信号保安システムへの
汎用装置適用のガイドライン

信号技術研究部　列車制御システム研究室
主任研究員　祇園 昭宏

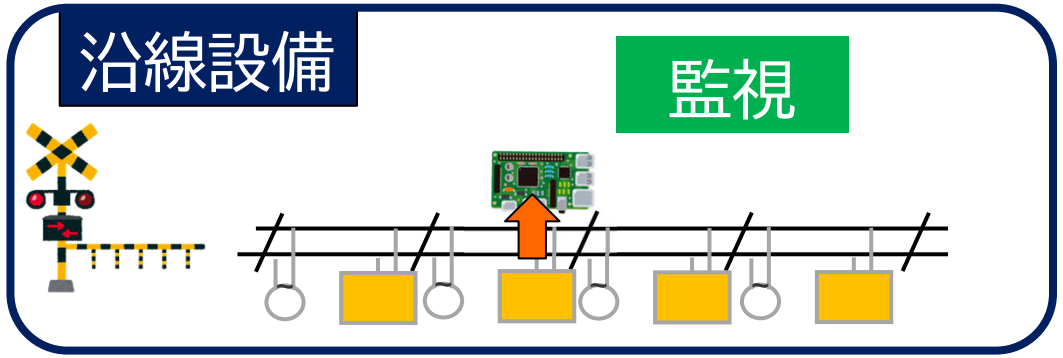
本日の発表

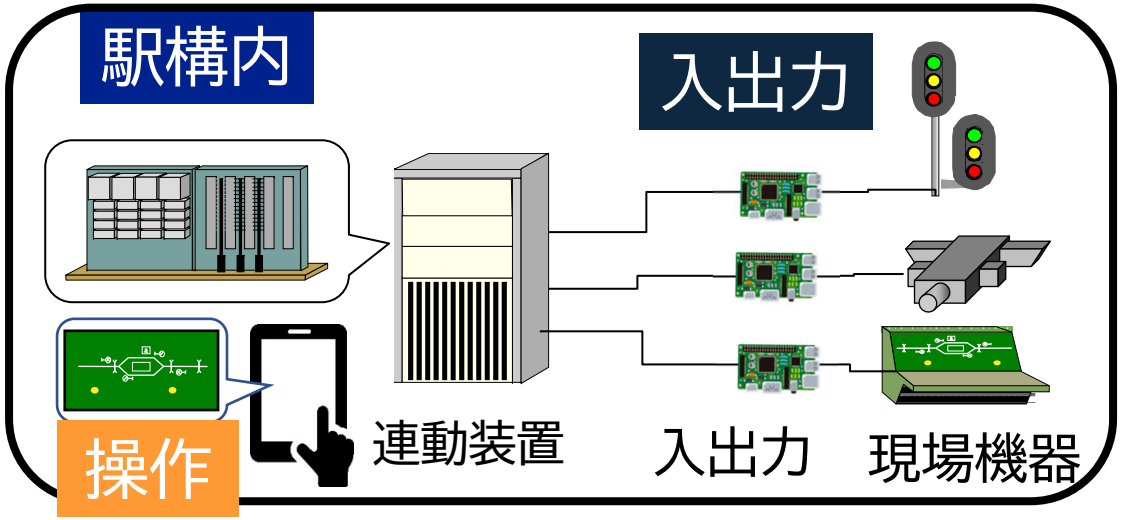
◆研究背景
◆ガイドラインの項目
◆汎用装置の適用における課題
◆安全要件の策定手法
◆操作用途の分析手法・構成手法
◆まとめと成果の活用

