シーケンス回路からFAIL SAFE計算機へ

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

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

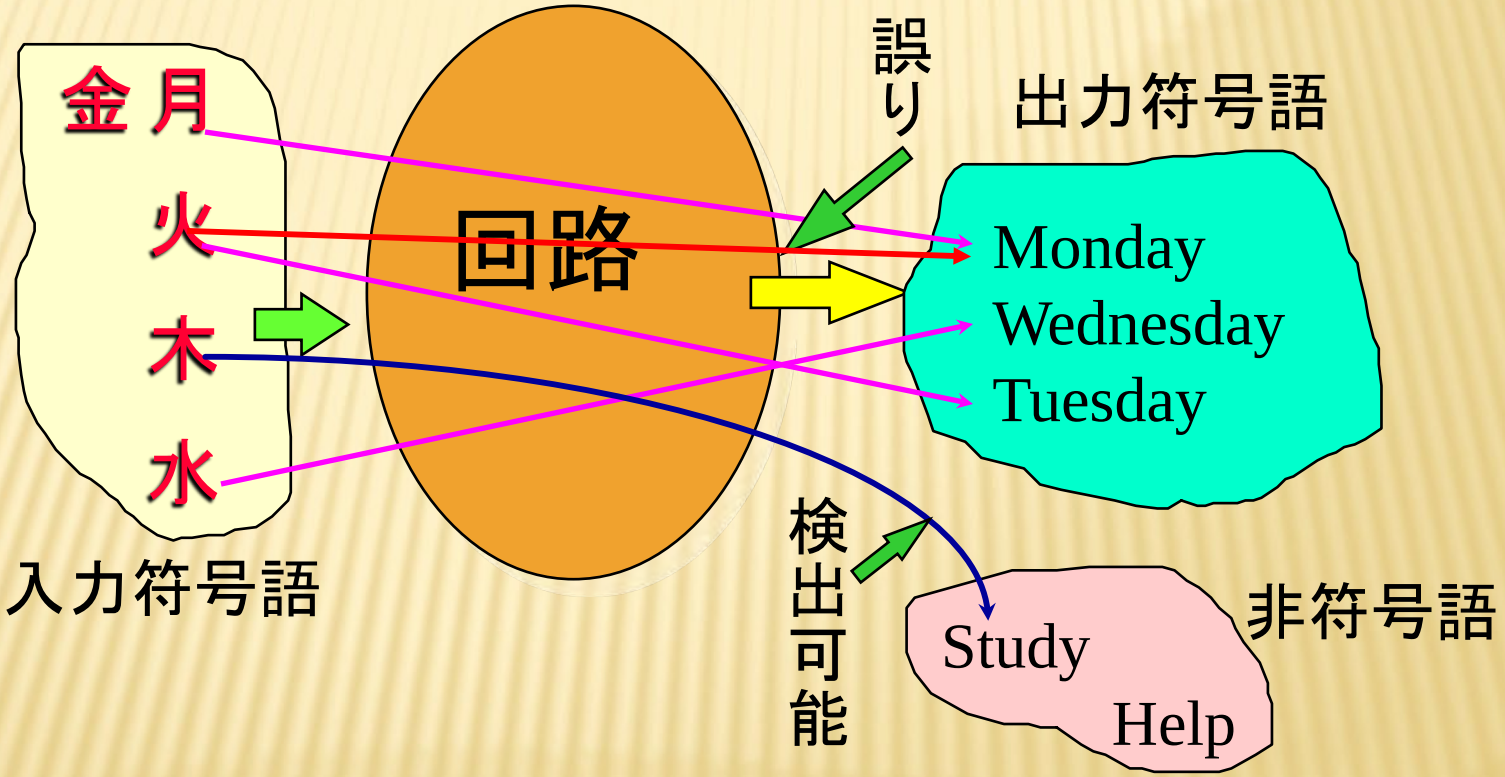
- Fault Tolerant Computing System
- 1980年の国際大会FTCS1980（京都）
  超高信頼化計算機システム
- Fault Tolerance＝耐故障？？
  容錯計算机

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や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/安全性に配慮し三重系多数決構成を
- 1970年代：IEEEは，system技術の研究として、回路レベル/システムレベルでの研究を活発化
  →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

回路の故障による影響


金
月
火
木
水
入力符号語
回路
誤り
出力符号語
Monday
Wednesday
Tuesday
検出可能
非符号語
Study
Help

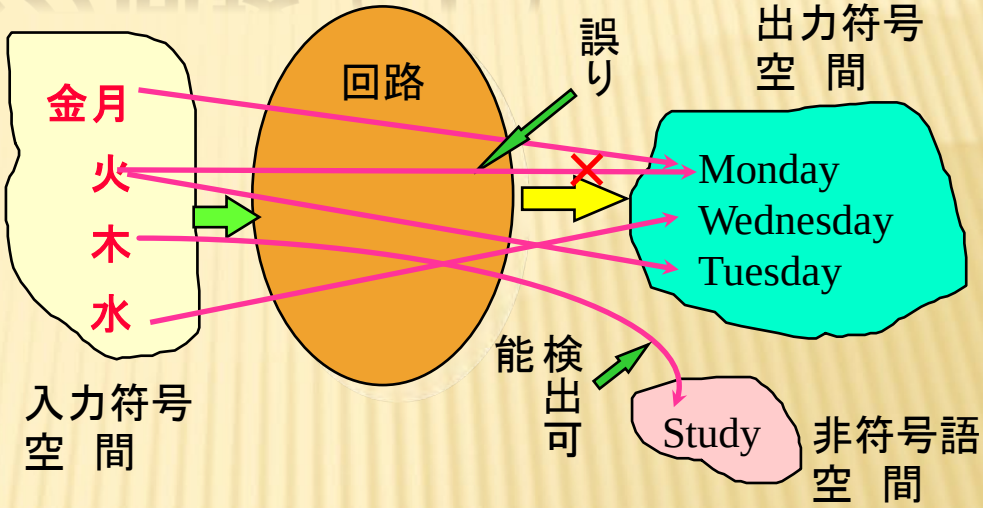
セルフチェッキング回路（１）

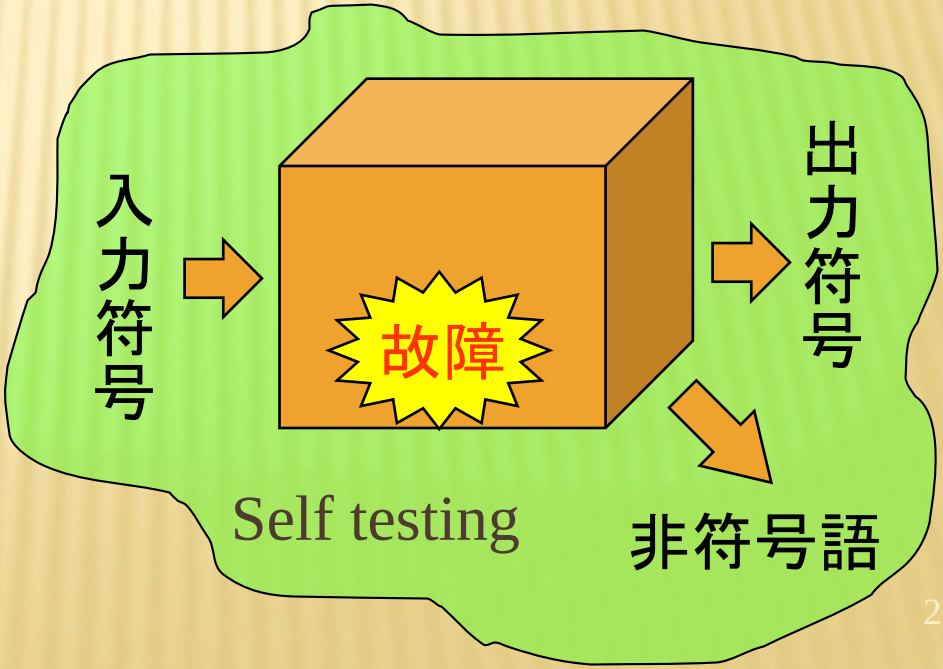
- 性質1:回路に故障が発生しても、非符号語を出力するまでは、正しい出力（符号語）を行うことを保証

  Fault Secure性

- 性質2: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）

  Self Testing性

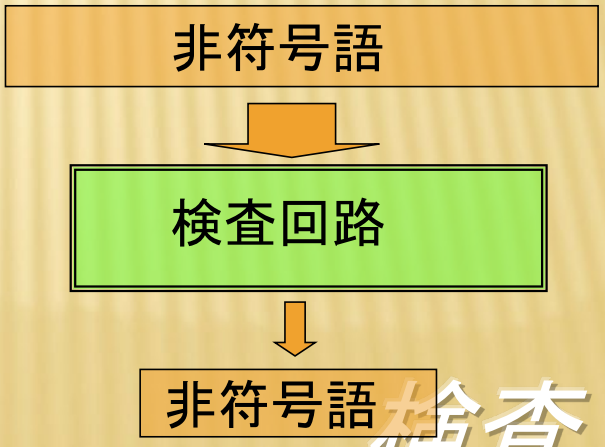




セルフチェッキング回路（２）

- 性質3:Self testing性と Fault secure性を満たせば
  →回路が故障していれば検出される。それまでは出力が正しい。
  Totally Self-checking；TSC性

