日本大学生産工学部　鉄道工学リサーチ・センター
特別シンポジウム
「国際協調による鉄道安全性向上の取り組み」

鉄道の次世代安全性（Safety 2.0の視点から）

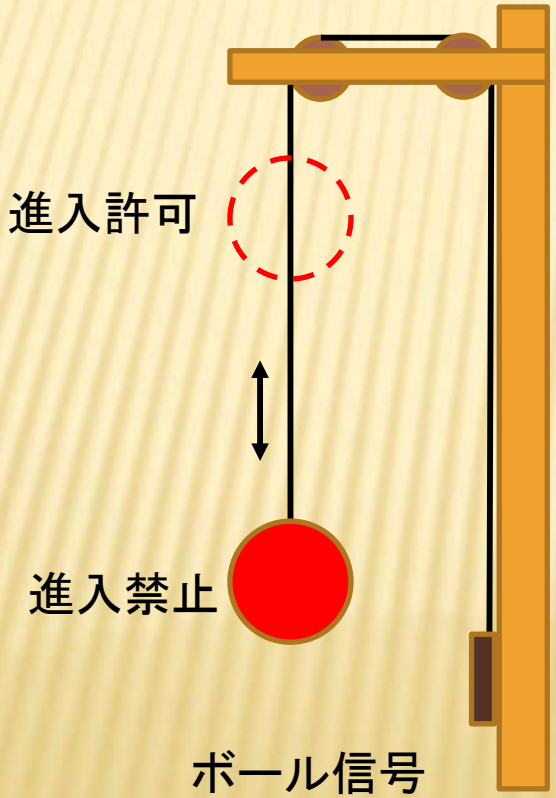
日本大学　名誉教授
東京大学大学院 新領域創成科学研究科
客員共同研究員
工学博士　中村　英夫

