Applied Computer Systems
ISSN 2255-8691 (online)
2026, vol. 31, no. 1, pp. 54–62
https://doi.org/10.2478/acss-2026-0005
https://content.sciendo.com

1862
RIGA TECHNICAL UNIVERSITY

User as the System Core: Evolution of the User-Aligned Systems Engineering Framework

Ashkan Yaldaie[1*], Jari Porras[2]
[1]*Järvenpää, Finland*
[2]*LUT University, Lappeenranta, Finland*

***Abstract* – Efficiency, convenience, and safety are the standard promises of modern engineered systems. However, the execution often fails to match this vision, leading to a disconnect where users become skeptical, frustrated, or simply unwilling to adopt the technology in their daily lives. To bridge this gap between technical potential and user reality, this paper proposes the User-Aligned Systems Engineering Framework (UASEF). While the framework is deeply rooted in the complexities of smart home research, its core principles are designed to be universally applicable, reorienting the engineering process to place the human element at the centre. UASEF mandates a structure built around a central core of security and trust by design, revolving through six iterative phases, moving beyond basic functionality to prioritize deep stakeholder analysis, transparent architecture, and critical factors like cost, accessibility, and embedded security. By deconstructing specific friction points such as usability barriers and privacy concerns, this study demonstrates that the design principles required for a smart home are actually vital for any complex system. Ultimately, UASEF provides developers with actionable guidance to create technology that is not merely functional, but inherently secure, intuitive, and capable of earning long-term user confidence.**

***Keywords* – Open architecture, security engineering, systems engineering, trust by design, user-centred design.**

I. Introduction

For decades, engineered systems in our homes, hospitals, vehicles, and financial institutions have promised to simplify life, improve safety, and make better use of resources [1]–[4]. Yet, there is still a clear gap between what these technologies can do and how people actually use them over time [5], [6]. Take smart homes as an example. Even though the market is expected to grow into hundreds of billions, user adoption is lagging behind these projections. The usual problems show up: the systems feel too complicated, devices do not work smoothly together, and people are unsure whether their data are truly protected [4], [7].

Usually, the problem is not that engineers cannot build these systems, but that users are often left out of the design. Take mobile banking as an example. Apps are convenient, but people still worry about security. How they behave depends greatly on their age, experience, and how risky they perceive it to be [8]. In digital health, the "ownership dilemma" leaves patients cut off from their own medical records, trapped in fragmented data silos [9]. When systems force users to choose between functionality and privacy or require technical skills that most people do not have, trust breaks down, and the system cannot deliver on its potential [10], [11].

To bridge this divide, this paper proposes a shift from technology-centric development to a User-Aligned Systems Engineering Framework (UASEF). This expanded model builds directly upon the User-Aligned Smart Home Development Framework (UASH-DF), which was originally designed to guide the creation of smart living environments that are not only technically robust but also empathetic and inclusive [4]. The original framework identified that for automation to be accepted, it must respect the "invisible boundaries" of daily life and address the deep-seated fears regarding surveillance and data misuse. By extrapolating these principles, we demonstrate that the challenges facing a homeowner trying to integrate a smart lock are fundamentally similar to those of a patient navigating a health portal or a driver managing over-the-air (OTA) updates in a connected vehicle [10], [12].

The evolved framework presented here follows six iterative steps, beginning with a rigorous definition of user and stakeholder requirements that goes beyond functional specifications to include emotional and contextual needs. It advocates for context-aware design that accounts for the specific environment, such as the privacy sensitivity of a personal office [13] or the safety-critical nature of an autonomous vehicle's mixed-criticality workload [12]. Furthermore, it emphasizes a transparent and open architecture to address interoperability crises seen in fragmented markets [4], and rigorous attention to affordability to prevent digital divides [11].

Crucially, the framework posits that security and trust cannot be treated as "add-on" features. In sectors like finance, institutional trust is a primary driver of adoption, often outweighing performance expectancy for certain demographics [8]. Similarly, in the automotive sector, the integration of third-party software creates vulnerabilities that require a "security by design" approach throughout the supply chain [12]. By embedding these considerations from the outset,

*Corresponding author's e-mail: ashkan952000@gmail.com
Article received 2026-02-21; accepted 2026-04-09

rather than patching them in post-deployment, we can create systems that maintain confidence among the people who rely on them [14].

This paper introduces the UASEF, a general approach to designing systems that place the user experience at the centre of every decision. The framework addresses not only functional requirements but also emotional, contextual, and social needs that often go overlooked in traditional system design. By examining common challenges such as privacy concerns, usability barriers, and fragmented system interactions across a variety of complex systems, we demonstrate how a user-centred perspective can inform better design in multiple domains. The goal is to move past systems that merely function and create systems that are intuitive, inherently secure, and fundamentally aligned with human expectations, capabilities, and values, ensuring that technology serves people rather than the other way around.

Building on this perspective, this paper addresses the following research questions:

RQ1. How can the principles of the User-Aligned Smart Home Development Framework be generalized into a domain-independent User-Aligned Systems Engineering Framework (UASEF)?

RQ2. How can UASEF guide system design across diverse domains to improve usability, trust, and alignment with user needs?

Exploring the first question helps reveal the fundamental principles that make user-aligned design effective and shows how the framework can be extended beyond smart homes to other types of systems. The second question examines how these principles can be applied in practice, guiding the creation of technologies that are more intuitive, secure, and closely aligned with user needs and expectations.

II. Literature Review

While interconnected systems have scaled rapidly, selling the vision of a more efficient, seamless future, the reality often falls short of the promise. A gap persists between technical potential and user adoption. We are learning that meeting engineering targets, such as uptime or functionality, simply is not the whole picture.