研究背景

■鉄道分野でも、保守の効率化・作業支援に汎用装置を活用

■保安用途における利活用への期待





- 可搬性の向上と設備コストの削減に公衆通信サービスの利用が想定

利活用の基盤となる考え方

課題認識

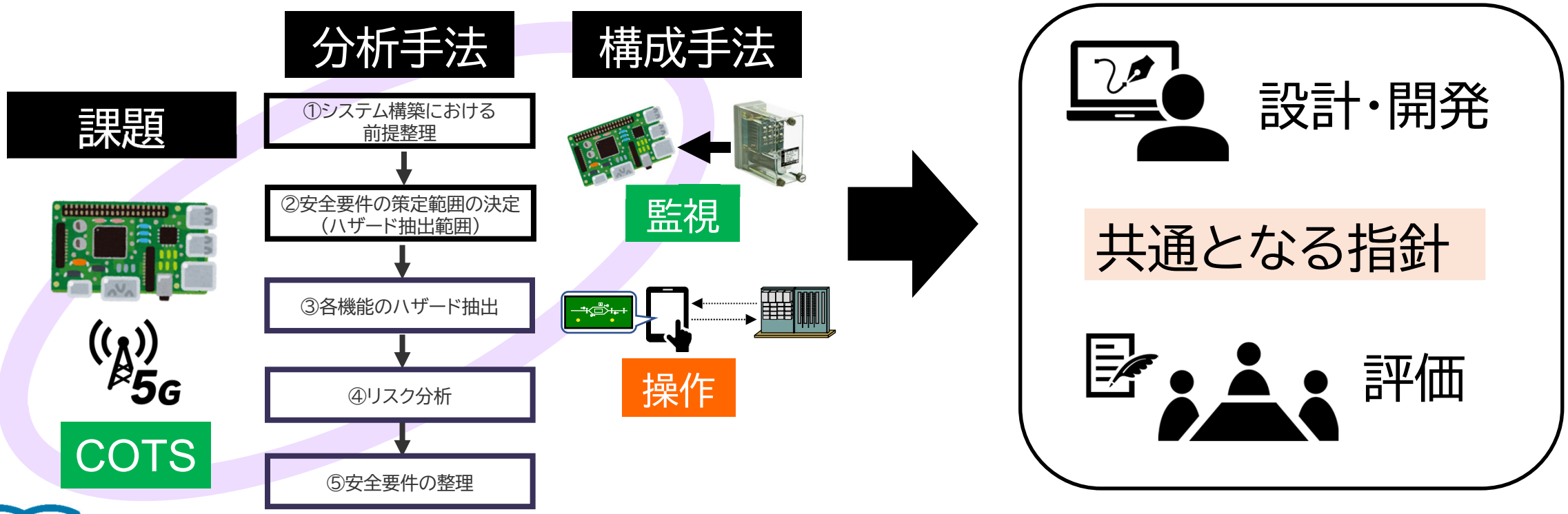
- 汎用装置の適用における課題
- 伝送・インテグレーションの課題

手法の一般化

- 安全要件の策定手法
- 構成手法(安全確保)

ガイドラインの項目

汎用装置の適用、伝送やインテグレーションにおける課題とともに
システム安全要件の分析手法、モデル毎の構成手法をとりまとめた



汎用装置を適用したシステムの安全要件の策定手順と構成手法を
開発と評価の共通指針として、ガイドラインとして整理

ガイドラインの項目

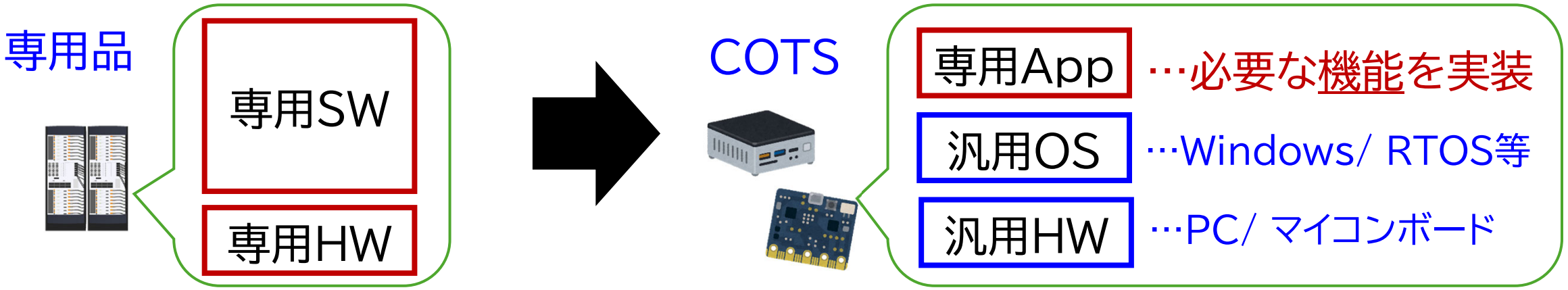
汎用装置の適用における課題

■汎用装置を適用するメリット

汎用品の利活用については**【商用オフザシェルフ】**という手法が知られる

COTS(**C**ommercial **O**ff **T**he **S**helf)

⇒システム開発や装置調達などで専用品に替えて市販品を取り入れること



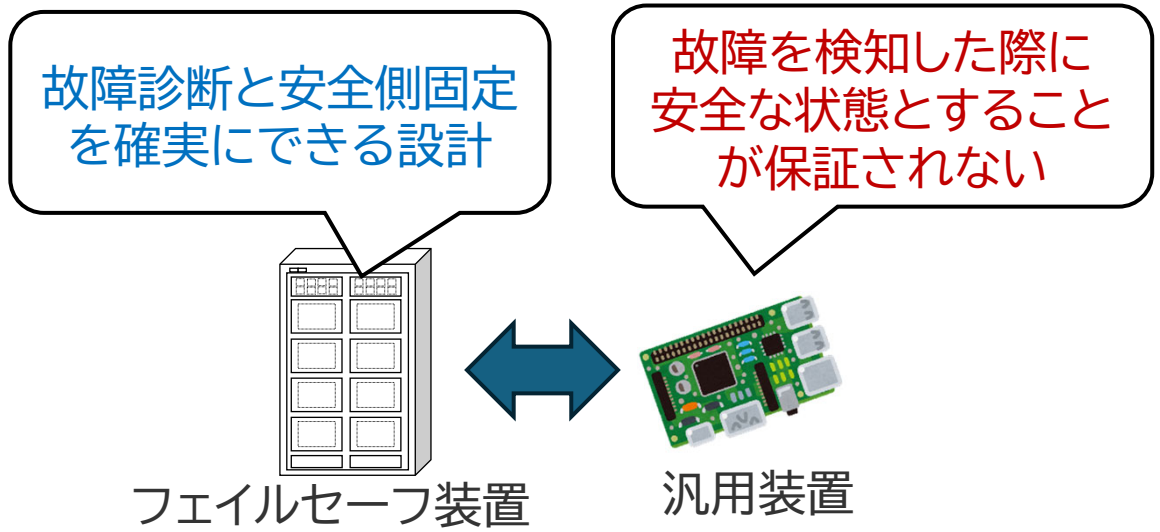
・機能テストや動作検証済、ユーザー環境での不具合対応も一部済
・開発コストを多数のユーザーで分担。低コストかつ高性能
・標準規格に準拠し、高い相互接続性