安全性を損なうリスク要因

- 人間の過誤
- 環境の変化
- ものの故障
  - ハードウェア故障
  - ソフトウェアバグ
- インタフェースの齟齬
- 故意の外乱

故障時の安全に配慮

1837：グレート・ウェスタン鉄道「ボール信号機」
レディング駅に設置



夜間は鯨油によるランプ

見えないときは停止

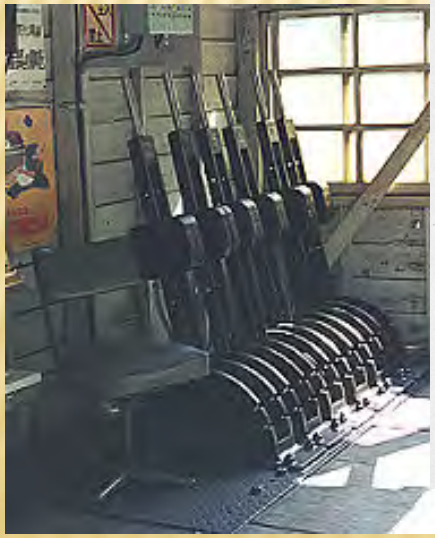
フェールセーフの原理

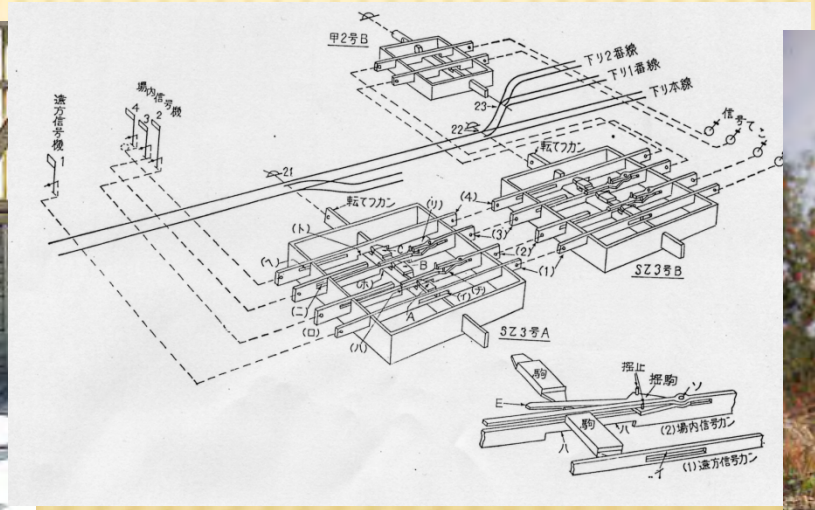
機械式時代：人間の過誤

- 信号機と転てつ機の直接的連動

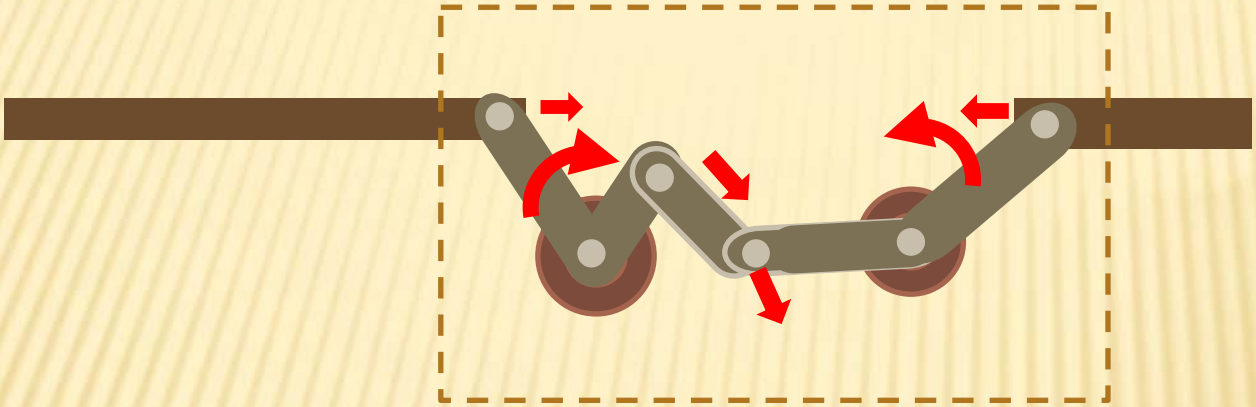
  人力による制御

  信号機と転てつ器の関係のチェック
  駒の切り欠きの勘合で安全を確認



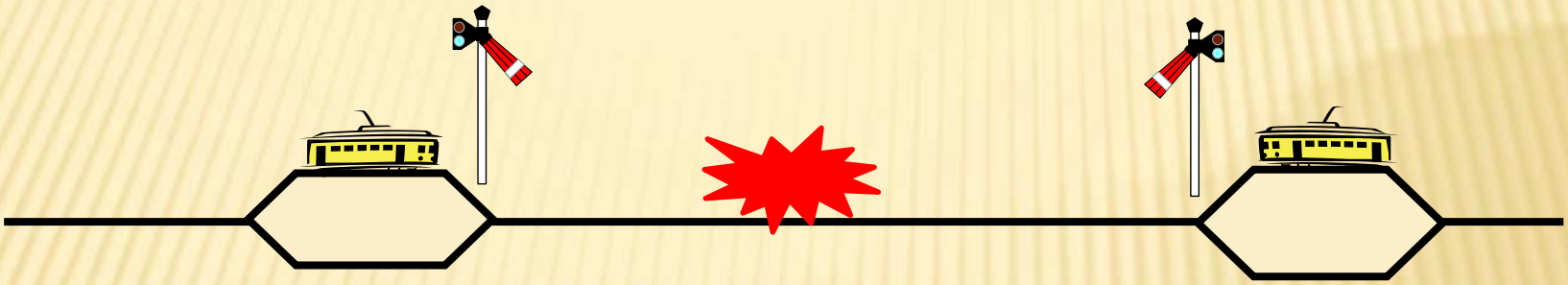


機械式時代　熱変動に対する対応



pipe compensator

構内信号機と転轍機はチェックOKでも



両駅からの出発に対し排他制御が必要

誤って出発許可

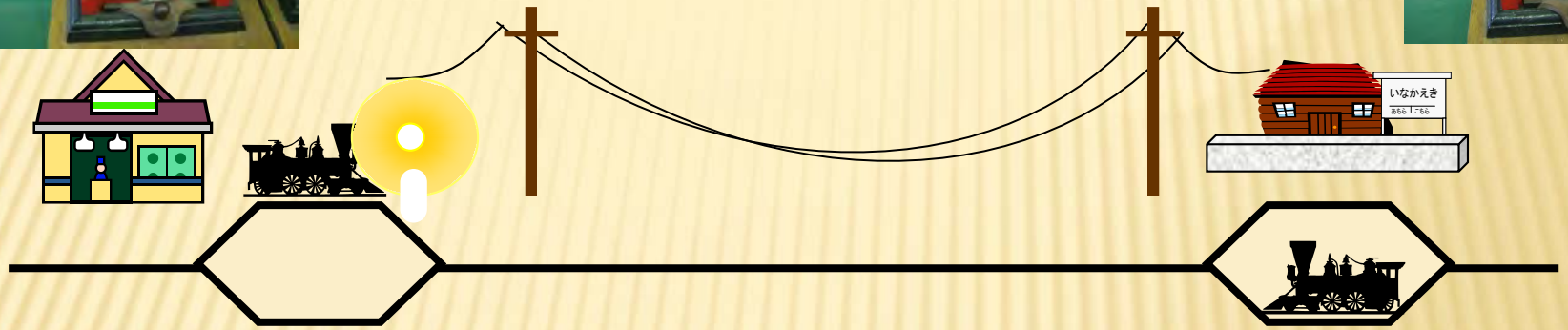
信号が停止なのに誤って出発

間違わないよう意識を高くもて

SAFETY 0,0

単線区間の安全

タブレットをやりとり



同一方向に連続して運転させるときには着駅でタブレットを納めて，両駅の駅長の共同作業により出発駅から取り出す。

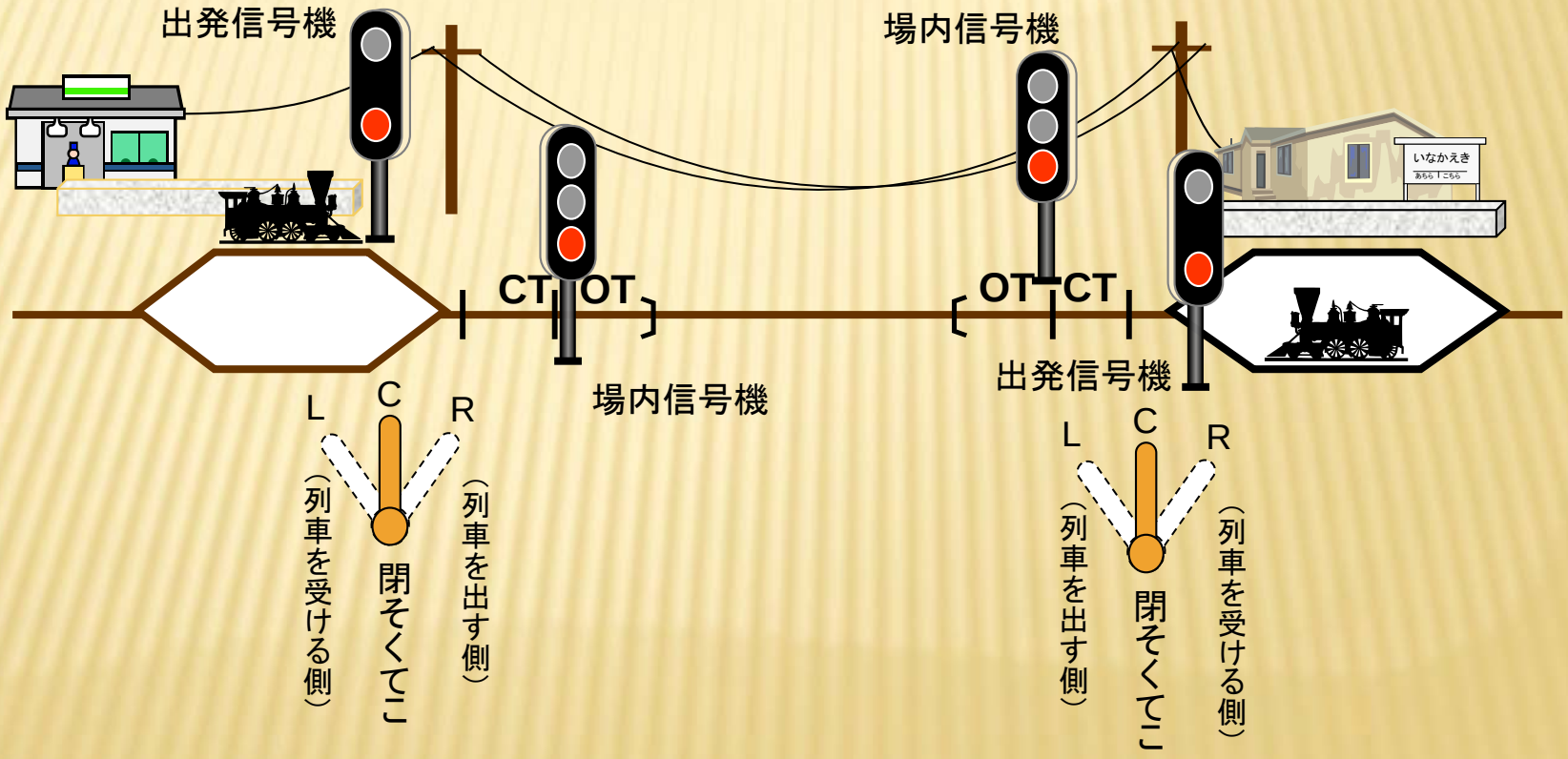
駅間で異なるタブレット

7

運転方向と進路設定を一体化：連査閉塞

＜仕組み＞

駅間の軌道回路に代わり、CTとOTの組合せで駅間に列車がいないことを検知する。取扱いは、連動閉そくと同じ。運転士は信号現示を見て出発すればよい。

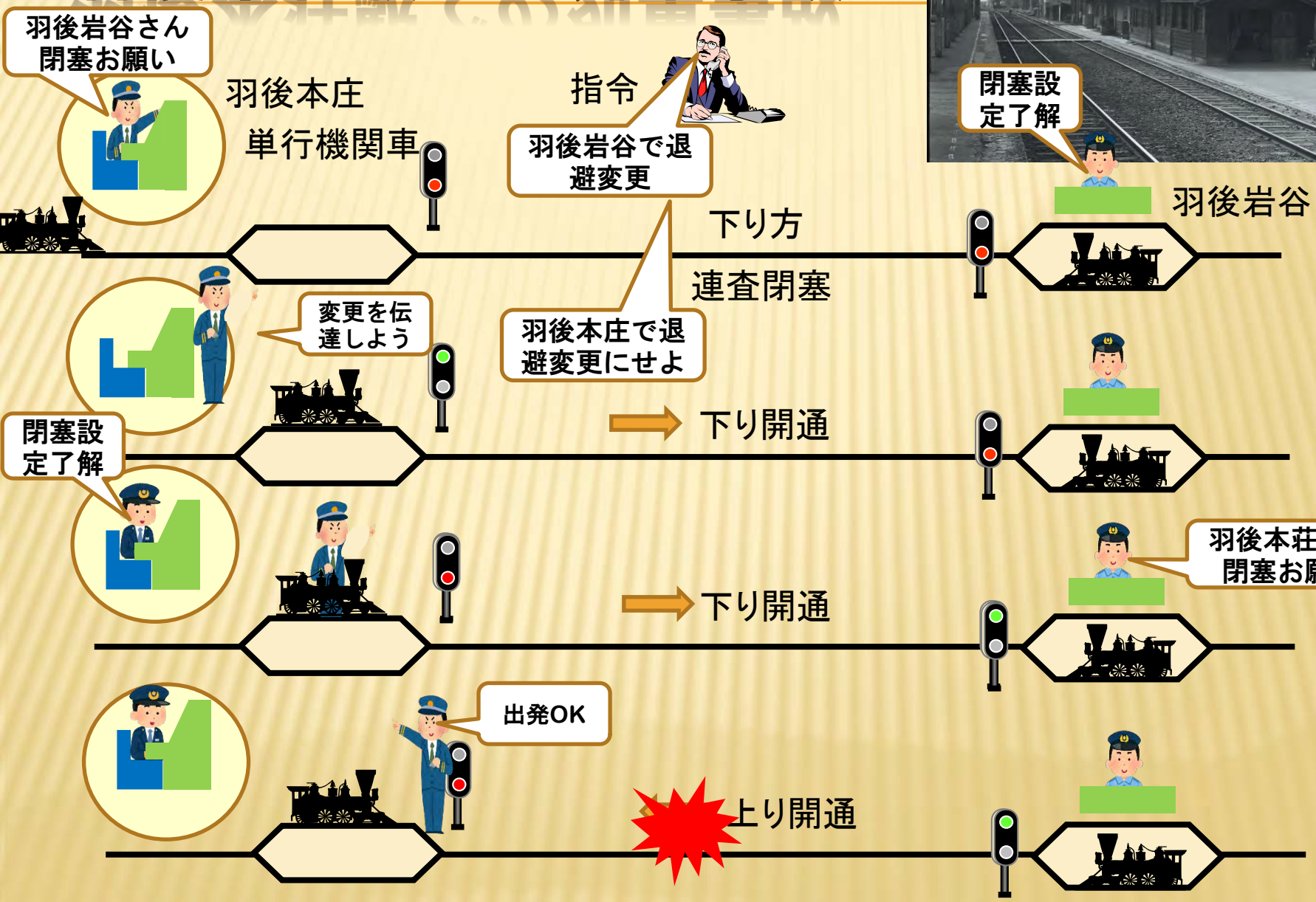


羽後本荘駅での列車事故

発生日: 1962年（昭和37年）11月29日

① 事故当日、下り単行機関車は、羽後本荘駅に約1時間遅延して到着していた。
② **指令変更により羽後岩谷駅で行き違える**こととなった。
③ 両駅で同区間の閉塞を施行（**羽後本荘駅側出発信号機が進行（青）を現示**）。
　助役が単行機関車の機関士に変更内容を伝達に出向く
④ 上り貨物列車、羽後岩谷駅に定時到着
⑤ 下り単行蒸気機関車は羽後本荘駅発車準備にまだ時間がかかる状態
⑥ **輸送指令は、「羽後本荘駅での行き違い」に変更を両駅に指令**
⑦ 羽後岩谷駅は閉塞打合を依頼、羽後本荘駅の信号掛との間で連査閉塞器を操作
⑧ これにより、**羽後岩谷駅の出発信号機が進行を現示**、上り貨物列車が発車
⑨ 羽後本荘駅の助役は、出発信号機が停止になったことを確認せずに出発合図
⑩ **両駅の中間部付近で正面衝突**

羽後本荘駅での列車事故



注意力のみの装置の限界

- さまざまな工夫により安全の仕組が高度化
  人間の過誤が事故を引き起こす

  注意力による事故防止：Safety0.0
- 人間の錯誤による事故を防止する取組み
- ATS-S形（国鉄1966年全国に設置完了）

  SAFETY1.0への移行
- ATS-S形の弱点を突いた事故が発生
- 安全を守る仕組みの充実を

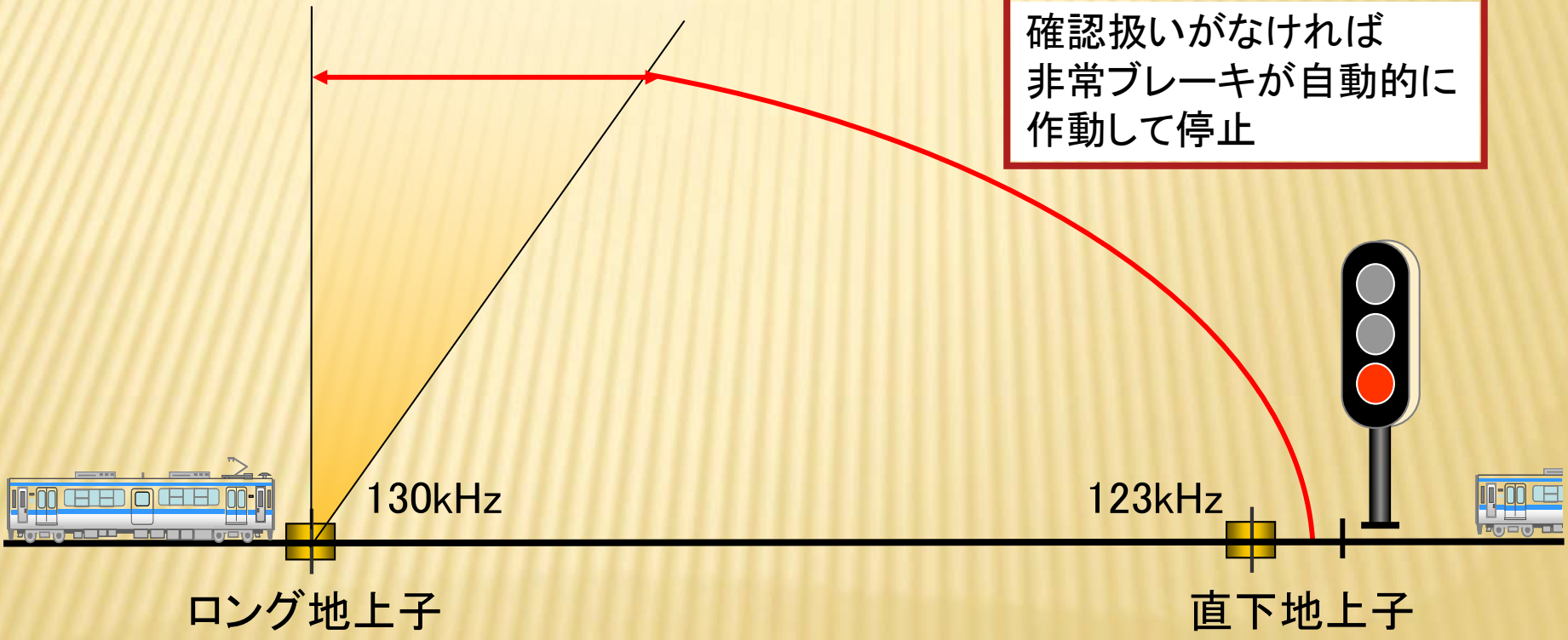
  シーケンス論理による高度化

ATS-S形の機能

警報ブザー鳴動　→　5秒間の間に確認扱い
→ブザーがチャイムに代わり警報持続

地上子通過

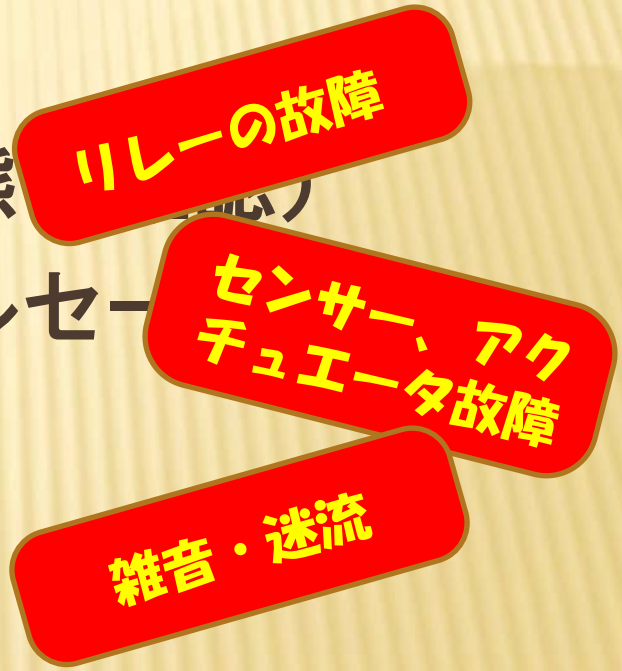
確認扱いがなければ
非常ブレーキが自動的に
作動して停止



出発信号や場内信号などの絶対信号機
など必要な信号機の直下に設置された

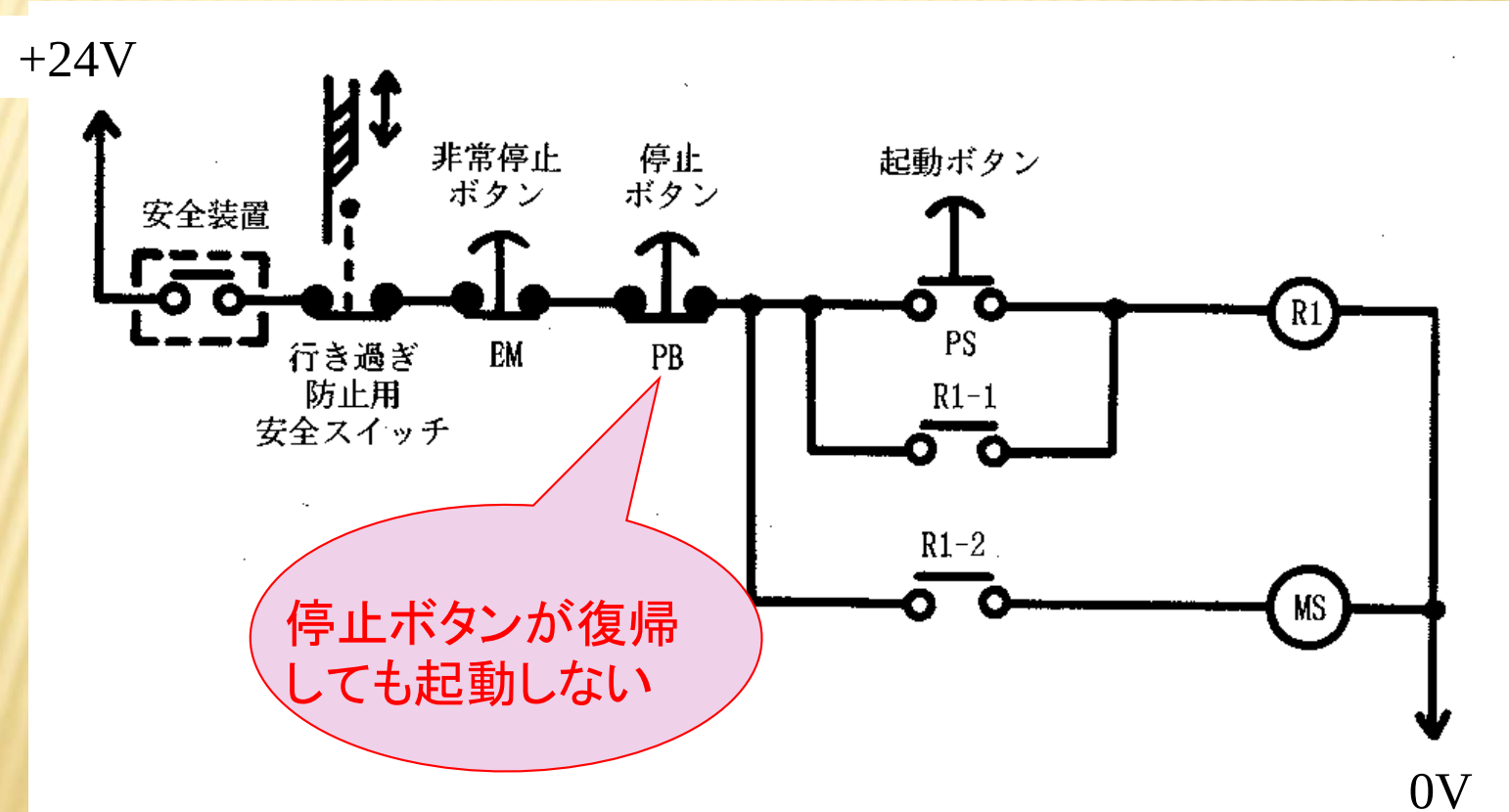
シーケンス論理による安全機能の充実

- センサー（安全への配慮）
- アクチュエータ（動作状態[illegible]）
- シーケンス回路をフェールセー[illegible]
- 論理による安全機能拡充
  - 再起動防止回路
  - 接近鎖錠
- 制御室の配置に自由度が
  - 通信技術による遠隔制御



