Applied Human Factors and Ergonomics (AHFE2025), Vol. 199, 2025, 1310–1320
https://doi.org/10.54941/ahfe1006942

Application of Advanced MBSE and System Automation to Improve Home Security System Solutions

Daijha Hilliard[1], Bhushan Lohar[1], Robert Cloutier[1], John T. Wade[1], and Saeed Latif[2]

[1]Department of Systems Engineering, University of South Alabama, Mobile, AL, 36688, USA,
[2]Department of Electrical and Computer Engineering, University of South Alabama, Mobile, AL, 36688, USA

ABSTRACT

This research emphasizes the usefulness of advancements in Model-Based Systems Engineering (MBSE) and system automation to enhance the system selection process for a diverse range of stakeholders. The study of this paper, while applicable to any domain, focused specifically on home security systems. As the home security market expands with increasingly complex and varied technological solutions, users often struggle to select a system that precisely meets their needs without being overwhelmed by technical specifications. This paper presents a novel methodology that addresses this challenge by combining the rigorous frameworks of advanced MBSE, requirements modeling, and the capabilities of AI-driven automation. The research details the application of this method to translate user-expressed needs and wants into clearly defined, verifiable requirements. These requirements, which serve as a blueprint of stakeholder desires, are organized into a series of models. This process, using SysML models, automatically generates a curated selection of home security systems tailored to each user. The methodology leverages a Model-Based Architectural Pattern (MBAP) approach to create a Model-Based Pattern Library (MBPL). This library serves as a storage of predefined security system models that encapsulate best practices and standard solutions for common configurations, such as intrusion detection and video surveillance. The process begins with a user assessment to identify needs and wants, followed by requirements and modeling. This information is then used to create a decomposition of the system, breaking down necessary details and components. This systematic decomposition ensures a thorough and detailed analysis of the system's needs. The findings confirm that the integration of stakeholder engagement, requirements writing, and architectural patterns provides a powerful framework for system development. This approach facilitates rapid system customization, improves design quality, and ensures alignment with industry standards. The research successfully modifies the conventional system development lifecycle, proving the utility of a model-based, automated approach in a real-world application. The results highlight a new paradigm for systems engineering, demonstrating how the synergy of MBSE and automation can lead to improved outcomes for both users and developers.

Keywords: Model based systems engineering (MBSE), Model-based architectural pattern (MBAP), System modeling language (SysML), Automation, Artificial intelligence, Requirements

INTRODUCTION

The designated System-of-Interest (SoI) for this research is the Home Security System, defined and analyzed utilizing a Model-Based Systems Engineering (MBSE) methodology. This SoI represents a system that, while comprised of simple functions, exhibits complex emergent behaviors. Its primary capability objective is to provide the user stakeholder with 'protection' against a defined set of dangers or threat scenarios. The system's architectural baseline has evolved significantly through technology insertion and advancement. This progression has enhanced system performance, notably enabling a 'lively view' capability, which delivers real-time data to the user regardless of their operational state (e.g., 'home' or 'away'). The 'importance of safety' is identified as a critical, non-functional requirement and a primary stakeholder concern. The Home Security System architecture must possess the full functional and non-functional abilities to satisfy this 'protection' desirement. To drive system improvement, various Systems Modeling Language (SysML) driven analysis processes will be executed against the model. As illustrated in Figure 1 below, this effort will specifically explore: (i) Operational Analysis (to define operational scenarios, activities, and stakeholder needs). (ii) Functional Analysis (to decompose system functions, and behaviors). (iii) Technical Analysis (to develop technical architecture of building blocks and allocation of functions).

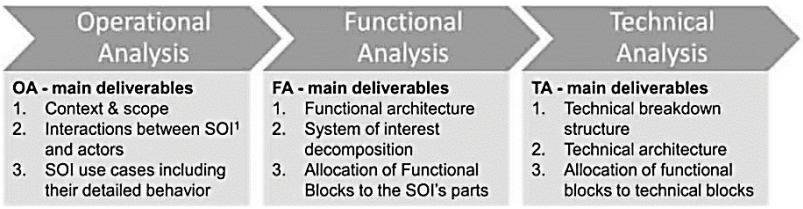

Figure 1: SysML analysis process (Baduel et al., 2018).

