スマート住宅の居住者様相を考慮に含めた安全標準策定

関山　守
共創場デザイン研究チーム

研究の目的

超高齢社会・リモートワーク・テレエデュケーション・居住者のQOL向上といった様々な社会課題への対応による新たな価値を生み出すスマート住宅の実現のために、スマート住宅に導入される安全なシステムの開発と実装について居住者の様相を考慮に含めた方法論を住宅関連業界と連携して開発、方法論を安全に関する国際規格として標準化を実施

課題

スマート住宅におけるサービスの実装：

現状：
単発的なサービスが居住者やサービス提供者によって導入/実装
・スマート家電+スマートスピーカー/スマートフォンによる運転操作
・人感センサ・機器運用情報に基づく居住者見守り
->包括的な安全対策はまだ不要？

将来：
複数のサービスが家電・住宅設備機器・センサ・IT機器を使用
複数のサービスが「測定・判断・運転」を自動的に処理
・空調管理システムとガス漏れ検知システムが自動窓開閉システムを共同利用
・居住者の登録済スケジュールに合わせた照明・住宅管理機器の連携動作
・屋内外人感センサによる居住者見守りサービスと防犯サービスの両立
・複数の居住者特性に合わせたテレワーク環境の動的な変更
・これらのサービスが同時かつ個別に住宅設備機器類の運転を行う
-> 単一居住者であっても複数のサービスが併存する可能性
-> 複数の居住者が同時に別個のサービスを機能させる可能性
　-> 複数サービスが行う運転が特定の居住者に対して危害の原因となる可能性
　-> 包括的な「安全」を確保するための対策が必要

スマート住宅において、各種サービスを実現する複数の機器連携システムが併存しつつ居住者に対して安全であるように連携システムを開発・実装するための統一的な方法論が必要である

-> 安全に関する国際規格として標準化

スマート住宅の機能安全とSOTIF

各種機器が連携動作を行う場合の「連携部分」に関する安全担保：
・個々の機器類は安全設計が為されている前提
・連携が原因となって生じる不安全（機能不全）を対象範囲
・連携機能のうちで、ユーザーに危害を及ぼす部分（安全関連系）に対する規定
　-> 使用するユーザーによって安全関連系が変化する
・故障による機能不全：機能安全による対処
・ミスユース（ユースエラー）/経年劣化や環境変化に伴う機能不全：SOTIFによる対処

安全分析においてユーザーの影響を考慮するように要請：
・対象ユーザーの明確化：ADL/IADLといった指標による明示
・「危害からの回避しやすさ」を安全分析の指標に追加

安全分析と対処に関する文書化と保持：
・住宅躯体、システム、各種機器の耐用期間差への対処
・住宅躯体変化およびシステム改変（サービス追加・除去）への継続的対処への要請
・定期的なシステムに対する安全分析への要請
・社会的な安全受容変化への追従

ミスユース（ユースエラー）への対処：
・ユーザーインターフェース等へのユーザビリティの考慮

ユースケース、安全分析事例の統合的な蓄積の推奨：

スマート住宅の将来像

住宅に新たに加わった機器がもたらす危害：

Googleサービスでの認証失敗によるスマートスピーカーの動作不具合
（2020年12月14日）

12月14日　午後8時46分（日本時間）、ログイン認証サービス「OAuth」を採用するGoogleの一連のサービスが使用停止：使用できない状況に突入

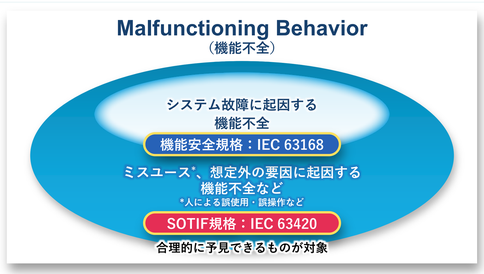
午後9時8分には、エラーの原因と修正方法が特定される
午後9時50分ころに、サービスが実際に復旧

原因：ユーザー情報の記憶域を移動させるメンテナンス作業でのエラー

影響範囲：Gmail, YouTube, Googleカレンダー, Google ドライブ, Googleクラウドサービス, etc

1時間ほどの間、Googleスマートスピーカーが動作しない状態：夜間での家電操作が不可能になる

Amazonでも11月25日夜に、AWSに接続するデータ分析サービスやクラウド型CDNサービスなどで不具合が発生
スマートリモコン、家電操作用IoTデバイスが数時間動作不能になる



IEC 63168（機能安全規格）：
・製品としての電気/電子システムの安全ライフサイクルを規定
・システムの故障に起因する機能不全への対処が目的
・危害発生モデルに合わせたハザード分析とリスクアセスメントの実施
・安全度水準（H-SIL）におけるA（危害回避の指標）を導入：AAL側面からの安全対応
・安全活動の実行プロセスと、プロセス実行のエビデンス保持
・エビデンスベースでの検証（Verification）と安全妥当性確認（Validation）の実施

