2019.6.7SNJ講演

2019年6月7日

「安全から見たシステムの変遷」

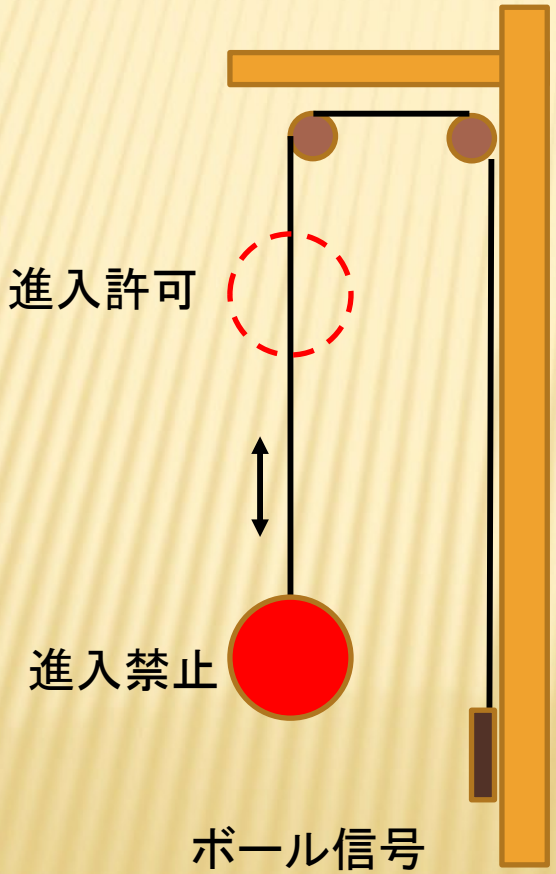
日本大学名誉教授　中村英夫

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
  - ソフトウェア
- 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