Users encounter friction that is not always technical; it is psychological and logistical. They grapple with trust issues, privacy anxieties, and the difficulty of weaving these systems into the fabric of everyday life. Here, we examine the logic and development of the User-Aligned Smart Home Development Framework (UASH-DF), using it as a lens to view similar challenges inherent in other complex environments.

A. The User-Aligned Smart Home Development Framework

The smart home domain has long been characterised by a fragmented market of closed ecosystems, inconsistent user interfaces, and significant user anxiety regarding data privacy. Despite a market projected to reach hundreds of billions of dollars, mass adoption has been hindered by a "technology-first" rather than "user-first" approach [15], [16]. To address these barriers, Yaldaie (2025) developed the UASH-DF, a structured framework designed to bridge the gap between theoretical capabilities and the lived realities of modern households [4].

The formation of the UASH-DF was not arbitrary; it emerged from a multiphase, mixed-methods investigation following Design Science Research (DSR) principles. Initially, a systematic literature review identified that while motion sensors and voice controls were advancing, they often prioritized functionality at the expense of security, or vice versa [11]. This was followed by an international survey revealing that while users desired security and energy management, they were deterred by high costs and setup complexity [10]. These insights drove the iterative development of a Raspberry Pi-based prototype [17], which was subsequently validated using the Technology Acceptance Model (TAM) [14].

As shown in Fig. 1, the resulting framework is built upon six interlocking phases intended to guide engineers and developers:

1. *Context-Aware Design*: Systems must be grounded in an understanding of the physical layout and social dynamics of the home, moving beyond generic automation to specific use cases like "entering/exiting" or "sleeping".
2. *Open-Source Platform Architecture*: To combat the frustration of vendor lock-in and discontinued services, the framework advocates for transparent, modifiable platforms that avoid subscription dependencies.
3. *Security and Trust by Design*: Serving as the precursor to UASEF's core, this phase demonstrated that security cannot be an afterthought. It operationalized the core concept for the residential domain by mandating secure defaults (e.g., key-based authentication) to fulfil the security requirement, and automated intrusion defences to guarantee system predictability, thereby fostering measurable user trust.
4. *Affordability and Accessibility*: Recognising budgetary constraints as a primary barrier, the framework prioritizes cost-optimised components and pre-configured system images to lower the technical barrier to entry.
5. *Ecosystem Compatibility*: To address fragmentation, systems must support open standards (like Matter) and integrate with major ecosystems (e.g., Alexa, HomeKit) via middleware, ensuring users are not forced into a single hardware silo.
6. *Continuous Behavioural Evaluation*: Finally, the framework posits that deployment is not the end; systems must undergo periodic TAM-based assessments to measure perceived usefulness and ease of use over time.

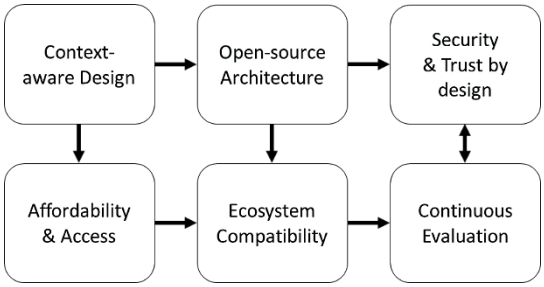

Fig. 1. The UASH-DF [4].

The UASH-DF essentially argues that a "smart" home is not defined by the number of sensors it contains, but by its ability to align with the human need for control, privacy, and simplicity [4].

B. Cross-Domain User-Centred Challenges

The challenges observed in smart home systems, such as usability barriers, trust deficits, and privacy concerns, are not unique. Similar patterns appear across other complex systems and highlight the need for a generalized user-aligned framework.

The disconnect between engineering prowess and user adoption identified in smart homes is mirrored in the domain of digital health. Just as smart home users struggle with fragmented ecosystems, the healthcare sector faces the "dilemma of comprehensiveness", where patient data remain siloed in provider-specific formats, preventing a holistic view of an individual's health history. Klementi et al. highlight that while technologies exist to aggregate these data, legal and semantic interoperability hurdles prevent the creation of a unified Personal Health Record (PHR) [9].

Furthermore, the "dilemma of ownership" in health data parallels the lack of control smart home users feel regarding their device data. Current architectures often store sensitive medical data on third-party servers, leaving patients legally entitled to their data but practically unable to exercise control over it [9]. This lack of agency erodes trust, a phenomenon also observed in smart homes where users fear unauthorized surveillance [10], [16].

From a usability perspective, the challenges are equally striking. In a study of mHealth applications in Bangladesh, Islam et al. found that despite high smartphone penetration, the usability of health apps was generally unsatisfactory, with violations of design heuristics such as "aesthetic and minimalist design" and "match between system and the real world". The study revealed that 61 % of usability problems were catastrophic or major, directly correlating with low System Usability Scores (SUS) [18]. Similarly, a scoping review by Tandon et al. found that while user satisfaction was frequently measured, deeper metrics like "learnability" and "actionability", meaning the user's ability to actually interpret and act on data, were rarely assessed. This suggests that, like some smart home technology, digital health often succeeds at capturing data but fails at making that data intuitively useful for the end-user [19].

The automotive industry is currently undergoing a transformation analogous to the smart home evolution, shifting from hardware-defined mechanics to Software-Defined Vehicles (SDVs) [12]. This paradigm shift promises flexibility and over-the-air (OTA) updates but introduces severe interoperability and security drawbacks similar to those addressed by the UASH-DF [4], as vehicles become "smart", the attack surface expands exponentially. De Vincenzi et al. note that the integration of third-party applications and libraries, which is necessary for the rich feature sets users expect, creates vectors for malware and unauthorized access, much like adding insecure IoT devices to a home network. The reliance on APIs to abstract hardware functions introduces vulnerabilities if these interfaces are misconfigured. Furthermore, the supply chain complexity in automotive engineering mirrors the fragmentation of the smart home market. Integrating software and hardware from diverse suppliers with varying cybersecurity standards creates weak links that can compromise the entire vehicle [12].