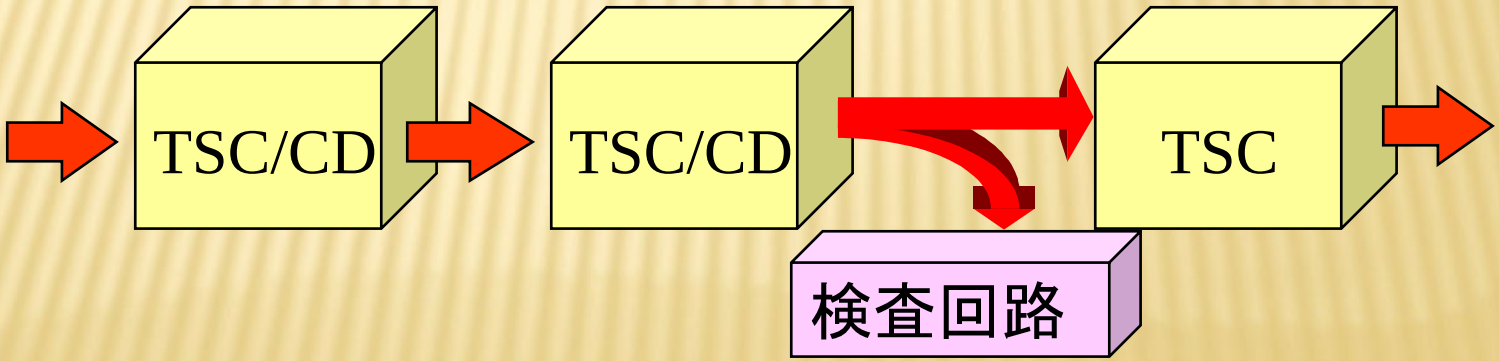
- 性質4：誤り（非符号語）入力時には必ず非符号語を出力　Code disjoint性
  検査回路の必須要件



検査　検査
検査
検査

セルフチェッキング回路の構成法

- 回路要素をトータリィセルフチェッキングで構成する。
- CD性が無ければ（非符号語入力を符号語にしてしまう可能性あり）前段に検査回路を



セルフチェッキング回路(SCC)の概念

- 通常動作中に故障の存在を検出できる回路
- 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
    - 誤り安全と誤り伝搬の概念
      - 故障して誤りがあっても安全側ならいい（誤り安全）
      - その誤りがどこかで検出されるまで誤り安全ならいい（誤り伝搬）

FAULT TOLERANT SYSTEMの事例

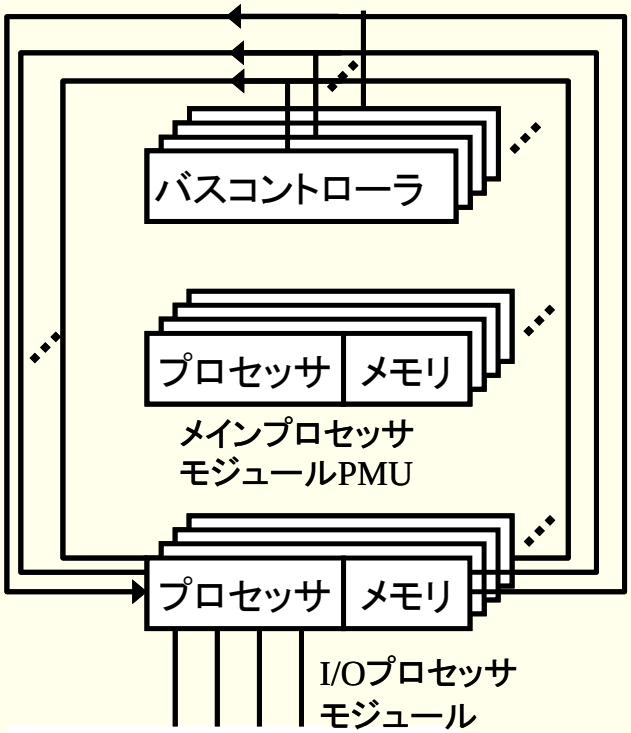
- 多重故障に対しても対応できる概念へ:SFS性
  - 故障が発生し非符号語を取るまでにさらに故障が発生しても、Fault-secure性が保証される
    SFS: Strongly Fault Secure性
  - 非符号語が検出されたときにシステム的に対応すれば、高度な信頼性や安全性が求められるクリティカルなシステムへの応用が可能
  - 鉄道等の保安制御用コンピュータに利用される
- 産業界で要求される高信頼システム
- Self checkingの概念でコンピュータの開発

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

FAULT TOLERANT COMPUTER SYSTEMの事例

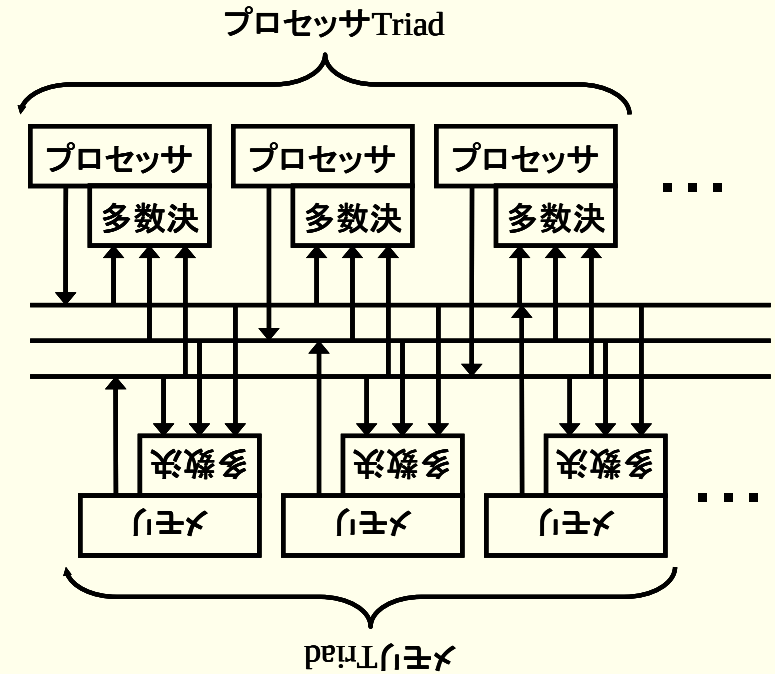
	高稼働率	安全制御	長寿命
1960	Tandem Non Stop 2		
	ESS		
1970			STAR
	Tandem Non Stop		FTSC
1980	Stratus/32	FTMP SIFT	
			SMILE
1990			

