# 論 文 内 容 の 要 旨

博士論文題目　Characterizing, Deriving and Validating Safety Properties of Integrated Services in Home Network System

氏　名　閻 奔

近年，家電機器やセンサから構成される Home Network System（HNS）の開発が行われている．HNS の利点は，複数の家電をネットワーク経由で連携制御することで，高付加価値サービスを提供できることである．ただし，HNS 連携サービスの開発・提供にあたっては，そのサービスがユーザや家財に対して安全であることを保証しなくてはならない．

本論文は，HNS の連携サービスの安全性を定義，抽出，検証するための枠組みを提案した．まず，HNS の連携サービスの安全性を定式化する方法を提案した．提案方法では，(1)個々の家電に要求される local safety，(2)複数の家電の連携時に要求される global safety，(3)連携サービスを取り巻く環境に対して満たすべき environment safety，という 3 つ観点から安全性を定義した．

次に，要求工学のアプローチを用いて，検証可能な安全性性質（safety property）を系統的に抽出する方法を提案した．具体的には，4 つのレベルから成るハザード解析モデル(HNS-HAM)を提案した．与えられた HNS モデルについて HNS-HAM を構築し，可能性のあるハザードを分析することで，safety property 集合とそれらに付随する操作が抽出できる．さらに， HNS-HAM の再利用性を高めるために，一般的なハザード・コンテキストで利用可能なハザードテンプレートの記法を提案した．

また，契約による設計（Design by Contract，DbC）を用いて安全性検証を行う方法を提案した．提案方法では，各オブジェクトが満たすべき性質を DbC における契約の集合と捉え，プログラムテスト時に動的に検証する．プログラム実行時に投げられる例外として契約違反を検出することで，安全性が検証できる．

これらの 3 つの提案により，HNS の開発者は，安全な HNS サービスを設計・実装することが可能となる．

| 氏　名 | 閻 奔 |
|---|---|

（論文審査結果の要旨）

一般家庭における生活の利便性や快適性を向上させるために，家庭内の多数の家電機器を連携させ，高付加価値なHNS連携サービスを開発・提供していくことは，近い将来における重要な課題である．そのサービスの開発においては，家庭内のユーザに対して安全性を保証することが必須であるが，家電機器は多種多様であり，かつ，家庭ごとに固定されていないために，保証すべき安全性をどのように定義するかが課題であった．また，家電の連携時の動作は複雑であり，周囲の環境に与える影響も複雑なため，安全性を系統的に保証することも従来困難であった．

このような問題に対し，本論文では，HNS連携サービスの安全性を，個々の家電に要求される性質，連携する複数の家電に要求される性質，連携サービスを取り巻く環境に対して満たすべき性質，という3つ性質に分けてそれぞれを定式化する方法が提案されている．これにより，多種多様な要因が絡み合うHNS連携サービスの安全性を，見通しよく定式化することが可能となっている．この成果は，当該分野の基盤となる技術であり，高い学術的価値が認められる．

次に，本論文では，与えられた家電機器，連携サービス，環境から，定式化すべき安全性性質を抽出する方法が提案されている．提案方法では，安全性が破られる状況を，そのコンテキスト，状態，オブジェクトの属性，オブジェクトのメソッドという4つのレベルでモデル化し，その結果に基づいて検証可能な安全性性質を導出することが可能となっている．さらに，導出結果を再利用可能とするためのモデルのテンプレートが提案されている．この成果は，新規性，有用性ともに高い価値が認められる．

さらに，本論文では，HNS連携サービスを構成する各オブジェクトが満たすべき性質をDbCにおける契約の集合と捉え，プログラムテスト時に投げられる例外を検出することで契約違反を動的に検証する方法が提案されている．テスト時に検証を行うことで，各家電の動作についての厳密なモデル化を行うことなく連携サービスの安全性の検証が可能となり，高い実用性が認められる．

以上の3つの成果により，従来形式的に整理し検証することが困難であったHNS連携サービスの安全性を，各家庭の環境に応じて系統的に定式化・検証することが可能となった．これらの研究成果は，一般家庭における生活の利便性・快適性の向上に貢献し，また，当該領域の学術研究の発展に大きく貢献するものであり，論文は博士（工学）論文として価値あるものと認める．