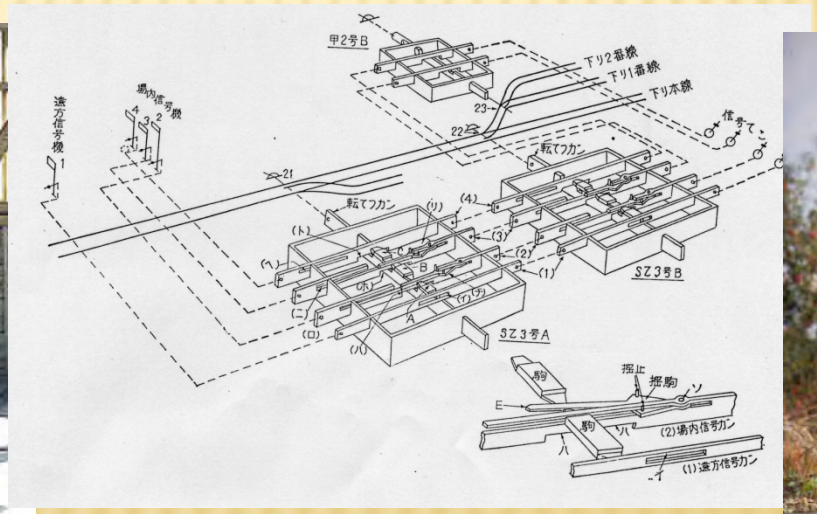
フェールセーフの原理

機械式時代：人間の過誤

- 信号機と転てつ機の直接的連動

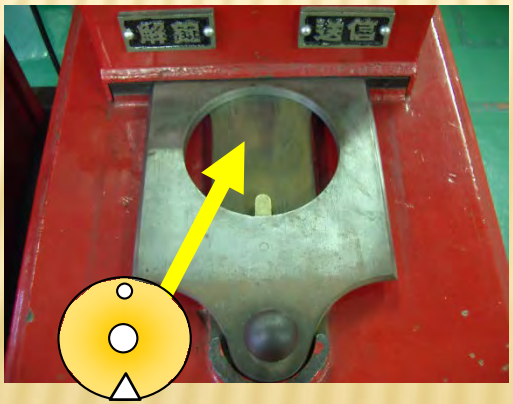
  人力による制御

  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



単線区間の安全

タブレットをやりとり



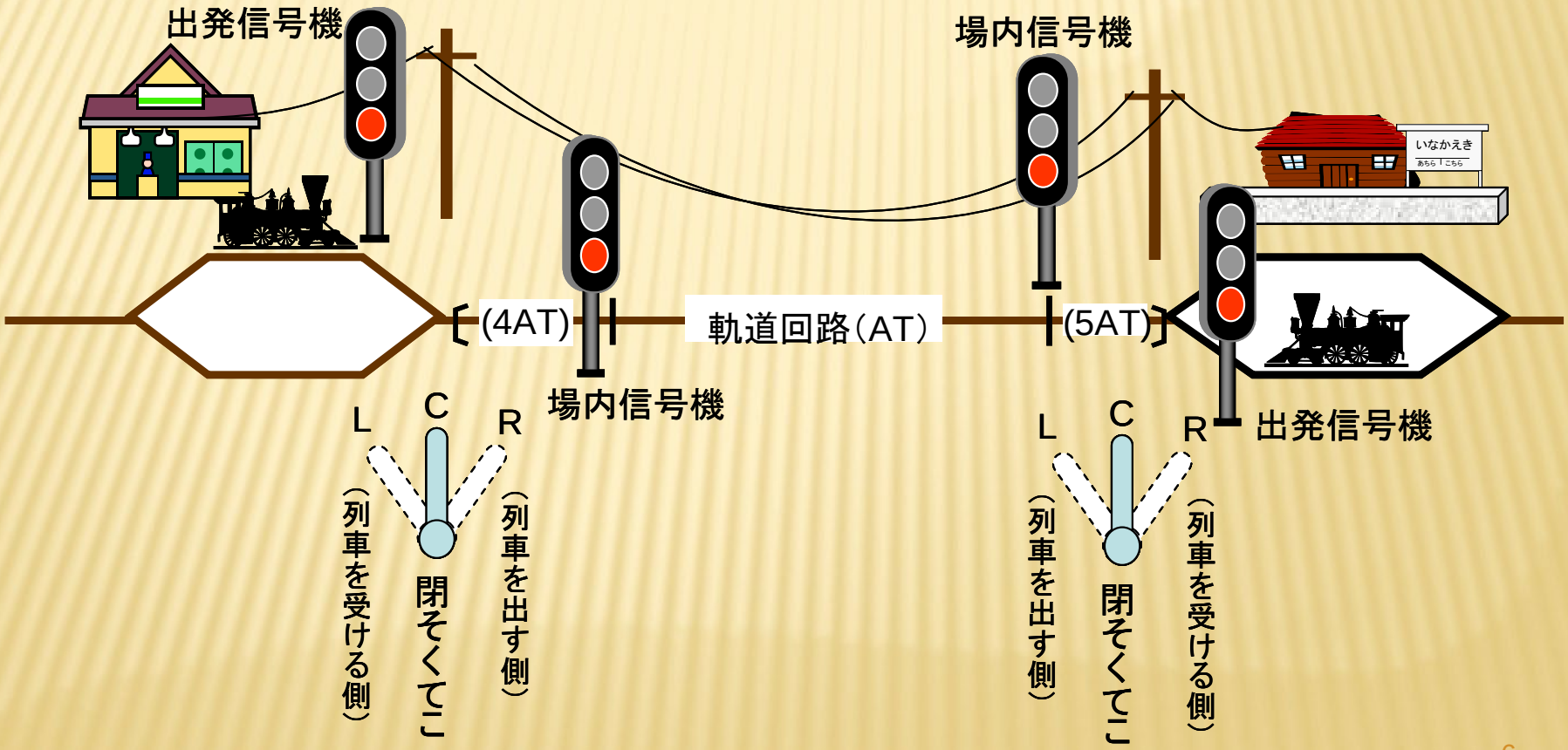
同一方向に連続して運転させるときには着駅でタブレットを納めて，両駅の駅長の共同作業により出発駅から取り出す。