汎用装置の適用における課題(①安全性)

汎用装置単独では、安全性を確保できないことが安全上の課題

■ FS装置(電子端末)の安全要件

	入力	出力
故障診断	照査ﾊﾟﾙｽ診断、 N/R監視	交番信号 ﾌｨｰﾄﾞﾊﾞｯｸ診断
故障診断の健全性	FS処理部が診断することで 健全性確保	
安全側固定	異常時、落下判定	落下固定



故障診断の内容と、その健全性を確保する方法を専用HW・SWで実現
汎用装置を適用する場合、同様の安全性は装置レベルでは確保できない

汎用装置の適用における課題(②セキュリティ)

汎用装置内部に脆弱性を含む恐れがあること、公衆通信サービスを介したサイバー攻撃の恐れがあることがセキュリティ上の課題

汎用装置

公衆通信サービス

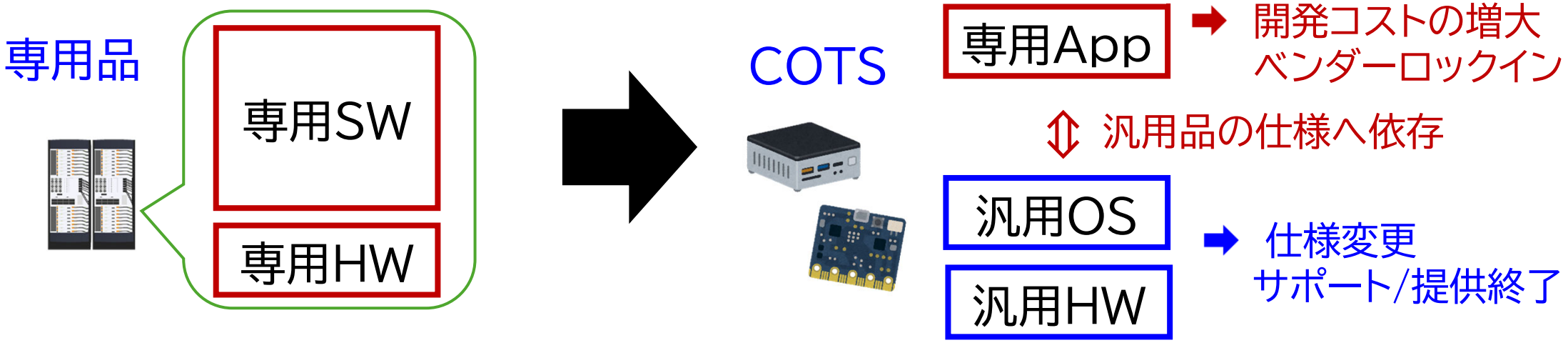
- 装置の脆弱性が利用されうる
  - ➢ 既知の公開された脆弱性
  - ➢ 入手性が高く、解析による発見
- 開発者モードやバックドアの存在
  - ➢ ユーザーからはブラックボックス

- 閉域網と異なり外部アクセス可能
  - ➢ 攻撃者に攻撃経路を提供
- アクセス制限のためのVPN機器はサイバー攻撃の主要なターゲット
  - ➢ OSS利用で既知となりやすい

脅威 は、**攻撃シナリオ**が**策定**できるか、**実行**できるかで定量化可能
汎用装置はシナリオ策定を容易とし、公衆回線は実行機会を増大

汎用装置の適用における課題(③インテグレーション)

特定製品への依存による仕様変更や提供終了のライフサイクルへの影響
高コスト化やベンダーロックインがインテグレーションの課題



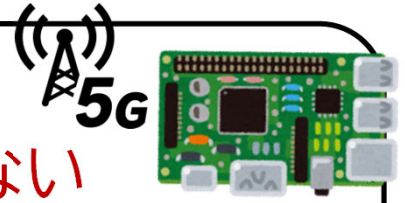
標準構成からの変更規模に応じて開発が高コスト化
システムが汎用装置に依存し、運用期間が確保できない恐れ

