

安全学と鉄道信号分野における安全性技術

公益財団法人鉄道総合技術研究所
情報通信技術研究部 福田光芳



目次

- 鉄道総研のご紹介
- 安全学と安全学研究会
- 鉄道信号分野の安全性技術の紹介
 - 鉄道信号の概要
 - 装置(ハードウェア)としての安全性技術の変遷
 - 列車を制御する方法(ソフトウェア)の変遷

目次

- 鉄道総研のご紹介
- 安全学と安全学研究会
- 鉄道信号分野の安全性技術の紹介
 - 鉄道信号の概要
 - 装置(ハードウェア)としての安全性技術の変遷
 - 列車を制御する方法(ソフトウェア)の変遷

目次

- 鉄道総研のご紹介
- 安全学と安全学研究会
- 鉄道信号分野の安全性技術の紹介
 - 鉄道信号の概要
 - 装置(ハードウェア)としての安全性技術の変遷
 - 列車を制御する方法(ソフトウェア)の変遷

鉄道総研のご紹介

- 国鉄の民営分割化に際して、国鉄の鉄道技術、鉄道労働科学に関する試験研究等を引き継ぐために財団法人として設立(1986)
⇒ 公益財団法人に移行(2011)

【事業所】

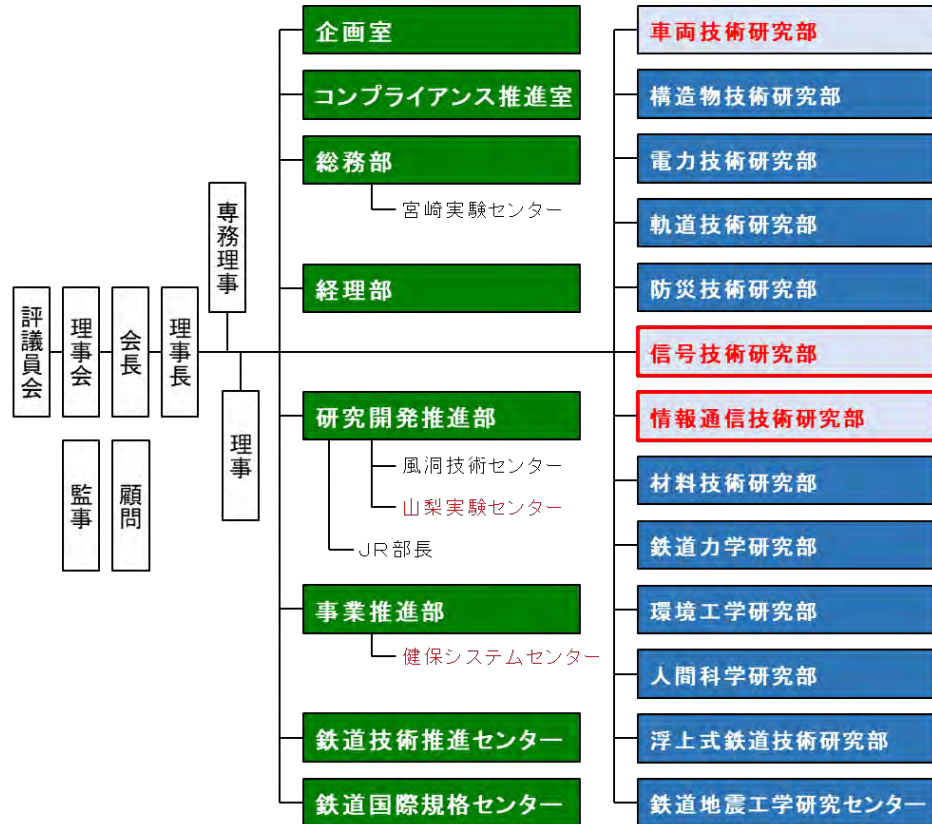
国立研究所
新宿オフィス

【実験所】

風洞技術センター(米原)
塩沢雪害防止実験所(新潟)
勝木塩害実験所(新潟)
日野土木実験所



鉄道総研のご紹介



13研究部・研究センター
550名(2021. 4)

鉄道総研のご紹介

車両技術研究部

構造物技術研究部

電力技術研究部

軌道技術研究部

防災技術研究部

信号技術研究部

情報通信技術研究部

材料技術研究部

鉄道力学研究部

環境工学研究部

人間科学研究部

浮上式鉄道技術研究部

鉄道地震工学研究センター

鉄道技術推進センター

鉄道国際規格センター

鉄道システム関わる広範な分野をカバー



目次

- 鉄道総研のご紹介
- **安全学と安全学研究会**
- 鉄道信号分野の安全性技術の紹介
 - 鉄道信号の概要
 - 装置(ハードウェア)としての安全性技術の変遷
 - 列車を制御する方法(ソフトウェア)の変遷

安全学

安全学(safenology)

- 安全に関する技術的側面(自然科学)、人間的側面(人文科学)、組織的側面(社会科学)を、安全哲学などの理念的側面の下で、合法的、合理的、かつ、ひとの理解と納得をえて、統一・統合化した学問体系

安全四学:向殿政男, 北条理恵子, 清水尚憲, 日本規格協会(2021) より引用

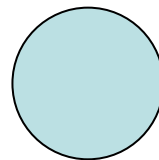
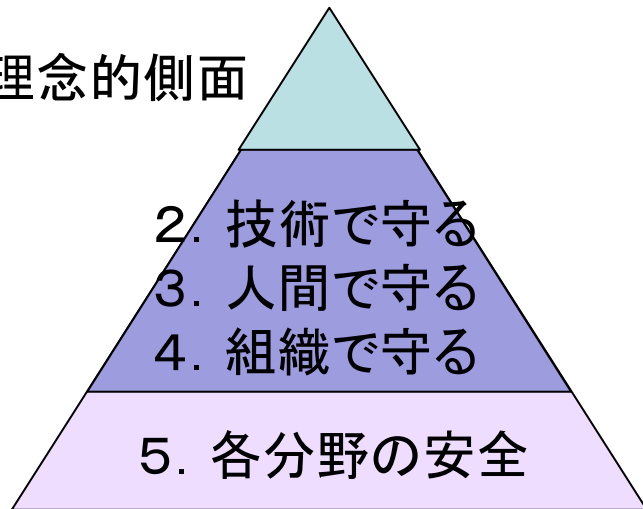


安全曼荼羅

安全曼荼羅(安全マップ)

- 安全学の構造

1. 理念的側面



6. 安全関連分野

(警察制度、裁判制度、保険制度等)

安全四学: 向殿政男, 北条理恵子, 清水尚憲, 日本規格協会(2021) より

安全学研究会

日本信頼性学会の研究会として2021年10月から活動開始

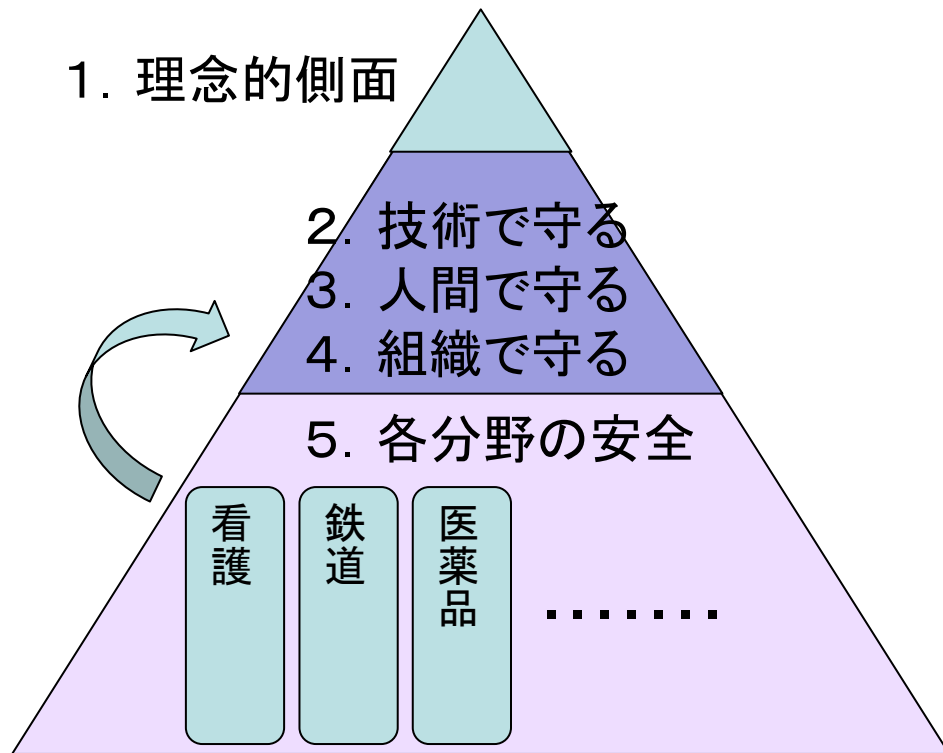
- 安全のための知見や技術は様々な技術分野・産業分野で閉じる形で経験則を蓄積・伝承したり、研究成果を議論したりして発展してきている。
- その多くは個々の分野に特化した技術として表現されており、他分野で活用することは難しい。
- 安全のための技術を体系化し、各分野で共通の議論ができるように安全学が提唱されている。
 - 安全学を拠り所とし、技術分野・産業分野を横断する形で安全のための技術を継続的に議論し、共有すべき知見や技術を蓄積・活用することを目的とする。