駅間で異なるタブレット

5

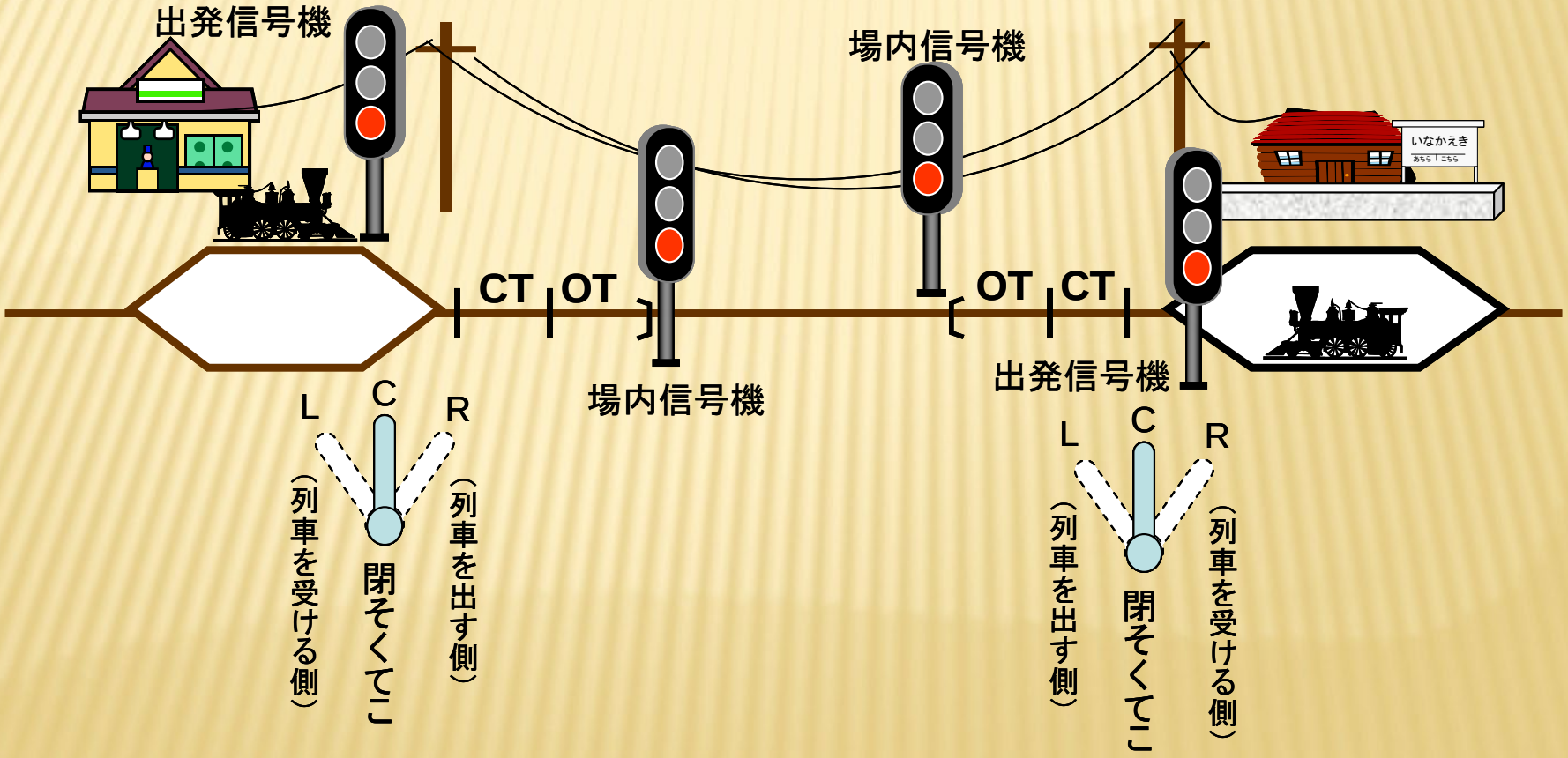
運転方向と進路設定を保障：連動閉塞

＜仕組み＞
軌道回路で駅間に列車がいないことを検知し、閉そくに反映。両駅の駅長の作業で運転方向を決定。駅間閉そくと進路設定OKで信号機が進行現示。運転士は信号現示を見て出発すればよい。



運転方向と進路設定を一体化：連査閉塞

＜仕組み＞
駅間の長い軌道回路に代わり、CTとOT（コラム参照）の組合せで駅間に列車がいないことを検知することにした。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

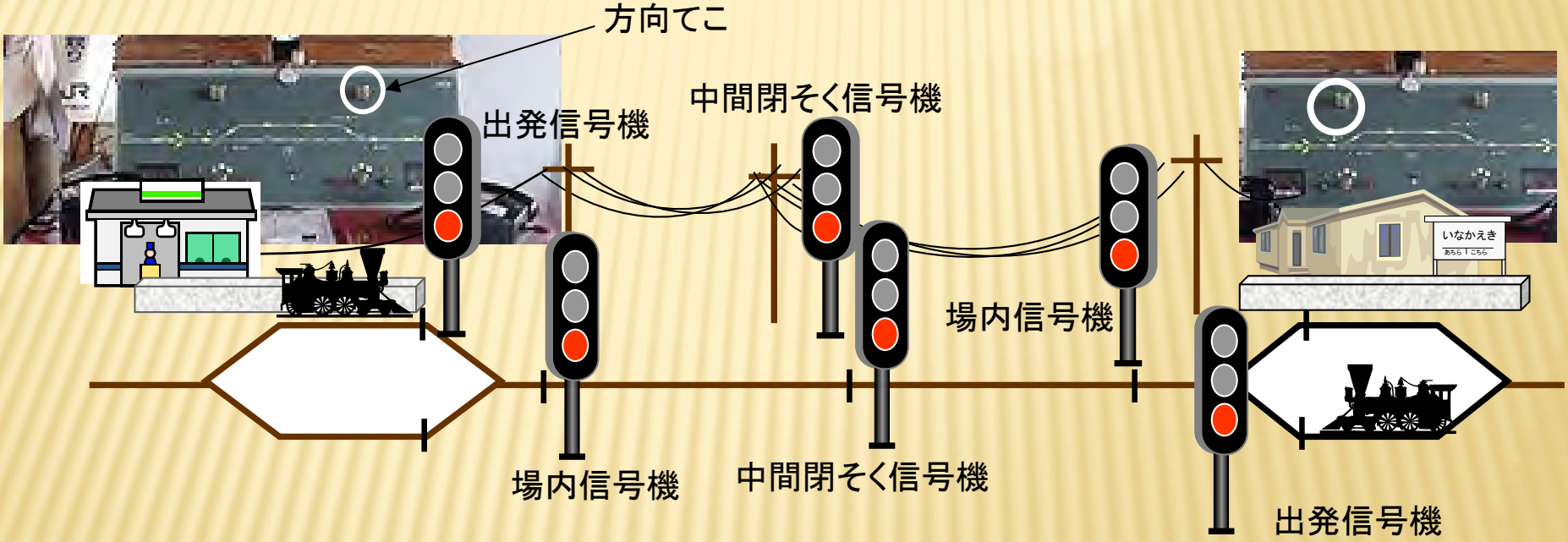
発生日: 1962年（昭和37年）11月29日

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）。
　助役が単行機関車に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、出発信号機の停止を確認せずに出発合図
⑩ 両駅の中間部付近で正面衝突