The home security system constitutes a representative problem domain wherein the proposed research methodology demonstrates significant utility. This particular SoI exhibits a multi-layered architecture, possessing diverse capabilities allocated to effectuating stakeholder (user) protection. The application of MBSE methodologies represents a superior instrumentation for the rigorous definition and visual articulation of requirements throughout the system acquisition lifecycle. Executing this MBSE-centric approach, synergized with automated frameworks leveraging Artificial Intelligence (AI), Machine Learning (ML), and Deep Learning (DL) algorithms, facilitates the generation of system models and reusable architectural patterns (Lohar, 2022). This consequently accelerates program schedules, generates a trade-space of viable solution alternatives for stakeholder decision analysis, and enhances the fidelity and correctness of the resultant system design. The fundamental paradigms inherent to Systems Engineering (SE) have primarily re-architected the solution space achievable by engineering disciplines. SE is

purposefully structured to prioritize the derivation and validation of design-driving requirements whilst concurrently establishing a holistic solution environment. This environment is engineered to encapsulate the complete system lifecycle (Shoshany-Tavory et al., 2023).

Within the SE discipline, MBSE is utilized to articulate the requirements specification of a SoI through diverse, formalized views. The elicitation and formalization of requirements, which codify the stakeholder needs and constraints, and the subsequent modeling activities, which transcribe these textual requirements into interconnected diagrams and analytical models. That are instrumental in achieving stakeholder validation and acceptance. Architectural patterns represent a critical component for instantiating an optimized framework during the system development lifecycle. These patterns abstractly define the system's allocated capabilities and functional behaviors (Lohar and Cloutier, 2022). A heterogeneous stakeholder population is categorized into distinct tiers of influence. Each tier exerts unique vectors upon the system's developmental trajectory. This taxonomy includes high-influence, moderate-influence, and low-influence stakeholder classes. High-influence, internal stakeholders (e.g., sponsors, organizational leadership, customers/acquirers) provide the strategic, high-impact vision defining the operational needs and capability gaps. Moderate-influence, external stakeholders (e.g., engineers, developers, suppliers, contractors) are coupled to the programmatic success of the development via tactical daily impacts, but they possess differentiated (i.e., reduced) authority regarding baseline change control. Low-influence stakeholders are typically regulatory or governance entities (e.g., legal counsel, compliance components) recognized as passive, lacking direct intervention in development activities, but utilized to ensure exogenous constraints and non-functional requirements are satisfied (Santos et al., 2025).

Stakeholder engagement yields high-order results and emergent outcomes beneficial to the holistic system. The prioritization of stakeholder involvement correlates positively with an increased probability of successful outcomes, manifested via effective decision-making, higher fidelity in risk and error determination, process optimization, and elevated customer satisfaction. Specific engagement strategies are enhanced through stakeholder integration, such as refined communication protocols for status reporting and system baseline updates. This cultivates an enhanced collaborative environment by accelerating trust establishment and conflict resolution during the system development lifecycle, proving beneficial to all entities vested in the system's realization (Santos et al., 2025). This concept is critical to all facets of the process required for system selection. There are discrete benefits to leveraging MBSE modeling artifacts, including: greater system efficiency derived from the integration of heritage project data, a robust impact on requirements analysis fidelity, and elevated communication bandwidth between stakeholders and engineers. The capacity to manage (or partition) complexity and the formalized instantiation of Verification and Validation (V&V) protocols, which facilitates risk mitigation during early lifecycle phases are also high-impact applications of MBSE models (Donatas

& Butleris, 2020). Systems engineering is a practical discipline for iterating capability improvements in any system domain.

Materials and Methods

The Home Security System-of-Interest is an engineered solution utilized to provide a protection capability to users within a defined residential boundary (Hilliard et al., 2025). As the technology baseline has advanced, the allocated capabilities of the system have evolved. Current solutions include functionalities such as remote system state control, automated configuration management (updates), and sensor-actuated alerts dispatched to the user interface. The primary mission requirement for the SoI is the mitigation of threats posed by criminal actors. The specific threat vectors relevant to this operational context are home invasions and burglaries. A burglary is a precise threat classification wherein an entity breaches a structure's perimeter with the intent to execute a secondary illicit action or theft. The "breaking and entering" nomenclature is often applied, although forcible ingress is not a required antecedent. This vulnerability is applicable to diverse structural types, including aircraft or commercial facilities. A home invasion is a differentiated threat scenario characterized by unauthorized ingress into an occupied structure, with the explicit intent to execute a threat action (e.g., intimidation, injury) against the occupants (Hunt, 2024). Multiple classifications of burglary threats exist. Each classification level is defined by variables such as the magnitude of asset loss (items stolen) and the extent of physical damage to the operational environment. The threat typology is enumerated as follows (McDuffey & Rivera, 2023):