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。

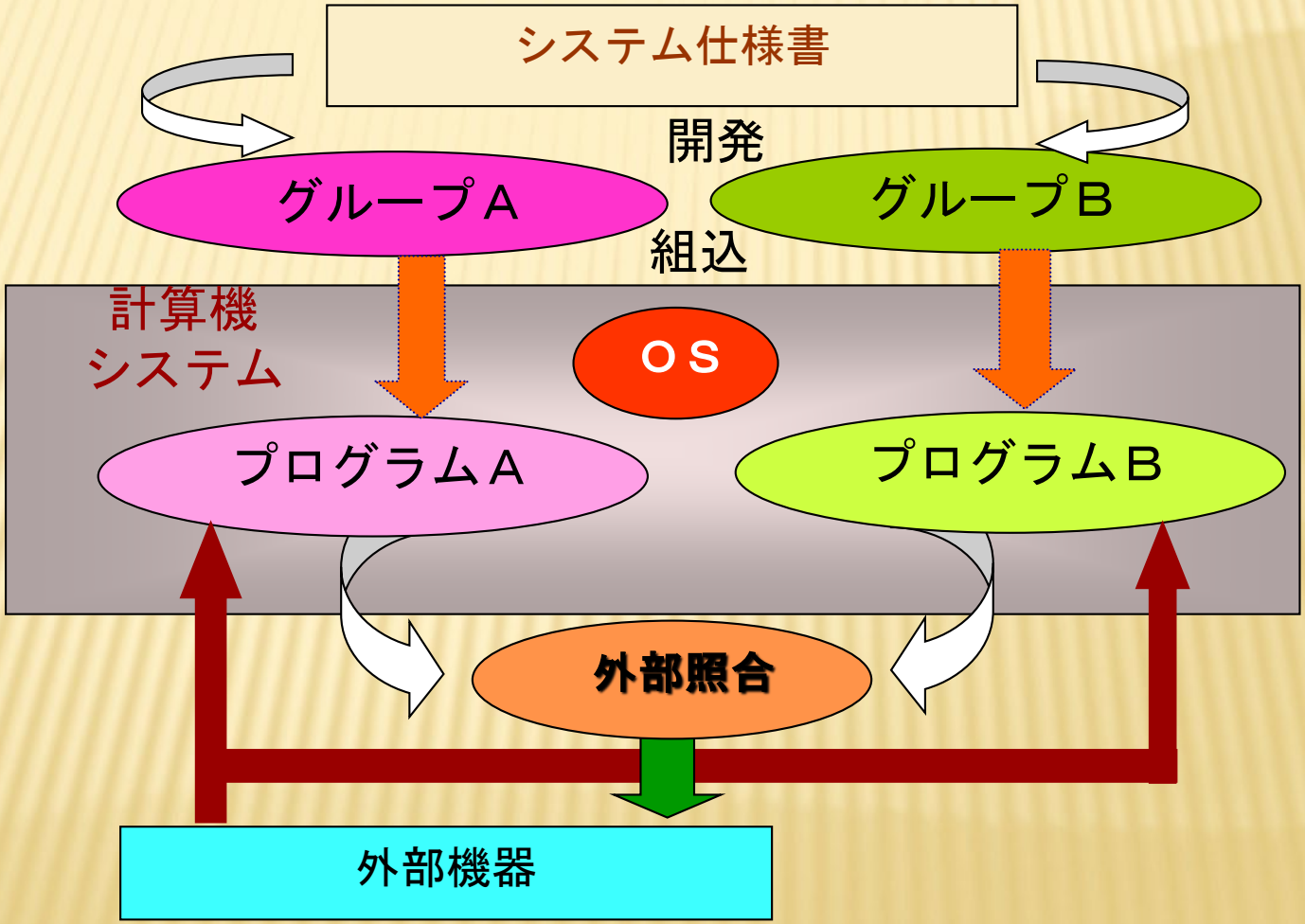
この診断を行うため,ハードウェアはバスレベルで同期が取られる。

図3　FTMPシステム

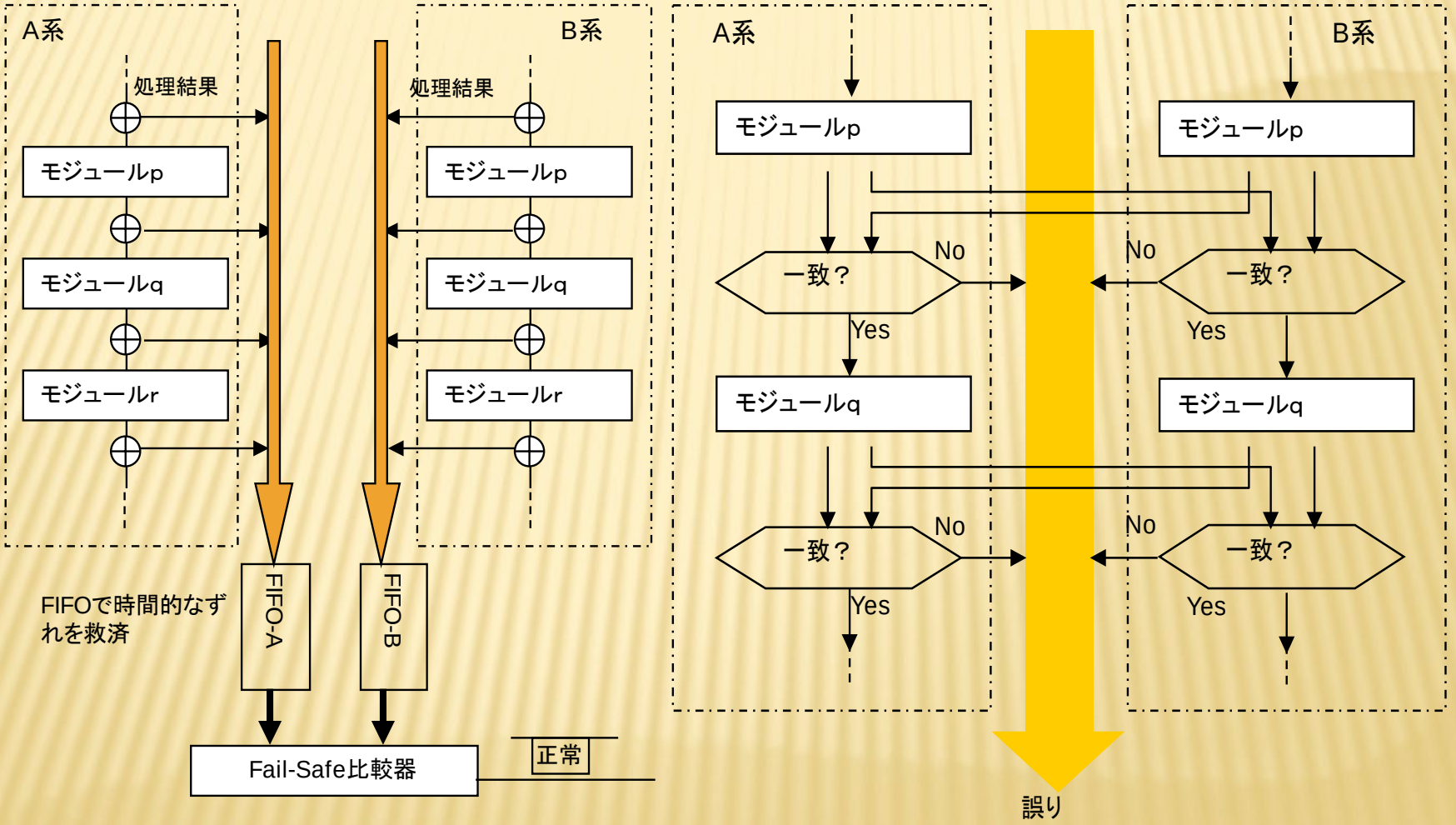
多様なフェールセーフ計算機システム

- 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）**

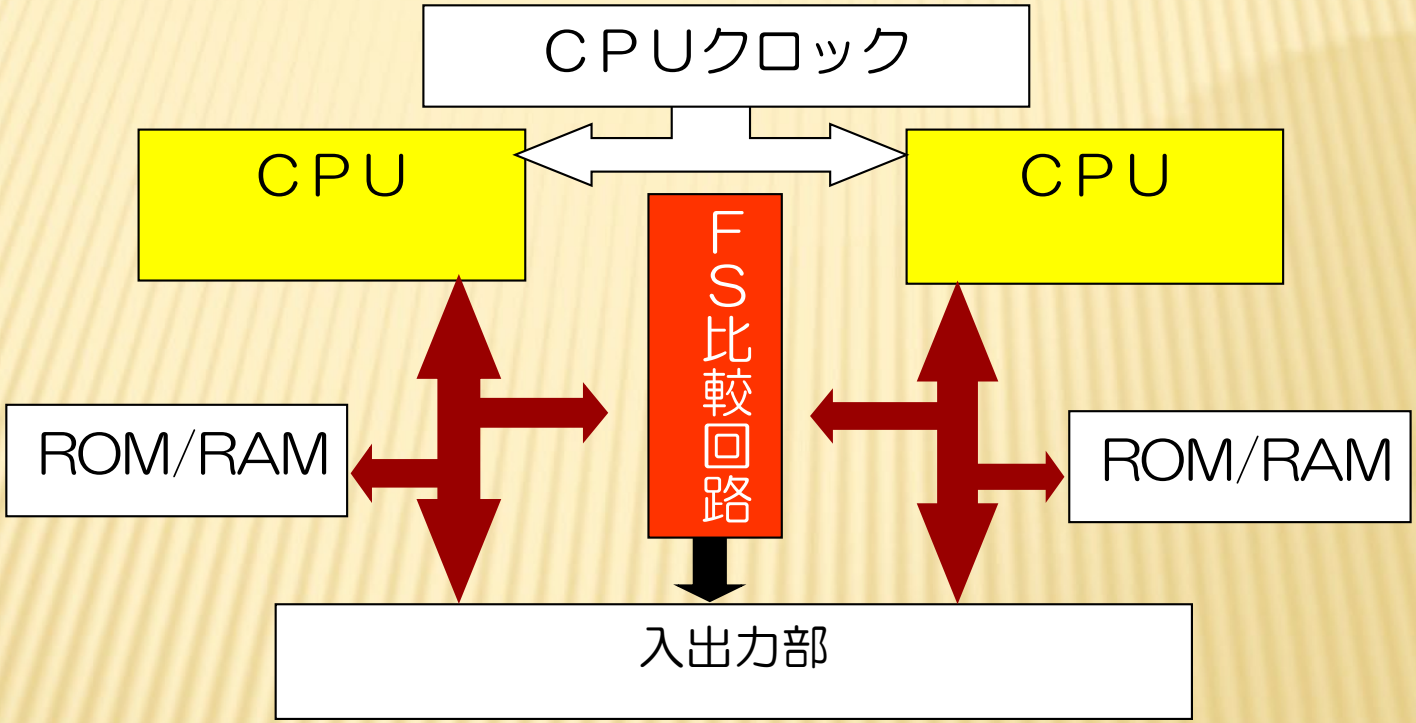
ソフトウェア多様化設計による手法