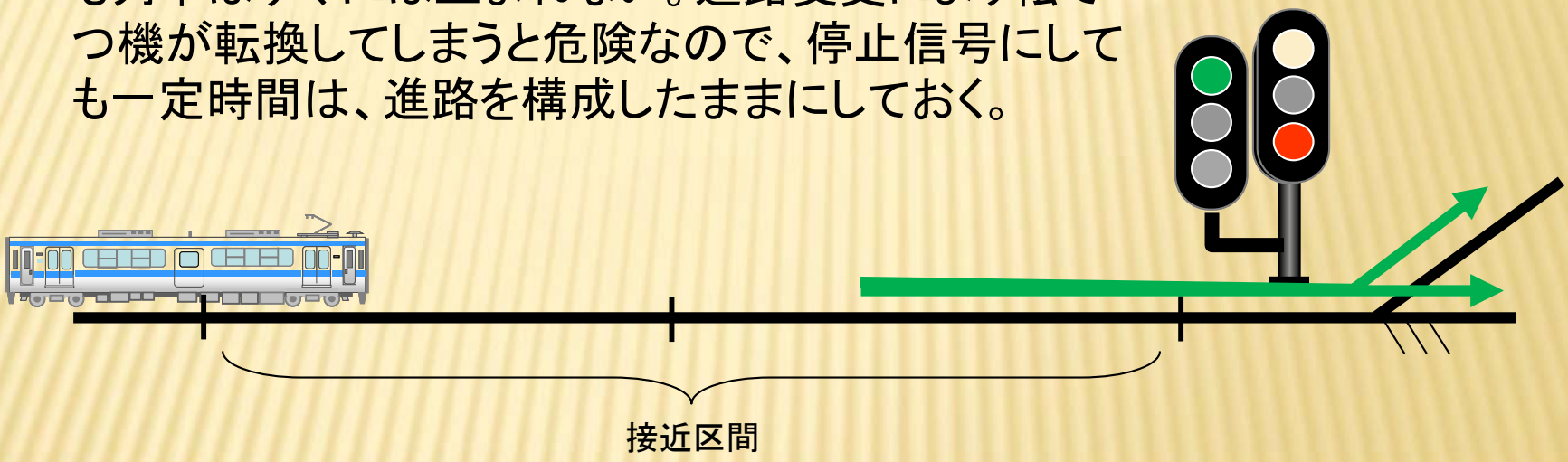
再起動防止回路の例

停止ボタンを押した
→停止ボタンを誤って復帰させたら動き出して事故に



接近鎖錠の例

列車が信号の近くにいるときに、信号機を引戻されても列車はすぐには止まれない。進路変更により転てつ機が転換してしまうと危険なので、停止信号にしても一定時間は、進路を構成したままにしておく。



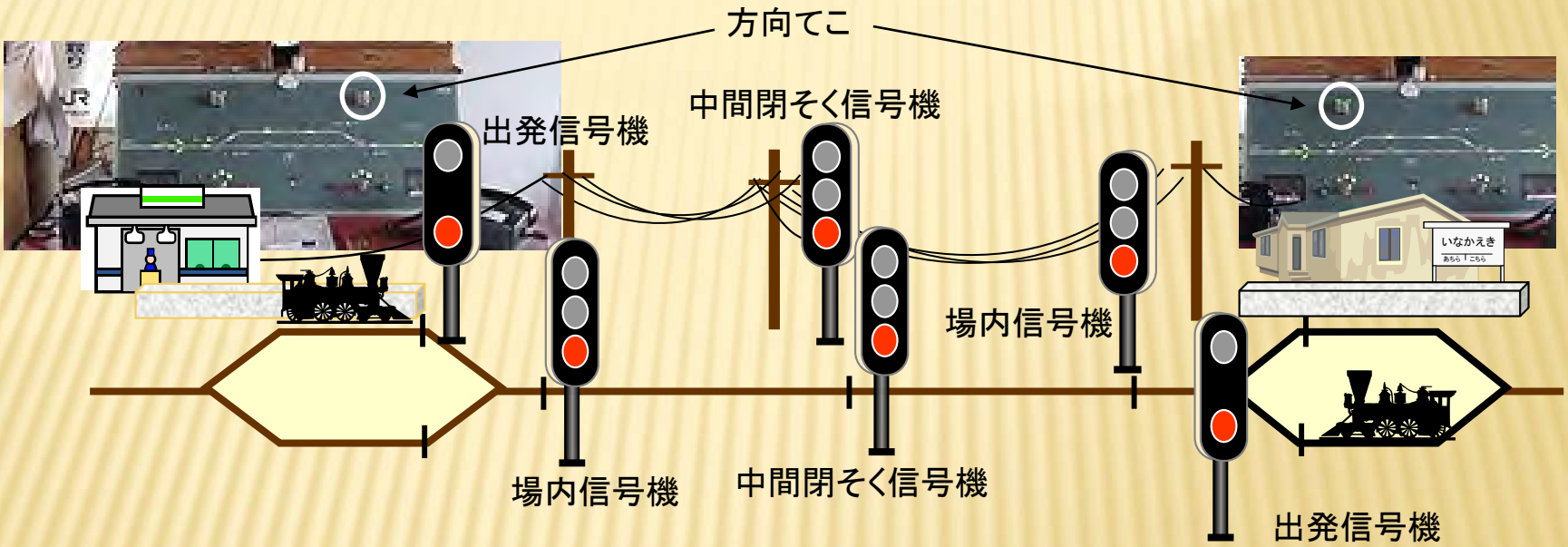
危険な状況を経験したらロジックにより防護策を講じる：産業界ごとに発展・充実化

安全性技術/ノウハウ

単線自動閉そく

＜処理＞

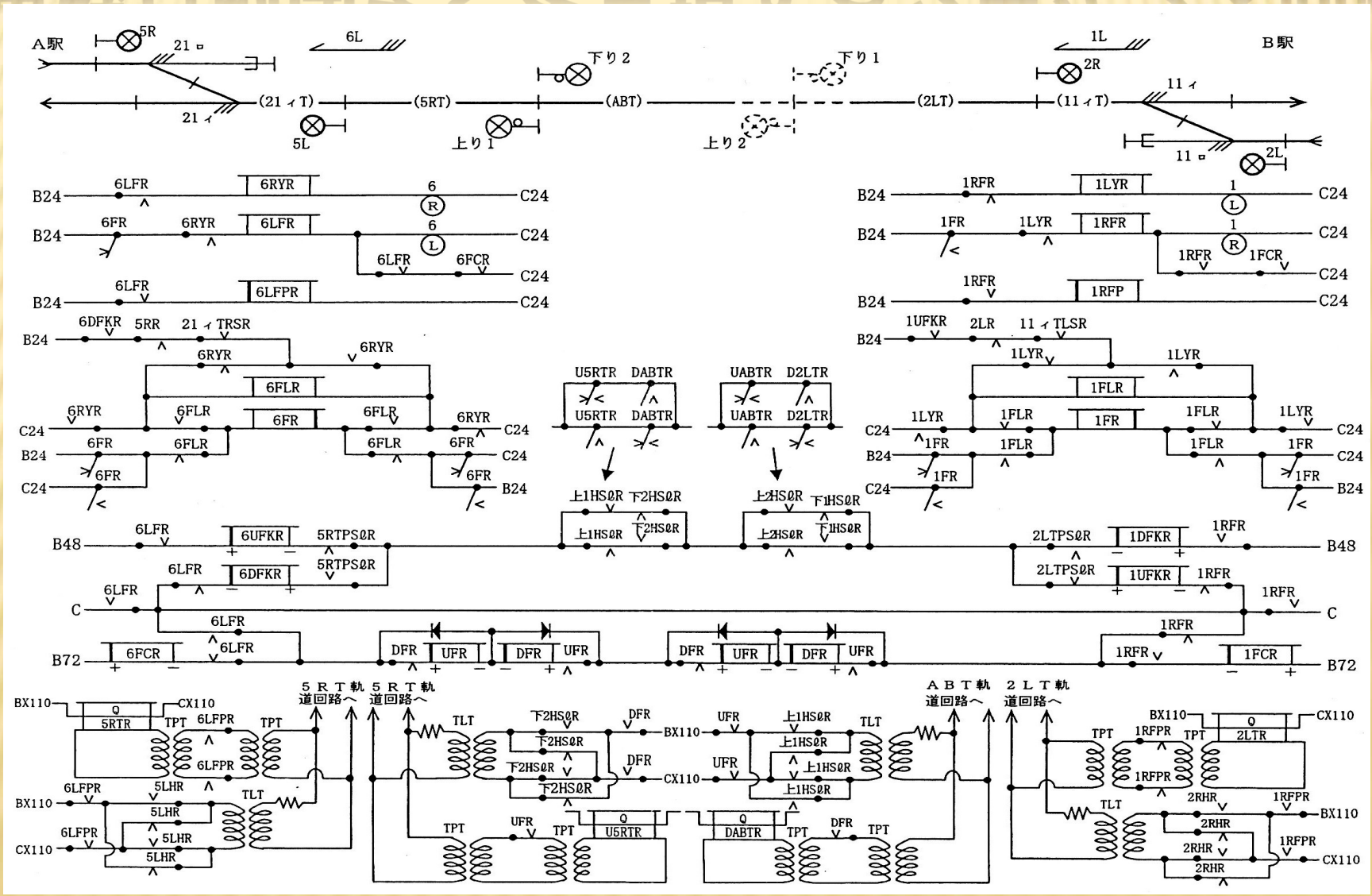
両駅の駅長が協調して運転方向てこを扱い、運転方向を設定。その方向の進路を取ると転てつ機が制御され信号機が進行現示になり、反対方向は停止現示に。



＜特　徴＞

リレーで構成された両駅の装置が両駅の駅長のてこの設定と軌道回路条件をもとに一連のシーケンス処理を遂行。駅間に複数の軌道回路を設けると、続行列車の運転も可能。CTC化時の基本インフラとされた。

単線自動閉そくを実現するシーケンス回路

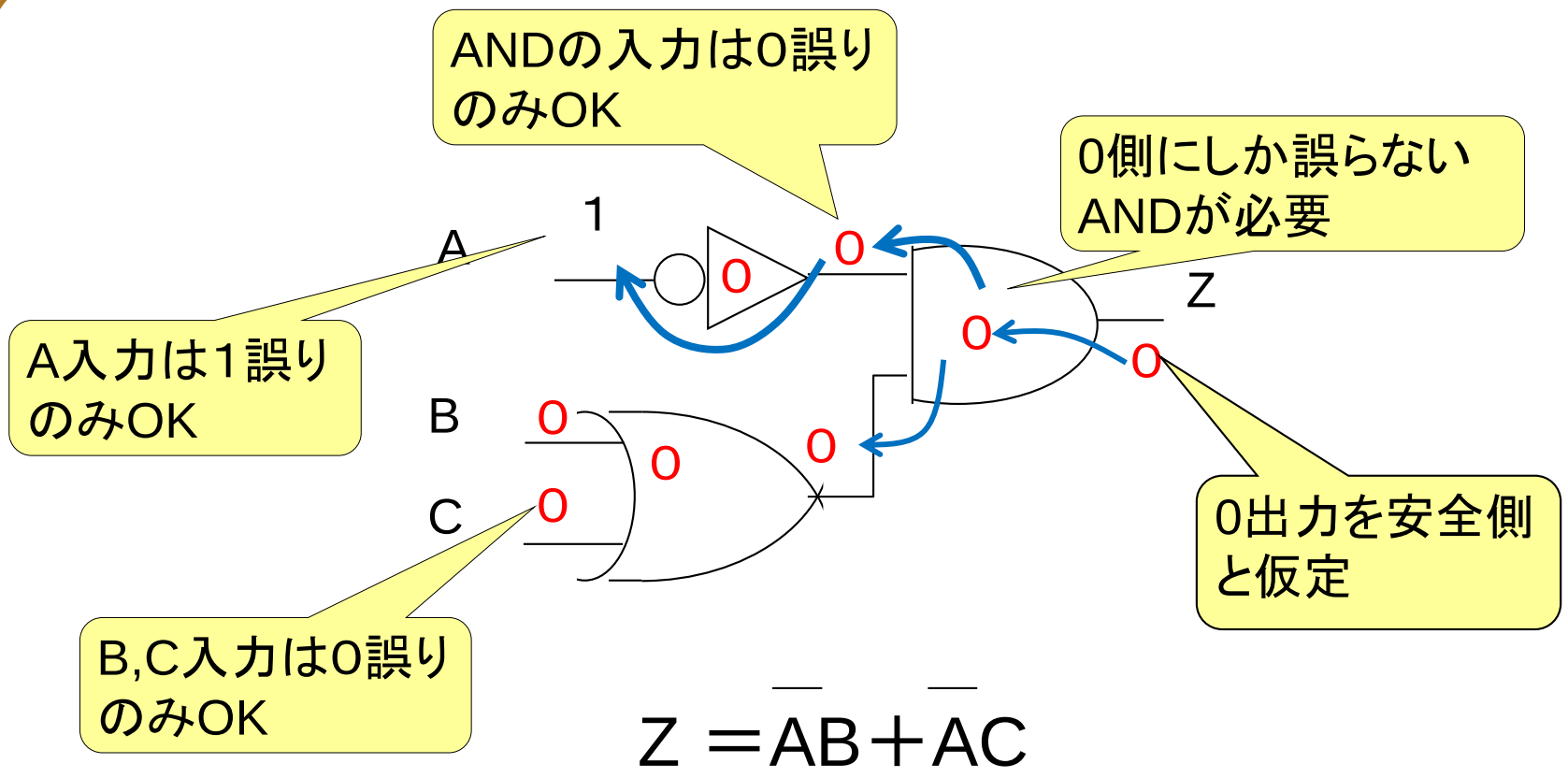


FAIL-SAFE論理の解明

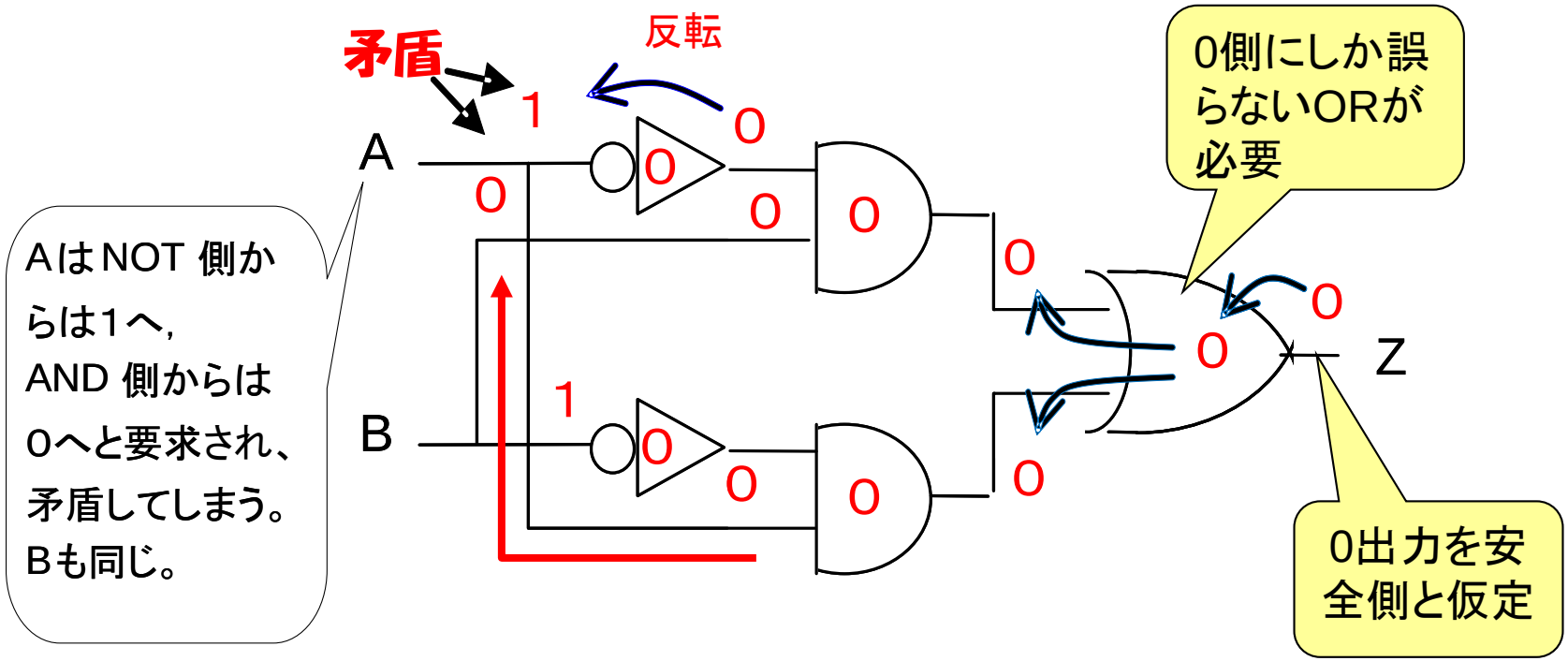
- 経験工学的に進歩してきたFail-Safeなシーケンス回路
- 回路レベルでのFail-Safeは日本で解明された
  - 鉄道の継電連動装置のFail-Safeの仕組みにメスが
  - 1965年にFail-Safe論理系の研究が発表されるや学会レベルで多くの研究が開花
  - 当時、Fail-Safe論理系の研究は日本の独壇場

