

2013-3-23最終講義 明治大学リバティータワーにて

安全学の夢に向かって

～論理・ファジィから安全へ～

明治大学 理工学部 情報科学科
理工学研究科新領域創造専攻安全学系
向殿政男

自己紹介

2012-11-17明治中・高校100周年記念講演より

- 1955 明治小学校 卒業
- 1958 明治中学校 卒業
- 1961 明治高校 卒業
- 1965 明治大学工学部 卒業
- 1970 明治大学大学院 工学研究科博士課程 修了
- 1970 明治大学工学部電気工学科 専任講師
- 1973 明治大学工学部電気工学科 助教授
- 1978 明治大学工学部電子通信工学科 教授
- 1989 明治大学理工学部情報科学科 教授
- 1992 明治中学・高校同窓会 総明会 会長
- 2009 明治大学校友会 会長

昭和生まれの明治一代男

私の研究のあゆみ

- 1. フェールセーフの研究**
- 2. 多値論理の研究**
- 3. ファジィ理論の研究**
- 4. 安全の研究**

1. フェールセーフの研究

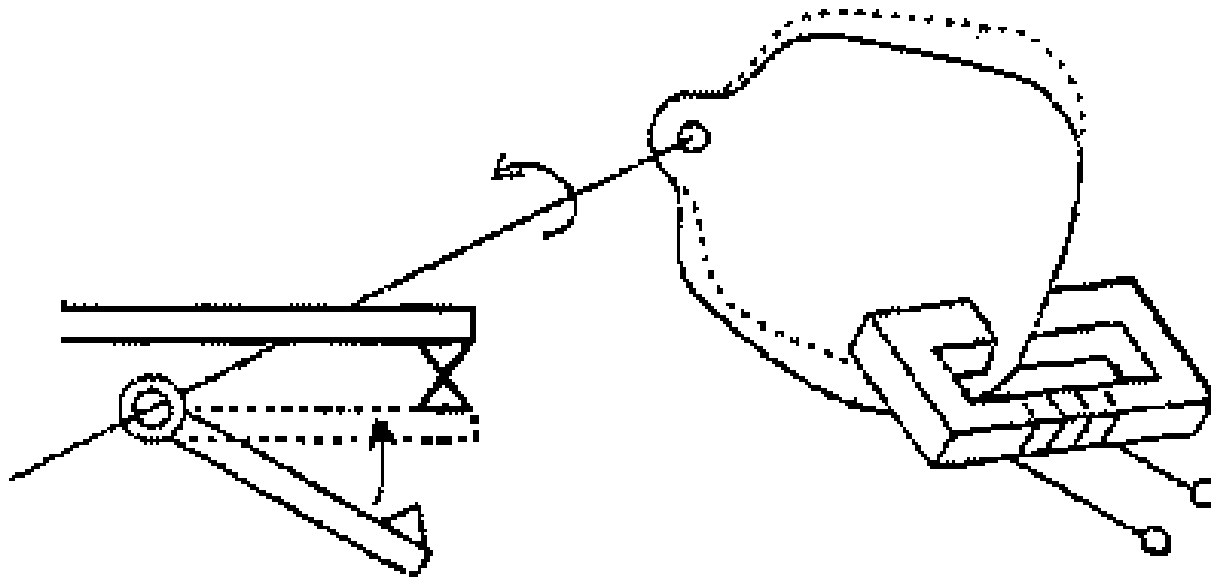
修士論文:「Fail-Safe AND 回路--特に3入力 Fail-Safe AND 回路について--」

博士論文:「Fail-Safe 論理の理論的研究」
安全＋情報＋論理の交差点から研究は始まる

フェールセーフという概念

- 故障しても(失敗しても)安全である
- 故障は認めるが、安全側の故障のみとする
- 故障すると、正しい機能を果たすか、または、ある決まった状態に固定される
- 重力等を利用する場合が多い
- 無条件安全の状態の存在が条件(例:止まれば安全)