チェックポイント照合方式

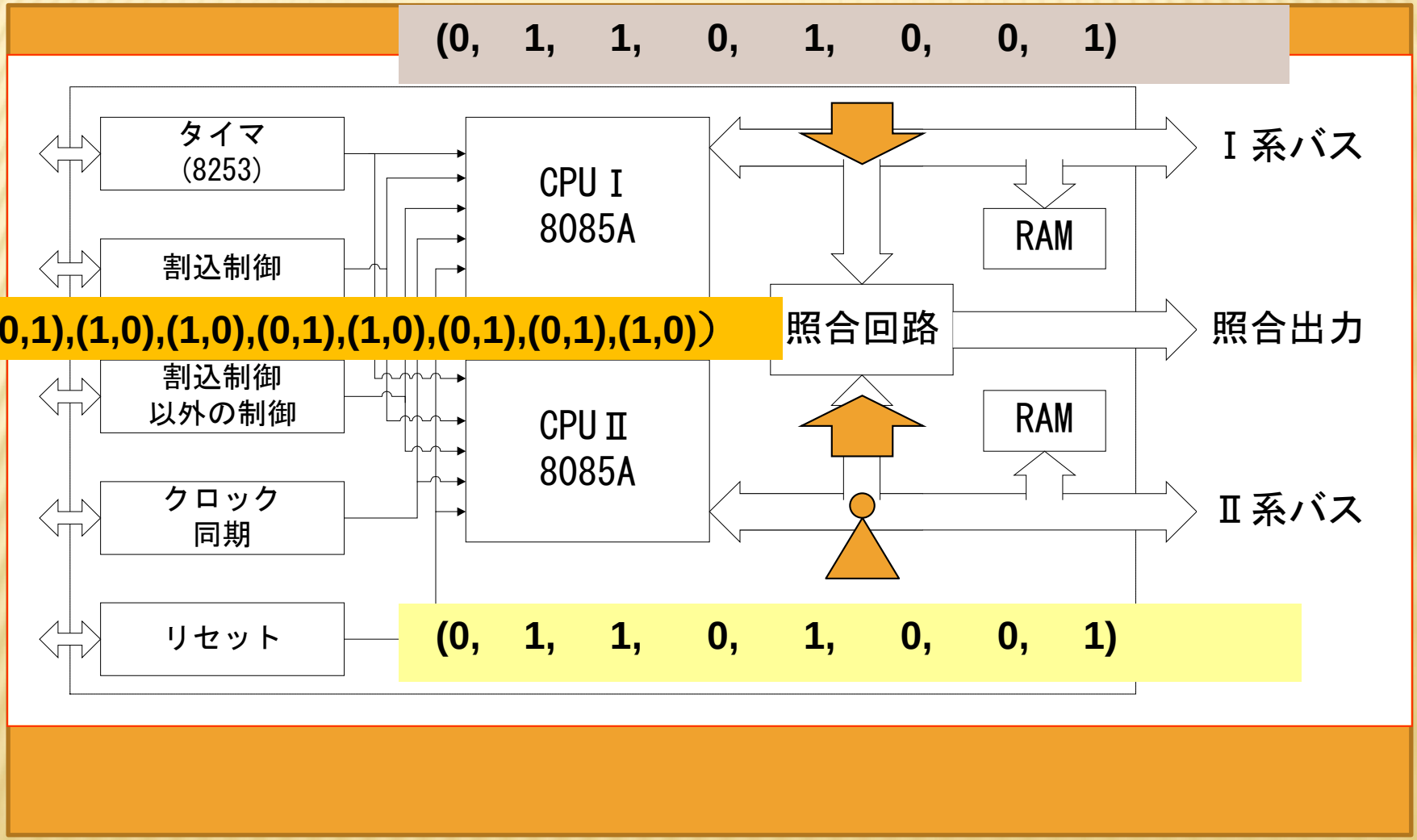


ハードウェアの密な同期照合方式

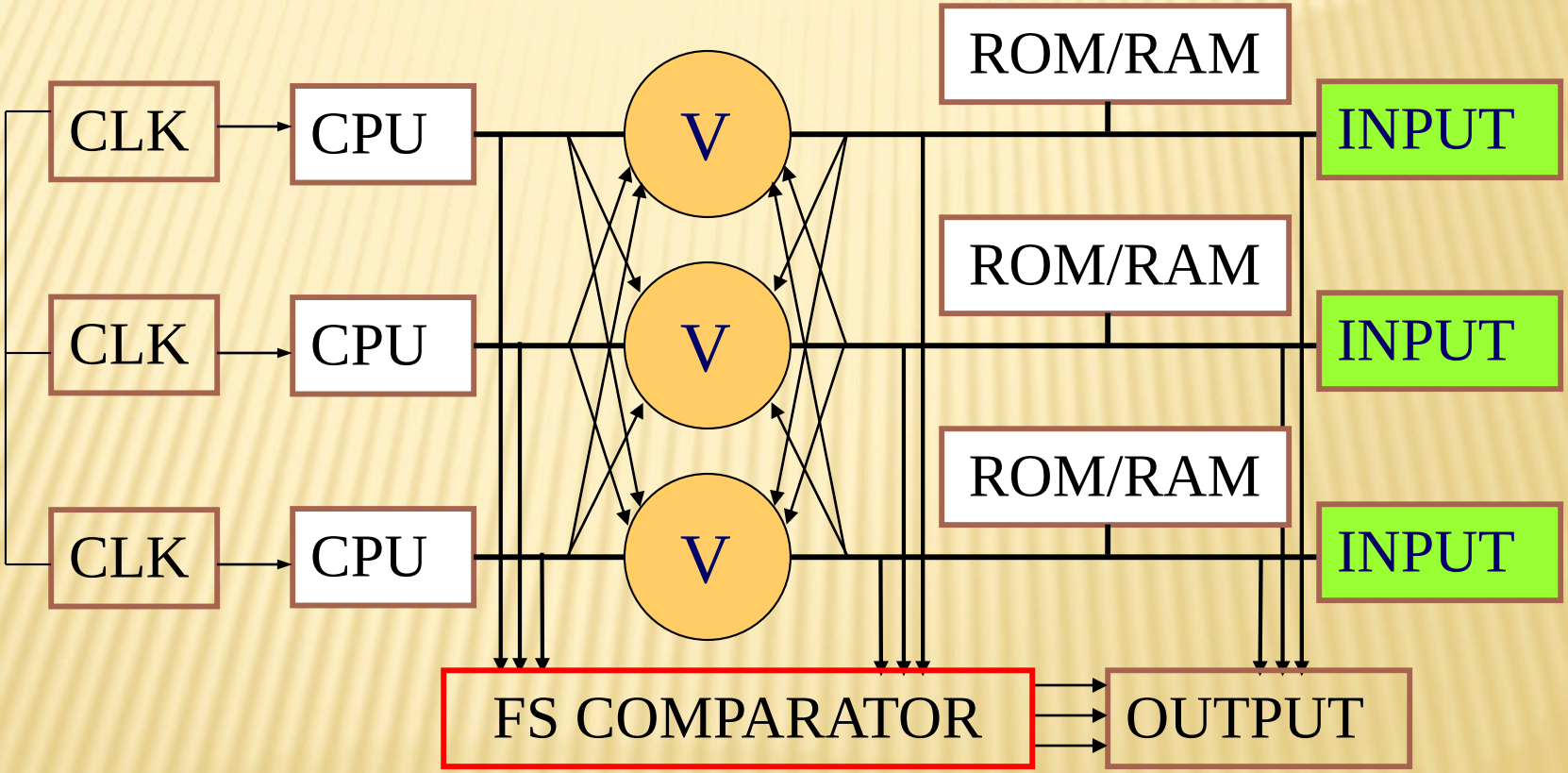


同一のプログラムがクロックレベルで同期して動作。バス上のデータは
ＦＳ比較回路で照合され，不一致時には安全側にシステムを固定

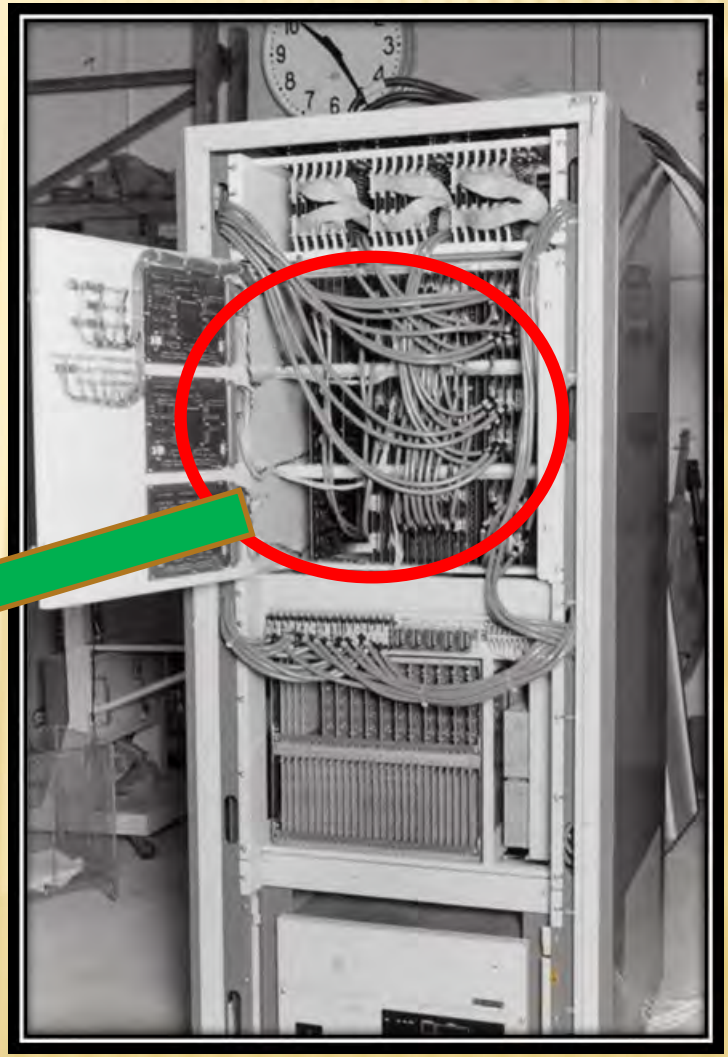
セルフチェッキング回路の実用例



3重系多数決フェールセーフ計算機



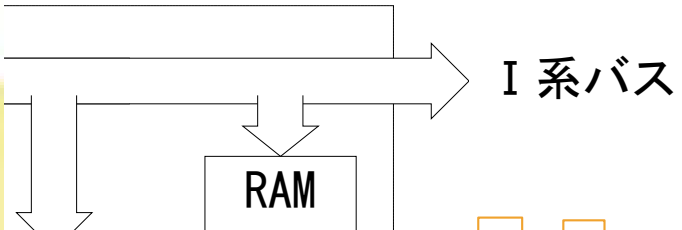
3重系多数決フェールセーフ計算機