I. First-degree burglary: This classification represents the highest severity scenario, entailing the presence of a lethal weapon and the intent to execute a robbery or violent attack against the stakeholder.
II. Second-degree burglary: This classification is analogous to the first-degree threat but is differentiated by the target boundary, specifying a non-residential facility (e.g., a shed or shop).
III. Third-degree burglary: This classification encompasses scenarios decoupled from violent intent, often assigned when unauthorized ingress occurs but the threat actor's objective is non-deterministic.
IV. Fourth-degree burglary: This classification typically involves the removal of assets from external, secured perimeters (e.g., fenced-in yards) associated with residential or business structures.

The SoI is composed of various subsystem components necessary to achieve correct functional operations. The surveillance capability is a critical, high-priority function. Closed-Circuit Television (CCTV) is an instrumentation utilized within the monitoring subsystem of the SoI. Legacy CCTV implementations are heavily utilized but exhibit specific constraints: 1) they require continuous Human-In-The-Loop (HITL) review of recorded video data for anomaly detection; 2) they impose high-volume data storage requirements, regardless of threat presence; and 3) they lack real-time stakeholder notification upon event detection. Consequently, an

intelligent surveillance subsystem architecture is proposed to remediate these deficiencies by automating intruder identification and data capture. Upon detection of motion signatures, the user stakeholder receives immediate notification (Bachayo et al., 2022). As technology has progressed, legacy CCTV implementations are being superseded by modern implementation models integrating advanced sensors, imaging components, and automated access control systems (Singh, 2022).

Figure 2: Home security system layout (Psiborg, 2021).

MBSE represents a formalized methodology utilized to enhance semantic precision and inter-disciplinary collaboration throughout the system acquisition lifecycle via generation of formalized requirements specifications and architectural artifacts (Shoshany-Tavory et al., 2023). The formalized requirements artifacts establish bidirectional traceability to the model elements, which serve to Verify and Validate (V&V) the elicited stakeholder needs (Menshenin et al., 2023). Figure 3 below illustrates the SIMILAR process model codifies the requisite procedural steps necessary to ensure rigorous execution of the system development lifecycle.

Within the modeling phase, the SysML functions as an instrumental enabling tool for achieving specified engineering objectives. The core paradigm for integrating SysML and model-based testing is predicated on the application of the SysML artifact and formal model-checking algorithms to execute continuous, high-fidelity safety analysis. This hybridized methodology seeks to leverage the standardized syntax and semantic usability of SysML in synergy with the automated analysis and formal verification capabilities inherent in model validation techniques (Wang et al., 2019). Regarding automation, advanced functional capabilities, such as High-Definition (HD) video data streaming and Artificial Intelligence (AI) and Machine Learning (ML) algorithms, are also instantiated within 5G/6G communication architectures. HD imaging sensors integrated into

the residential security SoI can transmit real-time telemetry to distributed User Interface (UI) devices, leveraging the high-throughput, low-latency capabilities of 5G protocols to achieve higher-fidelity and reduced-latency monitoring. The 5G infrastructure provides the requisite data-handling capacity for computationally intensive AI algorithms (e.g., facial recognition, object detection, anomaly detection), thereby enhancing the precision and overall effectiveness of the SoI (Dangi et al., 2019). Figure 4 below depicts the SE integration framework required for the transition and federation of the MBSE toolchain.

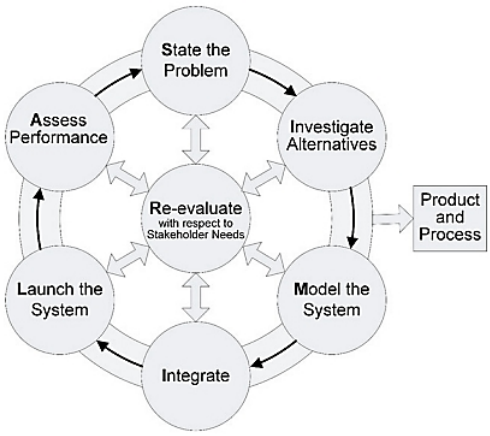

Figure 3: SIMILAR process used in systems design and development (Madni et al., 2023).