フェールセーフ電磁リレーの例



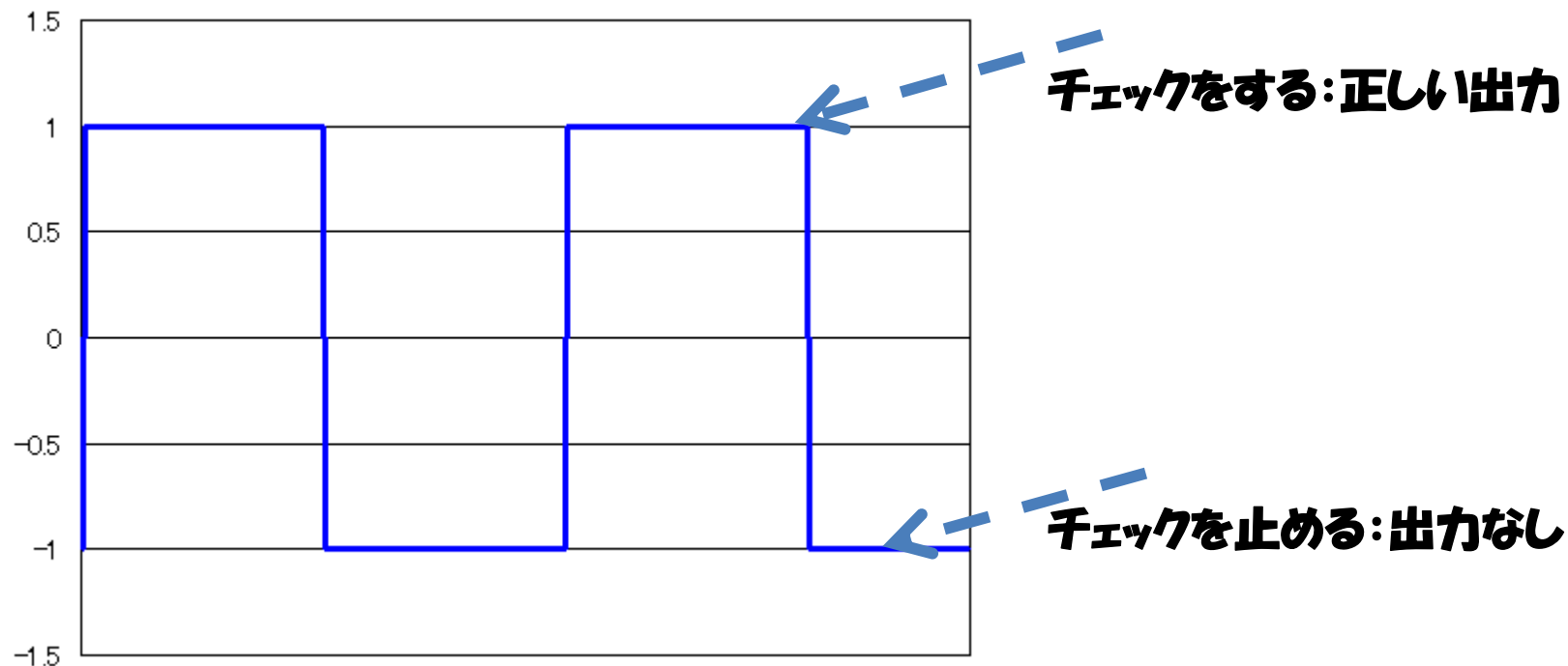
非対称故障特性

半導体(電子回路)は フェールセーフになるか？

- 重力は使えない
- オープン(開)、クローズ(閉) 何でもありだ！
- 基本的に対称故障であり、非対称故障特性(故障すると、ある一定の状態になる)は、ない！！

