., & Shiaeles, S. (2023). An Analysis of Cloud Security Frameworks, Problems and Proposed Solutions. *Network*, 3(3), Article 3. https://doi.org/10.3390/network3030018

CISA. (2023, October 25). *Secure-by-Design*. https://www.cisa.gov/resources-tools/resources/secure-by-design

Colnago, J., Devlin, S., Oates, M., Swoopes, C., Bauer, L., Craner, L., & Christin, N. (2018). *"It's not actually that horrible" | Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. https://dl.acm.org/doi/abs/10.1145/3173574.3174030

Di Nocera, F., Tempestini, G., & Orsini, M. (2023). Usable Security: A Systematic Literature Review. *Information*, 14(12), Article 12. https://doi.org/10.3390/info14120641

Egelman, S., Harbach, M., & Peer, E. (2016). Behavior Ever Follows Intention? A Validation of the Security Behavior Intentions Scale (SeBIS). *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, 5257-5261. https://doi.org/10.1145/2858036.2858265

Faily, S., Lyle, J., Fléchais, I., & Simpson, A. (2015). *Usability and security by design: A case study in research and development*. https://ora.ox.ac.uk/objects/uuid:7eb37d60-57a7-4b43-95f4-59955de08898

Ferreira, P., Caldeira, F., Martins, P., & Abbasi, M. (2023). Log4j Vulnerability. In Á. Rocha, C. Ferrás, & W. Ibarra (Eds.), *Information Technology and Systems* (pp. 375-385). Springer International Publishing. https://doi.org/10.1007/978-3-031-33261-6_32

Fidas, C. A., Voyiatzis, A. G., & Avouris, N. M. (2010). When Security Meets Usability: A User-Centric Approach on a Crossroads Priority Problem. *2010 14th Panhellenic Conference on Informatics*, 112-117. https://doi.org/10.1109/PCI.2010.17

Flechais, I., Mascolo, C., & Sasse, M. A. (2007). Integrating security and usability into the requirements and design process. *International Journal of Electronic Security and Digital Forensics*, 1(1), 12-26. https://doi.org/10.1504/IJESDF.2007.013589

Fu, K. K., Yang, M. C., & Wood, K. L. (2016). Design Principles: Literature Review, Analysis, and Future Directions. *Journal of Mechanical Design*, 138(101103). https://doi.org/10.1115/1.4034105

Garfinkel, S., & Lipford, H. R. (2014). Usable Security: History, Themes, and Challenges. *Springer International Publishing*. https://doi.org/10.1007/978-3-031-02343-9

Grobler, M., Gaire, R., & Nepal, S. (2021). User, Usage and Usability: Redefining Human Centric Cyber Security. *Frontiers in Big Data*, 4.

Hasso-Plattner Institute. (2018). What is Design Thinking. *HPI Academy*. https://hpi-academy.de/en/design-thinking/what-is-design-thinking/

Kamal, A. H. A., Yen, C. C. Y., Hui, G. J., Ling, P. S., & Fatima-tuz-Zahra. (2020). *Risk Assessment, Threat Modeling and Security Testing in SDLC* (No. arXiv:2012.07226). arXiv. https://doi.org/10.48550/arXiv.2012.07226

Khamis, M. H., Azni, Z. M., Aziz, S. H. A., & Aminordin, A. (2023). The Integration of Gestalt Theory to The Graphic Design. *International Journal of Academic Research in Business and Social Sciences*, 13(6), 2496-2502. https://doi.org/10.6007/IJARBSS/v13-i6/15449

Kim, E., Yoon, J., Kwon, J., Liaw, T., & Agogino, A. M. (2019). From Innocent Irene to Parental Patrick: Framing User Characteristics and Personas to Design for Cybersecurity. *Proceedings of the Design Society: International Conference on Engineering Design*, 1(1), 1773-1782. https://doi.org/10.1017/dsi.2019.183

Knapp, K. J. (2009). *Security Considerations in the Development Life Cycle: Computer Science & IT Book Chapter | IGI Global Scientific Publishing*. https://www.igi-global.com/chapter/handbook-research-modern-systems-analysis/21076

Laurel, C. T. U. 11301 S. R. (2024, March 18). *How UX Design Can Improve Cybersecurity: Designing with the User In Mind*. https://www.captechu.edu/blog/how-ux-design-can-improve-cybersecurity

Legrand, J. (2022, January 27). Humans and Cybersecurity—The Weakest Link or the Best Defense? *ISACA*. https://www.isaca.org/resources/isaca-journal/issues/2022/volume-1/humans-and-cybersecurity-the-weakest-link-or-the-best-defense

Lidwell, W., Holden, K., & Butler, J. (2010). Universal Principles of Design, Revised and Updated: 125 Ways to Enhance Usability, Influence Perception, Increase Appeal, Make Better Design Decisions, and Teach Through Design. *Rockport Publishers*.

Linsey, J. S., Clauss, E. F., Kurtoglu, T., Murphy, J. T., Wood, K. L., & Markman, A. B. (2011). An Experimental Study of Group Idea Generation Techniques: Understanding the Roles of Idea Representation and Viewing Methods. *Journal of Mechanical Design*, 133(031008). https://doi.org/10.1115/1.4003498

Marriott, M. (2018). Bringing gestalt to cyber security*. *In Relational Organisational Gestalt*. Routledge.