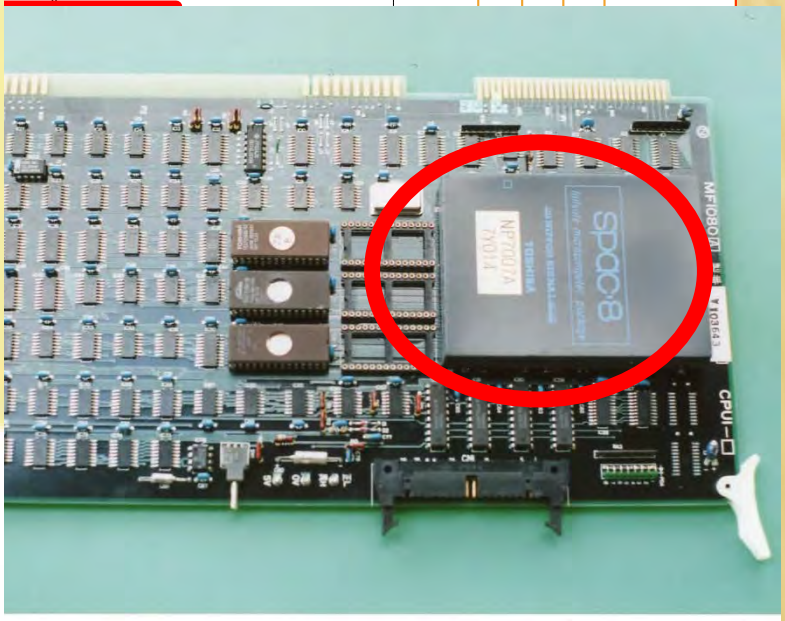


フェールセーフコンピュータ パッケージ：SPAC-8

8ビットフェールセーフコンピュータパッケージ

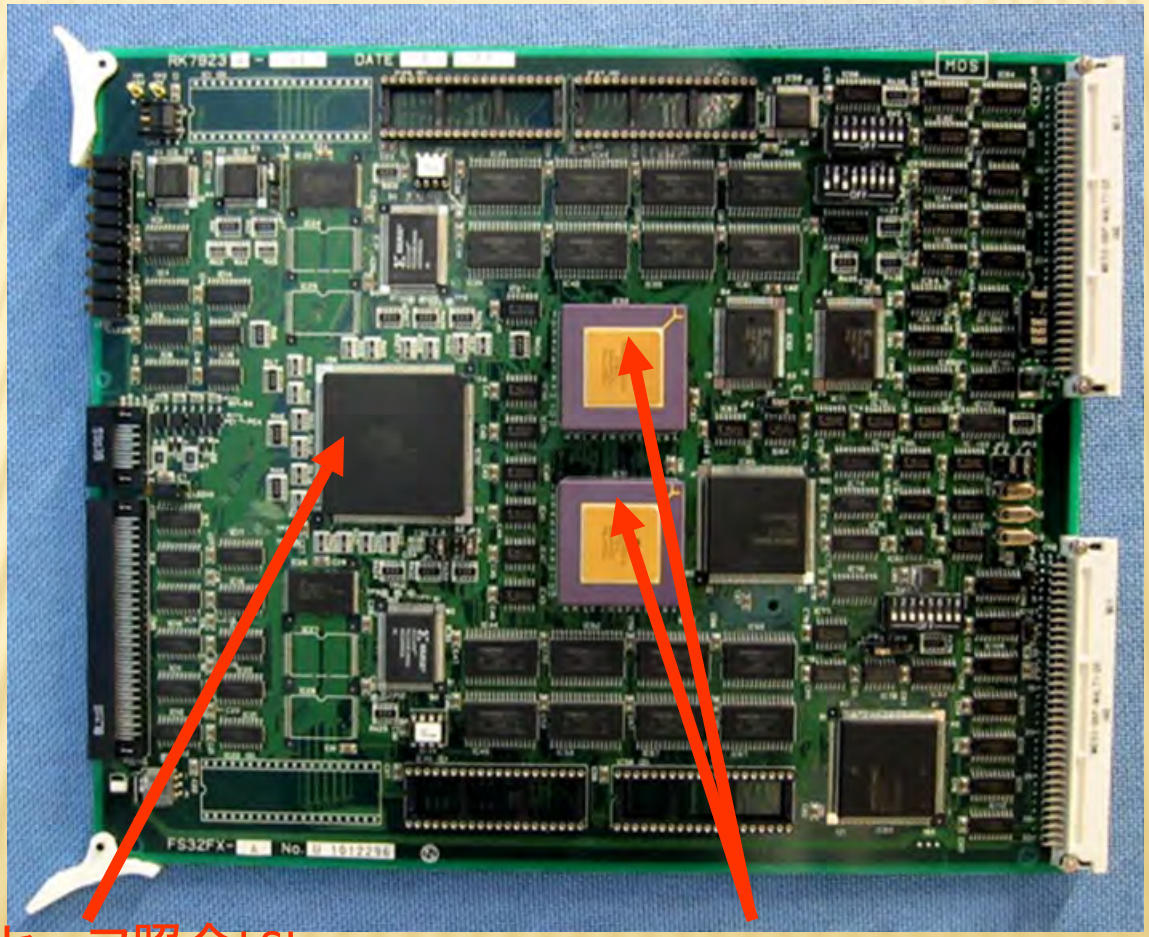
SPAC-8



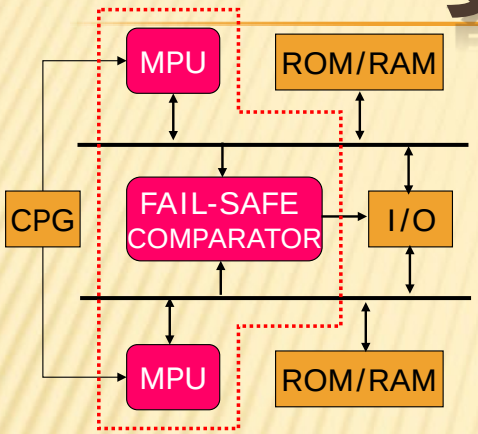


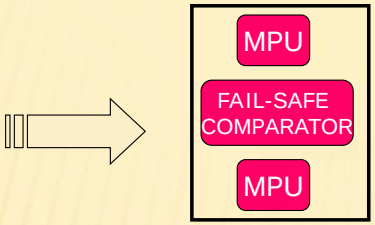
照合回路のLSI化

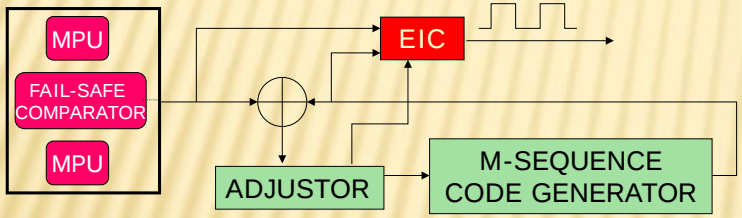
フェールセーフ32ビットボードコンピュータ (コアMPUは68020)