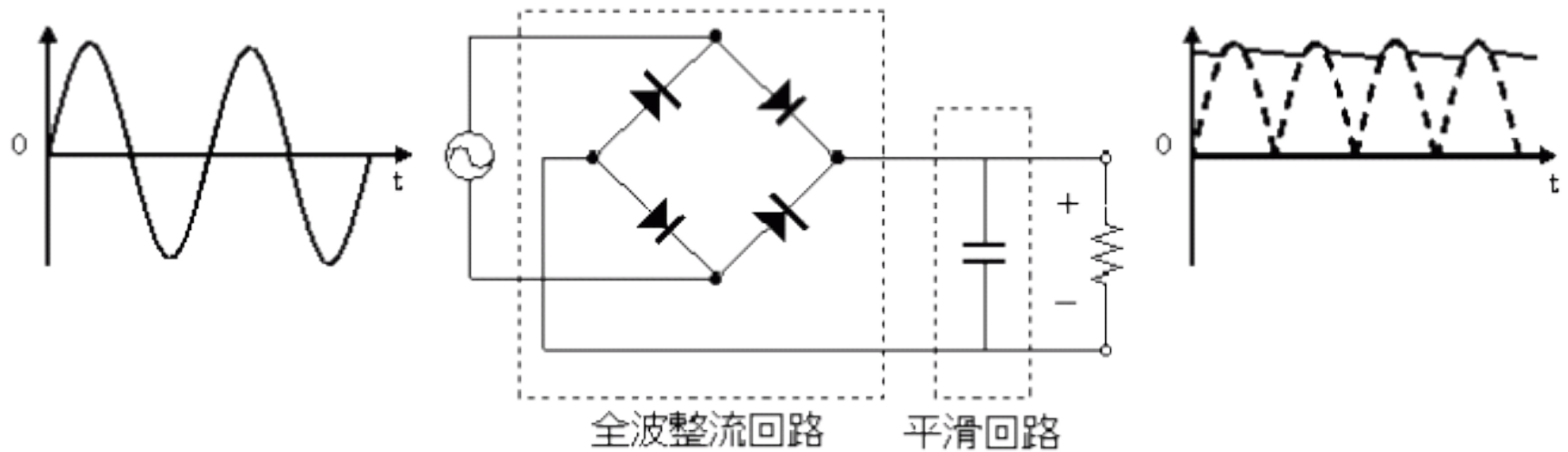
→半導体でフェールセーフなリレーを作れ(私の修士・博士論文): 恩師後藤以紀先生の紹介で電気試験所の実習生として研究