汎用装置の適用における課題

汎用装置の課題と留意点

閉域網での信号保安装置は、
1.装置が入出力の安全を確保
2.セキュリティリスクは低い
3.製品ライフサイクルが長い

公衆網と汎用装置は、
1.安全性が保証されない
2.セキュリティ上のリスクがある
3.製品ライフサイクルが短い

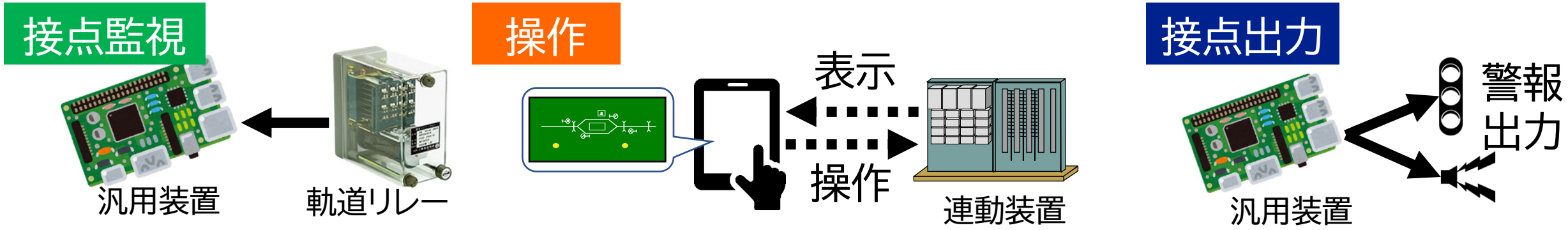


課題
- 装置単体で安全を確保できない
- セキュリティ対策が必要となる

COTS留意点
- 更新が容易であること
- 高コストとならないこと

システムの安全要件を定めて、安全を確保する安全分析手法
ライフサイクルの確保に留意する設計手法

想定するユースケース



各用途で**危険側となる事象**に至らないとする安全確保の考え方を構築

モデルケース	危険側事象	安全側のアベイラビリティ阻害事象
軌道リレー監視	リレー落下時に扛上状態と誤認	リレー扛上時に落下状態と誤認
連動装置操作	操作者の安全誤認となる表示 操作者の意図しない操作実施	操作者の危険誤認となる表示 操作者の操作を受け付けない
警報出力制御	警報タイミングで発報しない	指示誤認や装置故障による誤発報