Privacy concerns in SDVs also echo those in smart living environments. Just as smart home users worry about voice assistants recording conversations, vehicle users face risks of "valet attacks", where personal data synced via Bluetooth, such as contacts and call logs, remain accessible to unauthorized users like valets or rental car drivers due to flawed implementation of connection protocols [20]. Renganathan et al. demonstrated that despite encryption mechanisms, privacy was often compromised by system design that failed to account for the social context of vehicle usage, for example, handing keys to a stranger. This aligns with the UASH-DF's emphasis on "context-aware design", reinforcing that security protocols must account for human behaviour, not just technical specifications [4].

In the financial sector, the adoption of mobile banking (m-banking) apps illustrates the critical role of trust and risk perception, validating the UASH-DF's focus on "trust by design" [4]. Apau and Lallie applied the Extended Unified Theory of Acceptance and Use of Technology (UTAUT2) to m-banking and found that "perceived security" was the most significant predictor of behavioural intention to use these systems [8].

A critical challenge for system engineers is that trust is not a uniform metric. Interestingly, the perception of security in finance is heavily moderated by demographic factors, a nuance often missed in purely technical engineering frameworks. For instance, the effect of perceived security on the intention to use banking apps is stronger in younger men with high education, whereas institutional trust is a more critical driver for older women [8]. This mirrors findings in smart home research where different demographics (e.g., elderly users vs. tech-savvy youth) have vastly different thresholds for technology acceptance [4].

Furthermore, the "privacy paradox" observed in smart homes, where users express concern but still use devices, is present in fintech as well. However, Saprikis et al. found that for non-users of banking apps, "perceived risk" is a primary inhibitor, whereas active users are more concerned with

"anxiety" related to technical failure [21]. This suggests that the barrier to entry, related to trust and risk, differs from the barrier to continuance, related to usability and reliability, a distinction that supports the UASH-DF's requirement for continuous behavioural evaluation throughout the product lifecycle [4].

C. Synthesis

The literature reveals a convergent set of challenges across different domains. Whether it is a patient unable to access their complete medical record [9], a driver unknowingly leaking data to a valet [20], or a homeowner struggling to integrate incompatible devices [10], [11], the core failure is rarely a lack of connectivity or processing power. Rather, it is a failure to engineer systems that respect the user's need for control, transparency, and context-appropriate security.

The UASH-DF was formed to address these specific flaws within the residential domain by mandating that security and usability be treated as foundational architectural requirements rather than optional features [4]. The evidence suggests that this user-aligned approach is not only applicable to smart homes but is a necessary evolution for any engineered system embedded in the fabric of daily life. By generalising these principles, we can move from systems that merely function to systems that are trusted, adopted, and sustained.

III. Research Methodology

The development of the UASEF followed a two-stage methodological approach. The first stage involved the rigorous empirical validation of the precursor framework, the UASH-DF, through a multi-phase mixed-methods design. The second stage relied on a comparative literature review across adjacent technical domains such as automotive, healthcare, and financial technology to identify cross-sector parallels in user friction, which provided the basis for generalising the framework's core principles.

A. Validation of the Foundational Framework (UASH-DF)

UASEF is rooted in a four-phase research design executed to validate the UASH-DF. This process moved from theoretical exploration to practical implementation and behavioural assessment, ensuring the framework was not merely conceptual but grounded in empirical reality.

As introduced earlier, the foundational UASH-DF was validated through a four-phase Design Science Research (DSR) approach. This began with a systematic literature review [11] and an empirical needs assessment via an international survey [10] to capture user preferences. These insights drove the implementation of a tangible Raspberry Pi-based prototype [17]. Finally, a TAM-based behavioural evaluation confirmed that trust and privacy concerns acted as significant gating factors for long-term adoption [14].

B. Cross-Domain Comparative Review

Following the validation of the smart home framework, a broader narrative review was conducted to assess whether barriers identified in domestic environments, particularly those related to trust, security, and usability, were also present in other engineering contexts. This comparison revealed clear similarities in how users struggle to interact with complex systems across sectors, supporting the extension of the specialised UASH-DF into the more general UASEF. Although the cross-domain review was structured narratively to accommodate diverse field terminologies, it employed a rigid thematic extraction process. Domains were purposively sampled based on their high reliance on complex sociotechnical integration (automotive, healthcare, and finance). The generalisation process was strictly guided by mapping structural patterns against the precursor UASH-DF, utilising predefined evaluation criteria: security constraints, interoperability barriers, and measurable usability friction. This confirms that the core pillars of the original framework, including Context-Aware Design, Security by Design, and Continuous Behavioural Evaluation, are broadly applicable, guiding UASEF as a structured framework for creating systems that are secure, intuitive, and capable of earning long-term user confidence in diverse settings.

IV. Introducing the User-Aligned Systems Engineering Framework

The UASEF represents a structural evolution of the domain-specific smart home development. While derived from the rigorous validation of residential automation systems, UASEF is abstracted here as a generalised lifecycle for complex sociotechnical systems. Distinct from linear engineering models, UASEF is concentric: to keep the user safely at the centre of the system, it positions Security and Trust by Design not as a stage, but as the immutable engineering core around which six iterative steps revolve. This structure acknowledges that in modern connected environments, ranging from healthcare to automotive, trust is not a static feature but a dynamic outcome of system performance and security.