単線自動閉そく

＜処理＞

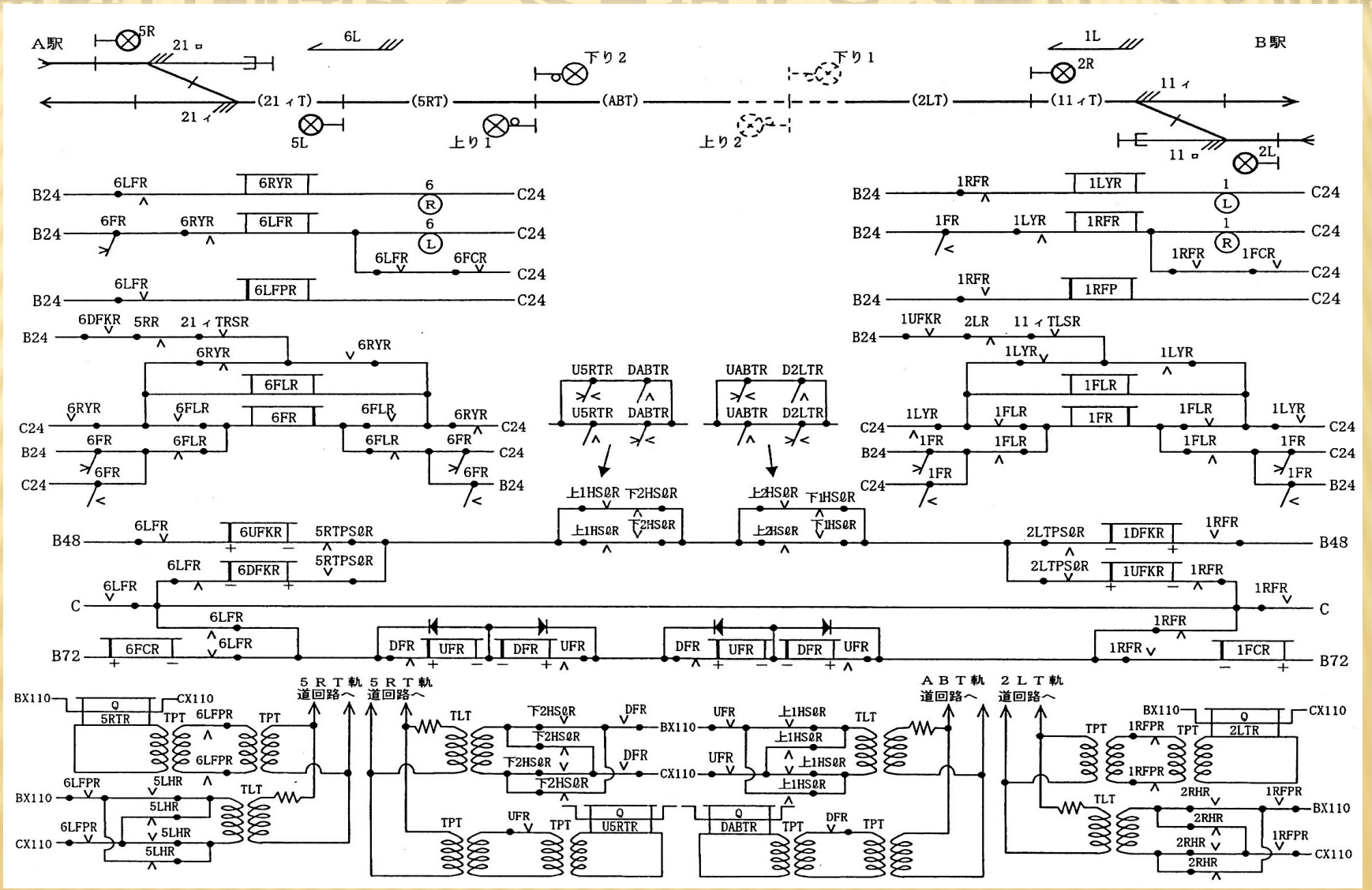
両駅の駅長が協調して運転方向てこを扱い、運転方向を設定。その方向の進路を取ると転てつ機が制御され信号機が進行現示になり、反対方向は停止現示に。