システムの危険側状態を特定し、検証によって防ぐ

安全要件の策定手法

システム構築における
前提整理

↓

安全要件の策定範囲の決定
（ハザード抽出範囲）

↓

各機能のハザード抽出

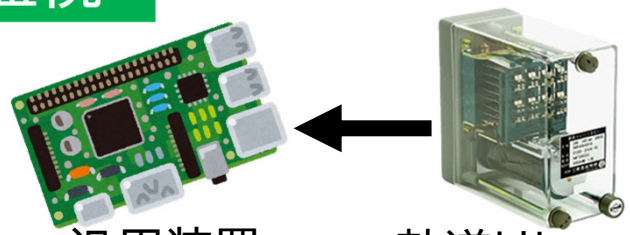
↓

リスク分析

↓

安全要件の整理

監視



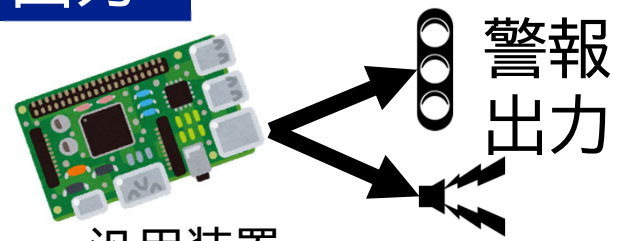
汎用装置　　軌道リレー

ハザード　入力の誤り

↓

危険側事象　扛上の誤認

出力



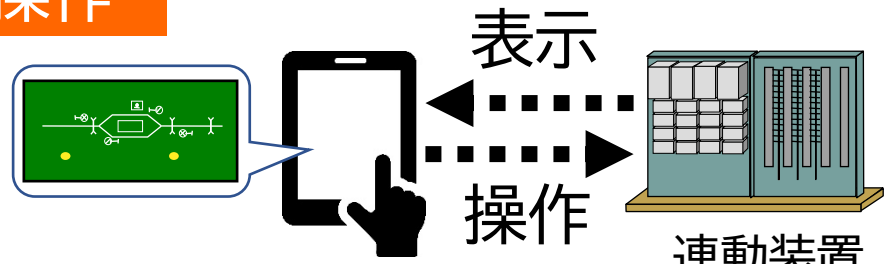
汎用装置

出力の誤り

↓

発報しない

操作



入出力の誤り

誤制御、誤表示

↓

誤ったてこ操作
危険側誤認

操作用途の安全分析

①システム構築における
前提整理

↓

②安全要件の策定範囲の決定
（ハザード抽出範囲）

↓

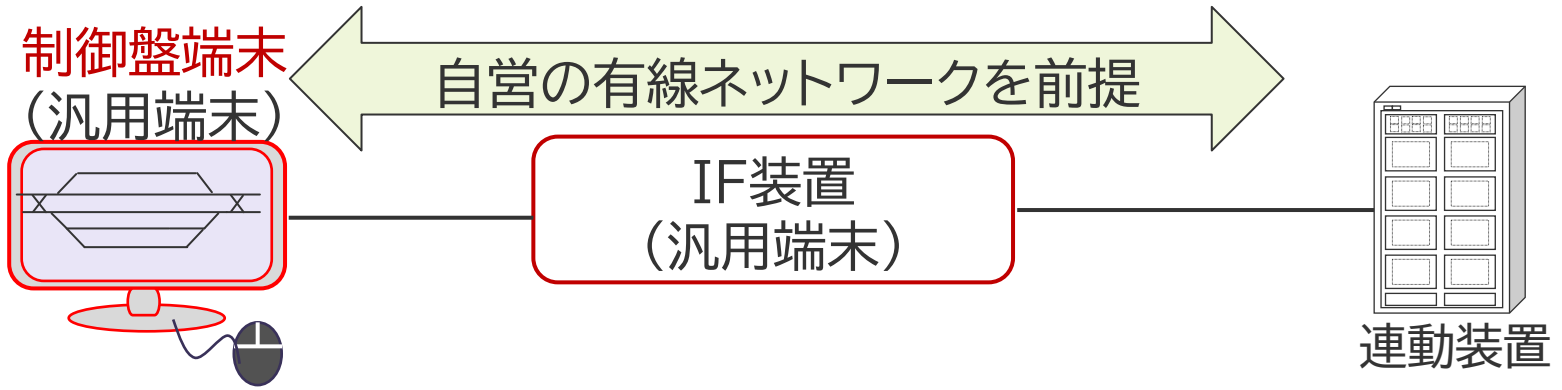