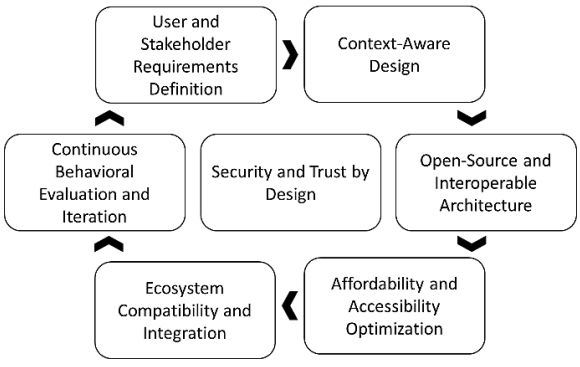

Fig. 2. The UASEF.

A. The Architectural Core: Security and Trust by Design

To prevent conceptual ambiguity, UASEF formally defines "Security and Trust by Design" as a unified sociotechnical construct. Here, Security by Design is defined as the structural enforcement of the confidentiality, integrity, and availability (CIA) triad through verifiable metrics (e.g., systematic risk assessments, encryption, and access controls) embedded from the concept phase [9], [22]. Trust by Design is defined as the intentional engineering of system transparency, predictable

behaviour, and data sovereignty, resulting in the user's measurable willingness to rely on the system [23]. Together, they form an immutable engineering core rather than retrospective add-ons. Literature indicates that "bolting on" security after development frequently fails to mitigate vulnerabilities in complex ecosystems like Building Automation and Control Systems or mHealth, where legacy protocols often lack intrinsic protection [24], [25]. Consequently, UASEF requires that every subsequent step in the lifecycle is formally validated against this combined definition, ensuring trust is a quantifiable engineering outcome rather than an abstract goal.

B. Stage 1: User and Stakeholder Requirements Definition

The first stage requires us to move beyond dry technical specifications and really dig into what users actually need. We see the consequences of skipping this in mHealth research [18]. If a system is hard to use or ignores diverse abilities, people simply stop using it [19]. It does not matter how effective the technology is on paper.

That is why UASEF insists on gathering requirements from more than just the end user. Consistent with established Requirements Engineering (RE) literature, we must include the entire ecosystem of stakeholders, such as caregivers in healthcare or maintenance crews in facility management. Their daily interactions with the system are critical for its long-term success [5], [19]. This stage emphasises identifying specific friction points, including high cognitive load or physical accessibility issues. While these are foundational elements of formal RE, they are frequently bypassed in rushed, "technology-first" implementations, leading to downstream adoption failures [18]. UASEF enforces these RE baseline practices as mandatory architectural prerequisites.

C. Stage 2: Context-Aware Design

Once requirements are defined, the system must be designed with an acute awareness of the lived context in which it operates. Research into smart office environments shows that privacy preferences are not absolute but shift with spatial and temporal conditions; for example, users may accept monitoring in public corridors but reject it in private workspaces [13]. UASEF requires engineering decisions to account for these contextual nuances. A system must dynamically adapt its behaviour, such as data collection granularity or alert frequency, based on the user's current environment and activity, so that its performance aligns with the user's situational expectations of privacy and utility [13], [23].

D. Stage 3: Open-Source and Interoperable Architecture

While open-source architecture is typically viewed as a developer-centric methodology, UASEF mandates it specifically as a safeguard for the end-user. Fragmentation and vendor lock-in are cited as primary barriers to the adoption of smart technologies [4]. To counter this, Stage 3 elevates the requirement for open standards, which the foundational UASH-DF previously categorised in the lifecycle under "Ecosystem Compatibility" to a foundational architectural mandate. By enforcing modular architectures and open data standards (like Fast Healthcare Interoperability Resources (FHIR) in healthcare) at this structural level, UASEF ensures systems can exchange data seamlessly across different platforms without requiring complex, proprietary bridges [26].

By prioritizing open-source components and modular data standards, developers are structurally encouraged to shift away from monolithic, centralised databases toward decentralised, user-owned data architectures. This architectural pivot leverages community-driven security auditing and ensures that the system remains viable even if a specific vendor ceases support, thus transforming abstract "user sovereignty" into a tangible engineering reality [9].

E. Stage 4: Affordability and Accessibility Optimisation

Technical sophistication often comes at a financial premium that excludes marginalized demographics. Studies on the adoption of health technologies by older adults indicate that cost and complexity are significant inhibitors [5]. UASEF explicitly integrates affordability as an engineering constraint in this step. This involves selecting cost-effective hardware (e.g., commodity sensors or Raspberry Pi-based nodes) and optimizing software to run on resource-constrained devices, ensuring that safety and convenience technologies remain accessible to users across the socio-economic spectrum [4], [5]. Accessibility here also implies integrating core user-centric design principles to accommodate varying levels of digital literacy, ensuring the system is usable by non-experts.

F. Stage 5: Ecosystem Compatibility and Integration

No system operates in isolation; it must function within a broader technological, organisational, and human ecosystem. Building upon the open standards established in Stage 3, this stage focuses on the practical execution of aligning those new interoperable designs with existing platforms, external services, and operational practices. The digital health sector offers a clear warning here. Projects often fail because new tools struggle to communicate with established electronic health records [26].

UASEF addresses this by requiring developers to create a clear map of trust relationships. They must define how the new system connects to existing nodes, including IoT devices, cloud platforms, and human users. The objective is to verify that integration acts as a bridge rather than a source of new security risks or operational delays [7].