＜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

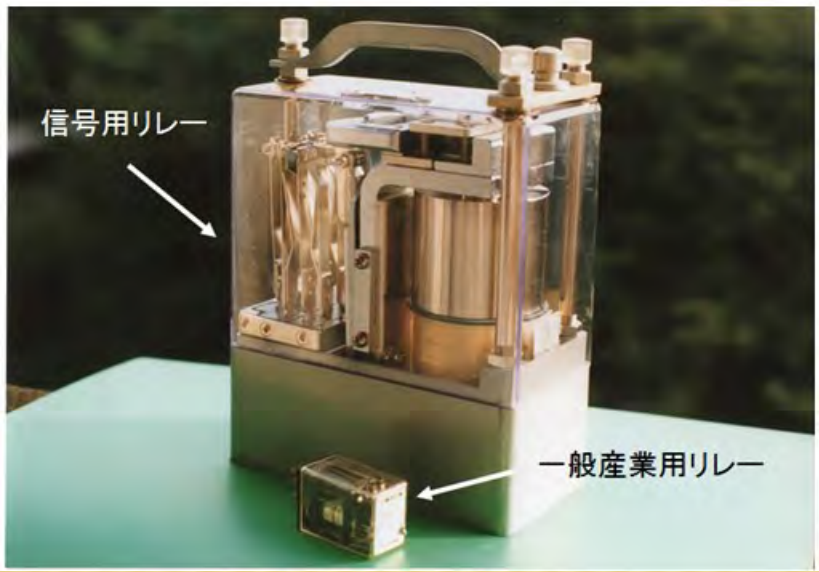


シーケンス論理による安全の確保

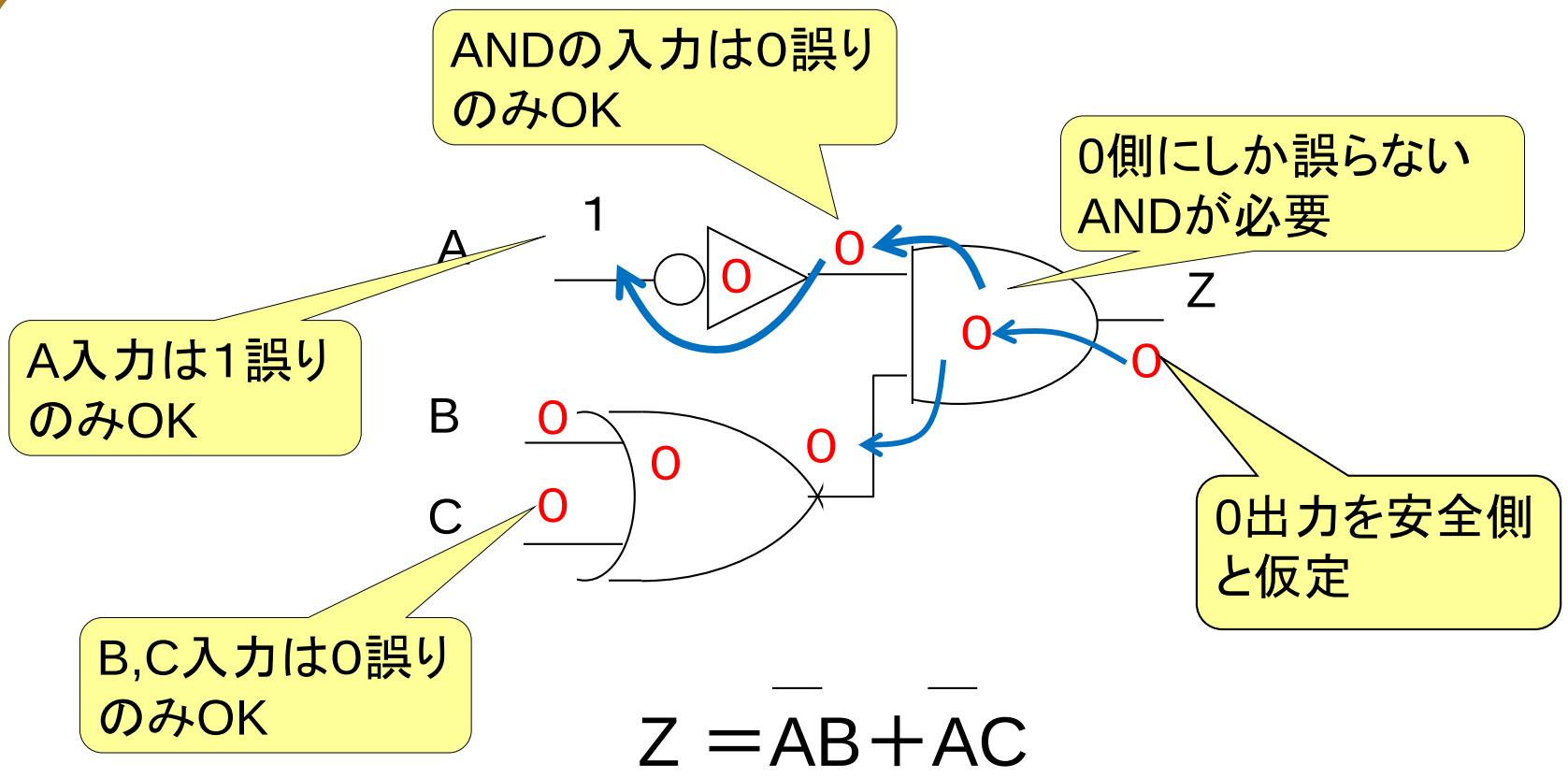
- センサー（安全への配慮）
- アクチュエータ（動作状態の確認）
- シーケンス回路をフェールセーフに
- 論理による安全機能拡大
  - 再起動防止回路
  - 接近鎖錠
- 制御室の配置に自由度が
  - 通信技術による遠隔制御