SAFETY 1.0の確実化

フェールセーフにできる回路



フェールセーフにできない回路



$$Z=\overline{A}B+\overline{A}B$$

FAIL-SAFE論理系の構成法

- 回路がユネイト（単調）であるなら、非対称誤り論理素子を用いて、たかだか一重系でFail-Safeな回路が構成できる。

- ユネイトでない回路をいかにして･･･
- 対象誤り論理素子では･･･
- 非対称誤り論理素子はどうやって･･･

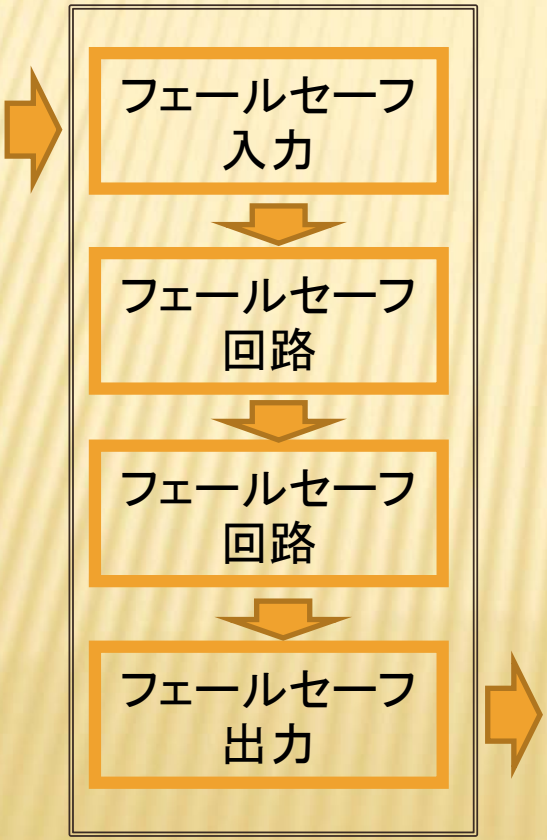
渡辺，高橋：フェイルセイフ形論理系の一般法，信学全大,72，(1965-11)

フェールセーフ論理系の研究の発展

- ユネイトでない回路のフェールセーフ化
- 対称誤り素子によるフェールセーフ実現法
- ２線式論理回路
- ３値フェールセーフ論理
- 順序回路のフェールセーフ化
- フェールセーフ論理回路の故障診断
- フェールセーフ論理素子の開発
- フェールセーフ論理系とセルフチェッキング回路の関係

論理をFSシーケンサーで実現していた

- この下での安全は、入力、論理、インタフェース、出力の全てをフェールセーフに



シーケンス論理は、ソフトウェアで実現できる。産業界は安全制御分野に利用できるFail Safe Computerの開発に注力。故障に着目したFault tolerance技術が利用された。

シーケンス回路からFAIL SAFE計算機へ

高信頼化とFAULT TOLERANCE

Fault-Avoidance:品質向上（QC)，Zero-Defect運動で故障しない製品を作る
Fault-Tolerance:故障を前提に，システム的に対処

- Fault Tolerant Computing System
- 1980年の国際大会FTCS1980（京都）
  超高信頼化計算機システム
- Fault Tolerance＝耐故障？？
  容錯計算机

W.C.Carter, et al.:Cost effectiveness of self-checking computer design, Dig. Paper, FTCS-7, pp117-123 June 1977.

システム的高信頼化技術 FAULT TOLERANCE

- 故障時の影響が無視できない航空宇宙分野
  大規模社会システム → 故障を前提として機能を維持するシステム的な高信頼化が必要
- 新幹線→信頼性/安全性の両立三重系多数決構成

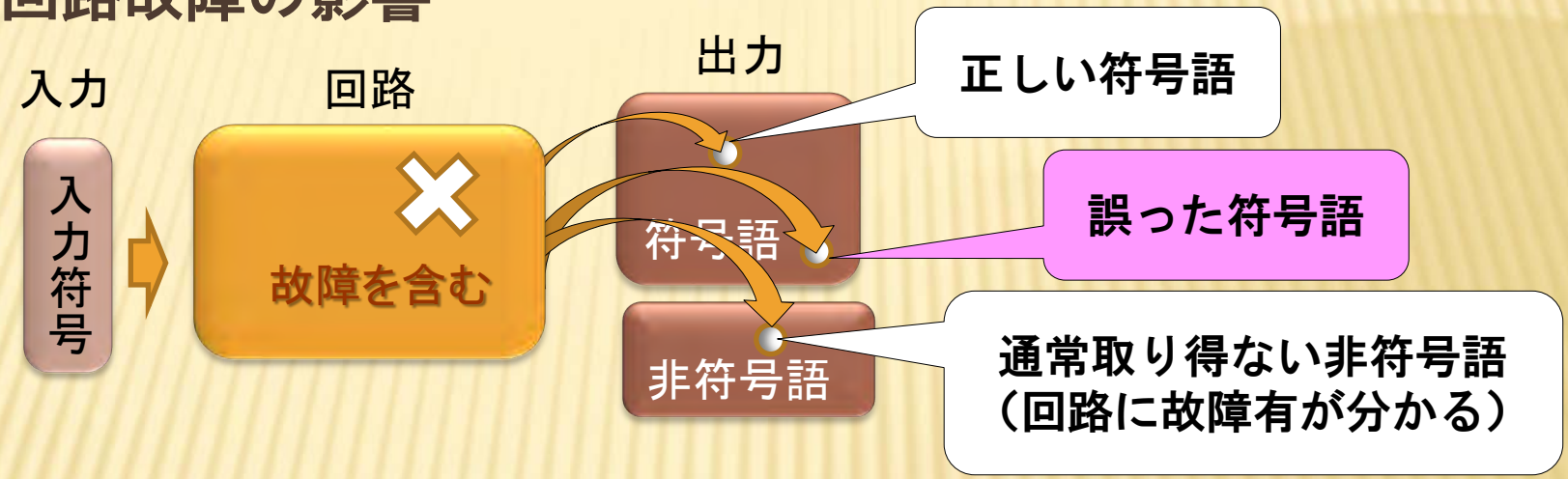
- 1970年代：IEEEは，回路/システムレベルでの高信頼化の研究を活発化→Fault tolerant computing
- フォルトトレランスを売り物にした製品・商品の出現→航空，宇宙産業，金融
  - 手法＝故障時を前提にしたシステム的対策、高信頼化の達成には有効

FAULT TOLERANCEを実現する回路(SCC)

- 通常動作中に故障の存在を検出できる回路
  Self Checking Circuit　(SCC)
- SCCを構成する基本的性質
  - Fault Secure: 回路に故障が発生しても、非符号語を出力するまでは、正しい出力（符号語）を行うことを保証
  - Self Testing:故障があれば通常の処理中に必ず検出される(故障時には通常の入力を与えていれば非符号語が出力される)
  - Code disjoint:誤り(非符号語)入力時には必ず非符号語を出力
- SCCのクラス
  - Totally Self Checking: 回路がFault SecureかつSelf Testing
  - Strongly Fault Secure:多重故障が発生しても故障が検出されるまでは出力が正しい

SELF CHECKING CIRCUIT(SCC)とは

- 回路故障の影響



性質1：符号語なら全て正しい（非符号語をとるまで） Fault secure

性質2：故障すれば教えてくれる（非符号語をとる） Self testing

性質1と性質2を備えた回路 Totally self-checking

W.C.Carter, et al.:Cost effectiveness of self-checking computer design, Dig. Paper, FTCS-7, pp117-123 June 1977.

FAULT TOLERANT SYSTEMの事例

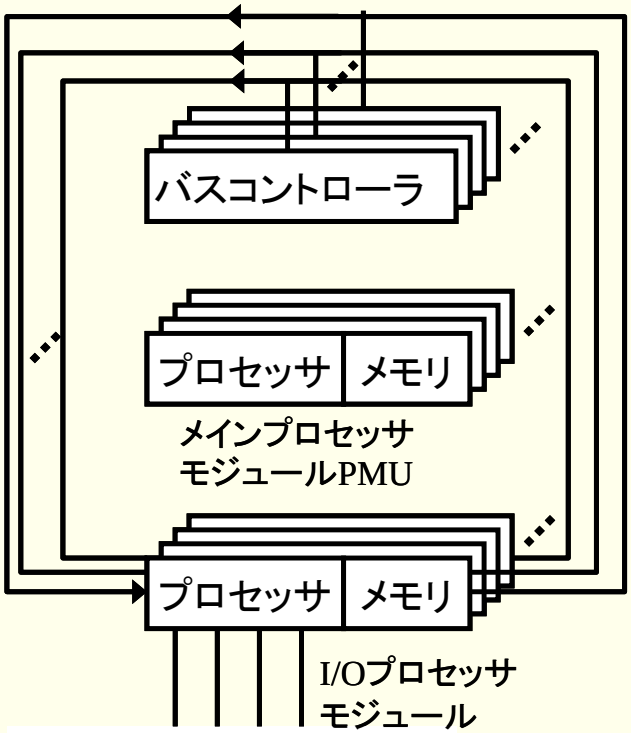
- 多重故障に対しても対応できる概念へ:SFS性
  - 故障が発生し非符号語を取るまでにさらに故障が発生しても、Fault-secure性が保証される
    SFS: Strongly Fault Secure性
  - 非符号語が検出されたときにシステム的に対応すれば、高度な信頼性や安全性が求められるクリティカルなシステムへの応用が可能
  - 鉄道等の保安制御用コンピュータに利用される
- 産業界で要求される高信頼システム
- Self checkingの概念でコンピュータの開発

ST: Self Testing, FS: Fault Secure, TSC: Totally Self Checking,

FAULT TOLERANT COMPUTER SYSTEMの事例

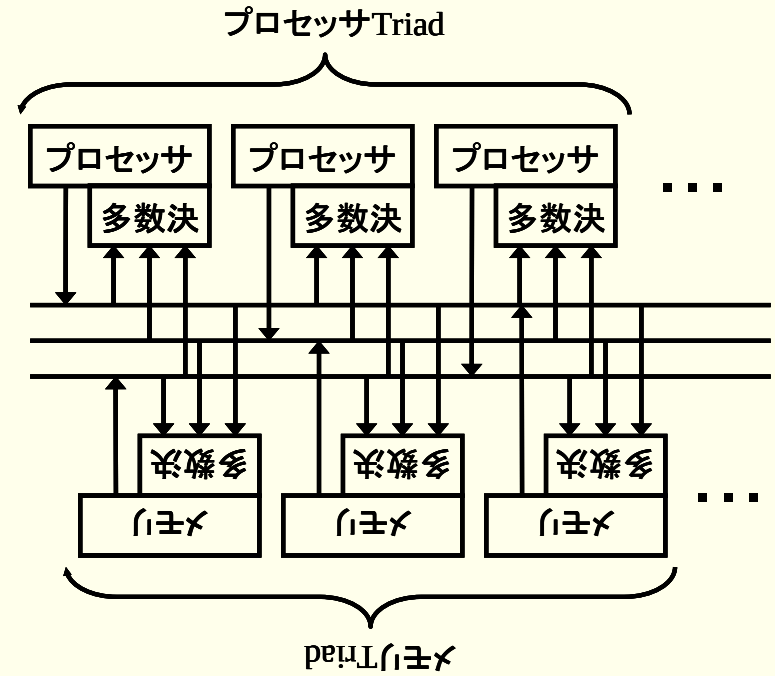
	高稼働率	安全制御	長寿命
1960	ESS		
1970	Tandem Non Stop		STAR FTSC
1980	Stratus/32	FTMP SIFT	
1990		SMILE	

フォールトトレラント計算機システム例



ソフトウェアレベルで同期を取り
多数決処理を行い診断する

図2　SIFTシステム



Triad中のエレメントの故障が多数決により検出された場合には，故障エレメントを外しスペアのエレメントを用いてTriadを再構築する。スペアが無いときには,正常2エレメントはスペアになる。