G. Stage 6: Continuous Behavioural Evaluation and Iteration

The final stage argues that deployment is merely a milestone, not the finish line of the engineering lifecycle. User trust is something earned over time through consistent performance. If a malfunction occurs and goes unaddressed, that confidence can evaporate in an instant [23].

To prevent this, UASEF mandates continuous, metric-driven behavioural evaluation. This stage requires the implementation of standardised telemetry, structured user feedback loops utilising validated instruments (e.g., customised TAM surveys), and automated anomaly detection logs. These mechanisms quantitatively and qualitatively compare the system's operational use against its baseline design specifications. This step ensures the system has room to evolve. It allows developers

to patch vulnerabilities and adapt features to meet shifting user habits, effectively sustaining the core requirement of trust for the entire life of the system [19], [27].

For the smart home domain, the initial UASH-DF validation used the TAM to measure key factors, confirming that trust and privacy concerns act as significant gating factors for long-term adoption, alongside Perceived Usefulness and Ease of Use. This approach to measuring trust and security as part of user acceptance can be extended and adapted for other domains. By leveraging this model, developers can customise the TAM instrument to address domain-specific variables, such as "perceived risk" in financial technology or "data ownership dilemma" in digital health, allowing for a structured, longitudinal evaluation of user confidence.

Since the framework does not restrict the evaluation method, other established user acceptance models, such as the Extended Unified Theory of Acceptance and Use of Technology (UTAUT2), can also be employed to capture context-specific factors, like performance expectancy or hedonic motivation, thereby enabling a comprehensive assessment across various sociotechnical domains.

H. Framework Synthesis and Authorial Perspective

Taken as a whole, UASEF reframes systems engineering as a trust-centred, user-grounded discipline rather than a purely technical exercise. The six stages are not designed to be executed once or in strict sequence. Instead, they form an iterative structure that continuously orbits the core principle of Security and Trust by Design. Weaknesses in any stage tend to surface elsewhere, most often as reduced user confidence, friction in real-world use, or system abandonment.

From the authors' perspective, the central contribution of UASEF is its explicit recognition that modern systems operate within heterogeneous, evolving ecosystems. These ecosystems include not only legacy infrastructure, but also parallel platforms, third-party services, regulatory constraints, organizational practices, and human actors. UASEF treats compatibility with this broader environment as a first-class engineering concern rather than a deployment-time afterthought.

The framework also challenges the persistent pitfall in "technology-first" industry practices frequently observed in fragmented smart home [15], [16] and mHealth [18] deployments where technical optimisation is prioritized over human context, leading to high abandonment rates [28]. By embedding affordability, accessibility, contextual sensitivity, and continuous behavioural evaluation into the lifecycle, UASEF positions the user as an enduring reference point throughout design, deployment, and operation. Trust is therefore not assumed or declared at launch, but continuously produced through reliable behaviour, transparency, and adaptability.

In this sense, UASEF deliberately collapses the artificial separation between social and technical dimensions of system design. Factors such as usability, cost, interoperability, and trust dynamics are framed as engineering variables with direct impact on system resilience and longevity. Although grounded in smart home research, the framework is intended to be transferable to any sociotechnical domain where systems must coexist with other technologies, institutions, and people over extended time periods.

V. Critical Discussion

While concepts like user-centred design, human-centred computing, and security by design are well established, UASEF sets itself apart by embedding these principles throughout the engineering lifecycle. Rather than treating user experience, trust, or security as interface-level concerns or late-stage validation checks, UASEF formalizes them as system-level constraints that shape architecture, integration, and long-term operation. Its novelty lies in positioning Security and Trust by Design as a persistent core around which all engineering activities iterate, rather than as a sequential phase. Derived from empirical validation in a concrete domain and then generalised across sectors, UASEF distinguishes itself from traditional linear methodologies (such as the standard Systems Engineering V-Model [29], [30]) and generalised Human-Centred Design (HCD) standards (such as ISO 9241-210 [31]).

While the V-Model frequently isolates security as a late-stage verification phase, and standard HCD primarily addresses trust at the interface level, established User-Centred Design (UCD) methodologies have long recognised that systems must be designed around holistic human contexts rather than mere interfaces. Industry tools, such as SAP Scenes for storyboarding and contextual mapping [32], successfully capture these complex stakeholder environments. However, UASEF does not attempt to reinvent UCD; rather, it introduces the concept of being "User-Aligned". In this context, "User-Aligned" specifically means taking the rich contextual and behavioural insights generated by established UCD practices and mathematically welding them to hard architectural constraints. UASEF formally fuses these disciplines by enforcing a structurally secure, trust-centred core as the immutable anchor for every iterative engineering phase, ensuring that UCD insights are structurally protected by design.

The shift from the domain-specific UASH-DF to the generalised UASEF reflects a fundamental change in approaching complex sociotechnical systems, synthesising insights from smart homes with parallel evidence from automotive, financial, and digital health domains to address the research questions.

A. Generalising the Framework: From Smart Homes to Universal Systems (Addressing RQ1)

Research Question 1 asks: How can the principles of the User-Aligned Smart Home Development Framework be generalized into a domain-independent User-Aligned Systems Engineering Framework (UASEF)?

The generalisation of UASEF is predicated on the discovery that user friction points are not unique to residential settings but are systemic across modern engineering domains. The UASH-DF originally identified that adoption failures in smart homes stemmed from a lack of trust, interoperability, and contextual awareness. By analysing adjacent fields, we confirmed that

these were universal barriers, justifying the abstraction of the framework's six stages.