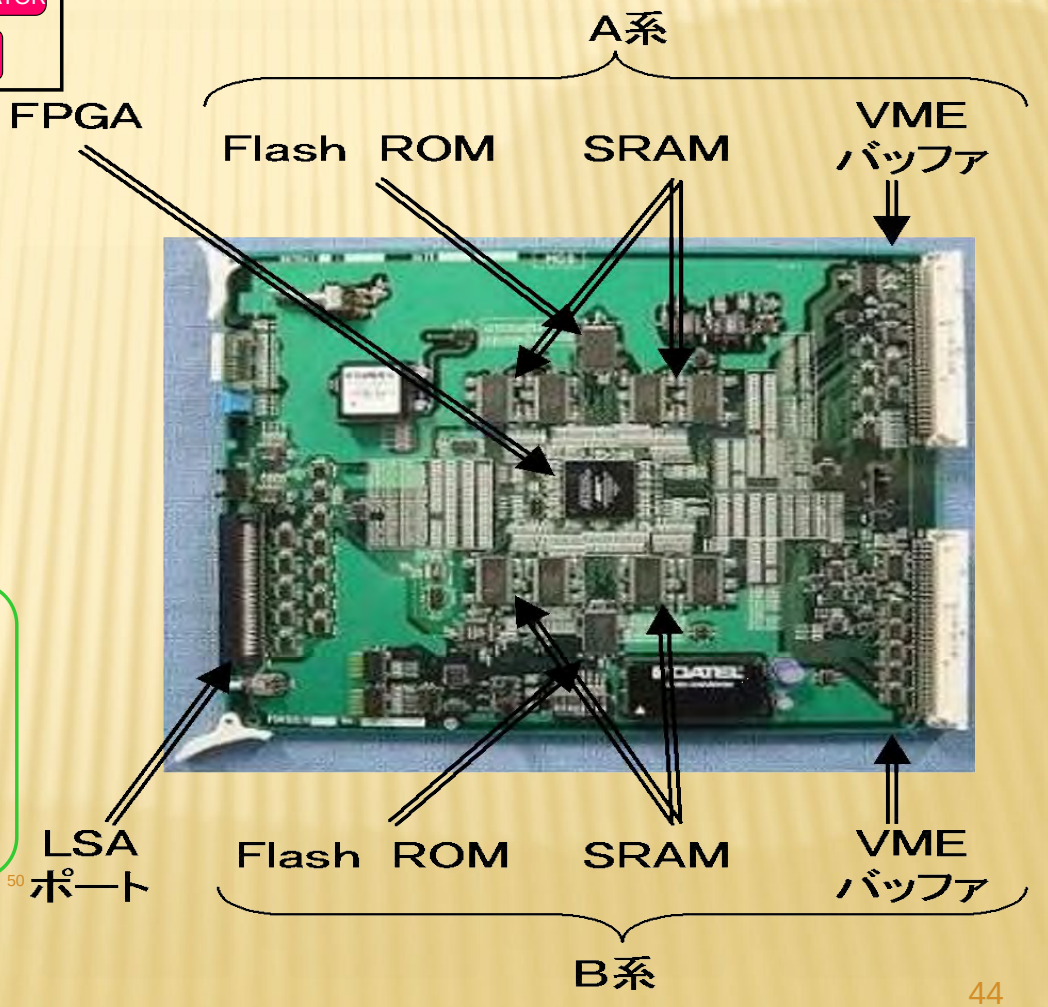


更なる高性能化への挑戦



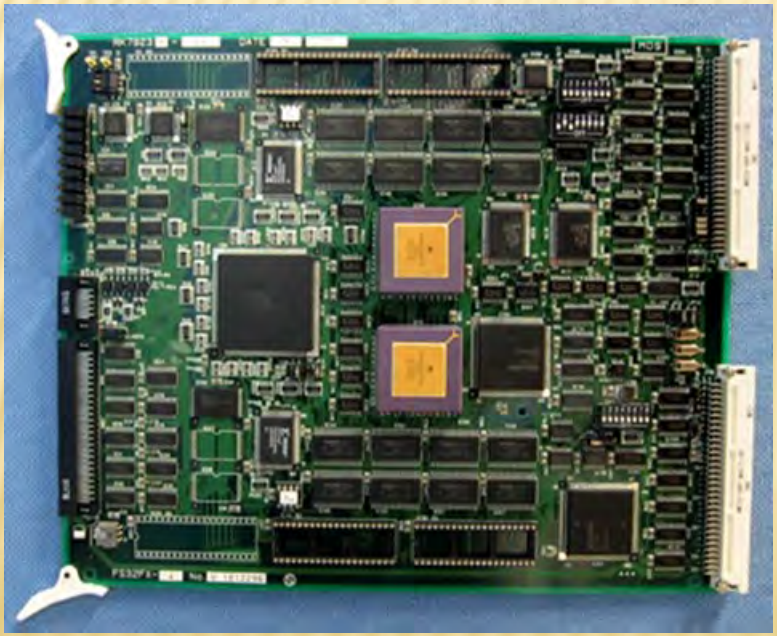




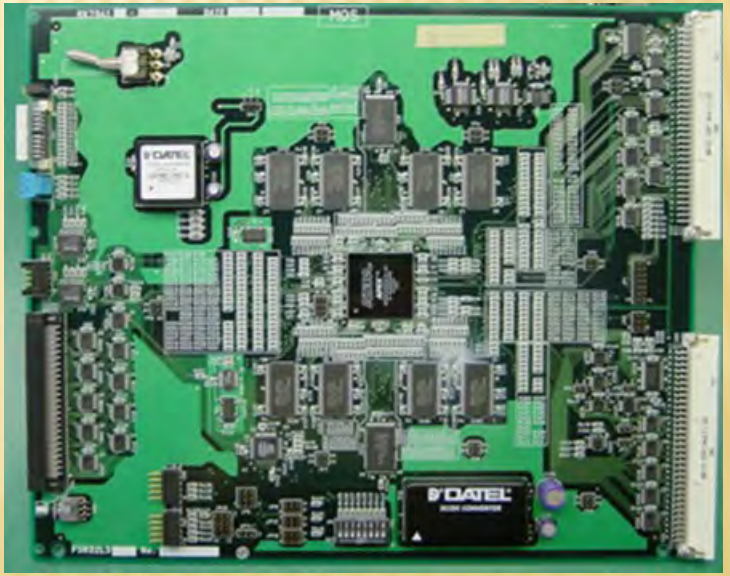


性能比較

- 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



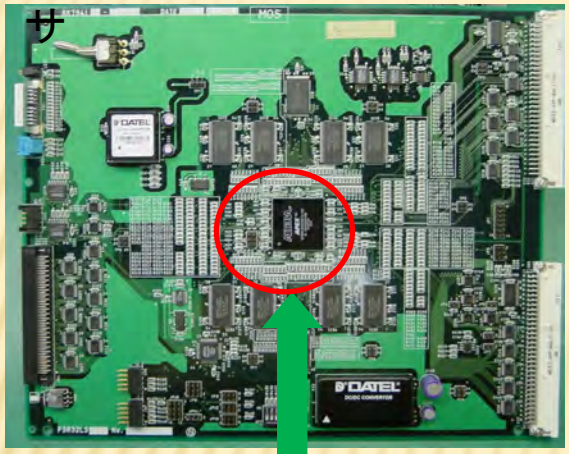
従来品

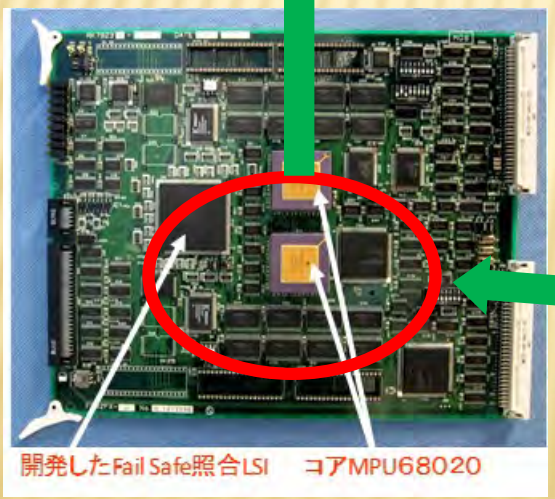


シングルチップFSプロセッサ使用品

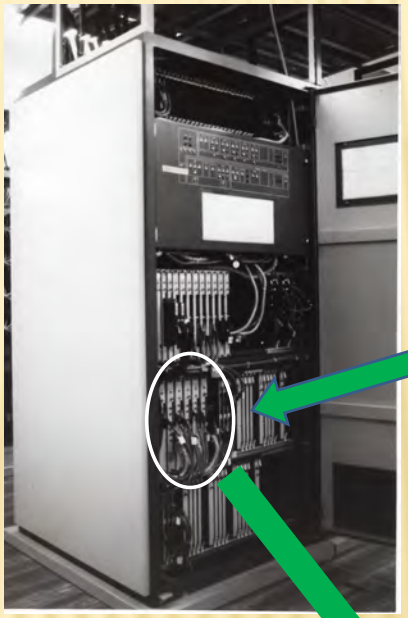
鉄道信号におけるFS-MPUの進歩

32ビットFS　RISCプロセッサ

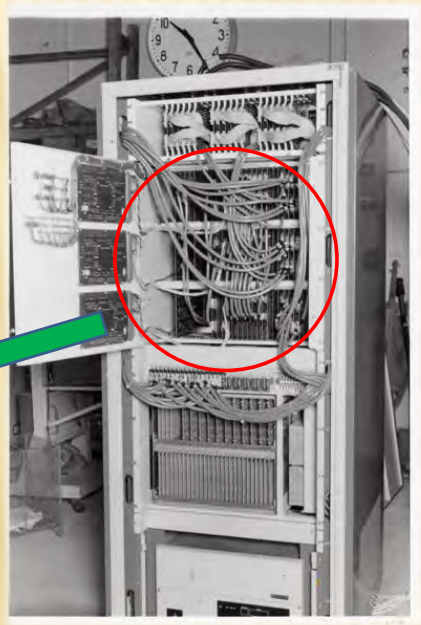


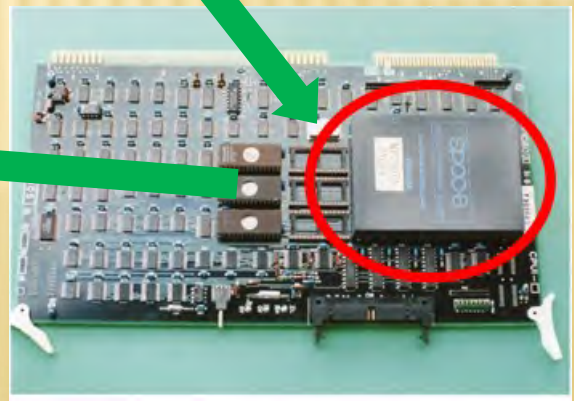


実用装置(1985)



試作装置(1980)