定期的なチェック→パルス波となる



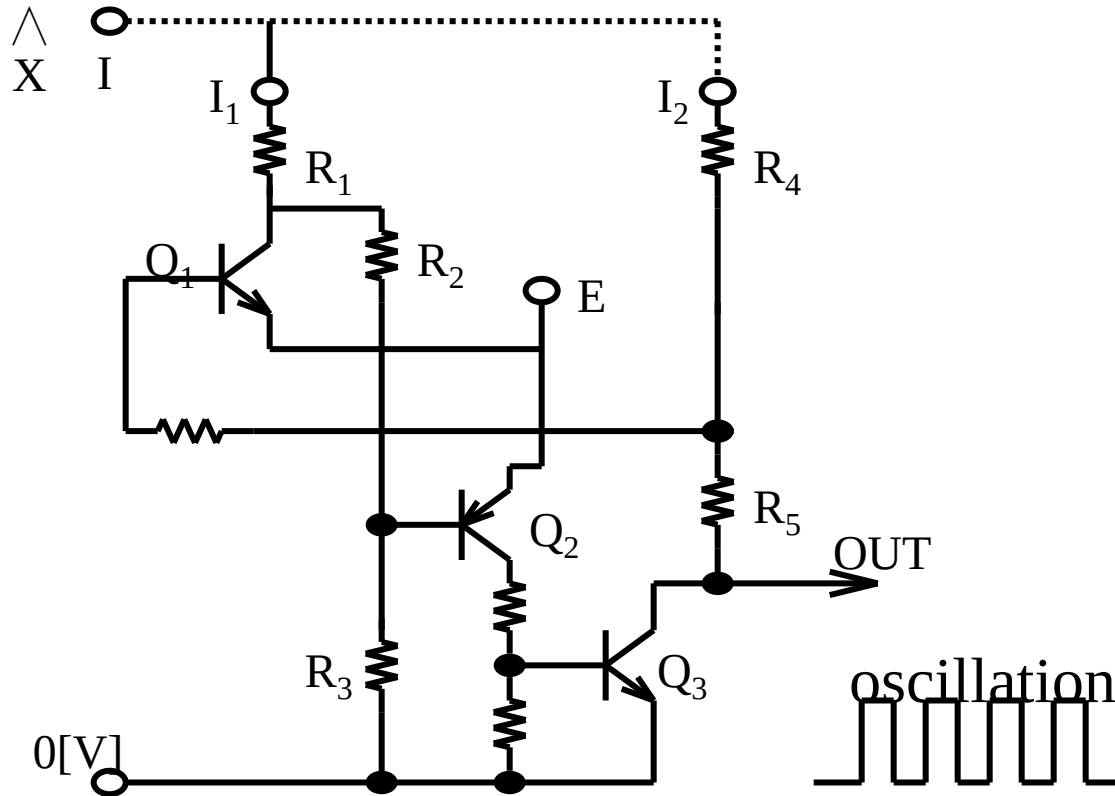
整流回路

平滑回路



フェールセーフ論理回路

(土屋誠治、駒宮安男、向殿政男⇒蓬原弘一)



oscillation

$$\left(\frac{(R_1 + R_2 + R_3)E}{R_3} \right) < I_1$$

window

$$I_2 < \left(\frac{R_1 + R_3}{R_3} E \right)$$

Both of inputs make oscillation

フェールセーフ論理回路

- すべてが正しい時だけ出力が出る
- 故障が生じると(いかなる故障であっても)出力は出ない
- 定期的にチェックを行い、その信号をエネルギーとして取り出す
- 対称故障を非対称故障にする原理
- 半導体でフェールセーフが 実現できた！

⇒ダイナミックフェールセーフ技術の発見

新しく見出された フェールセーフ実現のための原理

- エネルギーを利用した(重力はその一例)
- **ポテンシャル極大の概念**: 正しい状態をエネルギーの極大の状態に対応させる
- **ベクトル和の概念**: すべてが正しい時だけエネルギーの高い状態を保持する
- **エントロピー増大の原則**: エネルギーは放置すると拡散してしまう(逆はあり得ない)
- **ハイボールの原理**: 安全確認信号にはエネルギーの高い状態に対応させる