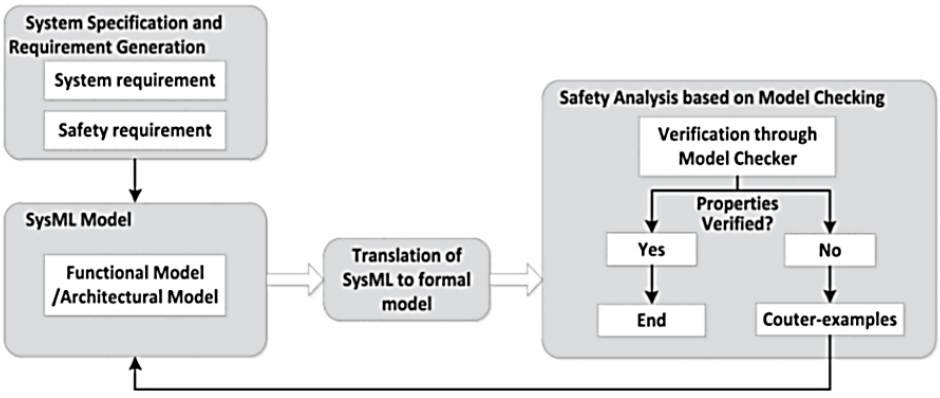

Figure 4: SysML model integration process (Wang et al., 2019).

The implementation of AI algorithms, instantiated within imaging sensors (cameras) and cloud-centric service architectures, is operationally effective in mitigating false positive (Type I error) rates. AI-enabled edge-processing within the imaging sensor subsystem facilitates real-time analysis of video telemetry, executing threat classification and flagging anomalies while

actively filtering spurious detections (e.g., non-threat signatures generated by insects or flora). Cloud-based AI service platforms deliver elastic, scalable computational solutions, enabling the ingestion and processing of high-volume data streams from geographically distributed sensor networks, thereby enhancing aggregate detection probability (*Pd*) and system accuracy (Lins et al., 2021).

Methodology

The proposed methodological framework for the optimization of the system selection process is instantiated via a 4-phase heuristic, enumerated as follows: Analyze, Categorize, Calculate, Determine

Analyze: This initial phase mandates stakeholder engagement. The identification of the complete stakeholder community and the rigorous elicitation of their inputs regarding system needs (i.e., capability gaps) are critical activities. All stakeholder inputs and engagement metrics shall be formally assessed and captured within the project repository during this phase. The definition of stakeholder wants and needs Concept of Operations and Operation Concepts (CONOPS/OPSCON) is a fundamental prerequisite for constraining the solution trade-space. Figure 5 below models (SysML *Use Case Diagram*) the active stakeholder ecosystem associated with the home security SoI. These stakeholders are integral to the governance and configuration management processes, ensuring their participation in all system change and update activities.