研究会活動の対象範囲

◆ 範囲

- 安全学に関わることであれば何でも
- プラスのリスクも対象
 - ✓ 具体事例の紹介はまだ
 - ✓ 納得いかない人も(“リスク”という用語を変えればokかも)
- セキュリティ
- ウェルビーイング
 - ✓ 除外していないが、安全があってこそそのウェルビーイングと考えると、まずは安全を重点的に進めるイメージ

研究会活動のイメージ



研究会活動のフレームワーク

研究会当日の議論

研究会での
発表資料

概念・用語の差異などの整理

安全性に関わる技術の
共通部分

ドメインの特情

③概念・用語を目次に対応させて資料作成

概念・用語の分野間の
対比資料

②共通部分を
抽出・整理

安全性に関わる技術の
共通部分

①アーカイブを
つくる

研究会での
発表資料+メモ

安全学の目次
(曼荼羅に対応?)

1. ...
2. ...
-

④ドメインの特情整理(参考)

ドメインの特情

目次

- 鉄道総研のご紹介
- 安全学と安全学研究会
- 鉄道信号分野の安全性技術の紹介
 - 鉄道信号の概要
 - 装置(ハードウェア)としての安全性技術の変遷
 - 列車を制御する方法(ソフトウェア)の変遷

鉄道システムと安全

鉄道システムの安全

- 車両の要素・・・走行の安定性や火災など
- 構造物の要素・・・土構造物、橋りょうなど
- 軌道の要素・・・レール間の幅や平面性、通りなど
- 環境の要素・・・強風、地震など
- 列車や進路の制御(鉄道信号の分野)

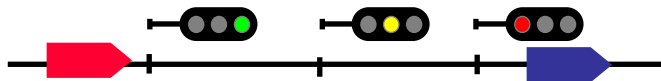
⋮

各分野の
要素以外に
作業の要素



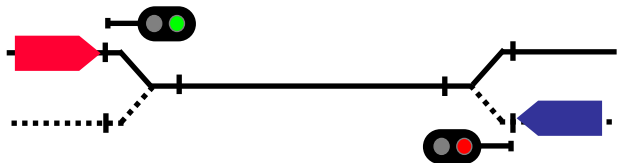
鉄道信号の主な役割

①衝突の防止



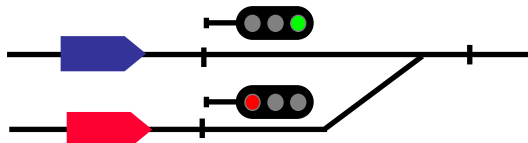
安全な間隔の確保、速度制御 → 閉そく、信号機、ATS

②衝突の防止



→ 閉そく、信号機、連動

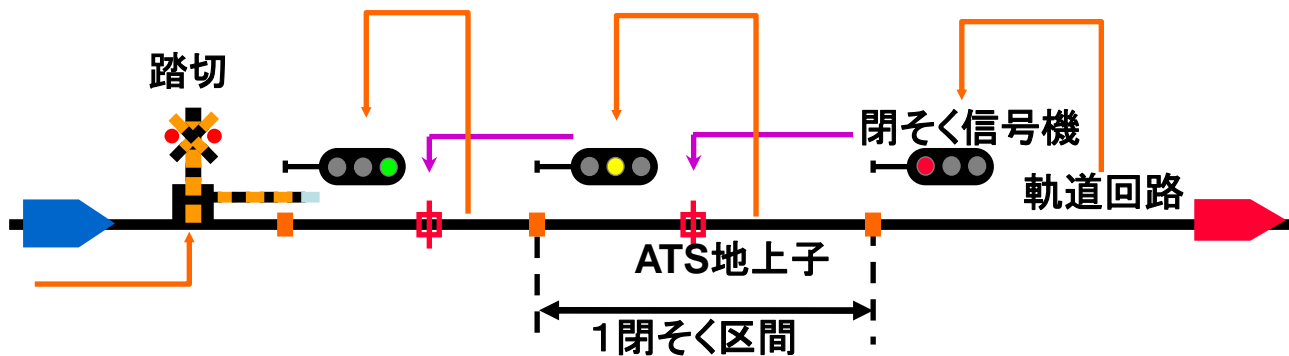
③接触、脱線の防止



信号現示とポイントの連鎖 → 信号機、連動

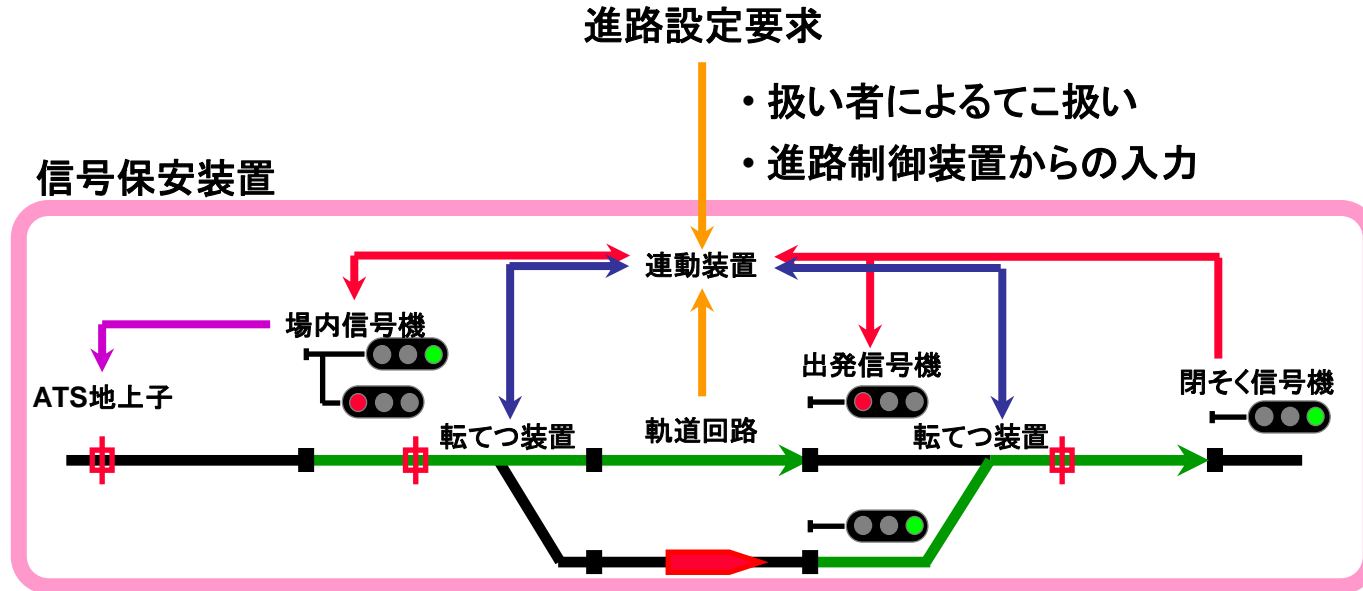
- 安全性
- 安定性
- 効率的な制御
(利便性の高い運行)
- コスト

信号保安装置の構成(駅間)



- ・交通信号機と現示(色)の意味と変化順序が異なる

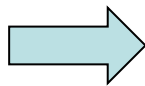
信号保安設備の構成(駅構内)



安全確保の基本的な考え方

安全な状態

- ・列車が停止している
- ・踏切が閉まっている



装置として安全側の制御

- ・停止現示(赤)となるような出力
- ・分岐器を動かさない
- ・踏切を閉める制御



安全側の制御を確実にを行うための技術
・・・技術の進歩とともに変化

Safety2.0／協調安全
などの新しい概念に
は至っていない
(実務・研究とも)

目次

- 鉄道総研のご紹介
- 安全学と安全学研究会
- 鉄道信号分野の安全性技術の紹介
 - 鉄道信号の概要
 - 装置(ハードウェア)としての安全性技術の変遷
 - 列車を制御する方法(ソフトウェア)の変遷