ハイボールの原理

日経ものづくり: 向殿

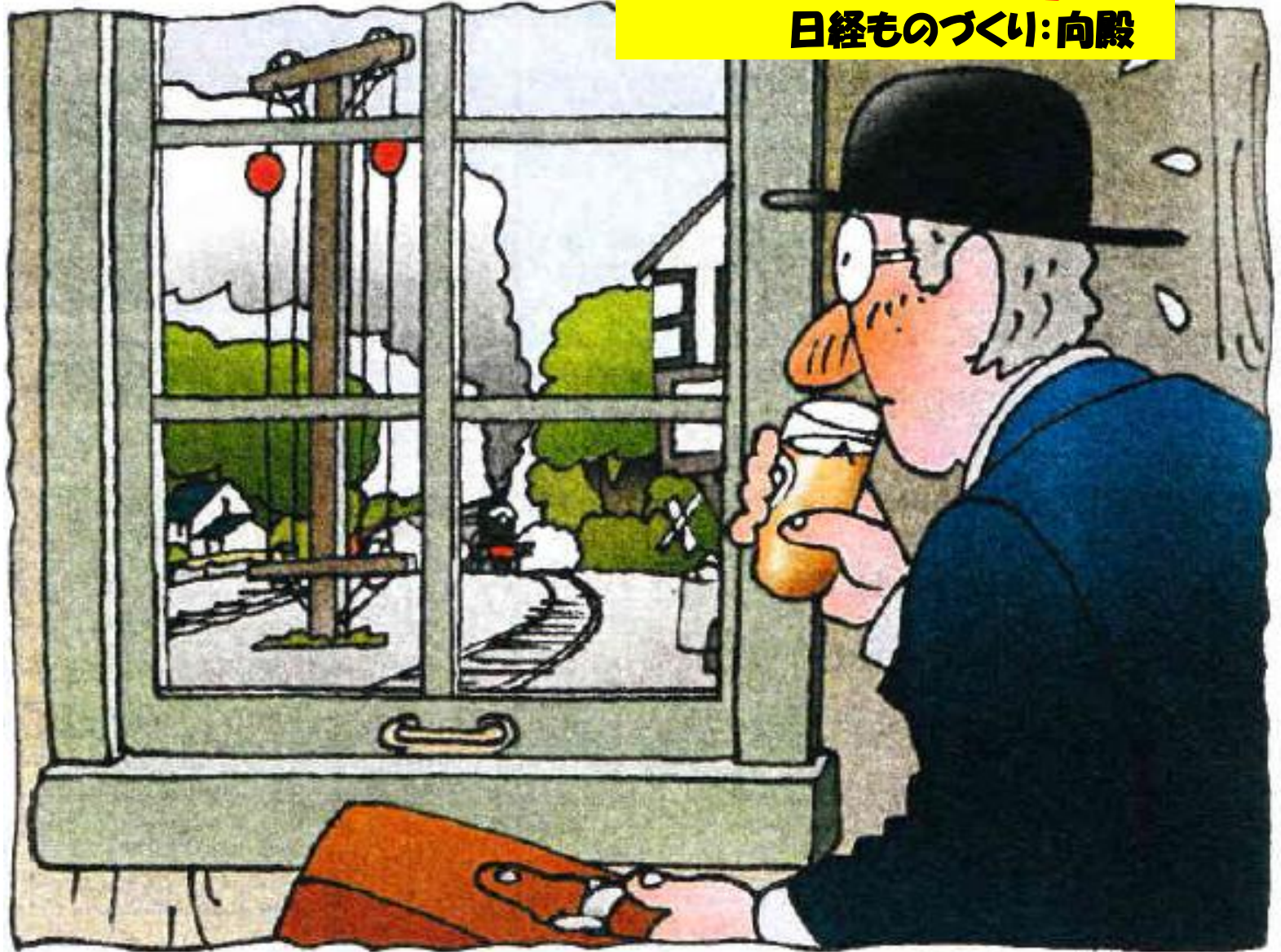