Martin, F., & Betrus, A. K. (2019). Digital Media Design Theories and Principles. In Martin F. & Betrus A. K. (Eds.), *Digital Media for Learning: Theories, Processes, and Solutions* (pp. 17-32). Springer International Publishing. https://doi.org/10.1007/978-3-030-33120-7_2

Mathis, F., Vaniea, K., & Khamis, M. (2022). Prototyping Usable Privacy and Security Systems: Insights from Experts. *International Journal of Human-Computer Interaction*, 38(5), 468-490. https://doi.org/10.1080/10447318.2021.1949134

Mathur, S., & Malik, S. (2010). Advancements in the V-Model. *International Journal of Computer Applications*, 1(12), 30-35. https://doi.org/10.5120/266-425

McGraw, G. (2012). Software Security. *Datenschutz Und Datensicherheit - DuD*, 36(9), 662-665. https://doi.org/10.1007/s11623-012-0222-3

Mckenna, S., Staheli, D., & Meyer, M. (2015). Unlocking user-centered design methods for building cyber security visualizations. *2015 IEEE Symposium on Visualization for Cyber Security (VizSec)*, 1-8. https://doi.org/10.1109/VIZSEC.2015.7312771

Moszkowicz, J. (2011). Gestalt and Graphic Design: An Exploration of the Humanistic and Therapeutic Effects of Visual Organization. *Design Issues*, 27(4), 56-67.

Naqvi, B., & Porras, J. (2020). Usable Security by Design: A Pattern Approach. In Moallem A. (Ed.), *HCI for Cybersecurity, Privacy and Trust* (pp. 609-618). Springer International Publishing. https://doi.org/10.1007/978-3-030-50309-3_41

NIST. (2021). Human-Centered Cybersecurity. *NIST*. https://www.nist.gov/programs-projects/human-centered-cybersecurity

Norman, D. A. (2013). *The design of everyday things*. MIT Press.

Pinochet, D. (2017). Discrete Heuristics. In Çagdas G., Özkar M., Gül L. F., & Gürer E. (Eds.), *Computer-Aided Architectural Design. Future Trajectories* (pp. 306-326). Springer. https://doi.org/10.1007/978-981-10-5197-5_17

Rao, V., Moore, G., Jung, H. J., Kim, E., Agogino, A., & Goucher-Lambert, K. (2021). Supporting Human-Centered Design in Phsychologically Distant Problem Domains: The Design for Cybersecurity Cards. *Proceedings of the Design Society*, 1, 2831-2840. https://doi.org/10.1017/pds.2021.544

Ross, R. (2007). Managing Enterprise Security Risk with NIST Standards. *Computer*, 40(8), 88-91. Computer. https://doi.org/10.1109/MC.2007.284

Saltzer, J. H., & Schroeder, M. D. (1975). The protection of information in computer systems. *Proceedings of the IEEE*, 63(9), 1278-1308. Proceedings of the IEEE. https://doi.org/10.1109/PROC.1975.9939

Sanders, E. B.-N., & Stappers, P. J. (2014). Probes, toolkits and prototypes: Three approaches to making in codesigning. *CoDesign*, 10(1), 5-14. https://doi.org/10.1080/15710882.2014.888183

Seong, Y., Nuamah, J., & Yi, S. (2020). Guidelines for cybersecurity visualization design. *Proceedings of the 24th Symposium on International Database Engineering & Applications*, 1-6. https://doi.org/10.1145/3410566.3410606

Shahzad, S., Joiner, K., Qiao, L., Deane, F., & Plested, J. (2024). Cyber Resilience Limitations in Space Systems Design Process: Insights from Space Designers. *Systems*, 12(10), Article 10. https://doi.org/10.3390/systems12100434

Spiekermann, S. (2012). The challenges of privacy by design. *Commun. ACM*, 55(7), 38-40. https://doi.org/10.1145/2209249.2209263

Tzavara, V., & Vassiliadis, S. (2024). Tracing the evolution of cyber resilience: A historical and conceptual review. *International Journal of Information Security*, 23(3), 1695-1719. https://doi.org/10.1007/s10207-023-00811-x

Van Der Kleij, R. (2022). From Security-as-a-Hindrance Towards User-Centred Cybersecurity Design. *Human Factors in Cybersecurity*, 53(53). https://doi.org/10.54941/ahfe1002209

Voss, M., Sauer, T., & Bozkurt, H. (2014). Using Design Heuristics in Idea Generation: Does it Take Expertise to Benefit? *DS 78: Proceedings of the 16th International Conference on Engineering and Product Design Education (E&PDE14), Design Education and Human Technology Relations, University of Twente, The Netherlands, 04-05.09.2014*, 574-579.

Wash, R., & Rader, E. (2021, January 1). Prioritizing security over usability: Strategies for how people choose passwords. | *EBSCOhost*. https://doi.org/10.1093/cybsec/tyab012

Yilmaz, S. (2010). Design Heuristics [Design Science, The University of Michigan]. *In The Design Society—A worldwide community* (pp. 1-246). https://www.designsociety.org/publication/33122/DESIGN+HEURISTICS

Yilmaz, S., Daly, S. R., Seifert, C. M., & Gonzalez, R. (2016). Evidence-based design heuristics for idea generation. *Design Studies*, 46, 95-124. https://doi.org/10.1016/j.destud.2016.05.001

Yilmaz, S., Seifert, C., Daly, S. R., & Gonzalez, R. (2016). Design Heuristics in Innovative Products. *Journal of Mechanical Design*, 138(071102). https://doi.org/10.1115/1.4032219