この診断を行うため,ハードウェアはバスレベルで同期が取られる。

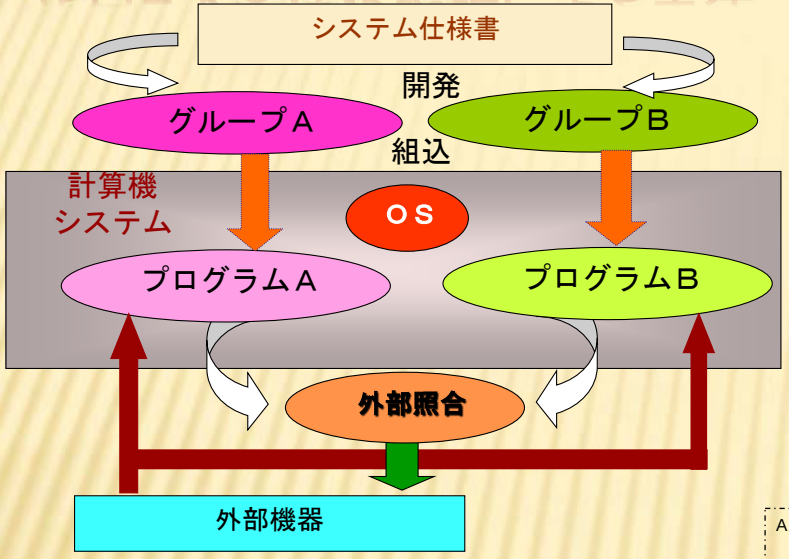
図3　FTMPシステム

多様なフェールセーフ計算機システムの出現

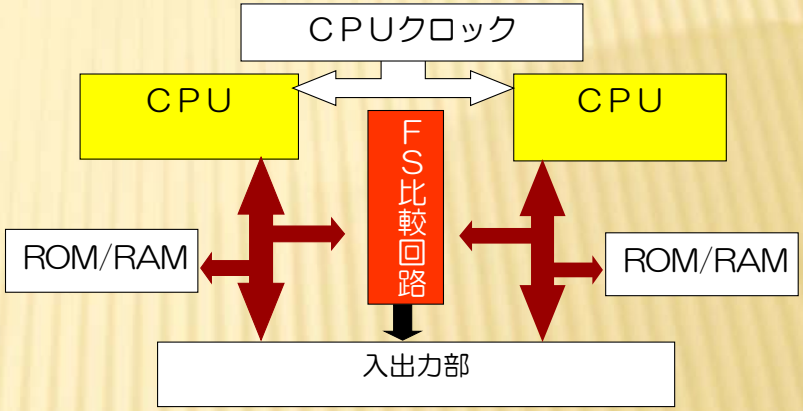
- フェールセーフ論理素子によるフェールセーフ計算機の開発：登戸駅の電子連動装置(1971)
- 出力照合
  - Nーバージョンプログラミング(デザイン・ダイバシティ)
- チェックポイント照合
  - データ・ダイバシティ
- セルフチェッキングの概念による方法
  - 故障検出→安全側に固定
    - バス同期式（ハード多重）