③各機能のハザード抽出

↓

④リスク分析

↓

⑤安全要件のまとめ



■ライフサイクル

- IF装置を設けることで連動装置の改修を最小化
- インターフェースの仕様を定めて互換性を確保

■セキュリティ

- クローズドシステムであるため除外

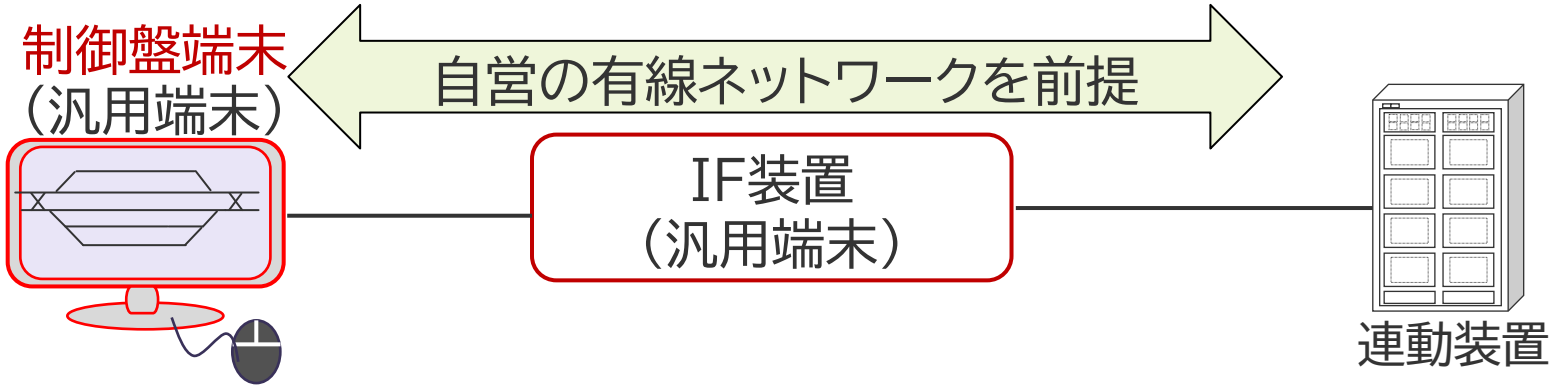
残る安全性の確保が構成上の課題

操作用途の安全分析

①システム構築における
前提整理

↓

②安全要件の策定範囲の決定
（ハザード抽出範囲）

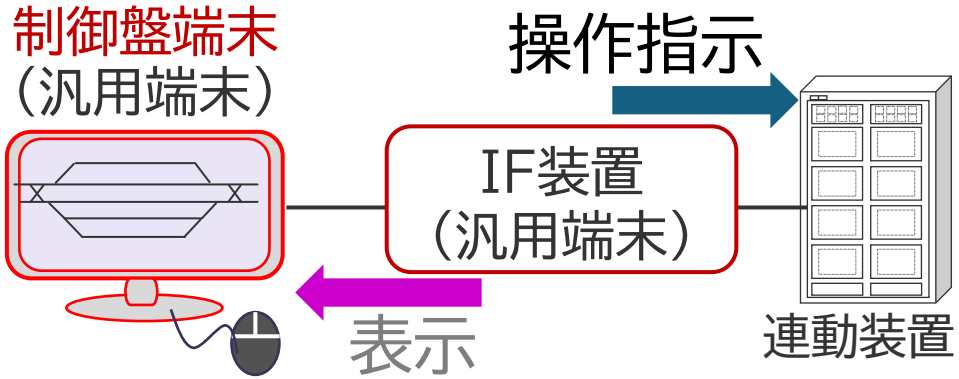


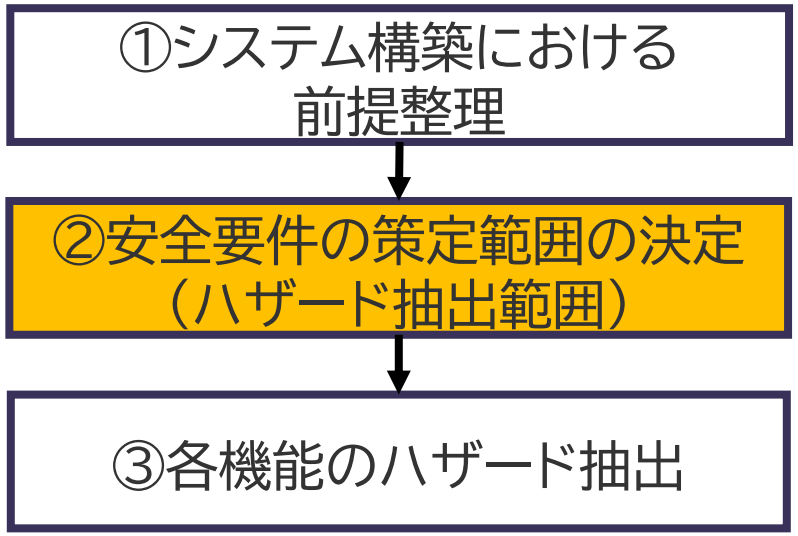
機能	装置	機能
操作	汎用装置	操作を連動装置に通知
	連動装置	汎用装置から操作内容を取得し、現場装置を制御
表示	汎用装置	連動装置から取得した現示・進路等の状態情報を表示
	連動装置	現示、進路、在線等を状態情報として汎用装置に通知