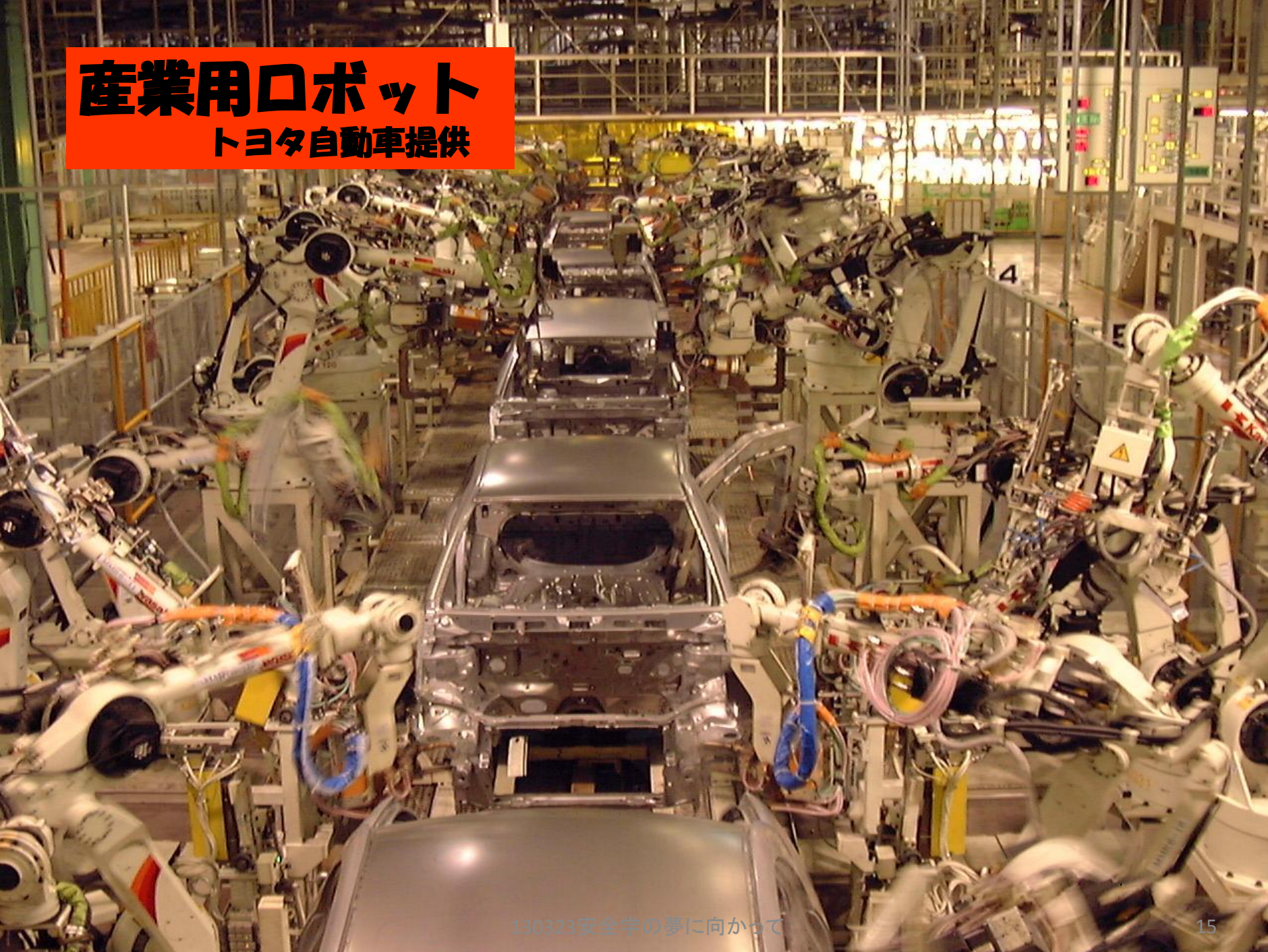