安全制御を目的にした様々な計算機

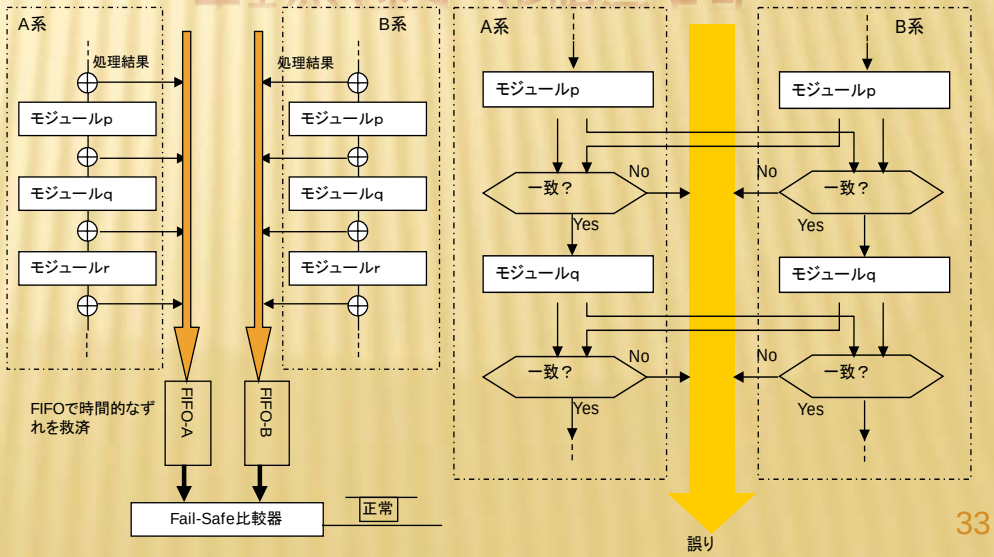
ソフトウェア多様化設計による手法



ハードウェアの密な同期照合方式

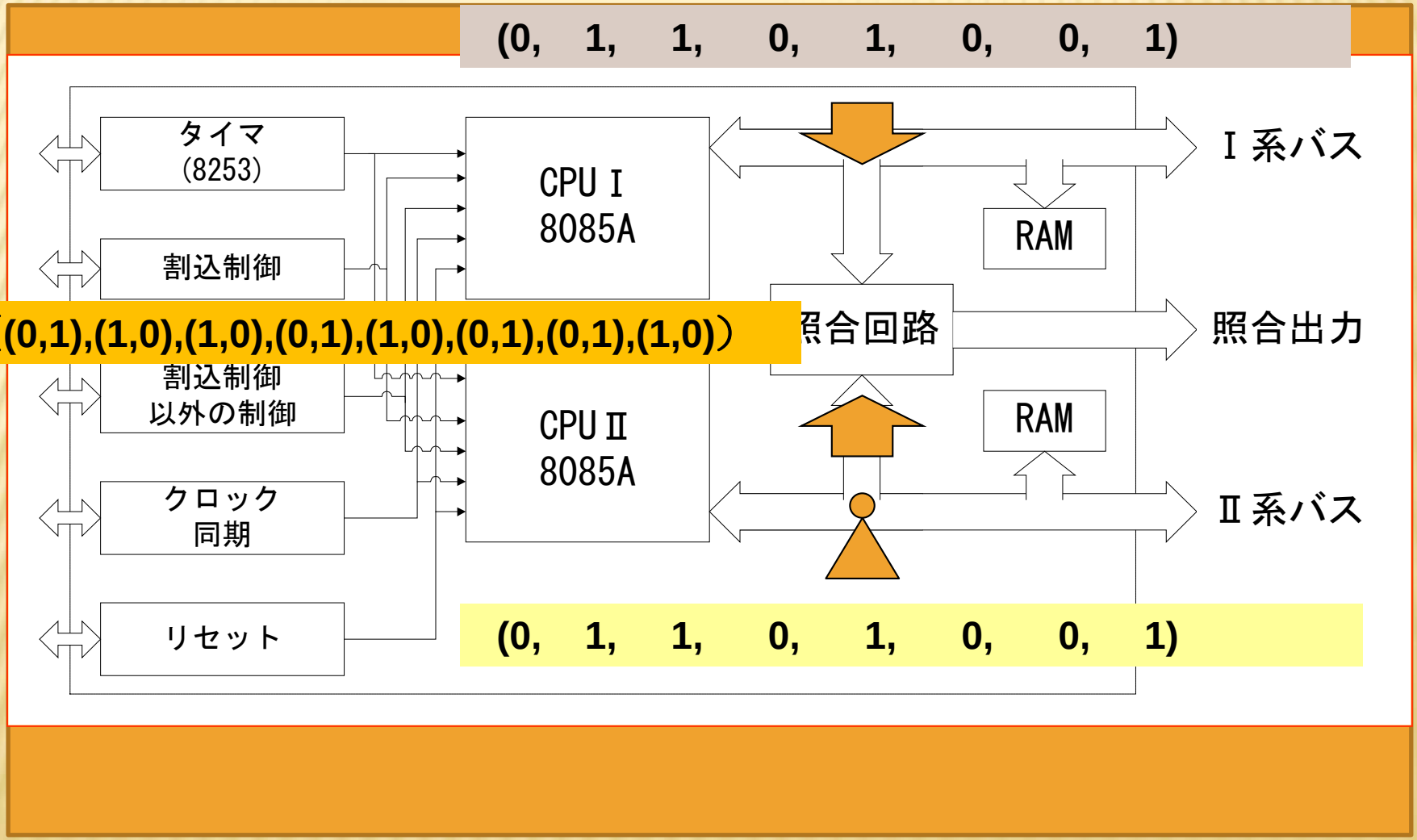


チェックポイント照合方式

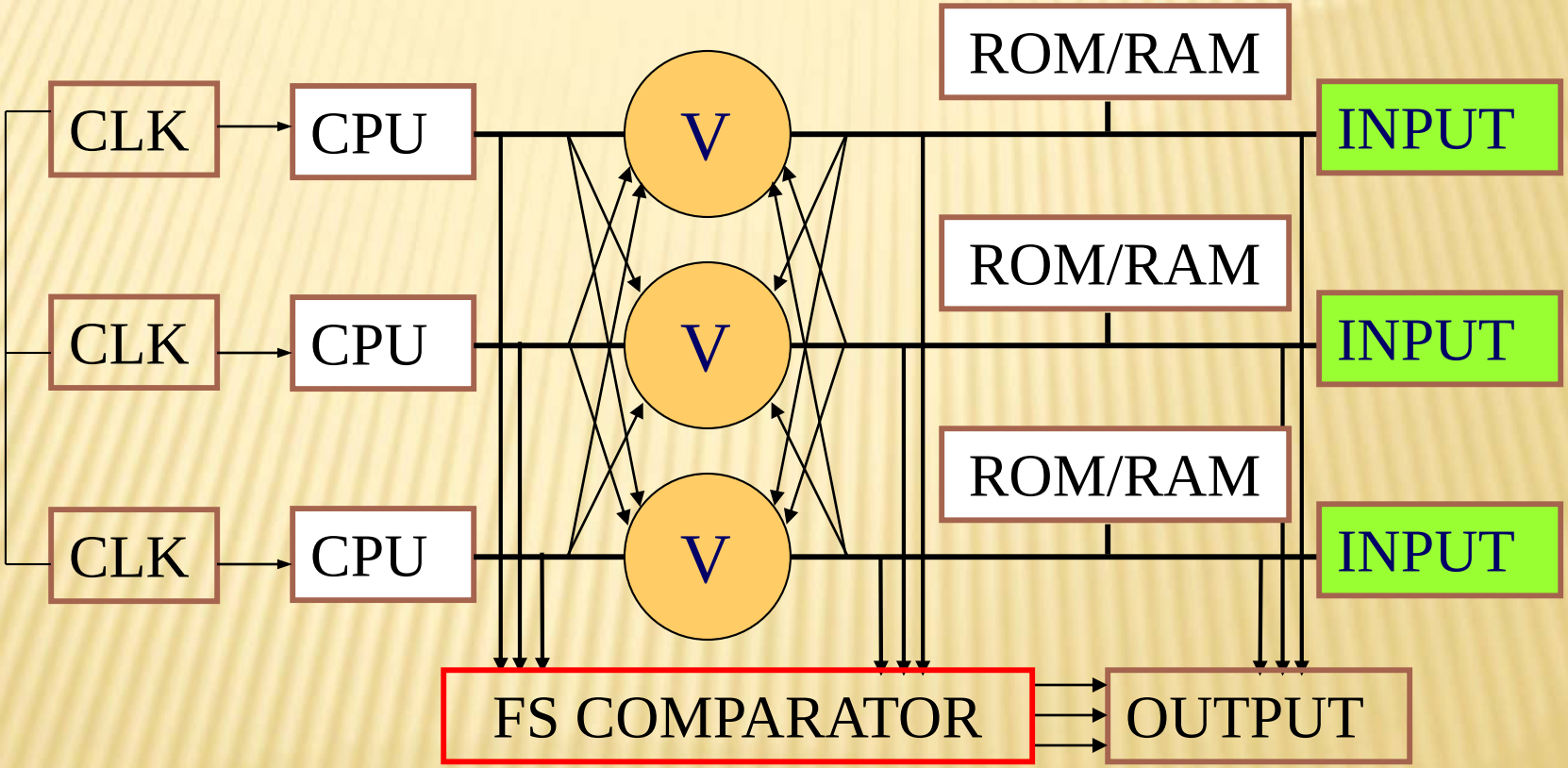


黎明期には相互に優劣が論じられたが、それぞれ安全性上は問題なく稼動

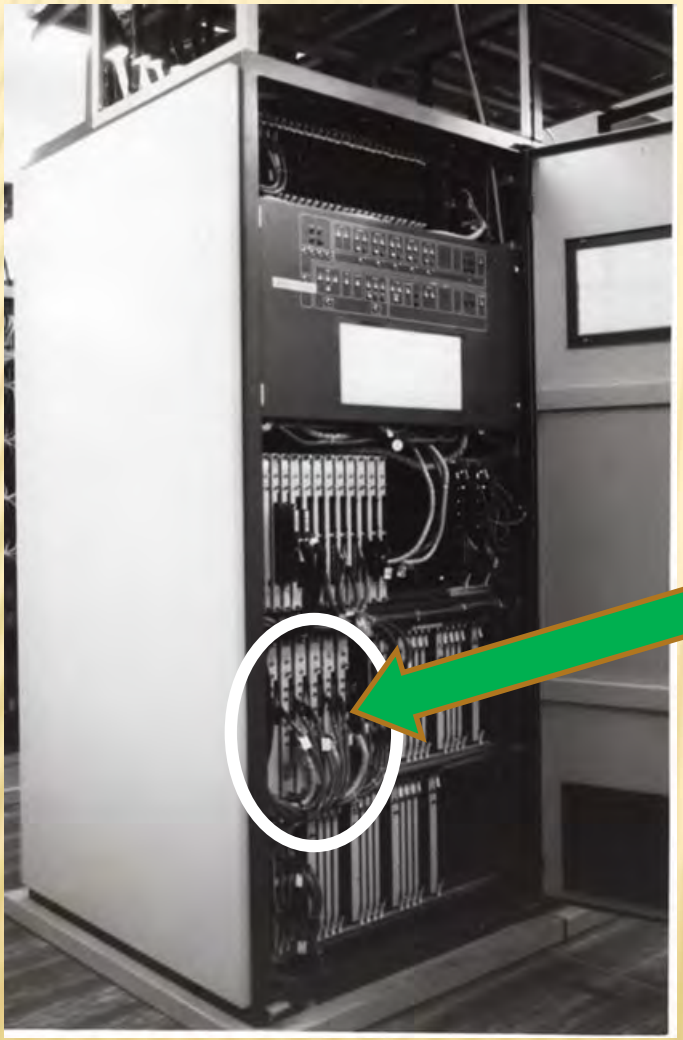
セルフチェッキング回路の実用例

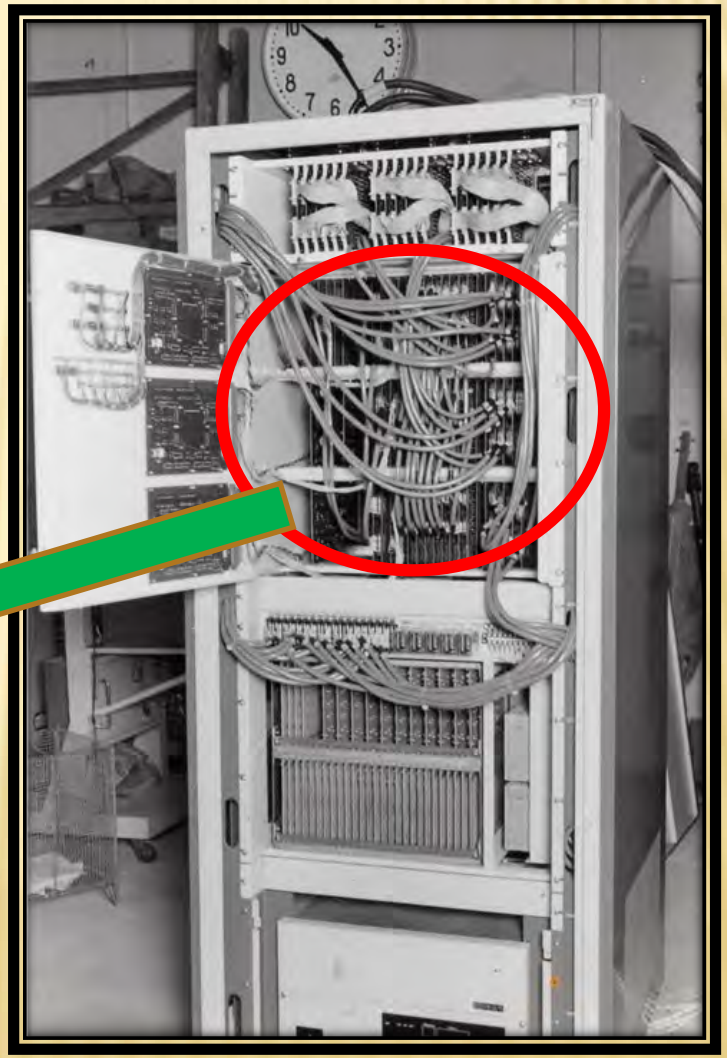


3重系多数決フェールセーフ計算機



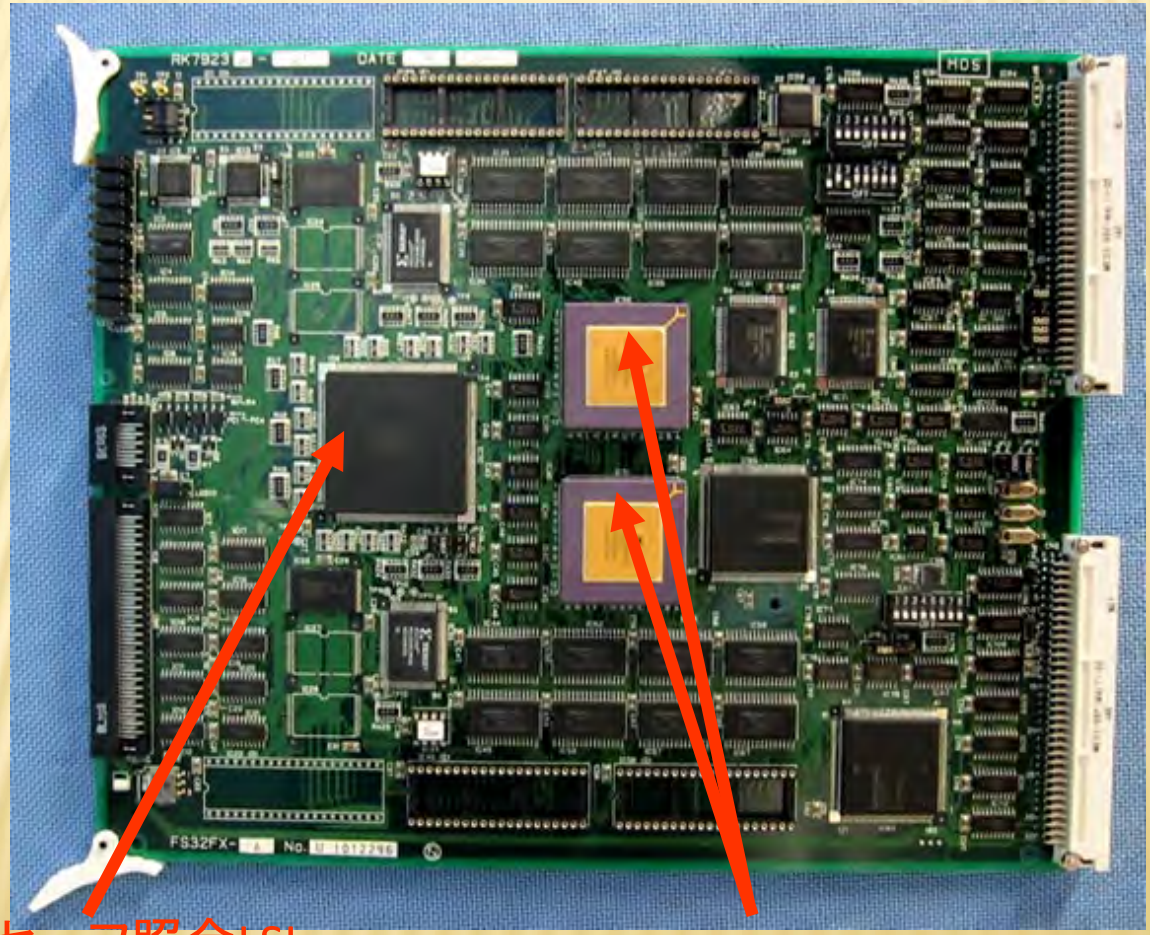
3重系多数決フェールセーフ計算機



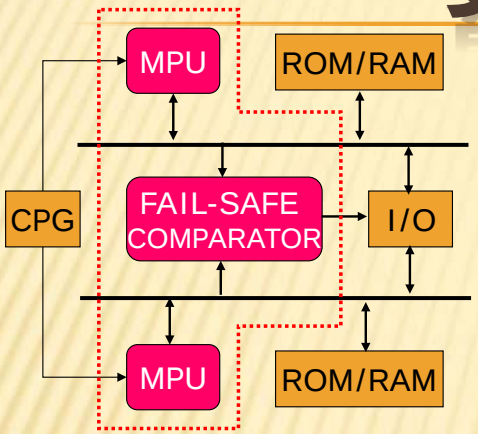


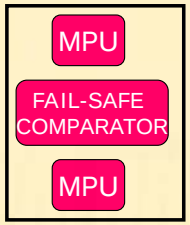
照合回路のLSI化

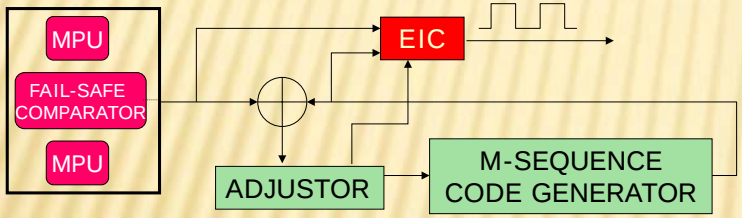
フェールセーフ32ビットボードコンピュータ (コアMPUは68020)

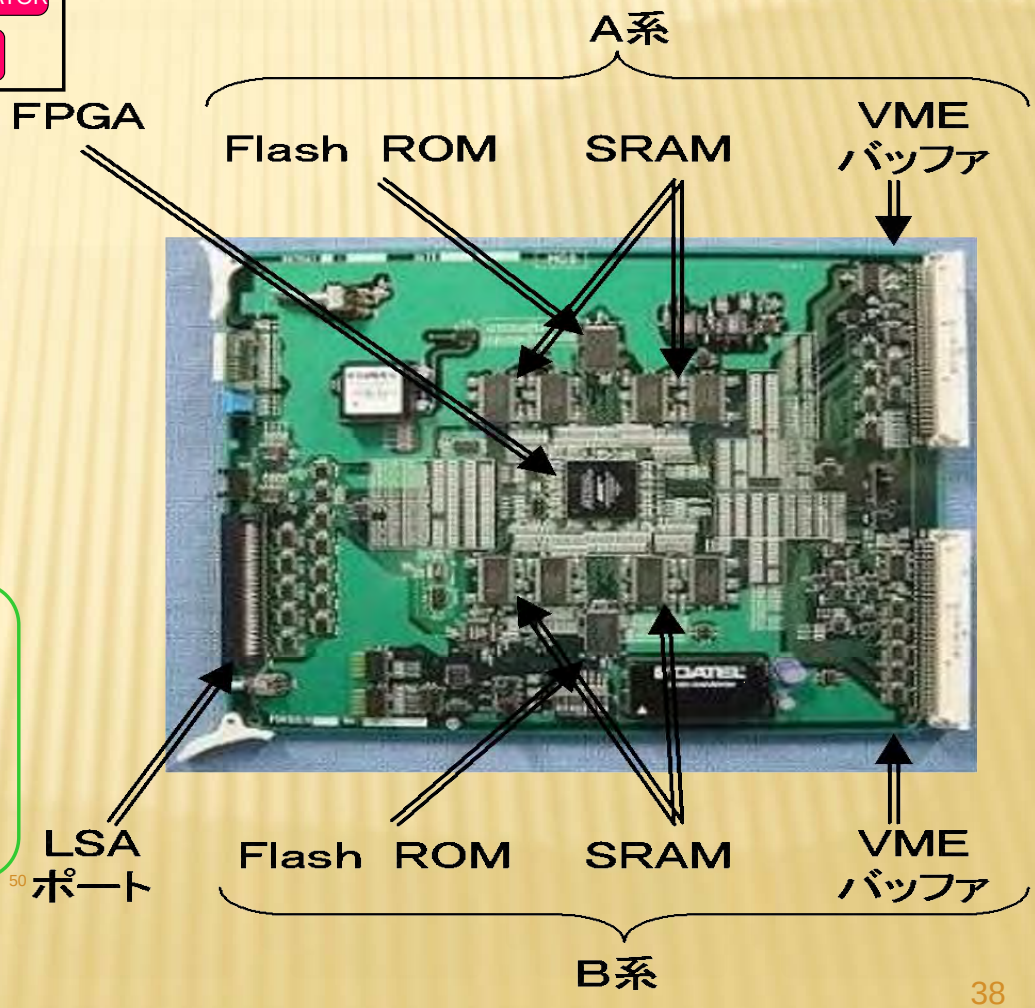


更なる高性能化への挑戦





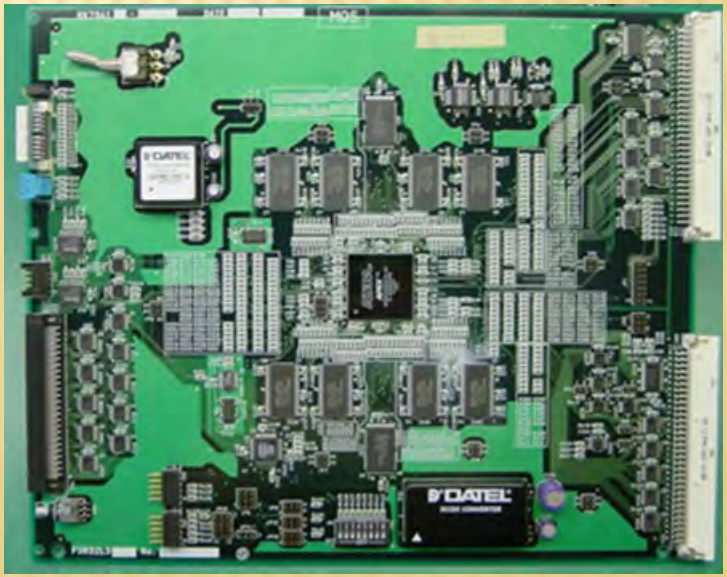




性能比較

- 処理能力
  - 32ビット整数のAND，OR　：　従来品比　20．64倍
  - 32ビット整数の乗算，加算、減算　：　従来品比　30．29倍
  - 32ビット浮動小数点の乗算，加算、減算　：　従来品比　43．59倍
- 消費電力　：　従来品比　15%削減
- 故障率（FIT）　：　従来品比　15%削減

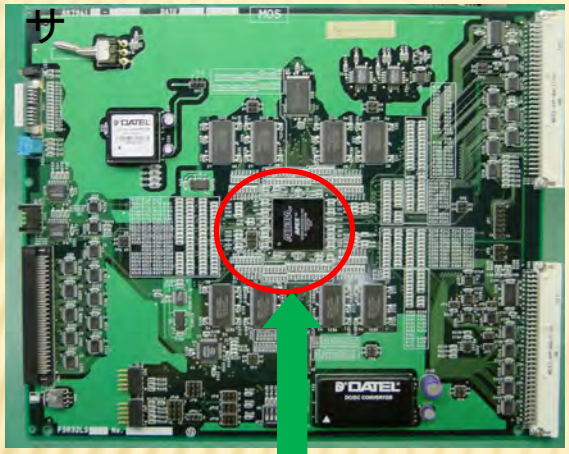
従来品



シングルチップFSプロセッサ使用品

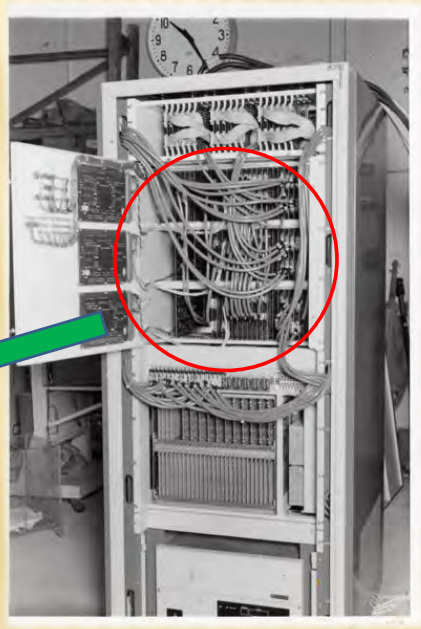
鉄道信号におけるFS-MPUの進歩

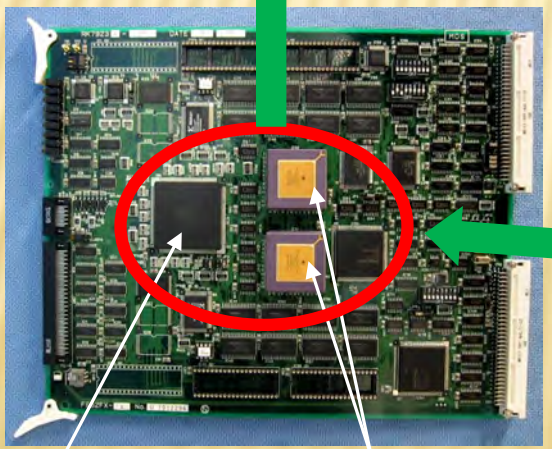
32ビットFS　RISCプロセッサ



実用装置(1985)