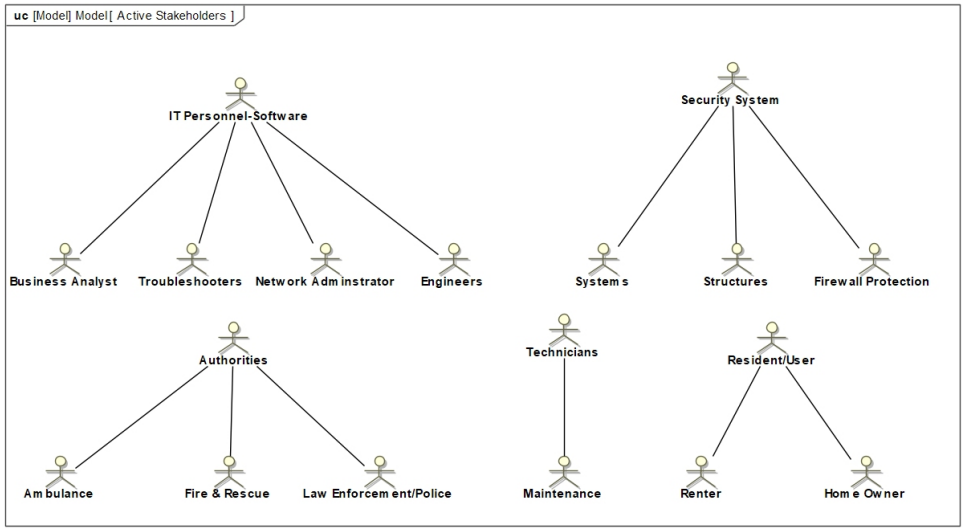

Figure 5: Home security system active stakeholder diagram.

Categorize: This phase executes the transformation of elicited stakeholder needs into a set of formalized, verifiable requirements. These requirement artifacts are instrumental in the V&V strategy, ensuring the resultant system is unambiguously and correctly architected to user specifications. Requirements shall be explicitly defined based on traceable stakeholder

inputs. The necessity for clear, atomic, and detailed requirements is paramount. These requirements are subsequently utilized to categorize functional commonalities and related needs, thereby organizing the architecture in preparation for the subsequent phase. Systems thinking paradigms are highly applicable during this analytical and decompositional activity.

Table 1: Sample requirements for the data transfer system.

ID	Name	Text
8	Data Alert Transfer	The data transfer system shall transmit alerts to users when intrusions of any kind occur.
8.1	Audible Alert	The audio alert assembly shall support an alarm with audible sensors once disrupted.
8.1.1	Audio Customization Options	The audio alert assembly shall support customization options for audible alerts.
8.1.1.1	Volume Audio Adjustments	The audio alert assembly shall provide alterable volume settings.

Calculate: This phase ingests the formalized requirements from the 'Categorize' phase, utilizing them as inputs for automation tooling. Automated frameworks, AL/ML algorithms, are employed to computationally generate an architectural pattern library and corresponding requirements diagrams (e.g., SysML *requirement diagrams*).

Figures 6 & 7 below illustrate the auto-generated architectural patterns and requirements diagrams for the first-level (*L1*) decomposition of the Data Transfer Subsystem, maintaining traceability to Requirement ID # 8 (per Table 1).

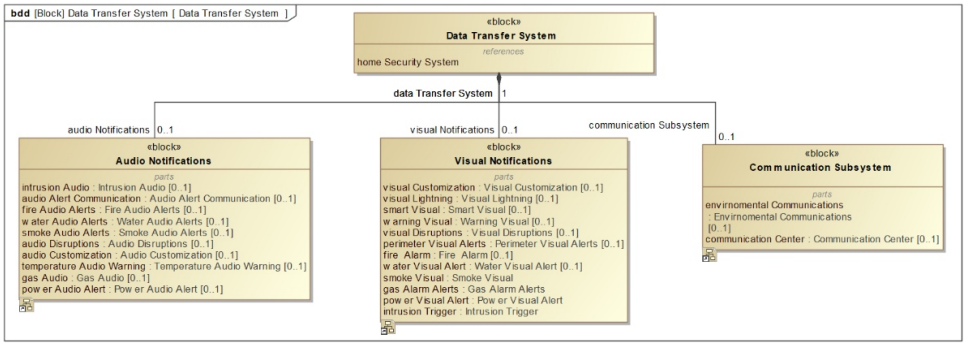

Figure 6: Data transfer system architectural pattern (*L1*).

The generation of architectural pattern artifacts and requirements diagrams will be executed for the target SoI. The formalized requirements artifacts serve as the verification baseline against which the diagrammatic models are validated. The workflow process exemplified in Figures 6 & 7 will be recursively applied to each subsystem and associated Configuration

Item (CI) within the SoI's Work Breakdown Structure (WBS) and System Breakdown Structure (SBS). These generated views will be captured and managed, ensuring persistent correspondence to system requirements and stakeholder needs.

