氏　　名	YANG, Zhengguo		
学位の種類	博士(情報科学)		
学位記番号	博情第 431 号		
学位授与年月日	令和 2 年 3 月 25 日		
論文題目	Architecture and Platform for Safe Cyber-Physical Home System		
論文審査委員	主査　丹　康雄	北陸先端科学技術大学院大学	教授
	篠田　陽一	同	教授
	リム　勇仁	同	准教授
	青木　利晃	同	准教授
	米田　友洋	国立情報学研究所	教授

論文の内容の要旨

Globe warming and weather anomalies, e.g., heatwaves, occur on this planet quite often in recent years, which affects the lives. These result in morbidities and mortalities. The indoor environment is, of course, affected in the viewpoint of safety. Moreover, people stay indoors for a large portion of their time. Therefore, safety problems related to abnormal indoor climate change have great affection for the indoor lives of occupants.

Conventionally, people take advantage of home appliances to adjust the indoor environment. With the development of home automation, networking, the introduction of the so-called artificial intelligence, and the smart grid, etc., the cyber world of smart homes becomes more and more complex. So, the indoor environment is adjusted by the cyber world may fail either due to its inability or malfunction. This cannot guarantee indoor environmental safety under the circumstance of weather anomalies. Thus, it is necessary to observe the indoor environment to detect or predict undesired safety events, based on which to design or select effective reactions to ensure the home environment safe.

The aim of this research focuses on home safety problem detection and prediction. Home safety problems in this work refer to indoor climate anomalies that will cause health problems to occupants. Thus, supportive architecture and platforms are necessary. To this end, a home safety architecture is proposed for supporting the observation of the indoor environment to detect and predict indoor climate anomalies. The architecture is based on Cyber-Physical Systems (CPS) and the Service Intermediary Model. For understanding the causality of home safety problem formation and identifying the causes of the indoor climate anomalies in the cyber world, I proposed an accident model and a hazard analysis technique, i.e., tailored STPA (System-Theoretic Process Analysis).

The proposed accident model is based on the STAMP (Systems-Theoretic Accident Model and Process) model. The accident model illustrates to connect the behaviors of smart home systems and the physical world to describe accident formation. To this end, I first proposed the concept of the Performers System, based on which to define terms like Behavior. Then I define terms and their relations to describe accident formation concerning the Performers System. I adopt indoor temperature data and empirical experience for demonstrating the validity of the proposed accident model.

For the tailored STPA, it mainly aims to also identify ICAs (Inappropriate Control Actions) of controllers. ICAs and UCAs (Unsafe Control Actions) are the causes of the occurrence of safety problems. I also proposed a procedure to identify system-level hazards and an LGLD (Landscape Genealogical Layout Documentation) approach for documenting the analytical results. The LGLD approach can clearly and straightforwardly represent the relations of the results. Some examples are used to demonstrate the practical usefulness of our proposals. I also practiced applying an innominate approach for hazard identification and analysis, which is based on the goal-based requirement engineering, guide words, and item sketch.

Based on the above-discussed proposals, I proposed ways of safety problem detection and prediction. I proposed a multiple-conformance approach to check the indoor temperature for detecting thermal problems. Conformance testing is a formal approach to check the validity of an implemented system against its specification. It is applied to check whether the indoor temperature conforms to the requirements of no thermal problems. I model required changes in indoor temperature by hybrid automata. The practical usefulness and performance of the proposed multiple-conformance approach that takes the hybrid-automata-modeled requirement as the specification are demonstrated through experiments.

For the safety problem prediction, I take heat shock during the bath as an example. I adopt Bayesian networks for the prediction. The structure of the Bayesian network is built by the proposed procedure concerning surveyed knowledge of heat shock. The conditional probabilities are elicited by a proposed procedure that takes advantage of the probability scale method with the proposed concept of degree of influence. The results show that it is feasible to adopt Bayesian networks to predict heat shock based on partially observed evidence.

Keywords: Home Safety; Smart Home Environment; Accident Model; Hazard Analysis; Indoor Climate Anomaly Detection; Heat Shock Prediction.

論文審査の結果の要旨

ICT 技術を活用し、一般家庭における日々の暮らしを支援することで、高齢化問題やエネルギー問題などの解決に資するスマートホームシステムの開発が近年急速に進んでいる。しかしながら、従来は単なるモノに過ぎなかった住宅が、家電のみならず、一つ一つの建材レベルでインテリジェント化し、能動的に動作するようになることで、今までは起こり得なかった安全上の問題が頻発する可能性が出てきている。本研究は、ほぼ手つかずであったこの課題に対して、従来の安全工学上の手法や検証手法ではスマートホームに対して必ずしも有効な成果をあげられるわけではないことを示し、スマートホームに適した概念整理から具体的な例をとりあげての危機検出手法の提案などを行ったもので、当該分野を新たに切り開いた論文と位置づけられる。

スマートホーム環境での安全性を担保するためには、明確に規定された仕様を満たすか否かという観点での議論は有効ではなく、物理空間上に存在している人間にとって危険な状況を何らかの形で定義し、様々なサービスによる機器の動作の結果において、人間にとって危険な状況に至らないようにすべく機器の動作に制約をかけることが必要となる。本研究では、「幅」をもった規定内に収まるか否かといった概念を取り入れるとともに、STAMP（System Theoretic Accident Model and Processes）の拡張を行い、スマートホームにおける安全という概念の定式化、ハザード分析、安全担保のためのシステム・アーキテクチャ、温熱環境を対象とした危険検出と、危険発生予測について議論が展開されている。家庭における温熱環境の異常は、熱中症およびヒートショックという形で我が国でも毎年数万人の生命を奪っている社会的な課題であり、これを具体例としてとりあげた評価や議論は単に概念的な提案という枠を超え、実用化に近い側面も有するものとなっている。

本研究の成果は、コンスーマーエレクトロニクス分野の IEEE 国際会議、信頼性分野の IEEE 国際会議において採択されるとともに、概念的な体系の提案という内容ながら、Impact Factor 2.2 の国際ジャーナルにも採録されており、専門家から一定の評価を受けたものといえる。また、本研究の遂行中に IEC においてスマートホームの機能安全に関する国際標準化活動が開始されたが、本論文もその動向を踏まえた形でまとめられている。

以上のように本論文は新たな領域における概念整理と概念提案といった基礎的な貢献から、具体的な例を用いた研究成果の活用方法までを示したものであり、学術的にも、また、産業界への貢献の面でも有効なものであり、博士(情報科学)の学位論文として十分に価値のあるものと認めるものである。