The Universality of Context: In smart homes, the UASH-DF emphasises that automation must respect the "invisible boundaries" of the household. This principle generalises effectively to smart office environments, where empirical data show that privacy preferences are spatially dependent; occupants tolerate monitoring in hallways but reject audio recording in private workspaces [13]. Similarly, in the automotive sector, the context of "valet mode" requires the system to dynamically restrict access to personal data when the vehicle is handed to a stranger, a privacy constraint often missed by purely technical security architectures [20]. Therefore, UASEF's "Context-Aware Design" stage is not about room layout, but about the situational appropriateness of system behaviour in any environment.

The Primacy of Trust: The UASH-DF placed security and trust as an important part of development because smart home users feared surveillance. This generalises directly to the financial sector, where "perceived security" is the strongest predictor of behavioural intention to adopt mobile banking applications, often outweighing convenience [8]. Furthermore, in digital health, the centralisation of data in national health information systems (like Estonia's EHIS) creates a "honeypot" for attackers, reinforcing why the transition toward decentralized, user-owned architectures (UASEF's Stage 3) is a necessary evolution for protecting sensitive medical records [9].

The Necessity of Interoperability: The fragmentation that plagues smart homes, where users must juggle multiple incompatible applications, is mirrored in healthcare by the dilemma of comprehensiveness, in which patient data remains siloed in provider-specific formats [9]. UASEF generalises the solution by mandating Open-Source Architecture and Ecosystem Compatibility, ensuring that systems across domains can exchange data seamlessly without vendor lock-in. Even in certain highly regulated or safety-critical domains where the underlying code cannot be entirely open, the use of open standards is critical, as the core idea must remain transparency and open standards for data exchange and integration.

B. Guiding System Design: Improving Usability, Trust, and Openness (Addressing RQ2)

Research Question 2 asks: How can UASEF guide system design across diverse domains to improve usability, trust, and alignment with user needs?

UASEF guides design by enforcing a nonlinear, iterative process where the human element is a constraint as rigid as voltage or bandwidth.

Redefining Usability through Stakeholder Inclusion: Traditional engineering often defines usability as interface efficiency. UASEF expands this by requiring the inclusion of all stakeholders in the "Requirements Definition" phase. In the mHealth domain, usability evaluations often fail because they focus solely on the patient, ignoring the "care partners" and clinicians who interpret the data [19]. By applying UASEF, designers are forced to account for these secondary users. Similarly, in mobile banking, reviews reveal that users are frequently frustrated by updates that break login functionality or biometrics [33]. UASEF's "Continuous Behavioural Evaluation" stage addresses this by treating deployment as the beginning of testing, ensuring that updates align with established user habits rather than disrupting them.

Operationalising Trust through Security by Design: Consistent with the framework's formal definition, UASEF improves trust by enforcing security as a foundational architectural requirement rather than a post-production patch. In the automotive industry, the rise of Software-Defined Vehicles (SDVs) has introduced attack surfaces via third-party APIs and supply chains [12]. When applied to this sector, operationalising "Security and Trust by Design" requires translating the core's demand for integrity and predictable behaviour into domain-specific mechanisms. This means implementing robust intrusion detection systems (IDS) and secure supply chain protocols before a vehicle ever hits the road. Furthermore, trust calibration is essential; users must not over-trust an AI system. For example, in built environment decision-making, UASEF encourages systems like PreservAI to provide explainable recommendations (e.g., regarding energy retrofits) so that human experts can validate the AI's logic, thereby aligning user trust with actual system capabilities [23].

Enhancing Openness and Accessibility: Finally, UASEF guides designers to prioritize affordability and open standards to prevent digital exclusion. Just as the smart home prototype employed Raspberry Pi hardware to reduce costs, mHealth architectures are encouraged to use Decentralised Content-Addressable Storage (DCAS) networks to lower the cost of securing data compared to centralised servers [9]. By enforcing Affordability and Accessibility Optimisation, UASEF ensures that critical technologies for home automation, health monitoring, and financial inclusion remain accessible to populations with lower income or limited technical literacy, who are often the most risk-averse [5].

However, in practice, engineers must often manage the trade-off between minimising cost (Affordability and Accessibility Optimisation, Stage 4) and maximising security robustness (Security and Trust by Design, Core principle). This reality requires a conscious, risk-based decision-making process to ensure cost savings do not compromise the essential safety or integrity of the system. This decision process should involve Risk Quantification, where engineers systematically assess the potential impact (e.g., financial, safety, privacy) of a security failure against the cost savings achieved by selecting a more affordable component.

Furthermore, it necessitates the Prioritisation of Core Requirements, meaning the core principle of Security and Trust must be maintained as the gating factor; any cost-optimisation decision that introduces a critical vulnerability or a high probability of user data compromise should be rejected. Finally, affordable engineering can be achieved not just by choosing cheaper components, but by employing a Layered Security Strategy that uses commodity hardware combined with robust, cost-effective software security measures, such as embedded

encryption and secure access controls, to maintain overall system integrity.

VI. Conclusion

This paper set out to address a problem that is consistently resurfacing across modern engineered systems: technical capability keeps advancing, yet user trust, adoption, and long-term engagement continue to lag behind. By tracing this gap from smart homes to healthcare, finance, and automotive systems, it becomes clear that the issue is not a lack of innovation, but a lack of alignment. Systems are built to work, but not always to live with.

The UASEF responds to this mismatch by reframing systems engineering around a simple but often neglected idea: users are not external to the system, they are part of it. Trust, security, usability, affordability, and context are not side constraints to be optimised later. They shape whether a system succeeds or quietly fails after deployment. By placing Security and Trust by Design at the core and surrounding it with iterative, human-centred stages, UASEF offers a structured way to turn this idea into engineering practice.