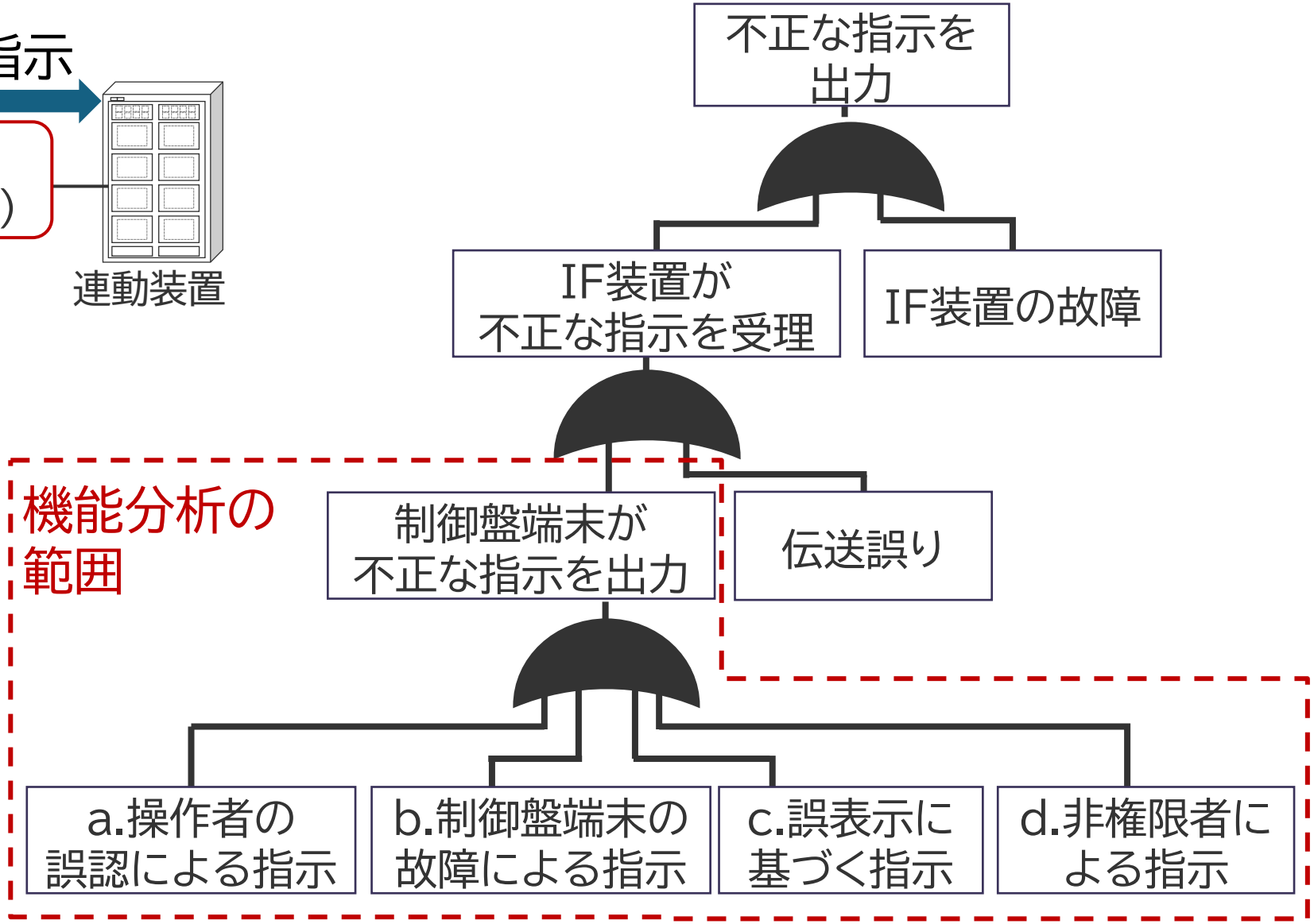
危険側事象

- 連動装置側が意図しない制御を実施および、意図した操作不能
- 操作者の危険側誤認となる表示

操作用途の安全分析


制御盤端末
（汎用端末）
操作指示
IF装置
（汎用端末）
表示
連動装置


①システム構築における
前提整理
②安全要件の策定範囲の決定
（ハザード抽出範囲）
③各機能のハザード抽出

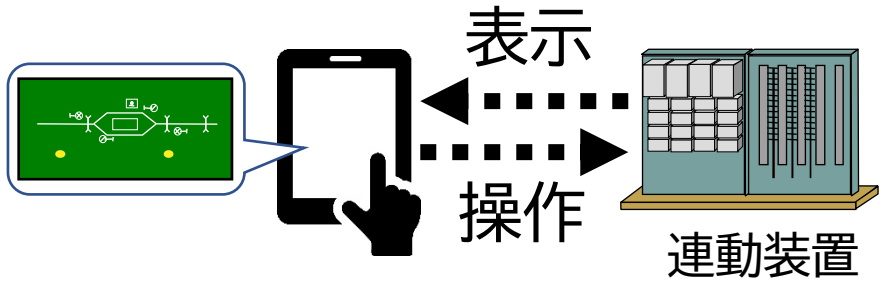

不正な指示を
出力
IF装置が
不正な指示を受理
IF装置の故障
制御盤端末が
不正な指示を出力
伝送誤り
機能分析の
範囲
a.操作者の
誤認による指示
b.制御盤端末の
故障による指示
c.誤表示に
基づく指示
d.非権限者に
よる指示

操作用途の安全分析

・てこ機能のハザード抽出

目的	てこ名称	危険側事象	安定阻害事象
列車の進行指示	信号てこ	－	誤制御・復位による 運行支障
制御条件の決定	駅扱いてこ		
	方向てこ		
	解放てこ	－	解放扱いの誤制御・復位
転てつ機の制御	転てつてこ	不正な単独転換	転換不能
対象の防護	踏切代用てこ	動作の不正解除 動作の誤表示	踏切の誤制御
	警報てこ		
	一斉停止現示てこ	不正解除	一斉停止の誤制御
	線路閉鎖てこ	*線閉不正解除*	*線閉誤制御*

操作用途の安全分析



①②前提整理、FT解析

リスクレベル	分類	発生し得る事象
Ⅰ	安定阻害事象	業務における支障
Ⅱ		一部の列車運行に影響
Ⅲ		複数の列車運行に影響
Ⅳ	危険側事象	インシデントや人的災害

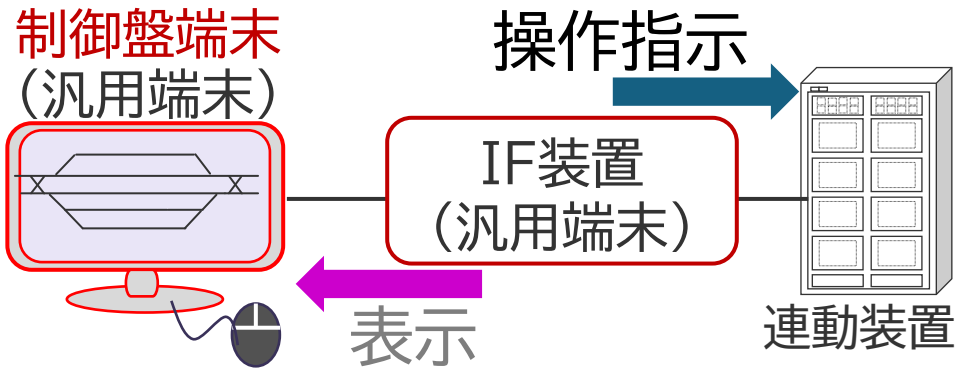
④リスク分析

③各機能のハザード抽出にて整

てこ	目的	誤制御、誤認によるリスク			誤表示によるリスク
		誤制御（制御）	誤制御（復位）	制御不能	
信号てこ	列車進行指示	Ⅰ	Ⅱ	Ⅱ	Ⅰ
駅扱いてこ	制御条件の決定	Ⅰ	Ⅰ	Ⅱ	Ⅰ
方向てこ		Ⅰ	Ⅰ	Ⅲ	Ⅰ
解放てこ		Ⅲ	Ⅲ	Ⅲ	Ⅰ
転てつてこ	転てつ機の制御	Ⅳ		Ⅰ	Ⅰ
踏切代用てこ	対象の防護	Ⅱ	Ⅳ	Ⅱ	Ⅳ
警報てこ		Ⅱ	Ⅳ	Ⅱ	Ⅳ
一斉停止てこ		Ⅲ	Ⅳ	Ⅳ	Ⅰ
線路閉鎖てこ		Ⅱ	Ⅳ	Ⅰ	Ⅰ