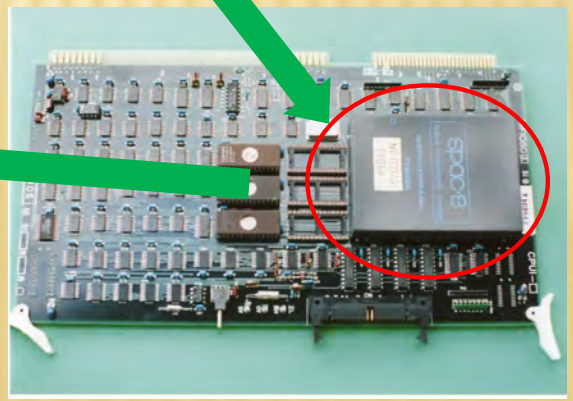
試作装置(1980)





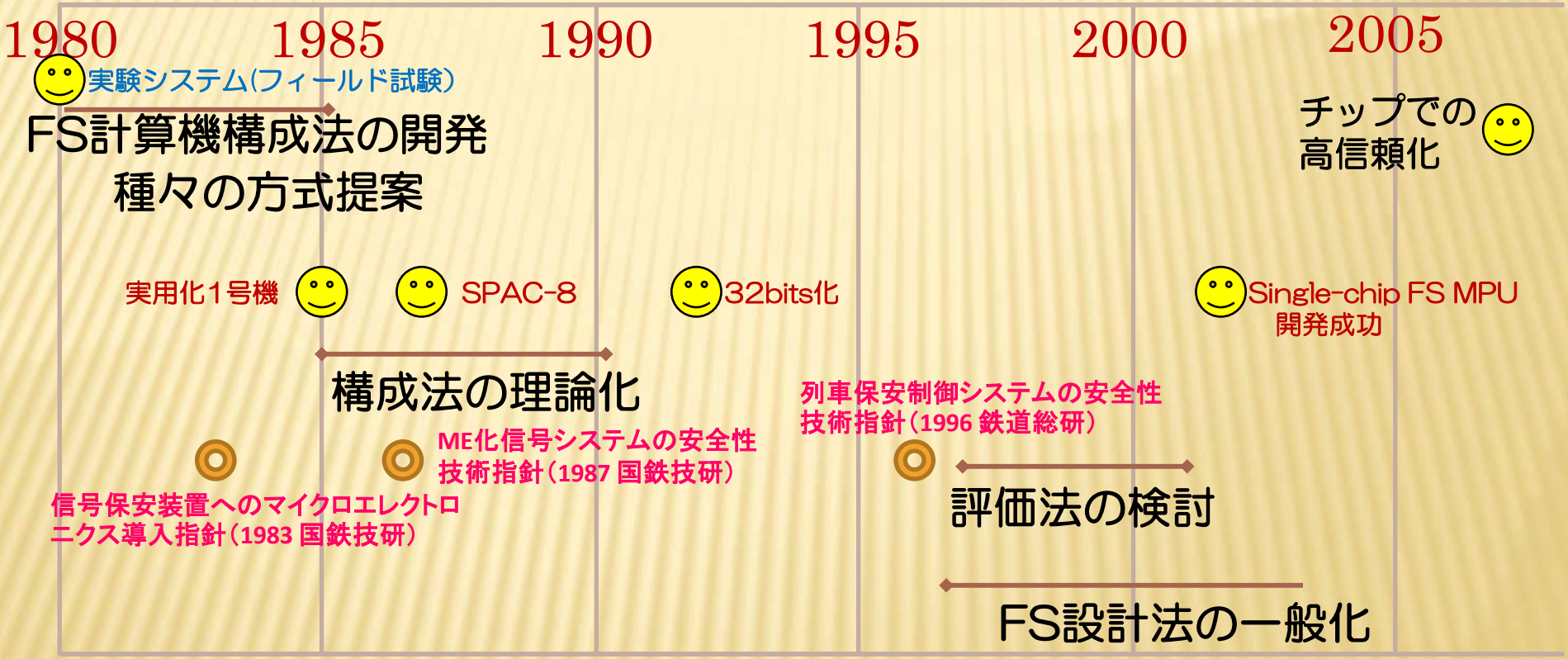
開発したFail Safe照合LSI　コアMPU68020

FS照合回路の
LSI化



SPAC-8

鉄道信号用FAIL SAFE計算機開発の流れ



フェールセーフ計算機を実現した技術

- 多様な方法論が生み出され実用化

Failを検出したらSafe側に

故障診断技術が鍵

COMPUTER化がもたらしたもの

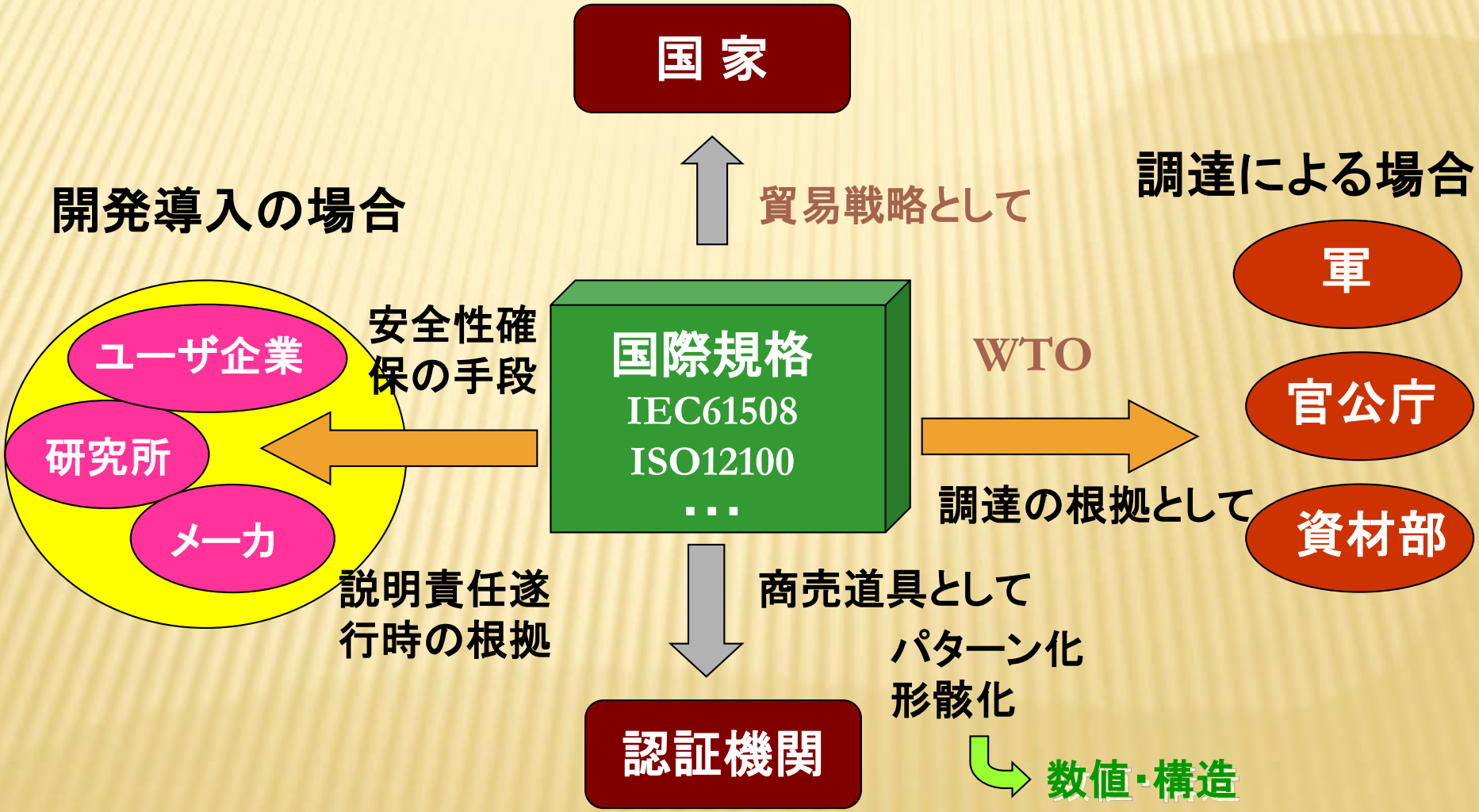
- **産業界独自の安全性技術はプログラム論理に**
- 産業界横断の共通な方法論が登場
  - フェールセーフなコンピュータが必須
    - 方法は多様、入念に配慮されたコンピュータはそれぞれ有効な実績
  - ソフトウェアの安全性が重要
    - バグに対する２つの見解→バグのないソフトは可能/不可能（Formal MethodとDesign Diversity）
  - 安全性の共通尺度としてRISKの登場
- 国際規格の登場

安全制御分野へのコンピュータ導入は軌道に乗り、様々なシステムが考案された。

この動きは、他の産業分野にも通じ、方法論が国際規格となり、認証文化が隆盛となった。…

計算機利用装置の安全を担う機能安全と認証

安全設計国際規格の多面性



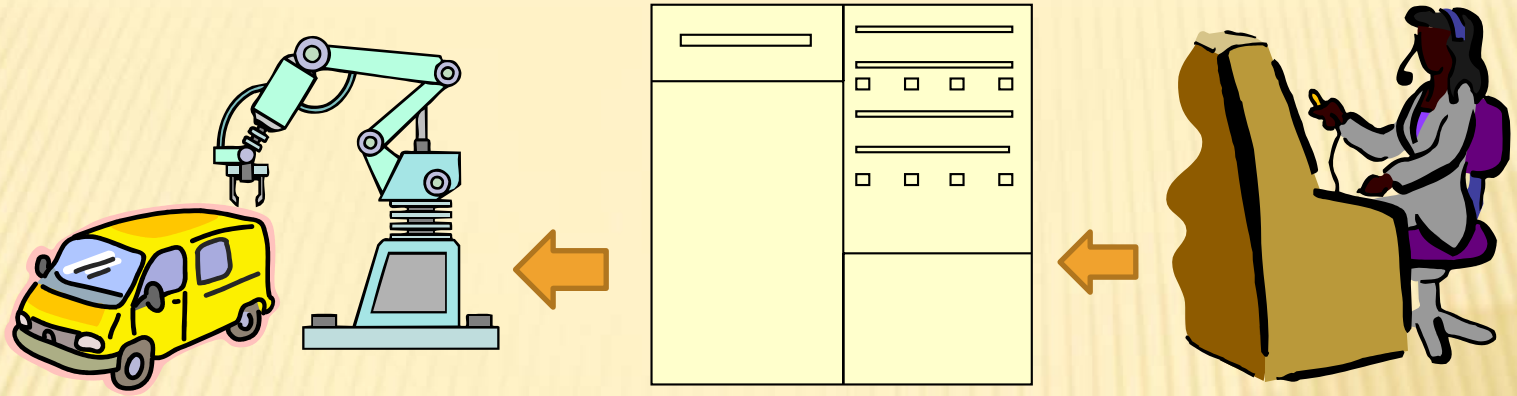
認証に伴う課題

- 機能安全規格：IEC61508
  ハードウェアの要件をも規定
- 共通源故障対策
  - 対象要素の機能喪失により誤処理に至るもの
    - クロックの誤り
    - 入力の誤り
  - 配線間短絡やクロストークによって生じるフェールセーフ機構（単一系）の誤り
  - **素子の同時同一故障の懸念**（集積化の課題）
    ASICはSIL３まで（IEC61508 ed.-2)
    果たして妥当か？

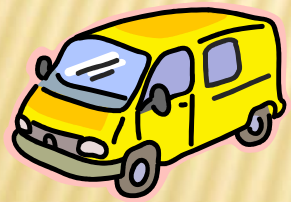
システムがこれから目指すべきIoT時代の信頼性・安全性方策とは

アーキテクチャの本質化によるアプローチ

Safety2.0時代の安全性



FAULTそのものを減少させる進化型の積極的方策：本質制御



システムのアーキテクチャに遡って検討→究極のシステムを構築

構成要素が相互に情報交換

→機能実現

Safety2.0時代の安全

期待される積極的高信頼化方策

- 与えられた設計図の中で高信頼化を図るのではなく、システム機能要件を実現するアーキテクチャにさかのぼって、高信頼化を実現

本質制御

- 制御情報を創り出す固有の制御装置を削減
- 要素間の情報交換で安全を実現（協調安全）
- 本質的に必要な要素のみで機能を実現するシステム
- 高度な機能を処理装置を設置せずに実現

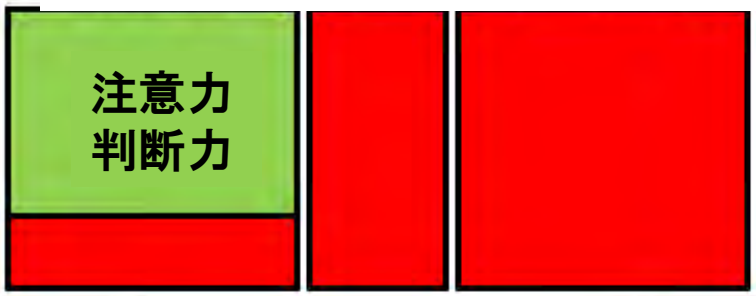
Safety2.0時代の安全

IOTによる本質制御の実現

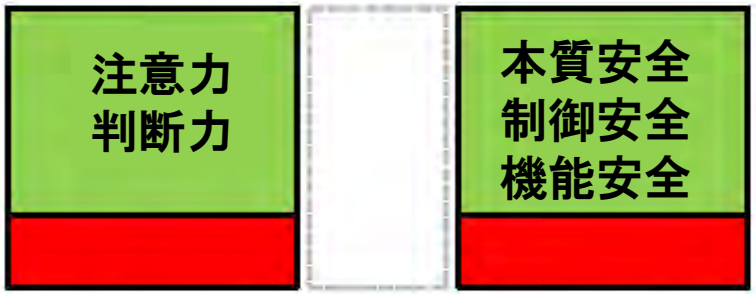
- 本質的に必要な要素間で相互に情報を交換し、機能・安全を実現（IoTに依拠した協調安全/高信頼化）
  - 制御のための中間処理部（制御装置）を削減
    - 信頼性向上
    - 安全性向上
    - 保全性向上
- 運転モードを複雑にしない
  - 本質的な要素のみで実現するシンプルで高機能なシステム（故障時には機能縮退させ、代替システムは用いない）