One of the key insights emerging from this study is that user-related failures tend to look different on the surface but share the same roots underneath. A homeowner abandoning automation, a patient unable to access their health data, or a driver unknowingly exposing personal information are all symptoms of systems that ignore context, overestimate user tolerance, or assume trust instead of earning it. The UASEF does not eliminate complexity, but it forces that complexity to be handled consciously, rather than passed on to the user.

Importantly, while the UASEF avoids prescribing a singular operational methodology, it establishes rigid, non-negotiable system-level constraints. As an engineering framework, it enforces strict boundaries around trust and user-alignment; developers retain the flexibility to select specific engineering and testing methods, provided those methods empirically satisfy the framework's core security requirements and continuous evaluation mandates. Its value lies in making human concerns explicit engineering variables, ones that can be designed for, tested, and revisited over time. While grounded in smart home research, the framework is intentionally domain-independent and applicable wherever systems operate close to people's daily lives.

Ultimately, the contribution of this study is not a new technology, but a shift in posture. When systems are designed with users as the system core rather than the final checkpoint, adoption becomes more than a rollout metric. It becomes a natural outcome. The UASEF offers a path toward systems that are not only functional and secure, but understandable, trustworthy, and sustainable in real-world use. The goal of engineering is moved from technical capability to human confidence.

References

[1] J. Yu, J. Huang, and Q. Yang, "Long-term adoption or abandonment of smart technology in the Chinese elderly home care environment: A qualitative research study," *Healthcare*, vol. 11, no. 17, Aug. 2023, Art. no. 2440. https://doi.org/10.3390/healthcare11172440

[2] Y. Chen, N. Shiwakoti, P. Stasinopoulos, and S. K. Khan, "State-of-the-art of factors affecting the adoption of automated vehicles," *Sustainability*, vol. 14, no. 11, May 2022, Art. no. 6697. https://doi.org/10.3390/su14116697

[3] M. B. Amnas, M. Selvam, M. Raja, S. Santhoshkumar, and S. Parayitam, "Understanding the determinants of FinTech adoption: Integrating UTAUT2 with trust theoretic model," *Journal of Risk and Financial Management*, vol. 16, no. 12, Dec. 2023, Art. no. 505. https://doi.org/10.3390/jrfm16120505

[4] A. Yaldaie, "From research to living rooms: Evaluating smart home technologies through systematic reviews, user studies, and practical implementations," Ph.D. dissertation, Lappeenranta-Lahti University of Technology LUT, 2025.

[5] A. Bertolazzi, V. Quaglia, and R. Bongelli, "Barriers and facilitators to health technology adoption by older adults with chronic diseases: an integrative systematic review," *BMC Public Health*, vol. 24, no. 1, Feb. 2024, Art. no. 506. https://doi.org/10.1186/s12889-024-18036-5

[6] J. Pulkkinen, K. Huttu, and M. Suhonen, "Systemic challenges in AI adoption in public social and health organizations in Finland: a technology-organisation-environment perspective," *J. Health Organ. Manag.*, vol. 39, no. 9, pp. 435–456, Dec. 2025. https://doi.org/10.1108/JHOM-06-2025-0309

[7] M. Aaqib, A. Ali, L. Chen, and O. Nibouche, "IoT trust and reputation: a survey and taxonomy," *Journal of Cloud Computing*, vol. 12, Dec. 2023, Art. no. 42. https://doi.org/10.1186/s13677-023-00416-8

[8] R. Apau and H. Singh Lallie, "Measuring user perceived security of mobile banking applications," *arXiv:2201.03052*, Jan. 2022. https://doi.org/10.48550/arXiv.2201.03052

[9] T. Klementi, G. Piho, and P. Ross, "A reference architecture for personal health data spaces using decentralized content-addressable storage networks," *Front. Med. (Lausanne)*, vol. 11, Jul. 2024. https://doi.org/10.3389/fmed.2024.1411013

[10] A. Yaldaie, J. Porras, and O. Drögehorn, "Who are smart home users and what do they want? – Insights from an International Survey," *Applied Computer Systems*, vol. 28, no. 1, pp. 114–124, Jun. 2023. https://doi.org/10.2478/acss-2023-0011

[11] A. Yaldaie, J. Porras, and O. Drogehorn, "The present state of home automation: A systematic literature review," *International Journal of Hybrid Innovation Technologies*, vol. 2, no. 1, pp. 23–46, Oct. 2022. https://doi.org/10.21742/ijhit.2653-309X.2022.2.1.03

[12] M. De Vincenzi *et al.*, "Contextualizing security and privacy of software-defined vehicles: State of the art and industry perspectives," Dec. 2024. [Online]. Available: http://arxiv.org/abs/2411.10612

[13] B. Li, A. Tavakoli, and A. Heydarian, "Occupant privacy perception, awareness, and preferences in smart office environments," *Sci. Rep.*, vol. 13, no. 1, Mar. 2023, Art. no. 4073. https://doi.org/10.1038/s41598-023-30788-5

[14] A. Yaldaie, J. Porras, and O. Drögehorn, "User perceptions of a home automation system: A TAM-based evaluation," *Applied Computer Systems*, vol. 30, no. 1, pp. 98–104, Jan. 2025. https://doi.org/10.2478/acss-2025-0012

[15] M. R. Reisinger, S. Prost, J. Schrammel, and P. Fröhlich, "User requirements for the design of smart homes: dimensions and goals," *J. Ambient Intell. Humaniz. Comput.*, vol. 14, pp. 15761–15780, Dec. 2023. https://doi.org/10.1007/s12652-021-03651-6

[16] S. FakhrHosseini, C. Lee, S.-H. Lee, and J. Coughlin, "A taxonomy of home automation: Expert perspectives on the future of smarter homes," *Information Systems Frontiers*, vol. 27, pp. 449–466, Apr. 2025. https://doi.org/10.1007/s10796-024-10496-9