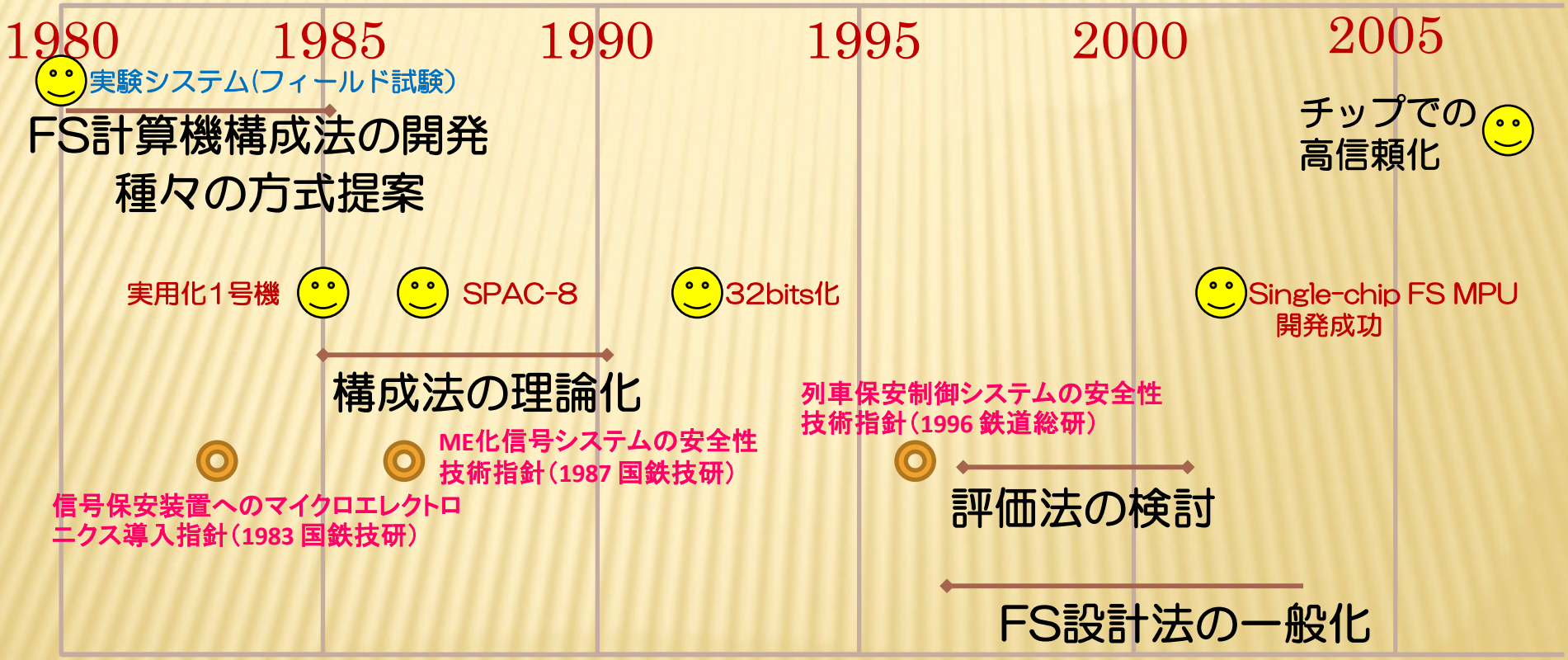




SPAC-8

FS照合回路の
LSI化

鉄道信号用FAIL SAFE計算機開発の流れ



COMPUTER化がもたらしたもの

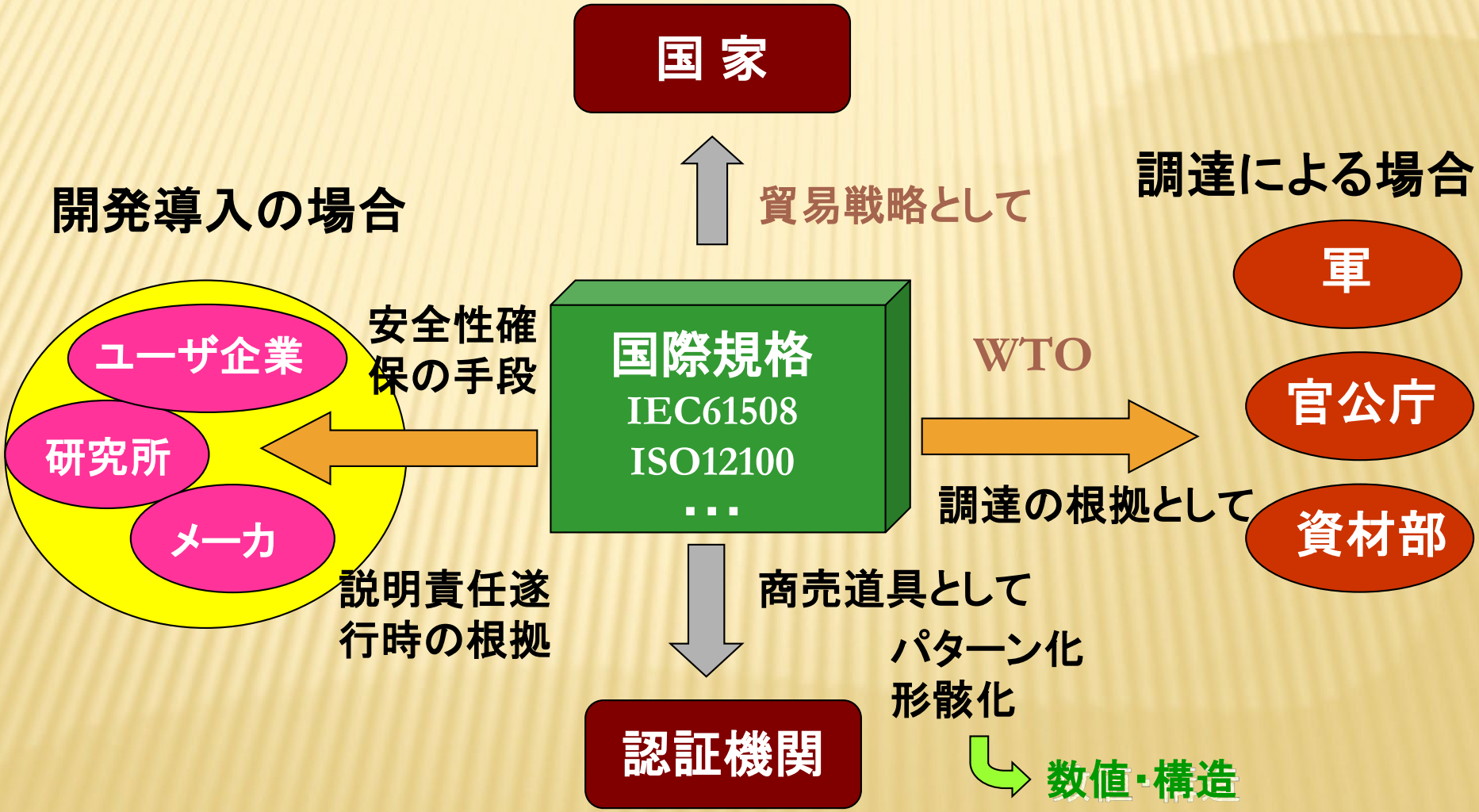
- **産業界独自の安全性技術はプログラム論理に**
- 産業界横断の共通な方法論が登場
  - フェールセーフなコンピュータが必須
    - 方法は多様、入念に配慮されたコンピュータはそれぞれ有効な実績
  - ソフトウェアの安全性が重要
    - バグに対する２つの見解→バグのないソフトは可能/不可能（Formal MethodとDesign Diversity）
  - 安全性の共通尺度としてRISKの登場
- 国際規格の登場

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



IEC61508規格における今日の問題

- 認証機関の要求が力を得る
  - 数量評価の重視
  - アーキテクチャの画一的解釈
  - 要件の単なる網羅
- 安全性立証という本来の思想が形骸化

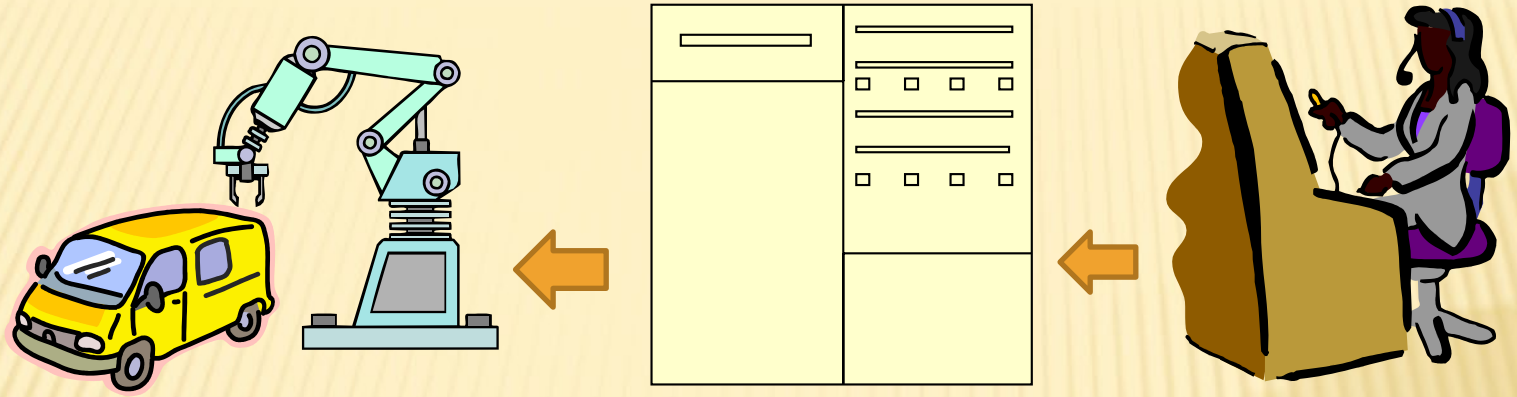
- 過去の経験や技術に触れない
- 技術の総合的・有機的な関係に無配慮
- 新たな技術開発への意欲を削ぐ

認証に伴う課題

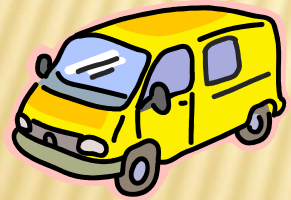
- 機能安全規格：IEC61508
  ハードウェアの要件をも規定
- 共通源故障対策
  - 対象要素の機能喪失により誤処理に至るもの
    - クロックの誤り
    - 入力の誤り
  - 配線間短絡やクロストークによって生じるフェールセーフ機構（単一系）の誤り
  - 素子の同時同一故障の懸念（集積化の課題）
    ASICはSIL３まで（IEC61508 ed.-2)
    果たして妥当か？

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



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

期待される積極的高信頼化方策

- 与えられた条件の中で高信頼化を図るのではなく、システムの機能を実現する本質的アーキテクチャにさかのぼって、高信頼化を実現

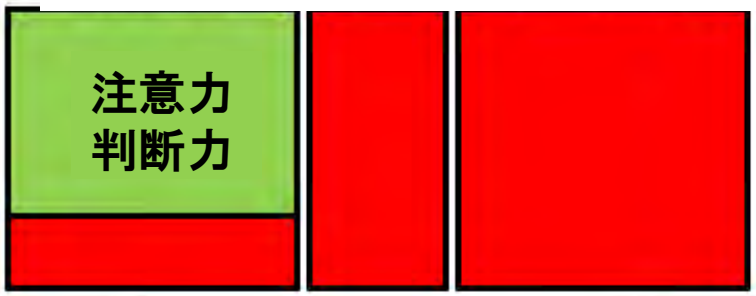
本質制御

- 制御情報を創り出す固有の制御装置を多く配置しない
- 本質的に必要な要素のみで実現するスマートなシステム
- 無線等で要素間の情報交換で安全を実現（協調安全）
- 高度な機能を処理装置を設置せずに実現