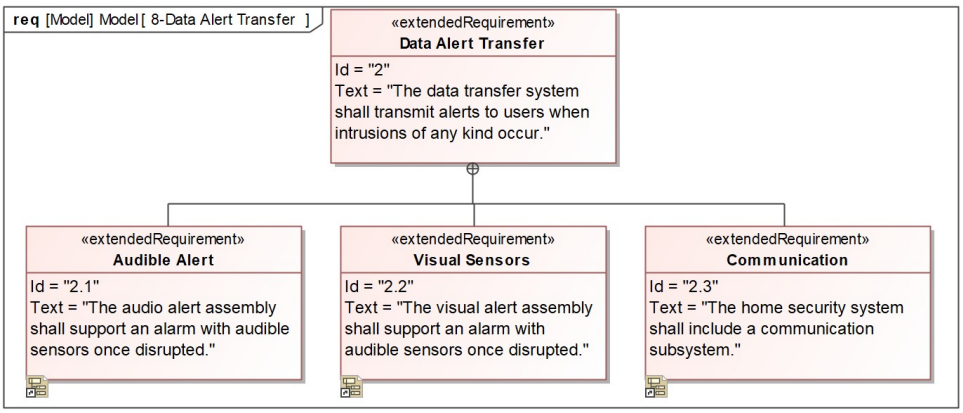

Figure 7: Data transfer system requirements diagram (*L1*).

Determine: This terminal phase involves the synthesis of all outputs from the preceding phases (1-3) to conduct a formal trade-space analysis and determine the most viable SoI solution. The generated portfolio of detailed system architectures (derived from the pattern library) is utilized to identify and present a curated set of solution options to the stakeholders, enabling a tailored system selection specific to each user profile. This methodology is efficacious in engineering a stakeholder-specific system baseline. This proposed research framework is posited to accelerate the system development lifecycle, increase engineering productivity (i.e., reduce man-hours), and ultimately enhance stakeholder satisfaction. The aforementioned phases are structured to remediate known deficiencies and gaps within extant system development and selection processes.

DISCUSSION

The objective of this research is to examine the efficacy and utility of MBSE advancements; specifically, its formalisms (e.g., SysML), toolchains, and methodologies, as applied to the home security systems. The benefits derived from the capabilities inherent in an MBSE approach are instrumental in mitigating diverse threat vectors against the stakeholder. This will enumerate the technological progressions of MBSE when integrated with the SoI, the operational utility of automated frameworks, and a description of how two specific technology enhancements can elevate operational effectiveness across any given problem domain. A *L1* decomposition of the SoI's physical architecture has identified eleven (11) constituent subsystems, such as the efficiency subsystem, connectivity subsystem, perimeter subsystem, surveillance subsystem, sensor subsystem, detection subsystem, fire alarm subsystem, data transfer subsystem, power subsystem,

automation subsystem, and the home security management subsystem. These 11 subsystems are prerequisite CIs for achieving the SoI's nominal operational state.

The requirements, as elicited from the stakeholder community, will be captured, and formally allocated to the system's functional baseline. In response, the proposed research methodology will computationally generate a system baseline tailored specifically to the validated stakeholder needs, introducing a novel paradigm for system selection and ensuring high-fidelity adherence to unique user profiles (Hilliard et al., 2025). This methodological framework is domain-agnostic. This research will optimize the systematic selection process for the SoI by leveraging the core tenets of MBSE. This proposal will specify advancements for discrete functionalities that are critical to the SoI's performance baseline. This modification to the systems engineering process will enhance the SoI's components and yield aggregate improvements in system robustness, program schedule acceleration, and milestone adherence throughout the development lifecycle.

CONCLUSION

In conclusion, the home security SoI serves as a representative exemplar domain for the proposed research methodology. The architectural complexity, emergent from the high interconnectivity of numerous CIs (e.g., Human-Machine Interface/control panel, perimeter sensors, environmental detectors [smoke, CO], motion sensors, imaging sensors), necessitates a formalized approach to ensure all performance requirements and latency constraints are met. The application of MBSE and automation can remediate identified fault-trees and significantly reduce the system's error budget. The utility of MBSE is significant. The system's non-functional requirements (e.g., scalability, flexibility) are demonstrably enhanced when MBSE is integrated into the core systems engineering workflow. SysML, as the standard-based formalism, is employed to graphically articulate the system specification. Concurrently, textual requirements artifacts are federated with the model, serving to organize the capability-based architecture and define the technical baseline required for system stability and iterative (spiral) capability enhancement (McGrath & Jonker, 2025). The SoI is a highly complex system that delivers a persistent protection capability to stakeholders. The demonstrated utility of reusable architectural patterns, formalized requirements diagrams (e.g., SysML *requirements*), and automation in expanding the viable solution trade-space for stakeholder analysis validates the novel contribution and future potential of this research.