安全を確保する方法

鉄道信号技術の変遷・・・安全を確保する方法(技術)の変遷

機械式信号装置

鉄管やワイヤなどの組み合わせ



電気技術の本格導入: 1920年頃～

リレー(継電器)による論理実装



ME(マイクロエレクトロニクス)技術の導入: 1985年頃～

同じアプリケーションの装置をコンピュータ化



情報技術の積極的利用: 1990年頃～

列車の新しい制御方法などを実現



汎用装置などの活用範囲拡大

安全を確保する方法

鉄道信号技術の変遷・・・安全を確保する方法(技術)の変遷

機械式信号装置

鉄管やワイヤなどの組み合わせ



電気技術の本格導入: 1920年頃～

リレー(継電器)による論理実

電気技術導入前の
フェールセーフ技術



ME(マイクロエレクトロニクス)技術の導入: 1985年頃～

同じアプリケーションの装置をコンピュータ化



情報技術の積極的利用: 1990年頃～

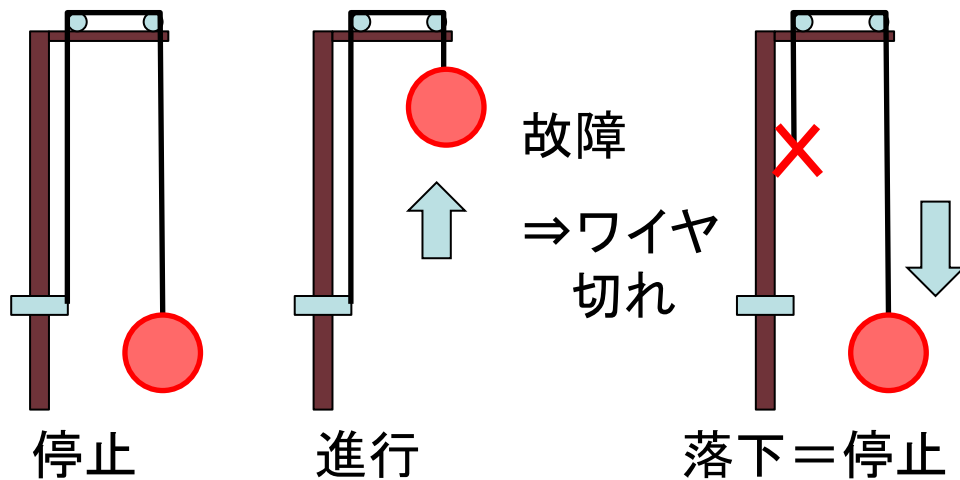
列車の新しい制御方法などを実現



汎用装置などの活用範囲拡大

機械装置を用いた安全性技術

信号機の安全性技術(ボール信号)



情報の割付け方が重要・・・逆だと危険

機械装置を用いた安全性技術

- ・エネルギー非対称性の利用・・・フェールセーフ技術の1つ
エネルギーの高い状態を**通常の状態**(進行信号現示など)に割り当て、故障時はエネルギーが低い側になるように設計
⇒ 故障時に安全側(停止信号現示)に制御

安全を確保する方法

鉄道信号技術の変遷・・・安全を確保する方法(技術)の変遷

機械式信号装置

鉄管やワイヤなどの組み合わせ

電気技術等を用いた
フェールセーフ技術

電気技術の本格導入:1920年頃～

リレー(継電器)による論理実装

ME(マイクロエレクトロニクス)技術の導入:1985年頃～

同じアプリケーションの装置をコンピュータ化

情報技術の積極的利用:1990年頃～

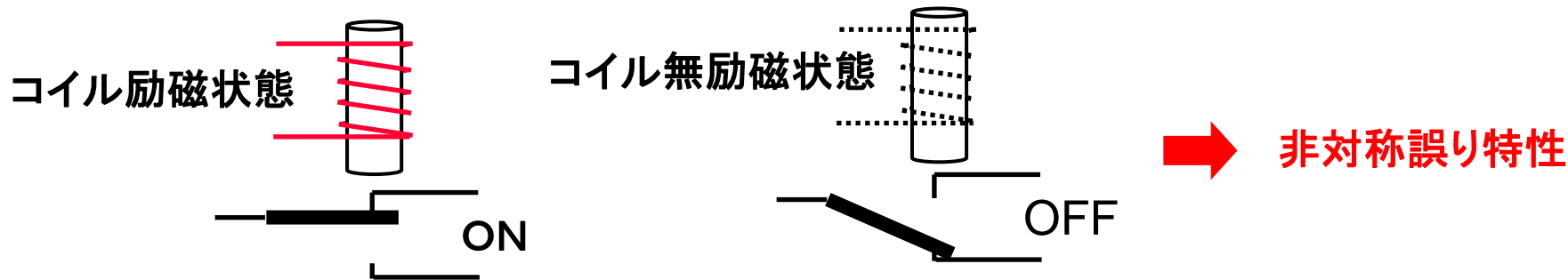
列車の新しい制御方法などを実現

汎用装置などの活用範囲拡大

電気をを用いた安全性技術

信号用リレー

重力やバネを利用し、故障時には必ずOFF側に故障
(ON側に故障する確率がきわめて低い)



