

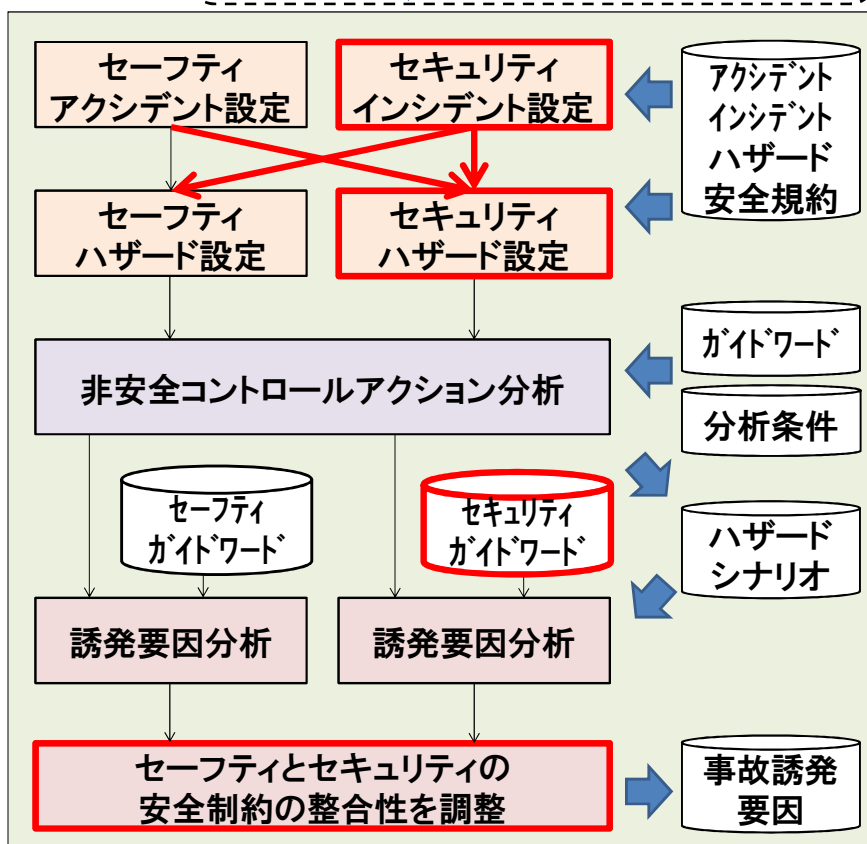
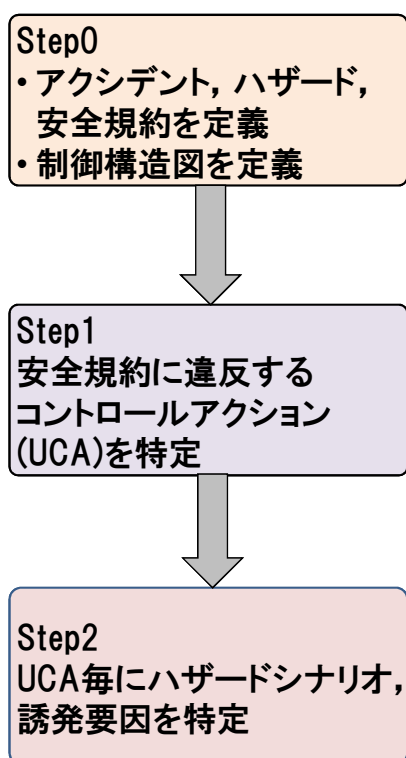
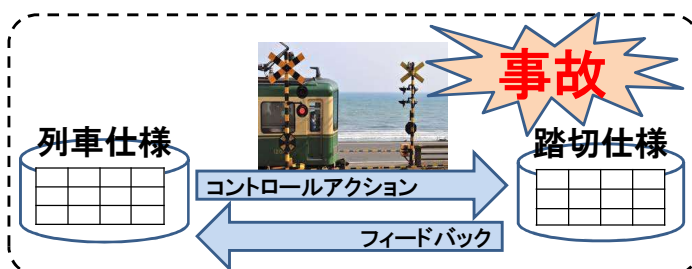


セーフティ・セキュリティ統合分析技術

【背景と課題】 人やモノ、システムが多様に連携するIoTでは、新たな連携が事故を引き起こし、「セーフティ」だけではなく「セキュリティ」の観点からも対策が必要です。しかし、「セーフティ」と「セキュリティ」は独立に発展してきており、統合的なアプローチが確立できていません。

【提案方法】 システム理論に基づく安全分析手法 STAMP/STPA を拡張し、「セーフティ」と「セキュリティ」の双方を同一フレーム上で統合分析を可能にします。そのために、(1)アクシデント・インシデントに至る両ハザードを設定、(2)セキュリティガイドワードを定義、(3)双方の安全制約の整合性をとるステップを設けます。

【今後】 シミュレーションによる相互作用の不備(非安全コントロールアクション)検出の自動化(済)、誘発要因分析、整合性調整の支援(自動化)を行います。



	脅威	要件	手法	着眼点	タイプ	分析	時間
セーフティ	偶発的 (エラー)	信頼性・可用性・保守性	FTA/ FMEA	コンポーネント異常	ブラックリスト	狭・深	長
セキュリティ	故意的 (悪意)	機密性・完全性・可用性	STAMP/ STPA	相互作用異常	ホワイトリスト	広・浅	短