FAIL-SAFE論理の解明

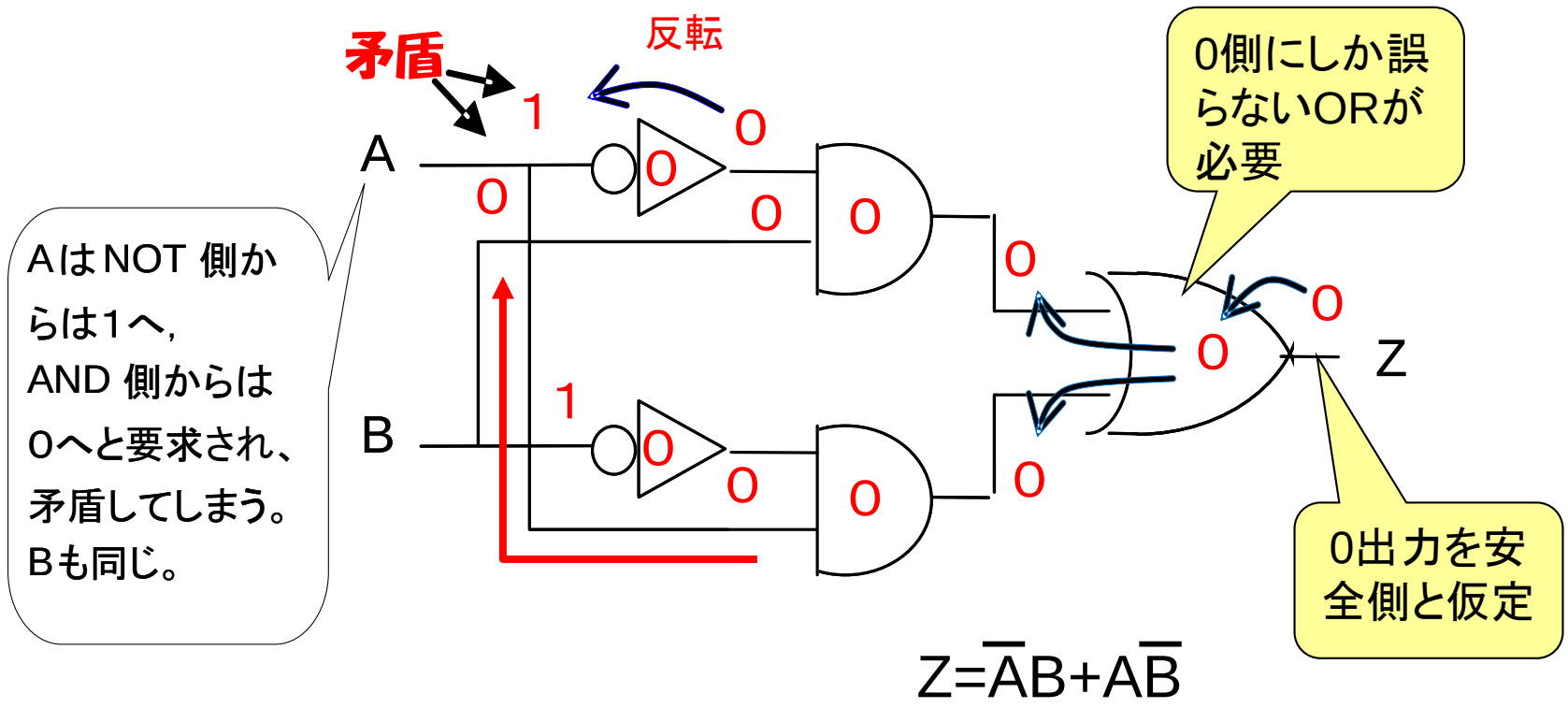
- Fail-Safe技術は経験工学的に進展してきた
- 回路レベルでのFail-Safeは日本で解明された
  - 鉄道の継電連動装置のFail-Safeの仕組みにメスが
  - 1965年にFail-Safe論理系の研究が発表されるや学会レベルで多くの研究が開花
  - 当時、Fail-Safe論理系の研究は日本の独壇場



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



FAIL-SAFEにできる回路とできない回路

$O_1=\overline{A}B+BC+CA$	できない	$O_1=\alpha B+BC+C\overline{\alpha}$
$O_2=\overline{A}B+\overline{A}C$	できる	$O_2=\alpha B+\alpha C$
$O_3=\overline{A}B+A\overline{B}$	できない	$O_3=\alpha\overline{\beta}+\overline{\alpha}\beta$
$O_4=\overline{A}B+BC+C\overline{A}$	できる	$O_4=\alpha B+BC+C\alpha$

ここで、$\overline{A}$ を　α　、$\overline{B}$を β とおくと

正関数はフェールセーフにできる

FAIL-SAFE論理系への誘い

- １，０の２値．０：安全側．１＞０と定義
- 正規入力　A＝{a1,…,an}

  誤り入力　A’＝{a1’,…,an’}が安全側とは

  →A≧A’すなわち任意のｊでaｊ≧aｊ’
- 回路の論理関数：F、　故障時の関数：F’
- 入力Aのときの出力：F{A}とする．

  回路の故障に対しFail-Safeなら

  F{A}≧F’{A}

  入力の誤りにも、回路の故障にも

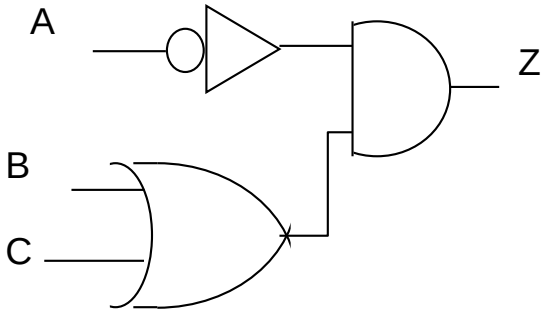
  F{A}≧F’{A’}成立ならフェールセーフ

S=(0,1,1,0,1,1,0,0)
T=(0,0,1,0,0,1,0,0)

P=(0,0,1,0,1,1,0,1)