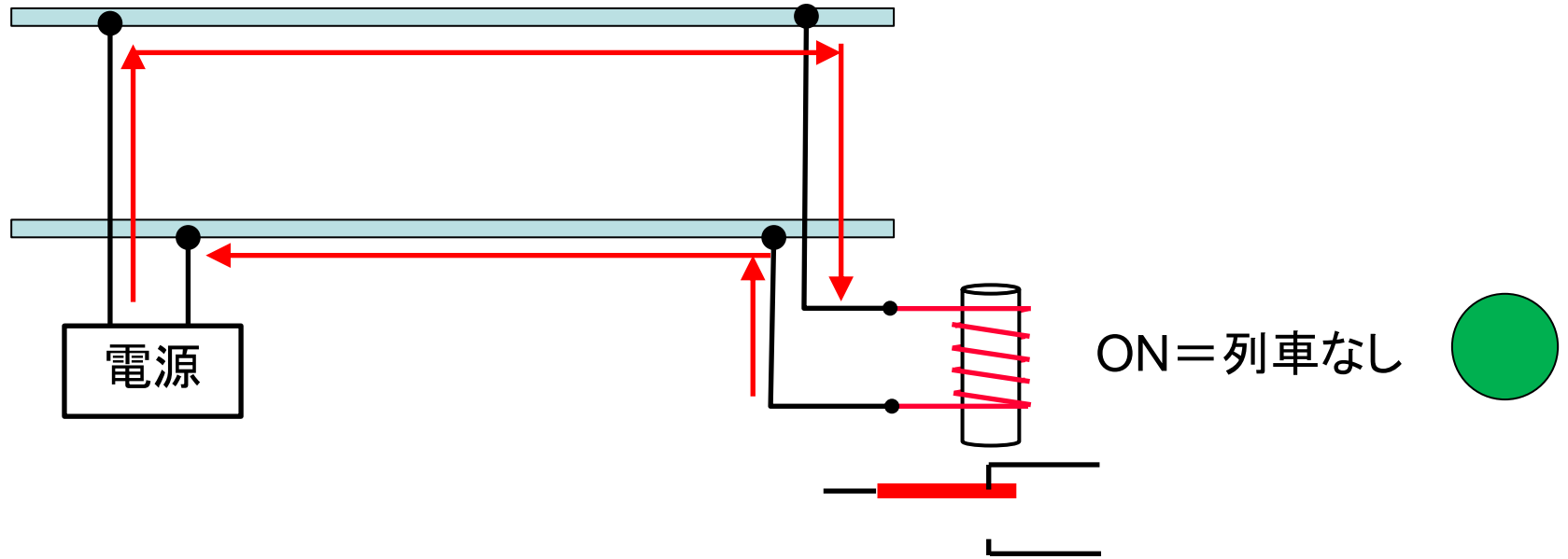
リレーがOFFの時に安全側制御になるように回路設計

⇒ OFFの時に赤信号になる

電気をを用いた安全性技術

軌道回路

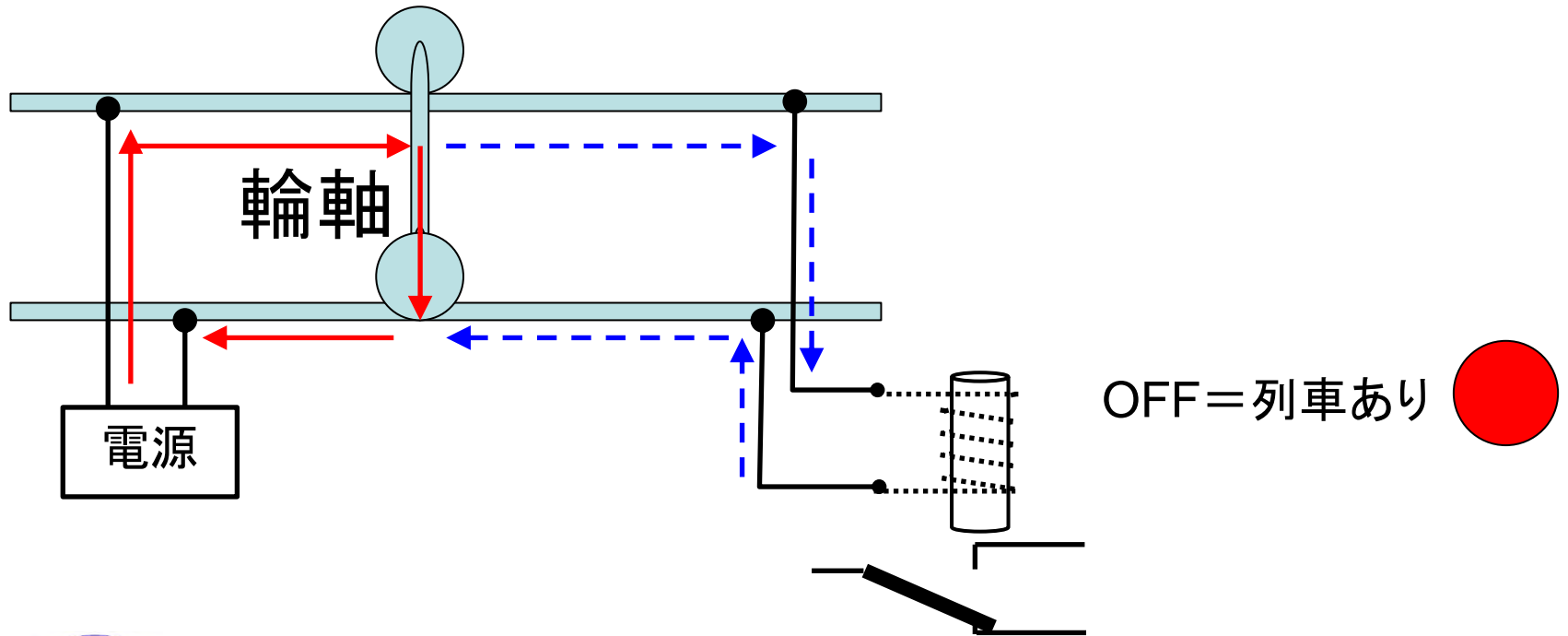
レールを電気回路の一部として区間内の列車の有無を検出



電気をういた安全性技術

軌道回路

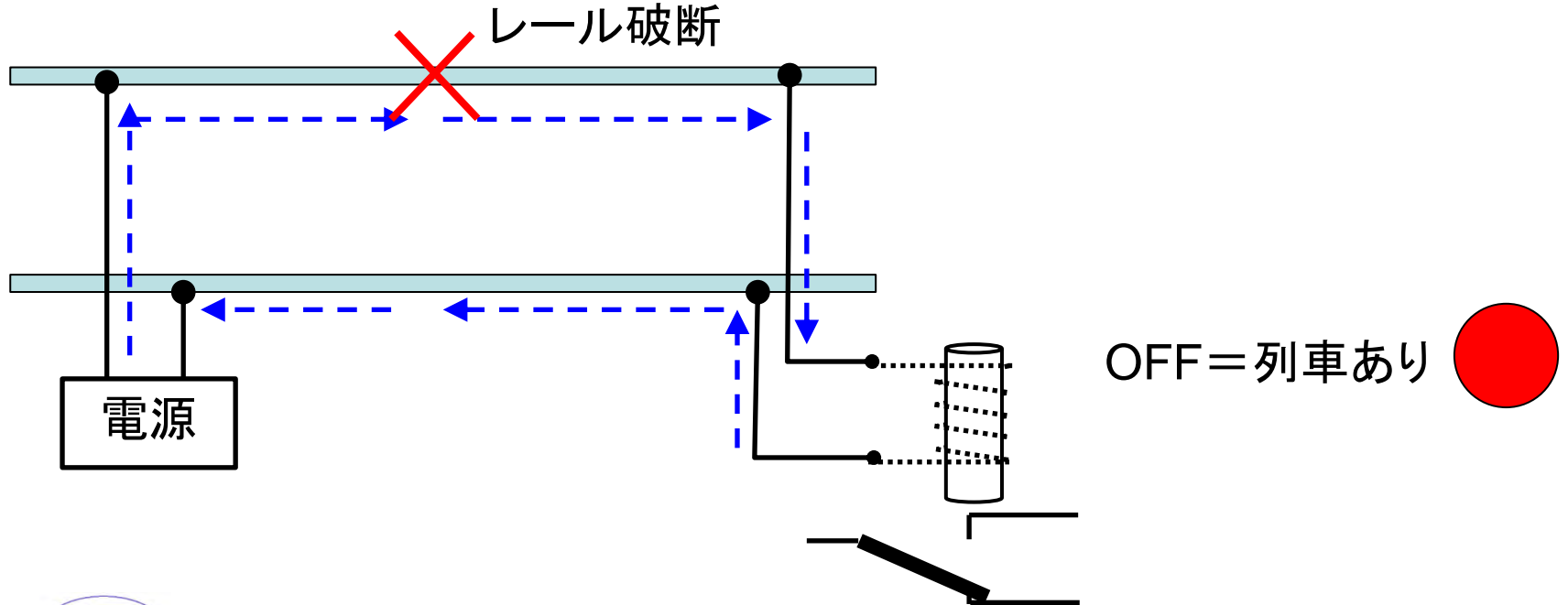
輪軸で短絡 ⇒ リレー-OFF



電気をを用いた安全性技術

軌道回路

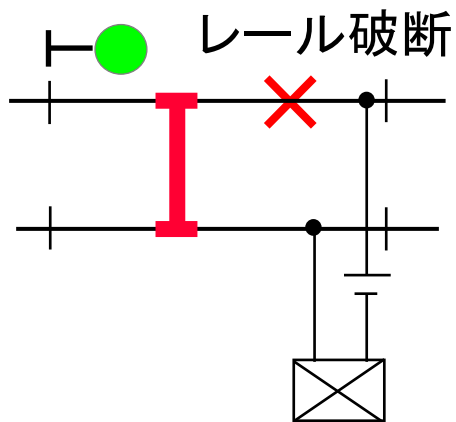
レール破断、機器故障 ⇒ リレーOFF



電気をを用いた安全性技術

軌道回路

開電路式を信号制御に用いるとどうなるか？



故障が発生した場合

状態が変化しない



故障検出できない



列車が進入してしまう

列車の通過で
警報を止める
場合に利用



システムの観点で
安全側制御を定義する
必要がある

安全を確保する方法

鉄道信号技術の変遷・・・安全を確保する方法(技術)の変遷

機械式信号装置

鉄管やワイヤなどの組み合わせ

コンピュータを用いた
フェールセーフ技術

↓
電気技術の本格導入:1920年頃～

リレー(継電器)による論理実装

↓
ME(マイクロエレクトロニクス)技術の導入:1985年頃～

同じアプリケーションの装置をコンピュータ化

↓
情報技術の積極的利用:1990年頃～

列車の新しい制御方法などを実現

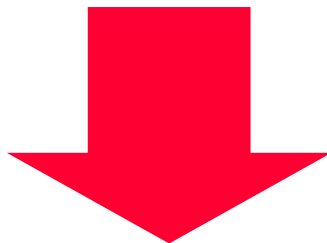
↓
汎用装置などの活用範囲拡大