イラスト: つだかつみ

産業用ロボットの安全

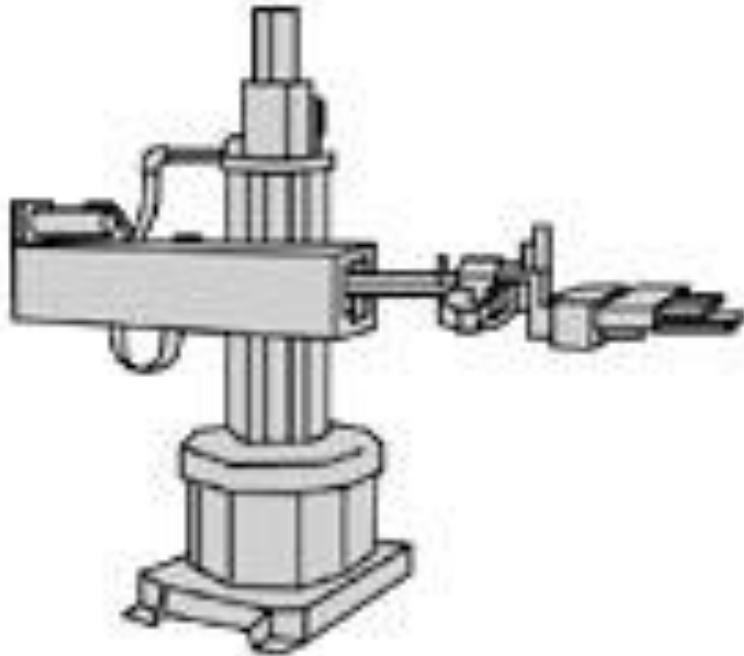
産業用ロボット

トヨタ自動車提供

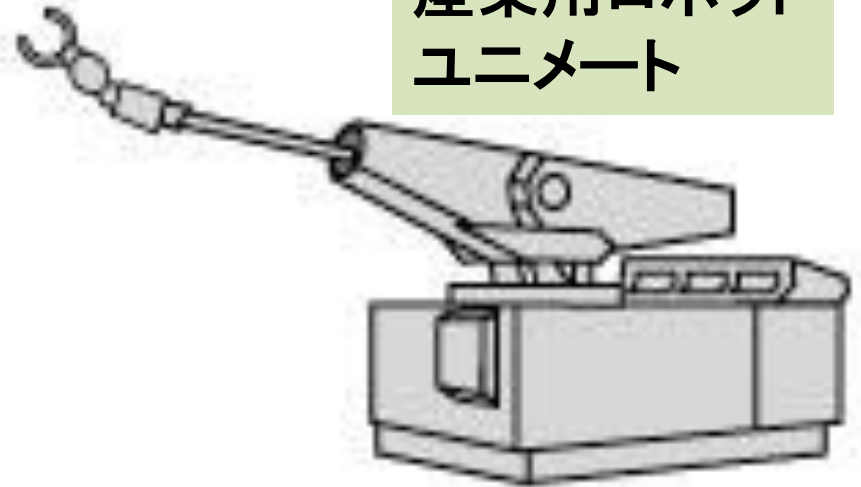


1970年代に油圧の産業用ロボットから始まった

産業用ロボット
バーサラン



産業用ロボット
ユニメイト



1967年東京機械貿易:バーサラン輸入、初公開

産業用ロボットにおける安全

- 1970年代、産業用**ロボット**に大型**コンピュータ**を接続して、知的な作業をやらせる研究をやった
 - **ノイズ**で**暴走**をして、初めてのロボット災害を経験しそうになる
 - プレス等の労働安全の世界では、
 - ・隔離の安全
 - ・停止の安全
- という**安全原則**のあることを知った。