IEC 63420（SOTIF規格）：新しい安全のフレームワーク
・IEC 63168（機能安全規格）が規定する構造に合わせる形で、SOTIF安全活動の部分を補完
・ミスユース、想定外の要因に起因する機能不全（システムは正常動作）への対処が目的
・人間のミスユース検討：ガイドワードによる網羅的分析
・設計時想定外要因への対処：運用段階における対策方針検討の要求

検討のための取組み

安全確保のための実現可能な方法論の検討：

産総研と建材・住宅設備機器の業界団体が核となって検討を実施
「機能安全」+「SOTIF(Safety of the intended functionality)」
　-> 検討内容を国際標準規格案として取りまとめてIECに提案

参画いただいている業界：
建材・住宅設備機器業界
家庭用電気製品業界
住宅業界
ホームセキュリティ業界
安全コンサルタント業界
認証団体
-> 業界団体および業界団体経由で個別に興味を有する企業が参加

今後の参画を検討中の業界：
システムインテグレーター・IT
金融（保険・銀行）
ヘルスケア・高齢者支援・介護予防

関連分野：
安全工学（機能安全・信頼性工学）
人間工学（ユーザービリティ・ユースエラー）
スマート住宅（ホームネットワーク基盤）
IoT社会（つながる社会）でのシステム開発
製品事故事例調査
->　研究機関・大学等の有識者を招聘

国際標準化の現況

IECのAALシステム委員会へ提案中：

機能安全規格：IEC 63168
　-> 2022年度に発行予定
SOTIF規格：IEC 63420
　-> 国内議論によるドラフト開発中

議論への主要参加国：
日本・韓国・中国・ドイツ・フランス・アメリカ
連携しているIEC技術委員会：
TC 59/61、SC65A、TC100、TC34、TC23など

国際規格提案に際して、関係するユースケース（15例）を提案
・複数機器連携由来での不安全事例
　・故障原因
　・ユースエラー原因
　・環境変化
-> IEC TS 63134に収録

住宅設備機器類の連携に関する安全担保の仕組みの開発：
国際標準として提案

「機器連携部分に関する機能安全」
「機器連携部分に関するSOTIF」として文書化
- 安全担保のための手続きを規定
- 高齢者/幼年者等がユーザーに含まれる：対処を明記
- 機器連携開発者に対する組織的安全への取組みを要請

産総研　（一社）日本建材・住宅設備産業協会
JEITA　JEMA　ALIA　プレハブ建築協会
NITE　NEDO　大学等　安全コンサル

住宅設備機器の連携に関する安全担保の仕組みの
普及基盤構築：

国内外での認証基盤・認証の仕組みの構築
国内基準の検討
普及のためのガイドライン・手引書の作成
接続可能機器類のリスト化等の普及基盤構築のための議論
実施

スマート住宅の連携機能を対象とする安全規格開発

	IEC 63168（機能安全規格）	IEC 63420（SOTIF規格）
経産省事業の名称	IoT社会実現に向けた 住宅設備連携における機能安全に関する 国際標準化	IoT住宅普及にむけた 住宅設備機器連携の機能安全に関する 国際標準化および普及基盤構築
実施期間	2016年度～2018年度	2019年度～2021年度
対象とする領域	IoT住宅（スマートホーム）に設置される、協調動作する複数の機器連携システム Cooperative multiple systems in connected home environment	
	システム故障に起因する機能不全	ミスユース、想定外の要因に起因する機能不全
事業内容	安全規格文書の開発と国際標準化の実施 安全規格文書の必要性を示すユースケースの開発 安全規格文書の国内での普及基盤構築	
国際での提案委員会	IEC SyC AAL　(Active Assisted Living) 高齢化社会等への対応のための自立生活支援に係る事業を検討する委員会	
現在の段階	FDIS段階	WD段階

安全規格提案先：IEC SyC AAL

高齢者等の自律生活支援に係る事業を取り扱う委員会
✓ 自律生活支援に関する分析のためのツールを複数開発

IEC 63240：AAL アーキテクチャモデル

AAL ユースケース分析：IEC TS 63134
AAL ユーザードメイン：
生活支援の度合いに応じたAALユーザの分類
AAL 用語集：IEC 60050 - 871
AAL アクターリスト：
積極生活支援に関するステークホルダを包括的に分析

AAL 分析のためのツール群

WG1 ユースケース
WG2 AAL構造検討
WG3 適合性評価
WG4 規制関連調査
MT6 AAL用語集メンテナンス
WG5 IoT住宅（スマートホーム）
WG7 IoT住宅（スマートホーム）におけるシステムの安全

SyC：System Committee：システム委員会
一つの技術委員会（TC）でカバーしきれない分野での標準化活動を実施、構成/運用は技術委員会と同等
現時点で6領域存在：Smart Cities, Smart Energy, Low Voltage DC, Smart Manufacturing, …

謝辞

本研究は，経済産業省「省エネルギーに関する国際標準の獲得・普及促進事業委託費：IoT社会実現に向けた住宅設備連携における機能安全に関する国際標準化（H28fy-H30fy）」「省エネルギーに関する国際標準の獲得・普及促進事業委託費：IoT住宅普及にむけた住宅設備機器連携の機能安全に関する国際標準化および普及基盤構築（H31fy-R3fy）」の委託事業の結果得られたものである