電子化信号システムの安全性技術

電子部品による回路

:リレーのような故障時の非対称性がない

➡ 故障時の動作が不定



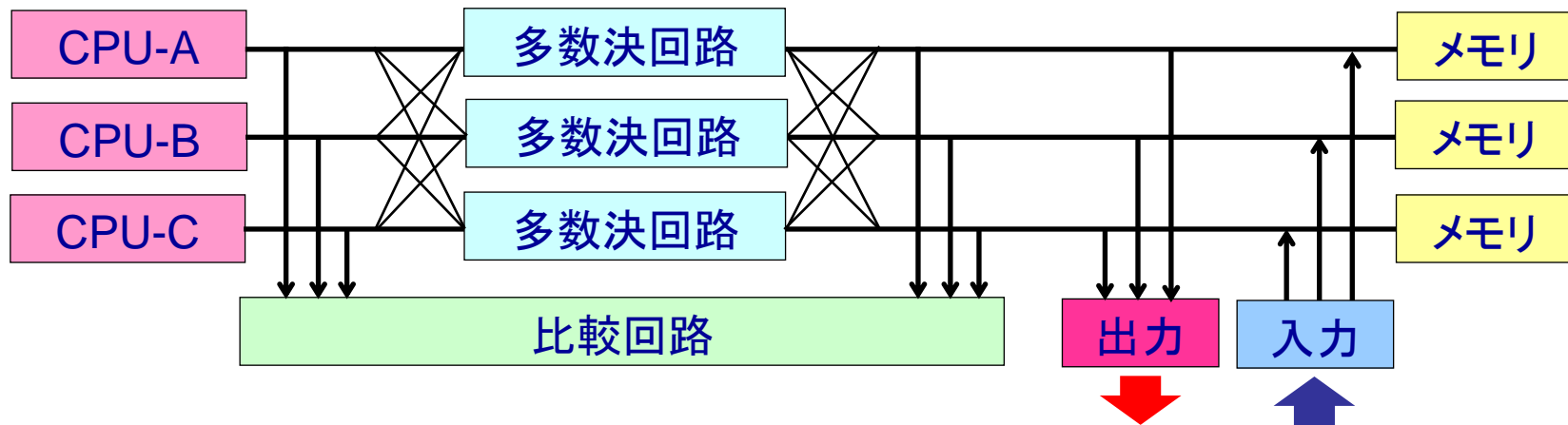
解決策

(コンピュータのインテリジェンス、
高速処理能力の利用)

- ◆ 冗長構成
- ◆ 自己診断、故障検出(高頻度、多箇所)
- ◆ 異常検出時の出力の安全側固定

電子化信号システムの安全性

3重系多数決(2 out of 3)

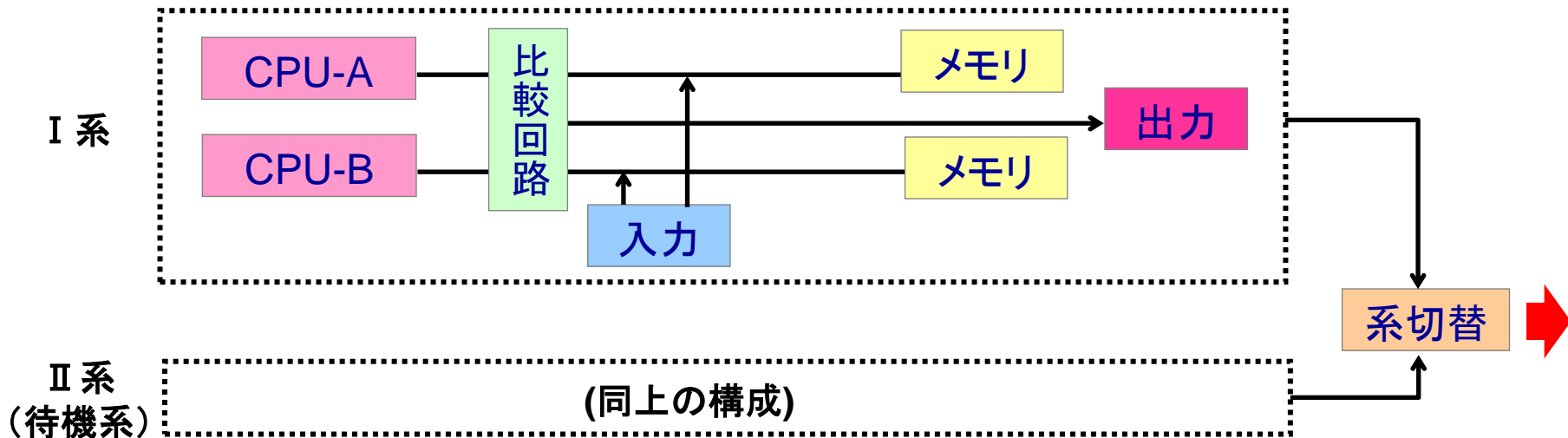


- 少なくとも2系の一致で外部出力
- 3系の内、1系故障時には動作継続

➡ 安全性
➡ アベイラビリティ

電子化信号システムの安全性

2重系構成



➤ I系、II系ごとにA系とB系の一致を照合

➔ 安全性

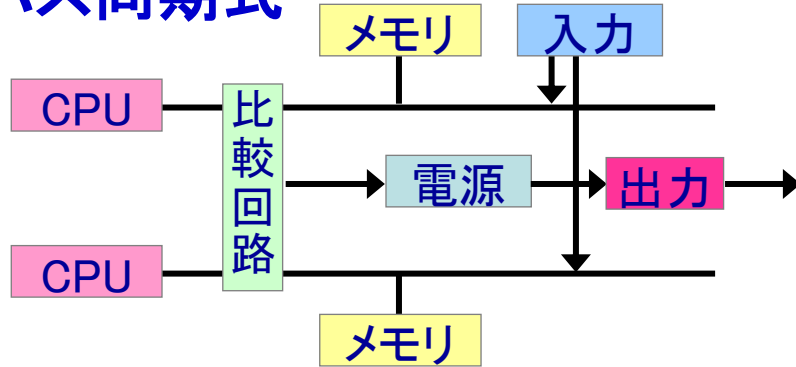
➤ I系(II系)故障時にはII系(I系)に出力系を切替

➔ アベイラビリティ

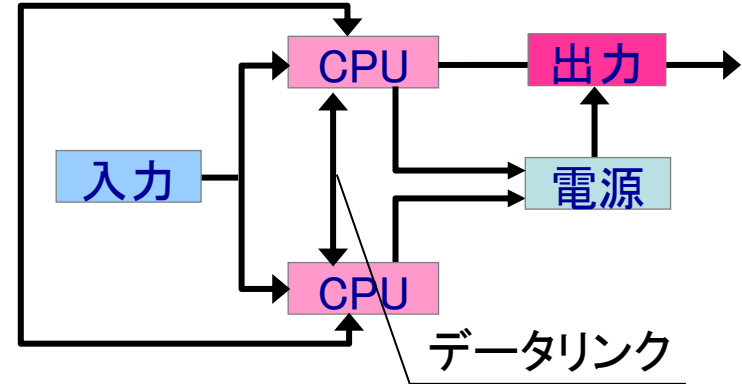
え

電子化信号システムの安全性

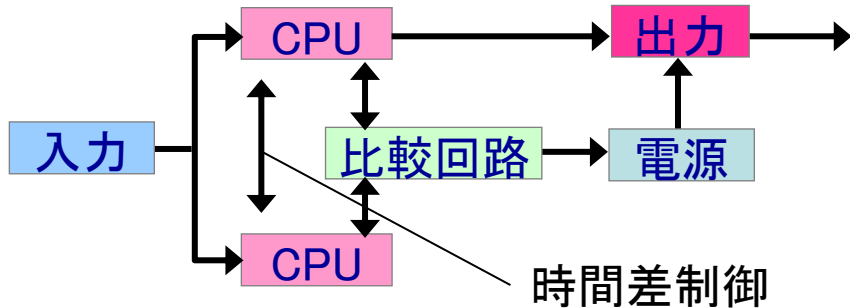
バス同期式



プログラム同期式

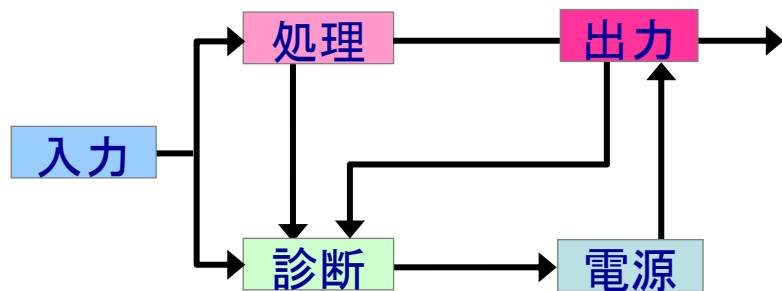


位相差同期式

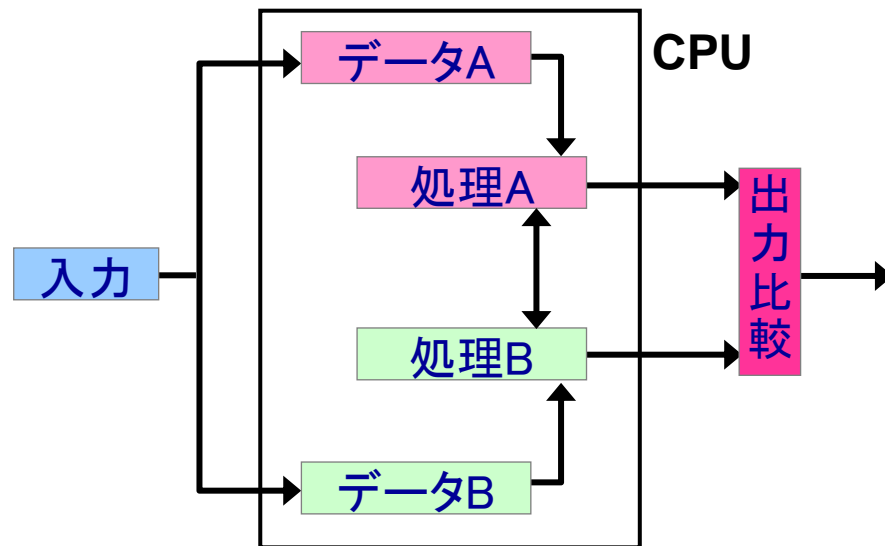


電子化信号システムの安全性

符号化プロセッサ



ソフトウェアダイバーシティ



フェールセーフの要素技術

ハードウェアの基本要件(1)