Safety2.0時代の安全

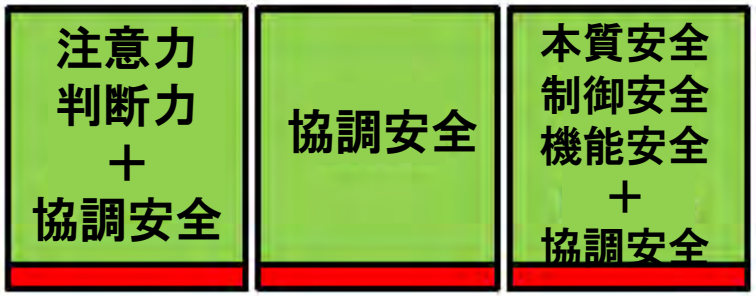
本質制御の具現化、IOT時代の安全文化



Safety0.0
■人による安全
・人の領域にもリスク
・人と機械の共存領域はリスク
・機械の領域はリスク



Safety1.0
■人と機械それぞれによる安全
・人の領域にもリスク
・人と機械の共存領域は撤廃
（隔離の安全）
・機械の領域にもリスク



Safety2.0
■人と機械の協調による安全
・人の領域のリスク最小化
・人と機械の共存を可能に
・機械の領域のリスク最小化

Safety2.0

ロボットや自動運転
i-Constructionなど
新しい産業の波を安全面から支援する

安全を端緒に、生産性向上、コスト低減などを同時に実現する

新時代にふさわしい安全の新コンセプト

IOT化がもたらすつながる時代の安全技術

- 固有の装置が開発されていた時代（機械式・電気式・電磁リレー利用）

SAFETY1.0

固有のフェールセーフ技術が開花

- コンピュータ化が成功した時代以降

高度な機能の付加が容易に

ネットワークを介して大規模複雑化

産業横断的共通土壌が構築され国際規格へ

- IoTの時代は本質制御で安全技術が高いステージに変貌

汎用装置もメッセージ情報交換で健全性が検証可能に

SAFETY2.0

シーケンス制御時代の対雑音戦略が変貌

- 現場機器の制御やリレー回路は、雑音を考慮しDC24Vの電流を用いていた
- 制御用信号電流も、雑音レベルに対し10dBのマージンを・・・

- ICT（通信利用時）には、符号技術（エントロピー）に依拠して雑音に対処

つながる安全にはセキュリティ対策が重要
CPU構成技術とオープン化を利用

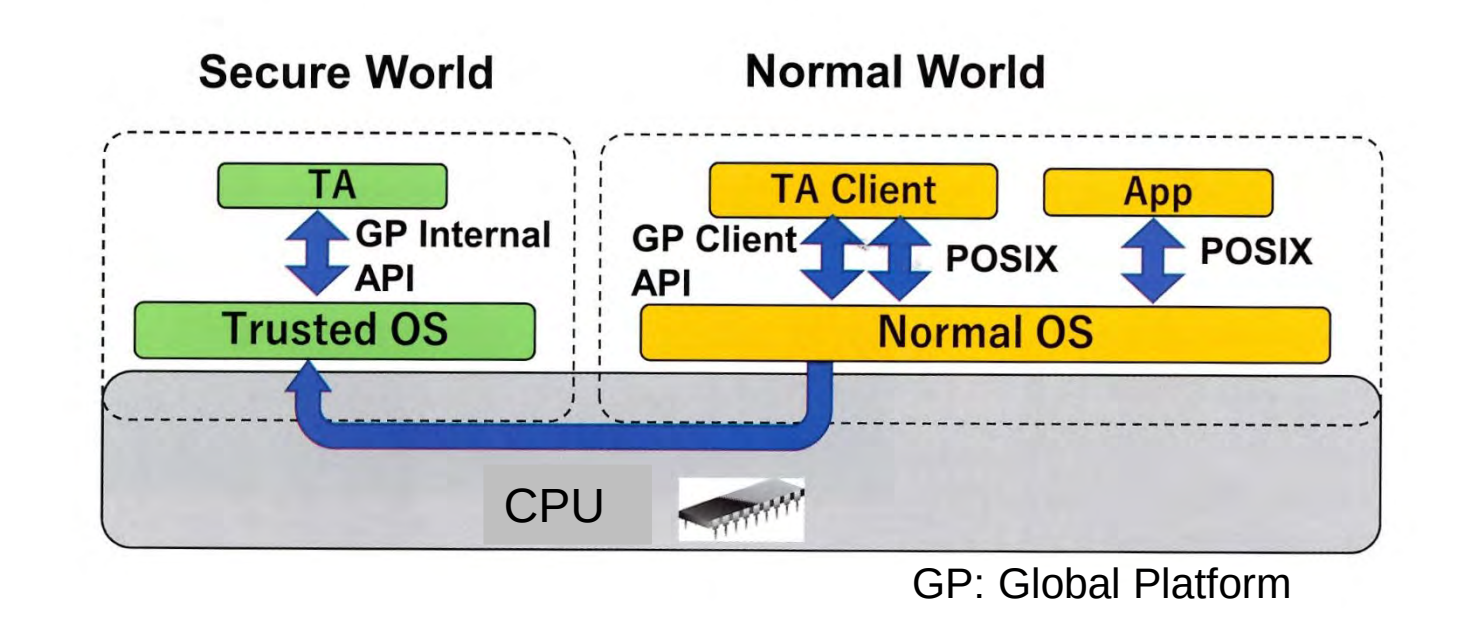
絶対に盗まれないセキュリティ対策技術をいかに実現する

- セミカスタムLSI技術の進展
  - PLA/PAL; Programmable logic array
  - Complex Programmable Logic Device
  - FPGA
    - IP-core: intellectual property core
    - ARM（必要なCPUをFPGAに実装できる）
- これから；命令セットアーキテクチャをオープンソースにする時代が→RISC-V (ファイブ)
  - オリジナルなコンピュータが作れる
  - セキュリティチェック用のコアを隠蔽

故意の外乱の脅威への対応

つながる安全

- IoTによる協調安全の実現には、セキュリティ確保が重要に
- 命令セットアーキテクチャ（ISA）を開放するRISC-Vに着目
- RISC-Vでは、TEE (Trusted Execution Environment)に対する配慮がなされている



須崎有康「TEEを中心とするCPUセキュリティの動向」Bulletin Jasa 2019 Apr. p16より

安全性に対する工学的視点からの考察

フェールセーフ入力
フェールセーフ回路
フェールセーフ回路
フェールセーフ出力

23

Safety2.0時代の下での方法論

IoT Equipment（汎用MPU）

・処理の連続性
・通番/タイムスタンプ
・データ内容の合理性

これらから汎用MPUの正常が診断できれば十分

Fail safe 計算機

センサー

FS論理素子二重系
N-Version Programming
Self Checking Circuit式
（バスlevel照合方式）
チェックポイント照合
位相差照合方式

アクチュエータ

Failを検出したらSafe側に

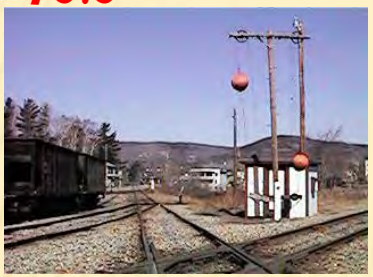
故障診断技術が鍵

IoT Equipment（FS-MPU）

システムの進歩と信頼性・安全性活動

Safety0.0

障害物を排除する
役割が求められた



無難を伝達する仕
組みが導入される

Safety 1.0

信号システムとして
高度に発展、
ATS/ATC整備

高速・高密度運転
を支えるシステムに

Safety 2.0

IoTに依拠した協調
安全を

機能向上に伴い高度化・複雑化
システムの守備範囲が広域に拡大

戦後・黎明期 → 構成要素の特性に依拠した安全性技術の創造　固有Fail safe技術

電子化・ME化 → 論理による安全性の確保、機能の拡充

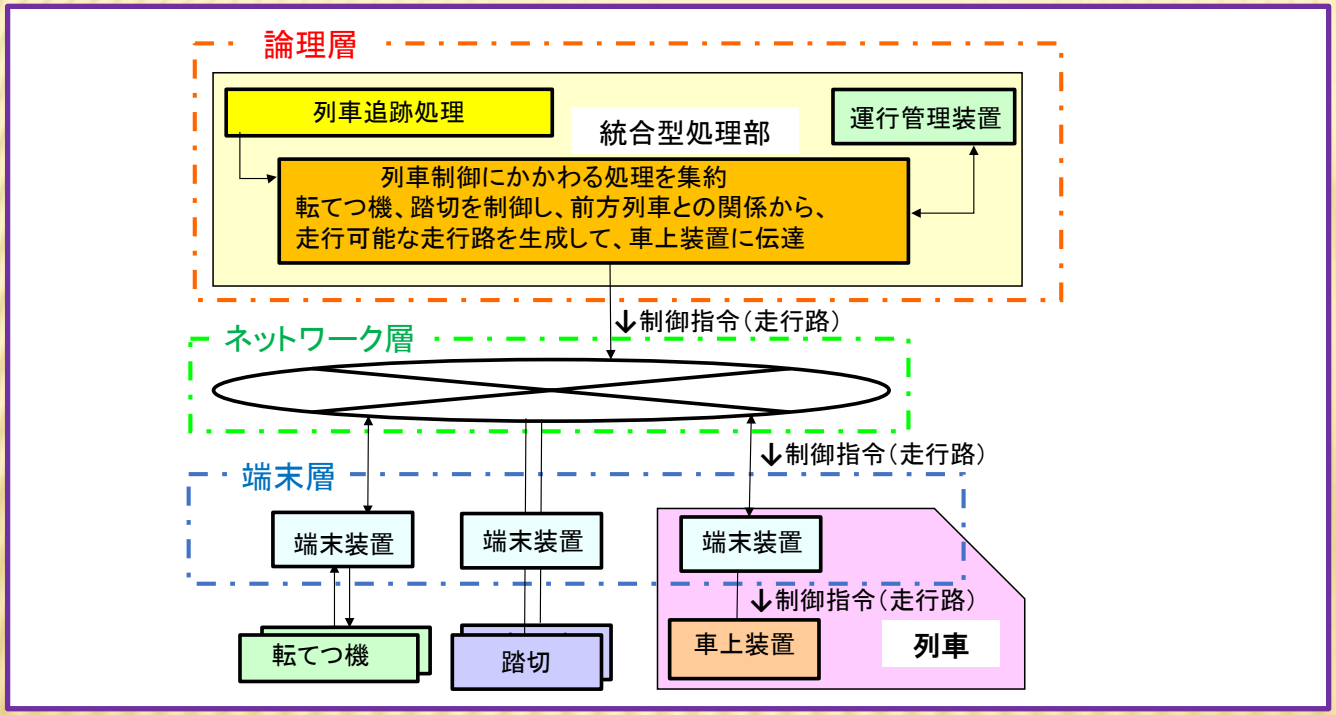
システム化 → 大規模複雑システムへの対応、Flexible system

今日・明日 → 本質制御；情報の交換による協調安全

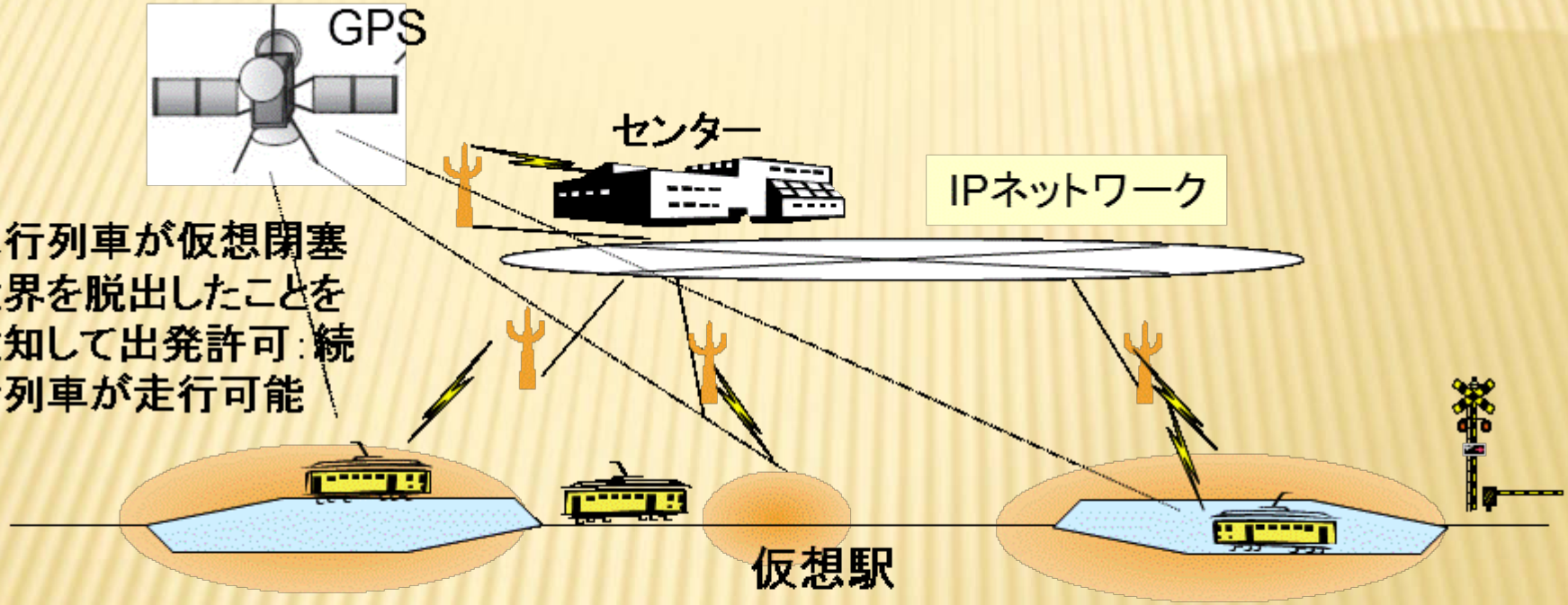
Safety2.0時代の安全 → IoTに依拠

つながる安全の鉄道における事例

明日の列車制御システムの構成



本質制御の鉄道システム：ATP閉塞システム



安全から見たシステムの変遷

Safety2.0時代の安全

RISK項目	機械式	リレー式	FS-CPU	＋ LAN	IoT利用
人間の錯誤	機械相互の連動で照査	接点論理でカバー	ソフトでカバー	動作監視で対応	安全制御から人間解放
オペレーションミス	人間の注意力・訓練	鎖錠論理、ATS等	鎖錠論理 動作の合理性検定	同左	安全制御から人間解放
高温	補償装置	器具箱	室内＋器具箱	室内＋器具箱	室内＋装置
ノイズ	ー	エネルギー	エントロピー＋エネルギー	エントロピー	エントロピー＋情報の合理性
故障	定期点検	Fail Safe 定期点検	Fault Tolerance	Fault Tolerance	必須な要素のみに削減
ハッカー	ー	ー	外部と遮断	暗号	暗号＋RISC-VのTEEに依拠

日本大学生産工学部　鉄道工学リサーチ・センター
特別シンポジウム
「国際協調による鉄道安全性向上の取り組み」

鉄道の次世代安全性（Safety 2.0の視点から）

終り

日本大学　名誉教授
東京大学大学院 新領域創成科学研究科
客員共同研究員
工学博士　中村　英夫