REFERENCES

Bachayo, A., Ahmed, Z., & Affrah, S. (2022). A Model Design for Smart Home Security System Using (IOT) with CCTCAMERA. International Journal of Computing and Related Technologies, 3(2), 29–42.

Baduel, R., Chami, M., Bruel, J. M., & Ober, I. (2018). SysML models verification and validation in an industrial context: Challenges and experimentation. In Modelling Foundations and Applications: 14th European Conference, ECMFA 2018, Held as Part of STAF 2018, Toulouse, France, June 26–28, 2018, Proceedings 14 (pp. 132–146). Springer International Publishing.

Dangi, R., Lalwani, P., Choudhary, G., You, I., & Pau, G. (2021). Study and investigation on 5G technology: A systematic review. Sensors, 22(1), 26.

Donatas, M., & Butleris, R. (2020). Integrating security requirements engineering into MBSE: Profile and guidelines. Security and Communication Networks.

Hilliard, D., Lohar, B., Lippert, K., Wade, J. T., & Latif, S. (2025). Model-Based Architectural Patterns Concept for Home Security System Solutions. Human Factors in Software and Systems Engineering, 181, 13. http://doi.org/10.54941/ahfe1006390.

Hilliard, D., Lohar, B., Lippert, K., Wade, J. T., & Latif, S. (2025). Model-Based Architectural Patterns (MBAP) for Complex System Solutions. https://doi.org/10.13140/RG.2.2.20167.82082.

Hunt, M. (2024, January 12). Burglary statistics 2024: Bankrate. Bankrate Press. https://www.bankrate.com/insurance/homeowners-insurance/house-burglary-statistics/.

Lins, S., Pandl, K. D., Teigeler, H., Thiebes, S., Bayer, C., & Sunyaev, A. (2021). Artificial intelligence as a service: Classification and research directions. Business & Information Systems Engineering, 63, 441–456.

Lohar, B., (2022). Development of New Space Systems Architecture in SYSML Using Model-Based Pattern Language. https://jagworks.southalabama.edu/theses_diss/75.

Lohar, B., & Cloutier, R. J. (2022). Towards a model-based pattern language for new space-based systems. https://doi.org/10.20944/preprints202208.0177.v1.

Madni, A. M., Augustine, N., & Sievers, M. (Eds.). (2023). Handbook of model-based systems engineering. Springer Nature.

McDuffey, T., and Rivera, J., (2023). Different Degrees of Burglary. Last Updated: Aug 9, 2023. Last accessed on Oct 30, 2025. https://www.legalmatch.com/law-library/article/different-degrees-of-burglary.html.

McGrath, A., & Jonker, A. (2025, July 22). What is model-based systems engineering (MBSE). IBM. https://www.ibm.com/think/topics/model-based-systems-engineering.

Menshenin, Y., Mordecai, Y., Crawley, E. F., & Cameron, B. G. (2023). Model-based system architecting and decision-making. In Handbook of Model-Based Systems Engineering (pp. 289–330). Cham: Springer International Publishing.

Psiborg.in (2021). Vidushi Gupta (CEO). Home Automation, IoT Based Monitoring, IoT Based Security Systems, IoT Sensors. Published on May 18, 2021.

Santos, A., David, B., Okunola, A., & Kurus, T. (2025). The Influence of Stakeholder Engagement on Lean Six Sigma Success in Engineering Projects.

Shoshany-Tavory, S., Peleg, E., Zonnenshain, A., & Yudilevitch, G. (2023). Model-based-systems-engineering for conceptual design: An integrative approach. Systems Engineering, 26(6), 783–799.

Singh, S. (2022, December 23). Benefits of security systems for home. HomeMate. https://homemate.co.in/blog/benefits-of-security-systems-for-home/?srsltid=AfmBOooNGGkJO_gplTTrVPIuhJOroMEIuwZhRm-B_ZMmJafAqqIzFpYf.

Wang, H., Zhong, D., Zhao, T., & Ren, F. (2019). Integrating model checking with SysML in complex system safety analysis. IEEE Access, 7, 16561–16571.