- 使用部品の**信頼性**が十分高い
- 同種環境での**実績ある素子**を使用する(そうでない場合は十分な試験を実施)
- 故障モードを**明確化**する
- 故障の**速やかな検出**
- 常時使用しない部位、診断回路自身も含めた**積極的な故障診断**(故障潜在化の回避)

フェールセーフの要素技術

ハードウェアの基本要件(2)

- ROM/RAMの診断、RAMの誤書換え防護
- 伝送:冗長符号の使用、十分に小さい見逃し誤り、情報更新の確認
- 誤り検出時: 確実な安全側制御、故障系の切離し
- 冗長系を構成する各系の独立性(共通原因故障がないこと)

フェールセーフの要素技術

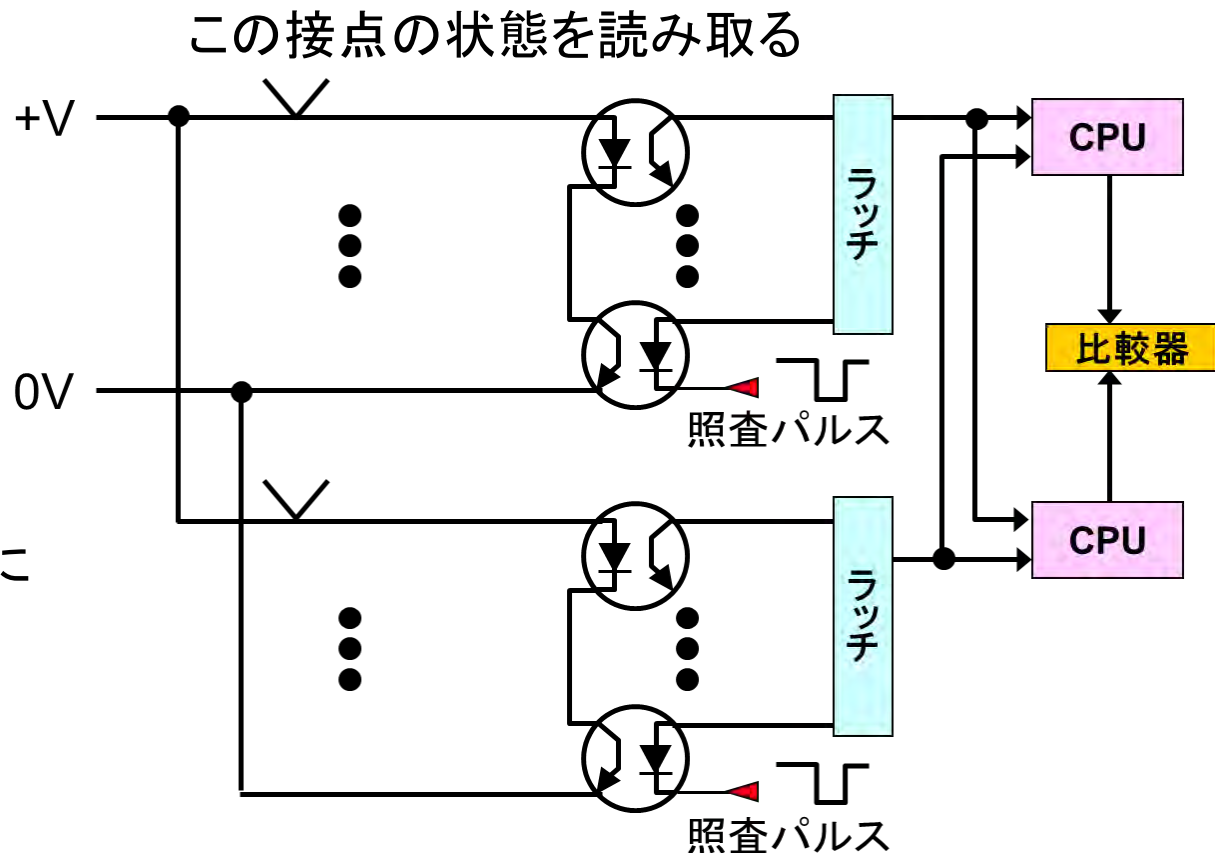
デジタル入力

・入力“0”により安全側制御となるように割付け

⇒“0”固定故障は安全
⇒“1”固定故障を検出できればよい

・照査パルスにより、強制的に“0”を入力させる

⇒“1”固定故障を検出



安全性の考え方

鉄道信号技術の変遷・・・安全を確保する方法(技術)の変遷

機械式信号装置

鉄管やワイヤなどの組み合わせ



電気技術の本格導入:1920年頃～



リレー(継電器)による論理実装

ME(マイクロエレクトロニクス)技術の導入:1985年頃～



同じアプリケーションの装置をコンピュータ化

情報技術の積極的利用:1990年頃～



列車の新しい制御方法などを実現

汎用装置などの活用範囲拡大

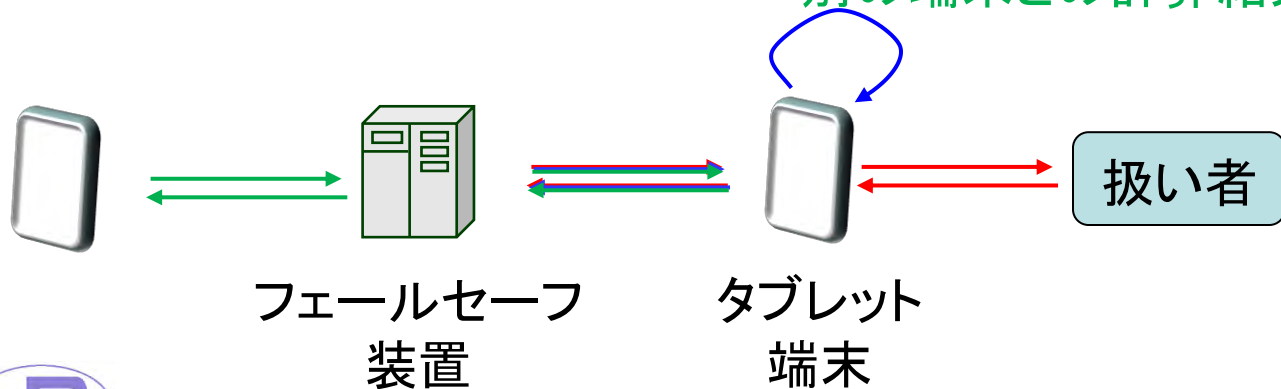


電気技術等を用いた
フェールセーフ技術

安全性技術の新しい方向性

タブレット端末を保安用途に使用したい

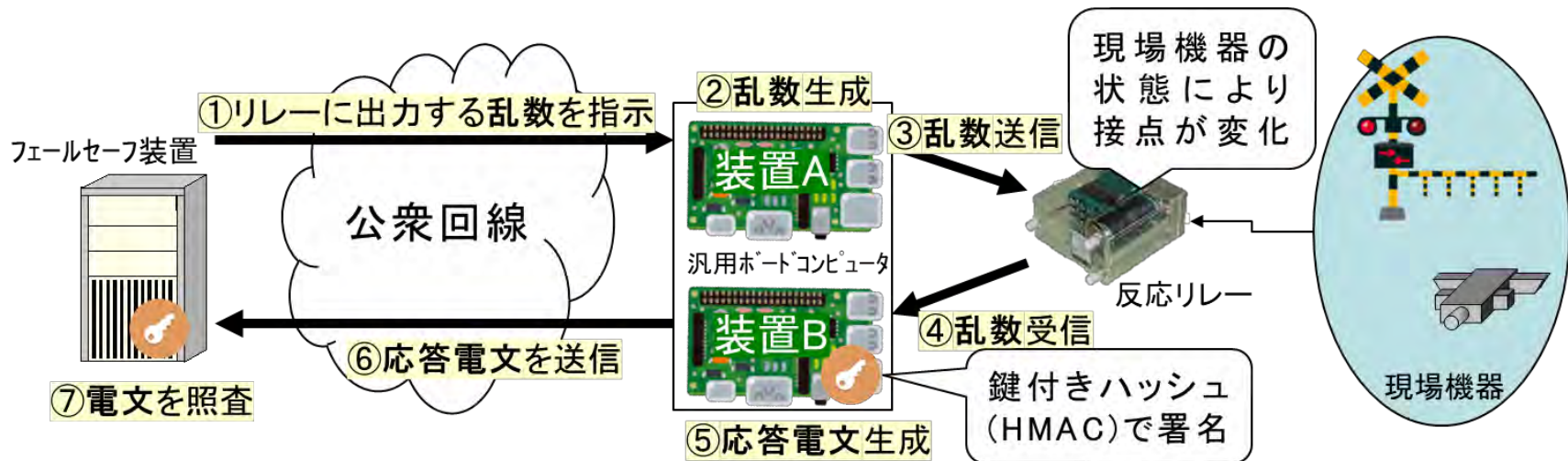
- タブレット端末だけでは安全性は確保できない
 - 表示・入力異常 → 扱い者を含めたフィードバック
 - 警報音の異常(警報不能) → スピーカ・マイクによるフィードバック
 - 計算処理の異常 → 別の端末との計算結果照合



安全性技術の新しい方向性

汎用ボードコンピュータを保安用途に使用したい