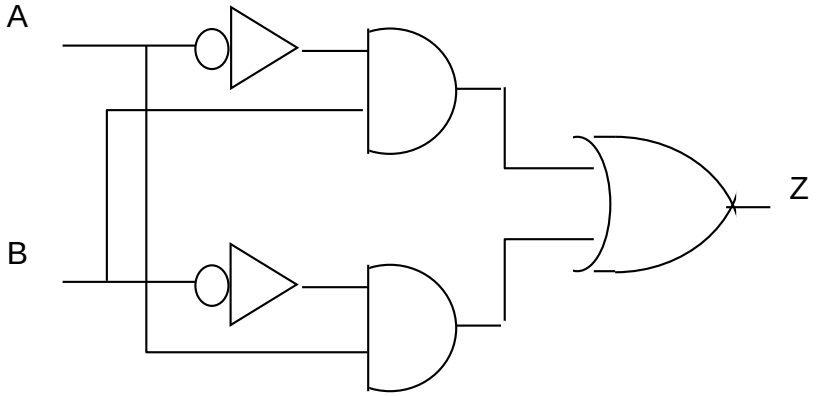
S ≧ T,　S ≧ P

2つの回路の差とユネイト性



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

正入力もしくは負入力しか用いてない



単調（ユネイト）な回路

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

正入力と負入力が混在

FAIL-SAFE論理系の構成法

- 回路がユネイトであるなら、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)