[17] A. Yaldaie, J. Porras, and O. Drögehorn, "Innovative home automation with raspberry pi: A comprehensive approach to managing smart devices," *Asian Journal of Computer Science and Technology*, vol. 13, no. 1, pp. 27–40, Apr. 2024. https://doi.org/10.70112/ajcst-2024.13.1.4260

[18] M. N. Islam, Md. M. Karim, T. T. Inan, and A. K. M. N. Islam, "Investigating usability of mobile health applications in Bangladesh," *BMC Med. Inform. Decis. Mak.*, vol. 20, Dec. 2020, Art. no. 19. https://doi.org/10.1186/s12911-020-1033-3

[19] A. Tandon *et al.*, "Human factors, human-centered design, and usability of sensor-based digital health technologies: Scoping review," *J. Med. Internet Res.*, vol. 26, Nov. 2024, Art. no. e57628. https://doi.org/10.2196/57628
[20] V. Renganathan, E. Yurtsever, Q. Ahmed, and A. Yener, "Valet attack on privacy: a cybersecurity threat in automotive Bluetooth infotainment systems," *Cybersecurity*, vol. 5, Oct. 2022, Art. no. 30. https://doi.org/10.1186/s42400-022-00132-x
[21] V. Saprikis, G. Avlogiaris, and A. Katarachia, "A comparative study of users versus non-users' behavioral intention towards M-banking apps' adoption," *Information*, vol. 13, no. 1, Jan. 2022, Art. no. 30. https://doi.org/10.3390/info13010030
[22] A. Llaria, J. Dos Santos, G. Terrasson, Z. Boussaada, C. Merlo, and O. Curea, "Intelligent buildings in smart grids: A survey on security and privacy issues related to energy management," *Energies (Basel)*, vol. 14, no. 9, May 2021, Art. no. 2733. https://doi.org/10.3390/en14092733
[23] A. Behzadan and A. Dabiri, "Factors influencing human trust in intelligent built environment systems," *AI and Ethics*, vol. 5, pp. 5841–5855, Aug. 2025. https://doi.org/10.1007/s43681-025-00813-6
[24] V. Graveto, T. Cruz, and P. Simões, "Security of building automation and control systems: Survey and future research directions," *Comput. Secur.*, vol. 112, Jan. 2022, Art. no. 102527. https://doi.org/10.1016/j.cose.2021.102527
[25] L. H. Iwaya, A. Ahmad, and M. A. Babar, "Security and privacy for mHealth and uHealth systems: A systematic mapping study," *IEEE Access*, vol. 8, pp. 150081–150112, Aug. 2020. https://doi.org/10.1109/ACCESS.2020.3015962
[26] L. Assom, T. Karunaratne, and A. Larsson, "Harmonizing patient-centric requirements for secure digital health services in heterogeneous settings," *BMC Health Serv. Res.*, vol. 25, Feb. 2025, Art. no. 235. https://doi.org/10.1186/s12913-024-11978-x
[27] B. Mohajeri and J. Cheng, "'Inconsistent performance': Understanding concerns of real-world users on smart mobile health applications through analyzing app reviews," in *Adjunct Proceedings of the 35th Annual ACM Symposium on User Interface Software and Technology*, New York, NY, USA, Oct. 2022, Art. no. 12. https://doi.org/10.1145/3526114.3558698
[28] T. Greenhalgh *et al.*, "Beyond adoption: A new framework for theorizing and evaluating nonadoption, abandonment, and challenges to the scale-up, spread, and sustainability of health and care technologies," *J. Med. Internet Res.*, vol. 19, no. 11, Nov. 2017, Art. no. e367. https://doi.org/10.2196/jmir.8775
[29] D. D. Walden, G. J. Roedler, K. J. Forsberg, R. D. Hamelin, and T. M. Shortell, *Systems engineering handbook: a guide for system life cycle processes and activities*. Wiley, 2015.
[30] K. Forsberg and H. Mooz, "The relationship of system engineering to the project cycle," *INCOSE International Symposium*, vol. 1, no. 1, pp. 57–65, Oct. 1991. https://doi.org/10.1002/j.2334-5837.1991.tb01484.x
[31] International Organization for Standardization, "Ergonomics of human-system interaction – Part 210: Human-centred design for interactive systems," Geneva, 2019. [Online]. Available: https://www.iso.org/standard/77520.html. Accessed: Apr. 08, 2026.
[32] SAP AppHaus, "Scenes: A tool to create storyboards." [Online]. Available: https://apphaus.sap.com/resource/scenes. Accessed: Apr. 08, 2026.
[33] Y. Amirkhalili and H. Y. Wong, "Banking on feedback: Text analysis of mobile banking iOS and Google app reviews," Mar. 2025. [Online]. Available: http://arxiv.org/abs/2503.11861

Doctor **Ashkan Yaldaie** is a lead software developer and researcher in software engineering. He holds a B.Sc. in Business Information Technology from Haaga-Helia University, an M.Sc. in Computer Science from Lappeenranta–Lahti University of Technology (LUT), and a Doctor of Science (Technology) from LUT. His work focuses on the intersection of software engineering research and industrial practice.
E-mail: ashkan952000@gmail.com
ORCID iD: https://orcid.org/0000-0002-8726-2825

Professor **Jari Porras** is a Doctor of Science (Technology) at Lappeenranta–Lahti University of Technology (LUT). He specialises in software engineering with a focus on distributed systems, and his research spans parallel and distributed computing, wireless and mobile systems, and sustainable ICT.
E-mail: jari.porras@lut.fi
ORCID iD: https://orcid.org/0000-0003-3669-8503