- 2台1組とし、フェールセーフ装置で照査
- 暗号技術を適用して公衆回線も利用可能



目次

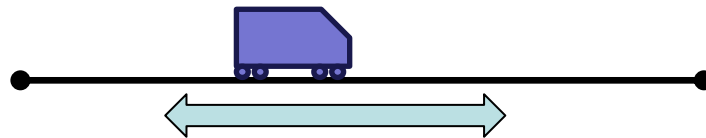
- 鉄道総研のご紹介
- 安全学と安全学研究会
- 鉄道信号分野の安全性技術の紹介
 - 鉄道信号の概要
 - 装置(ハードウェア)としての安全性技術の変遷
 - 列車を制御する方法(ソフトウェア)の変遷

列車を制御する方法の変遷

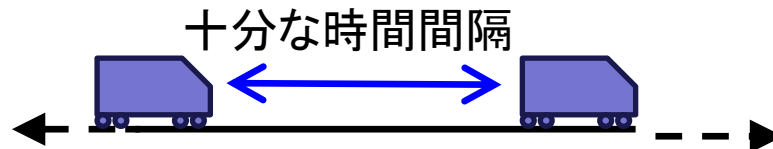
- ①列車同士の追突の防止方法
- ②クローズドループ

列車同士の追突の防止方法の変遷

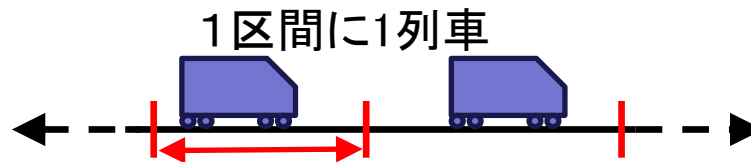
1編成が往復
⇒ そもそも追突しない



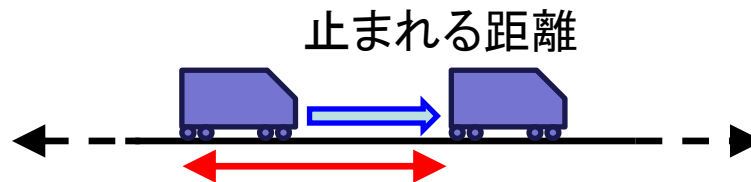
少ない列車が走行
⇒ 時間を管理



多数の列車が走行
⇒ 固定的な区間で管理

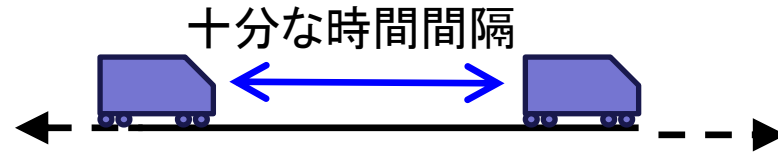


走行状態に合わせて
区間の長さを変化させる



列車同士の衝突の防止方法の変遷

少ない列車が走行
⇒ 時間を管理



時間を計測する機能

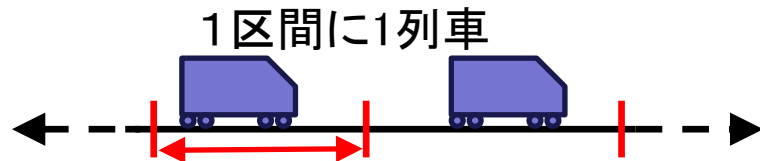
次の区間への進入許可を
指示する機能



ON/OFFの出力

列車同士の衝突の防止方法の変遷

多数の列車が走行
⇒ 固定的な区間で管理



列車の有無を検知する機能 ⇒ ON/OFFの情報

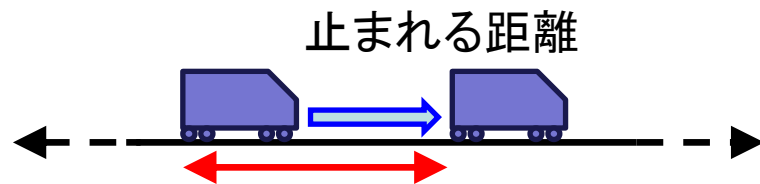
次の区間への進入許可を
指示する機能 ⇒ ON/OFFの出力

※実際にはR/Y/Gのような
多段の出力に拡張

区間の長さはブレーキ性能、
速度(最高速度等)、勾配など
から事前計算し、工事施工

列車同士の衝突の防止方法の変遷

走行状態に合わせて
区間の長さを変化させる

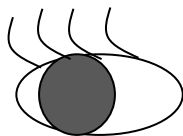


走行可能な範囲の決定(停止すべき位置の決定)