操作用途の安全分析

・安全要件のまとめ

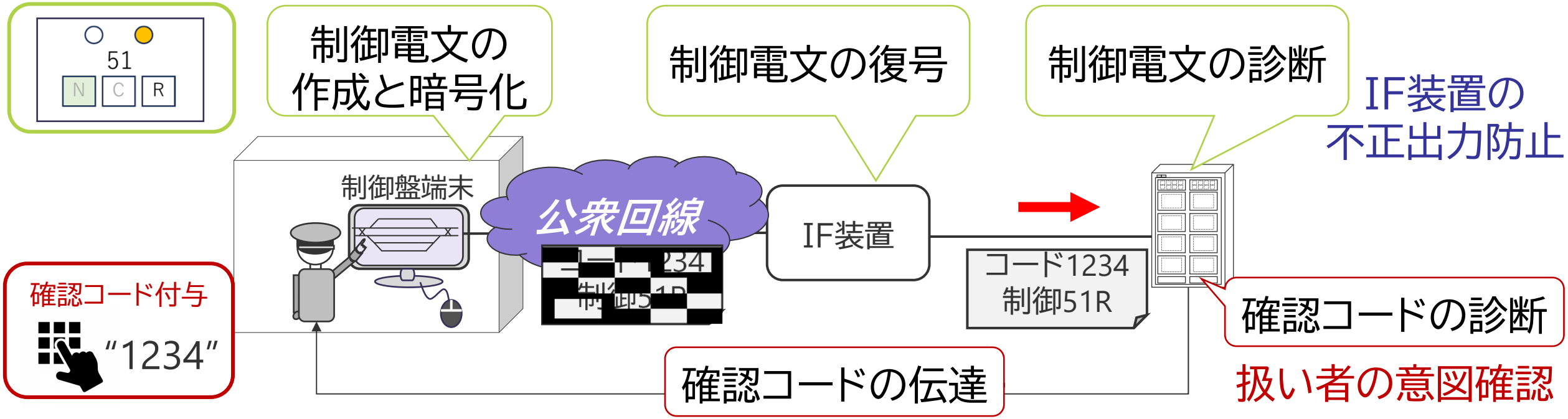


- IF装置の故障に対する安全確保
- 「誤制御・誤表示・制御不能」に対する安全確保

事象	安全要件
誤制御	• IF装置の出力が操作者の意図したものであること • 誤扱い対策を行うこと、扱い者の限定
制御不能	• 冗長構成による信頼性の確保
誤表示	• 制御盤端末の表示する情報が連動装置の出力と同じことの確認

操作用途の構成手法

誤制御への対策



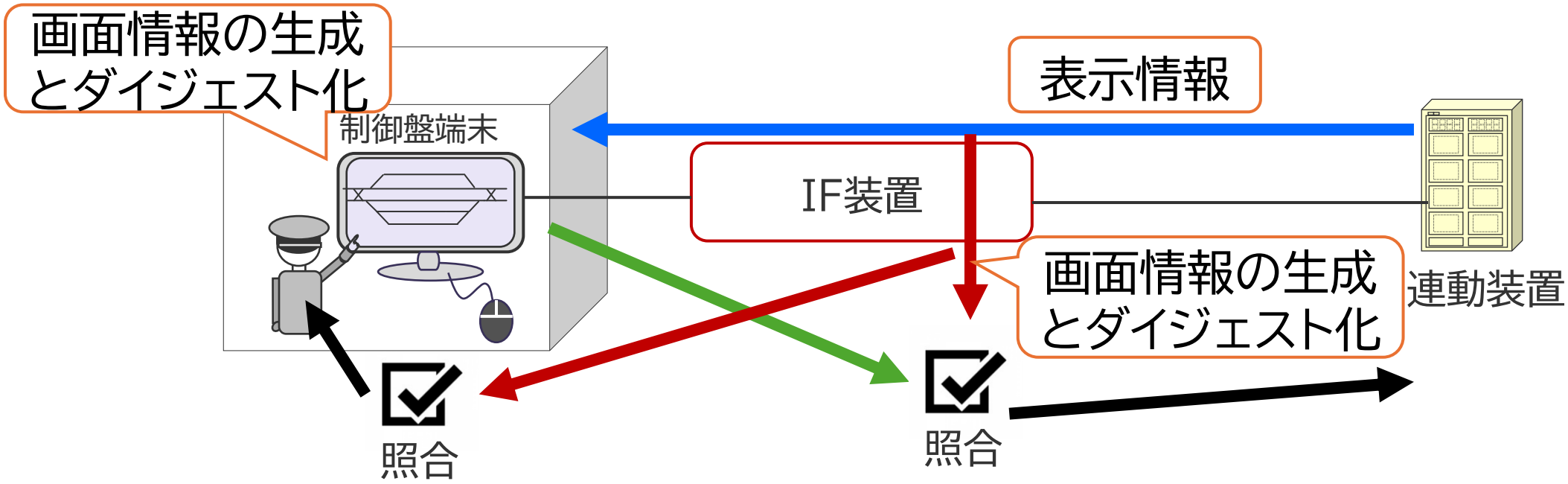
・制御電文の暗号化により、端末の不正出力を防ぐ
・取扱者の確認を介在させることで、操作意図を確認する

IF装置を復号装置とし、フィードバックループを構成

操作用途の構成手法

誤表示への対策

連動装置が出力する情報と、汎用端末に表示されている情報を照合



画面情報照合の冗長化により、単一故障による見逃しを防ぐ

まとめと成果の活用

◆まとめ

- 信号保安システムへの汎用装置の適用において、設計と評価の共通指針となるガイドラインの策定をおこなった
- ガイドラインに示した、適用の課題と安全分析の手法について操作用途を例にユースケース毎の分析と構成手法を紹介した

◆成果の活用

- 設計支援や安全性評価を本ガイドラインに基づき実施し、汎用装置を用いた信号保安システムの設計や、公衆通信サービスを用いた信号保安システムのセキュリティ確保を実現する

参考文献

- 祇園昭宏, 岩田浩司:高い安全性を要する用途への汎用モバイル端末の適用, 鉄道総研報告, Vol.33, No.7, pp.35 - 40, 2019
- 祇園昭宏, 福田光芳, 中澤幸弘:汎用端末を用いた保安用途向け接点入出力システムの構成手法, 鉄道総研報告, Vol.36, No.8, pp.17-22, 2022