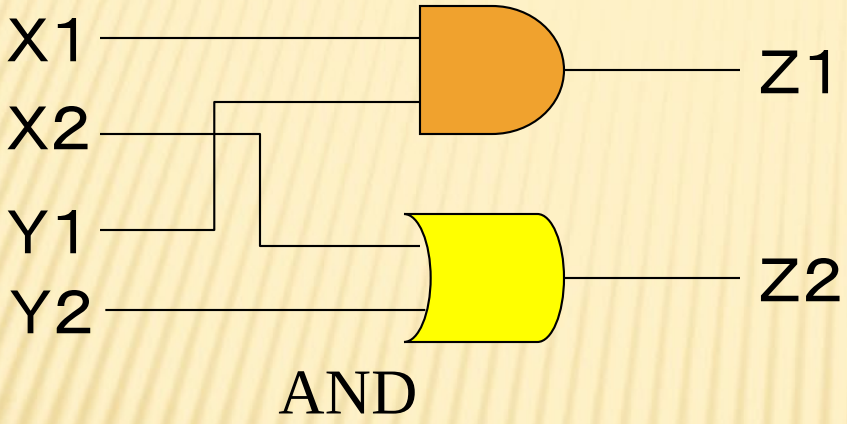
２線式論理（TWO RAIL LOGIC）

- フェールセーフにならない回路を
  フェールセーフにするには
- 対称誤り素子でフェールセーフを実現するには

1→（1，0）　0→（0，1）

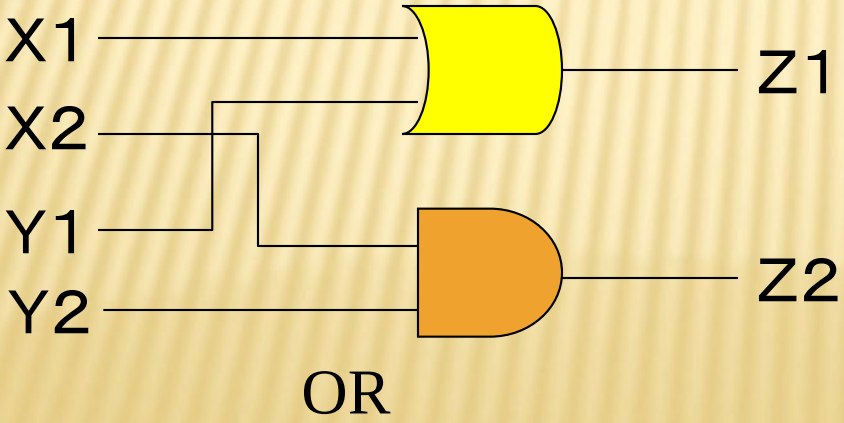
（1，1），（0，0）→誤り

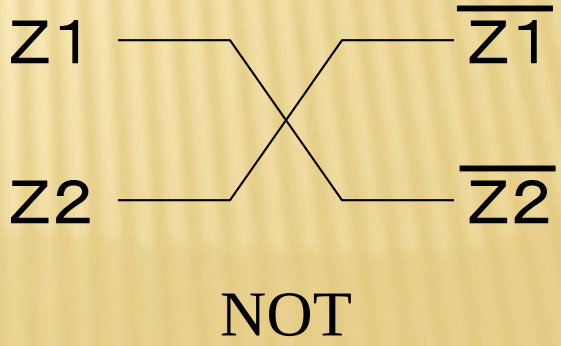
２線式論理の基本素子



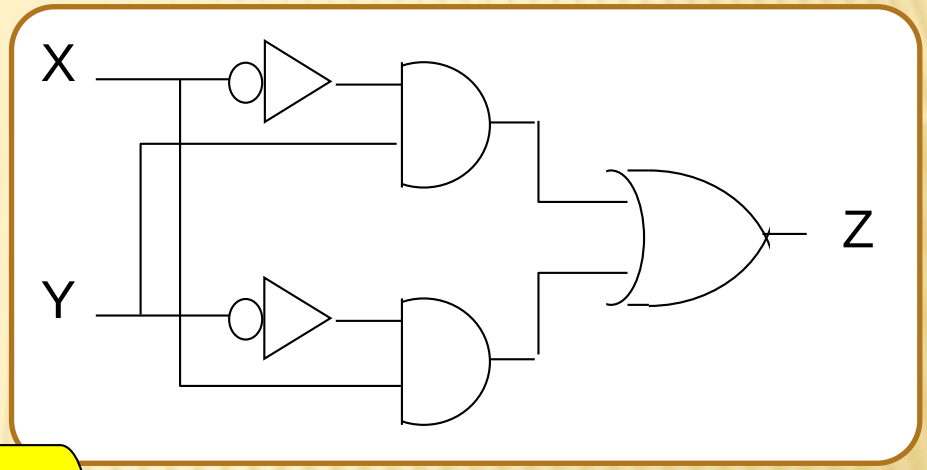
X ;(X1,X2),　　Y ;(Y1,Y2)

X	Y	AND	OR
(0,1)	(0,1)	(0,1)	(0,1)
(0,1)	(1,0)	(0,1)	(1,0)
(1,0)	(0,1)	(0,1)	(1,0)
(1,0)	(1,0)	(1,0)	(1,0)

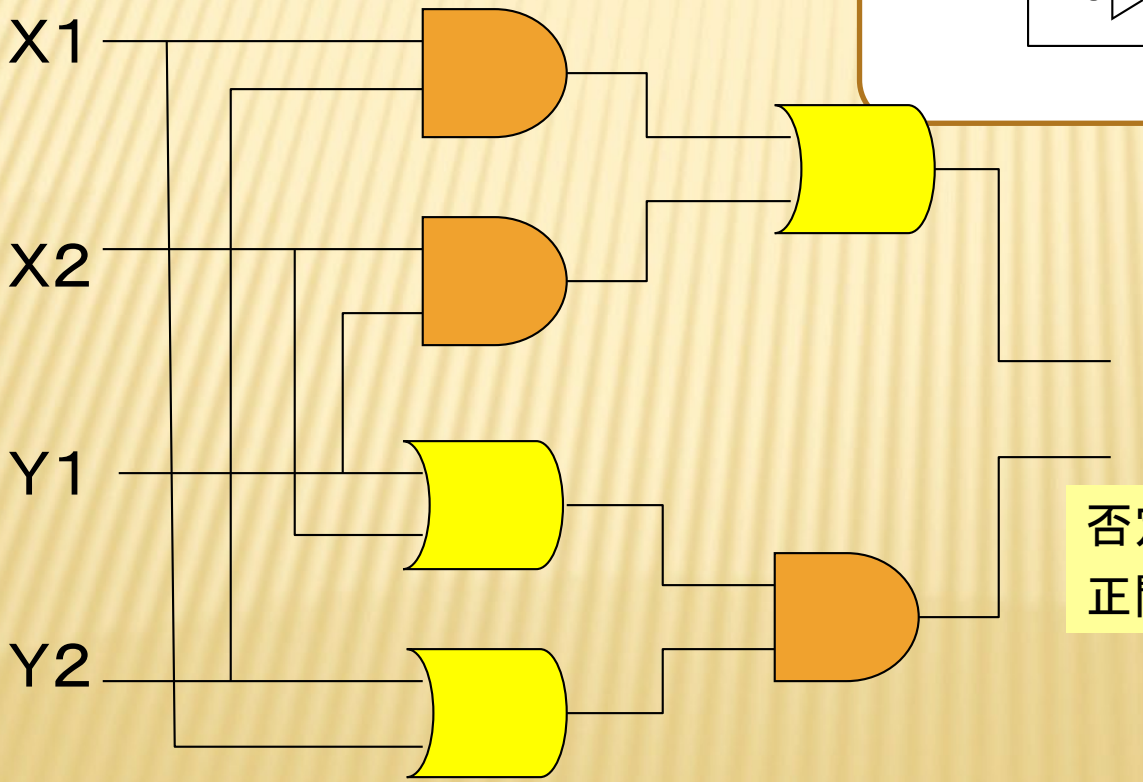




２線式論理によるFAIL-SAFE化



$Z=\overline{X}Y+X\overline{Y}$



否定を用いない→正関数

正関数→ユネイト関数

3値フェールセーフ論理

2線論理の非符号語(0,0)，(1,1)を誤り入力として物理量に割り当て→3値論理

C型フェールセーフ論理(AND)

入力 状態値	0	ϕ	1
0	0	ϕ	0
ϕ	ϕ	ϕ	ϕ
1	0	ϕ	1

Φ型フェールセーフ論理（AND）

入力 状態値	0	ϕ	1
0	0	0	0
ϕ	0	ϕ	ϕ
1	0	ϕ	1

フェールセーフ論理素子の開発

開発年代	回路構成・素子
1962	過飽和リアクトル
1966	RC 結合マルチバイブレータ
1966	パラメトロン
1967	しきい値発振型
1968	２重化冗長（トランジスタ，抵抗）
1968	単極性コアトランジスタ
1975	２重化照合（トランジスタ，抵抗）
1980	定電流ダイオード，フォトカプラ
1983	周波数論理方式