停止できる速度の算出

列車への制御指示方法の変遷

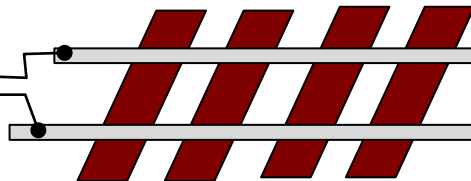
色灯信号機



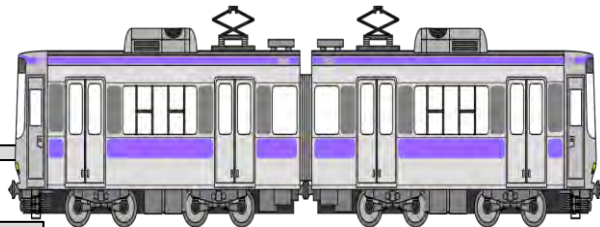
光で情報伝達 ……数種類の情報

電気信号による情報伝送

送信器



受信器



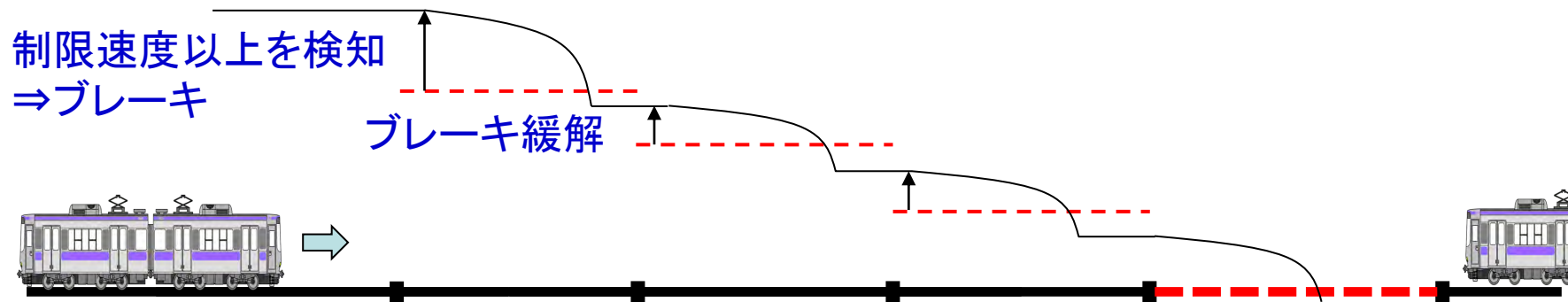
レール伝送(アナログ伝送) ……数種類の情報

レール伝送(デジタル伝送) …… ~100bit

無線伝送 ……数100bit ~

列車への制御指示方法の変遷

数種類の情報で制御 ⇒ 階段上の制限速度により停止まで制御

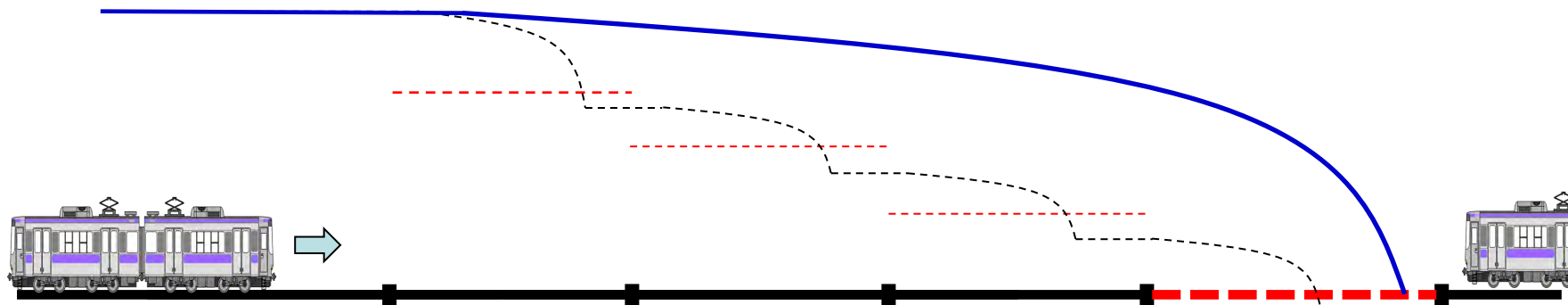


その時々での時点での制限速度を指示

- 情報が途絶すると、安全が確認できない
- 車両性能(ブレーキ性能等)を加味した制御は困難(非効率)
- 区間ごとの余裕距離が必要となるので列車間隔を短くできない

列車への制御指示方法の変遷

数10bit以上の情報で制御 ⇒ 停止までの連続的な制限速度で制御

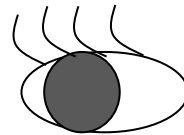


「停止すべき位置」あるいは「停止すべき位置までの距離」を指示

- 情報が途絶しても、停止すべき位置までの安全は確保(信号の範囲)
- 車両側にデータベースを持たせることにより、車両性能や勾配などの条件に応じた制御が可能
- 区間ごとの余裕が不要となるので列車間隔を短くできる

クローズドループ以前の考え方

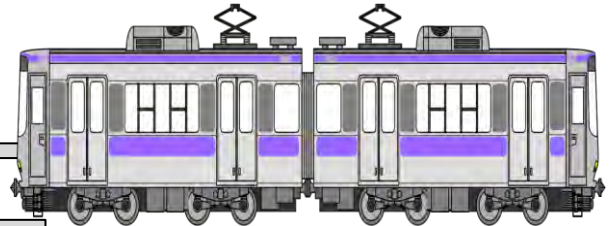
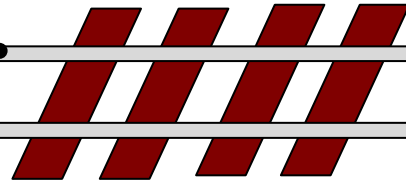
色灯信号機



光で情報伝達

レールによる
伝送

送信器



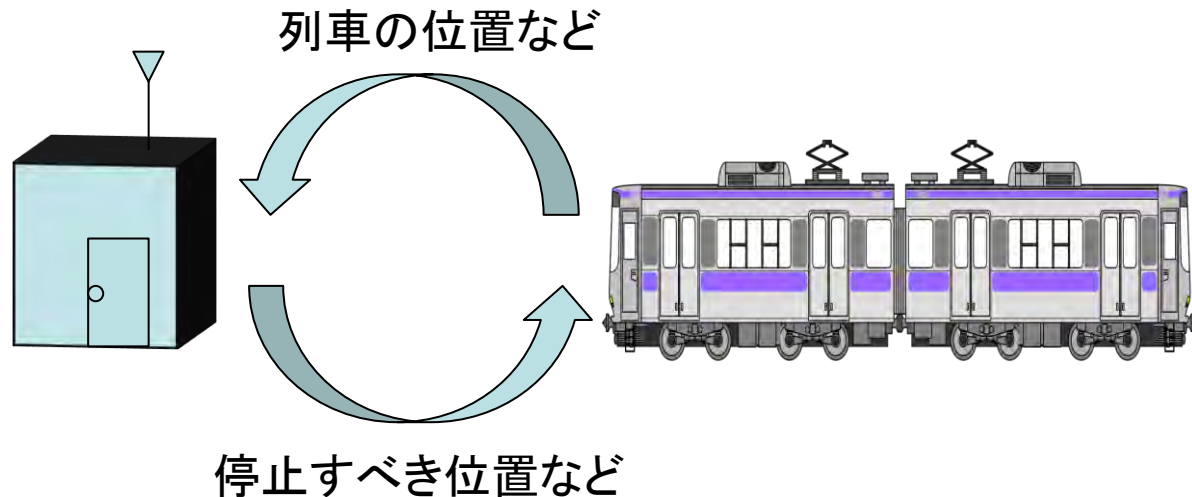
受信器



電気信号で情報伝達

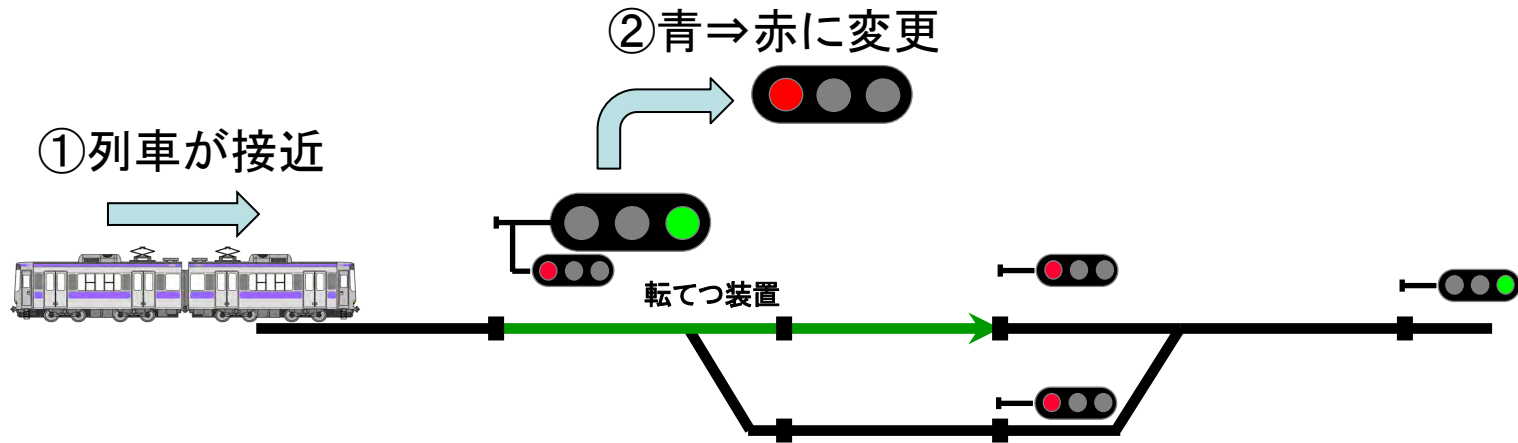
- ・受信したことを返信する機能(媒体・手段)がなかった
- ・正しい情報を受けとれなかった場合は、停止の指示と判断・制御
⇒ これにより安全を確保

クローズドループ



- ・安全性向上・・・通信相手が正常に動作していることを確認しながら制御
- ・効率的な制御・・・列車の走行状態等に応じた制御指示を行うことも可能

効率的な制御の例



③(現状) 赤信号までに停止できるか、停止したかを判断できない
⇒ 一定時間が経過するまでは、転てつ装置を固定したままにする

③(新) クローズドループで停止可否、走行／停止状態を把握可能
⇒ 一定時間が経過しなくても、安全が確認できれば、次の制御を実行できる
(安全性向上・運行効率の向上)

まとめ

- 安全学と安全学研究会
 - ある程度知見がまとまった段階で発表等
- 鉄道信号分野の安全性技術の紹介
 - フェールセーフを原則として、技術の進歩に応じて実装方法(安全確保方法)を進化させてきた
 - 伝送可能な情報量の増大に応じて、列車を制御する方法を進化させてきた
 - ⇒ 安全性向上、効率的な制御