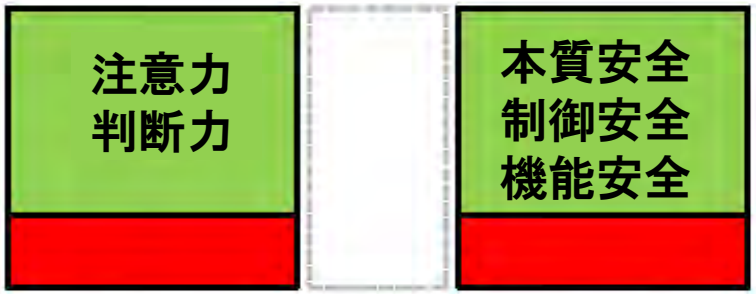
IOTによる本質制御の実現

- **本質的に必要な要素間**のみで相互に情報を交換し、機能を実現（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）

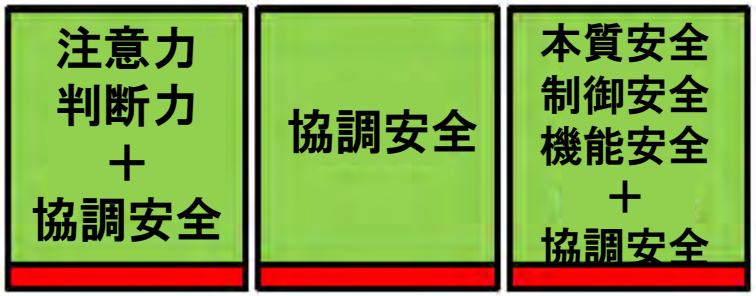
本質制御の具現化、IOT時代の安全文化



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）

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

シーケンス時代の耐雑音戦略が・・・

- 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
- センサーに用いられる電流も、雑音レベルに対し10dBのマージンを・・・

- コンピュータシステムの下ではエントロピーによる対応も有効

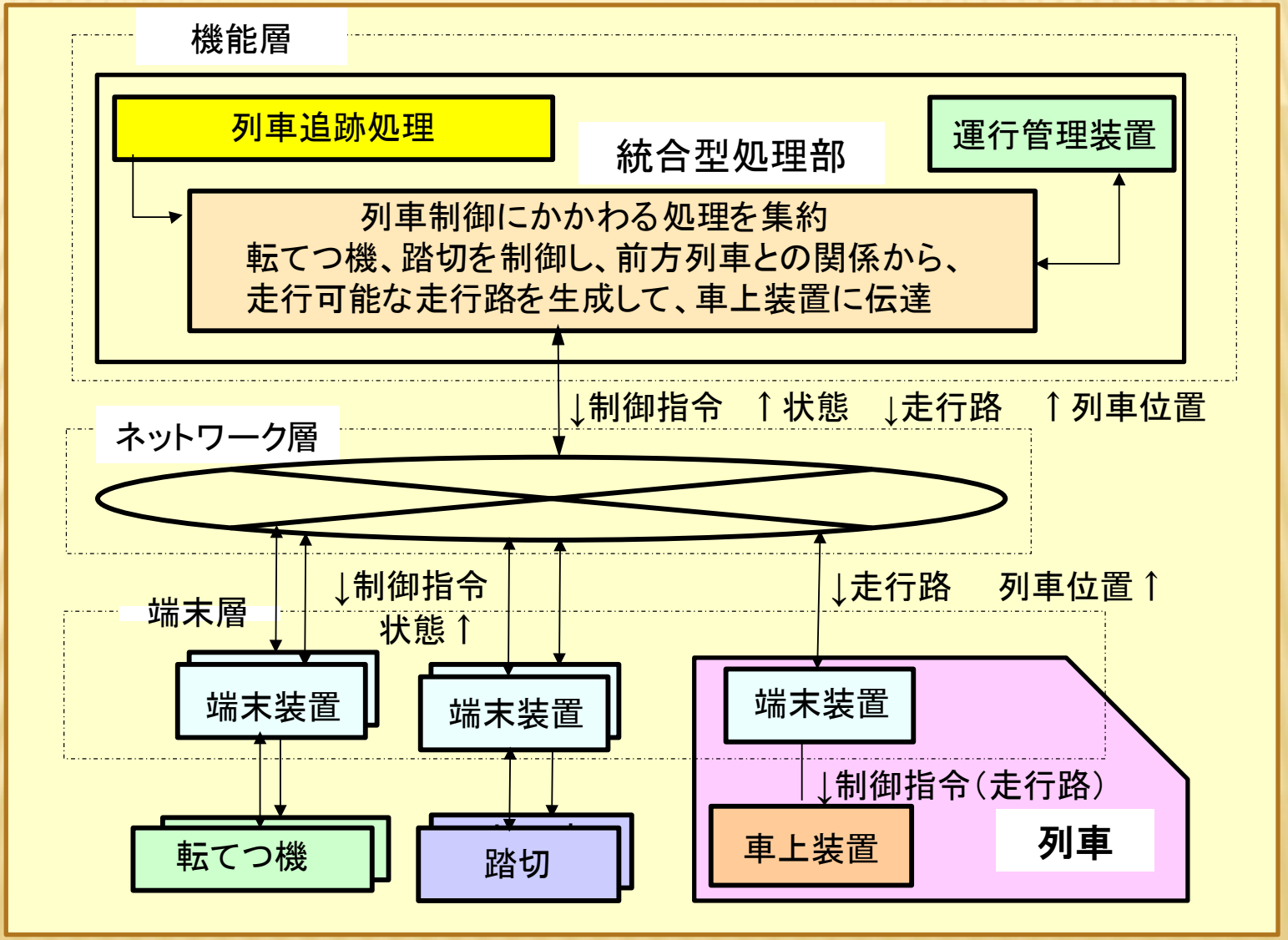
技術進歩とオープン化

- セミカスタムLSIを！
  - 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）
- 命令セットアーキテクチャをオープンソースに→RISC-V
  オリジナルなコンピュータが作れる

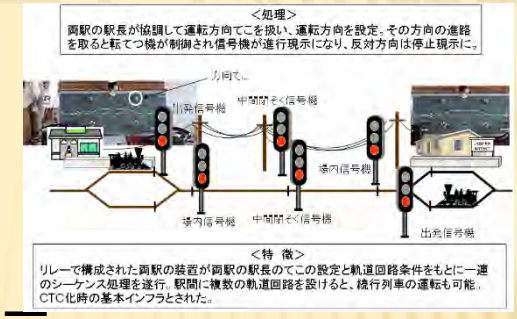
故意の外乱の脅威への対応

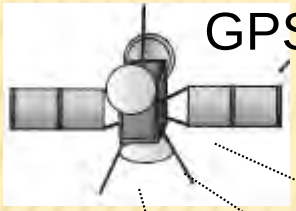
- IoTによる協調安全の実現には、セキュリティ確保が重要に
- 命令セットアーキテクチャ（ISA）を開放するRISC-Vに着目
- RISC-Vでは、TEE (Trusted Execution Environment)に対する配慮が注目されている

鉄道における事例：UTCS



本質制御の鉄道システム：ATP閉塞システム

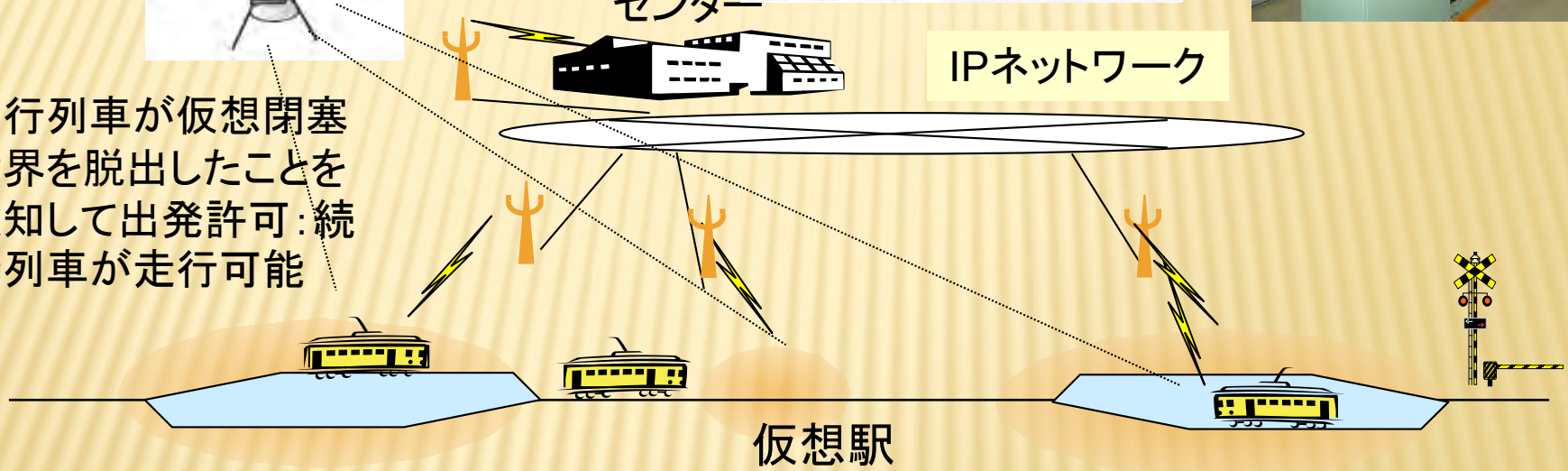




センター

IPネットワーク

先行列車が仮想閉塞境界を脱出したことを検知して出発許可：続行列車が走行可能



次駅到着までに,さらにもう一つ先の駅までの走行許可を得ることで通過や、追越し運転を実現

駅停車パターン制御により、過走防護のための踏切鳴動時分増加もなし

安全から見たシステムの変遷

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	安全制御から人間排除
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	安全制御から人間排除
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	RISC-VのTEEに依拠

2019年6月7日

2019.6.7SNJ講演

「終」ら見たシステムの変遷」

終り

日本大学名誉教授　中村英夫