2. 多値論理の研究

フェールセーフ研究から多値論理へ

安全	危険
----	----

図1 安全か危険か（2値論理）

少なくとも3値論理が必要だ！！

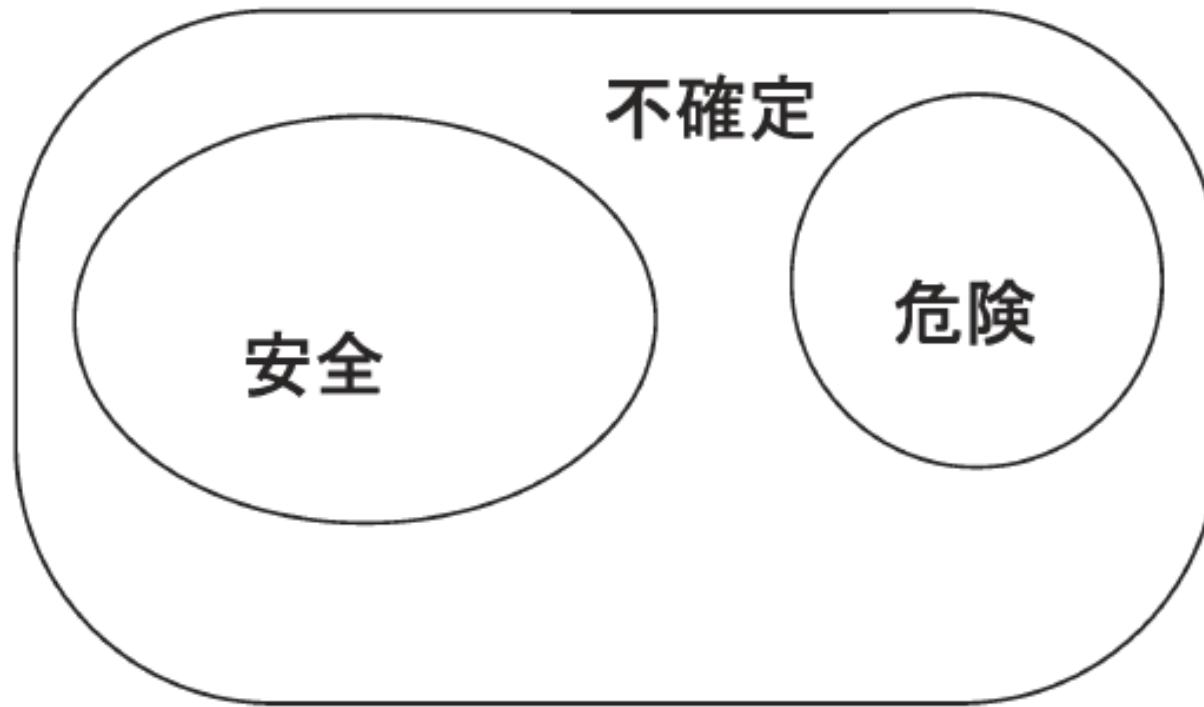


図2 安全か危険か不確定か（3値論理）

130323安全学の夢に向かって

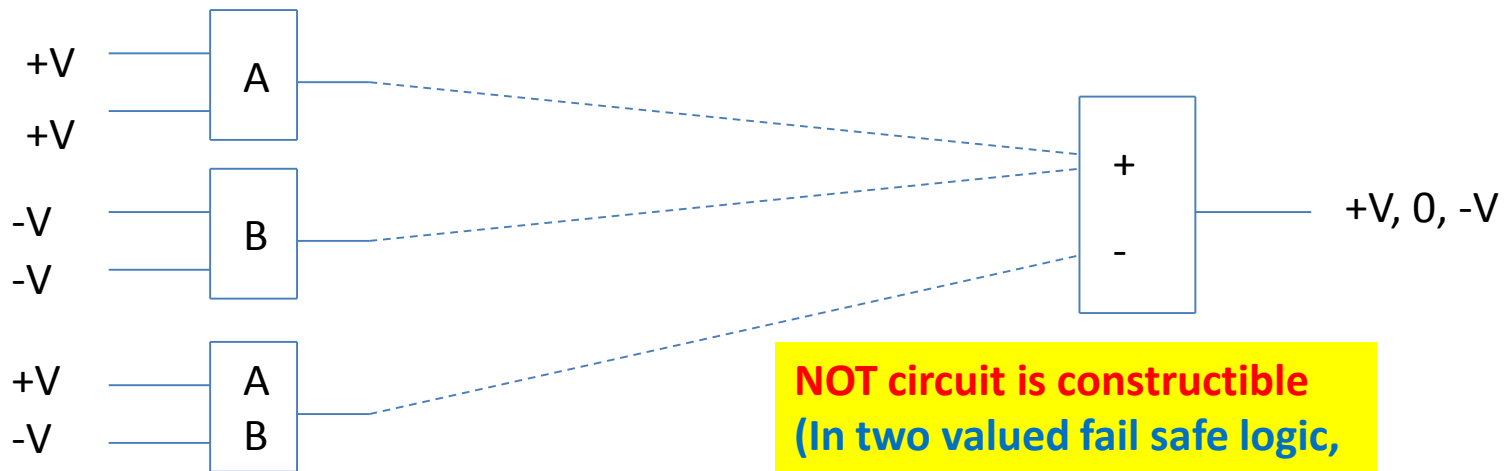
多値論理という概念

～安全は2値論理では片付かない!～

- 1 : イエス、安全、緑の信号
- 0 : ノー、危険、赤信号
- $\frac{1}{2}$: 分からない、故障、不明、..
- 2値論理から3値論理へ
- 3値論理から多値論理・ファジィ論理(度合い付き論理)へ

- $+V$ [v] truth value $\{1\}$
- 0 [v] truth value $\{\frac{1}{2}\}$ --- no energy
- $-V$ [v] truth value $\{0\}$
- Three elements of oscillator and rectifier

フェールセーフ3値論理回路の構造



NOT circuit is constructible
 (In two valued fail safe logic,
 we can not use not element)

C型フェールセーフ論理

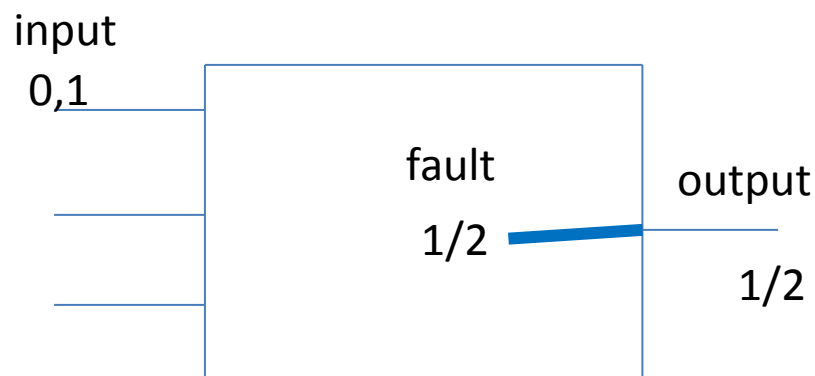
b \ a	0	1/2	1
0	0	1/2	0
1/2	1/2	1/2	1/2
1	0	1/2	1

C Fail-safe :AND $a \odot b$

b \ a	0	1/2	1
0	0	1/2	1
1/2	1/2	1/2	1/2
1	1	1/2	1

C Fail-safe :OR $a \vee b$

C-type Fail-safe logic systems



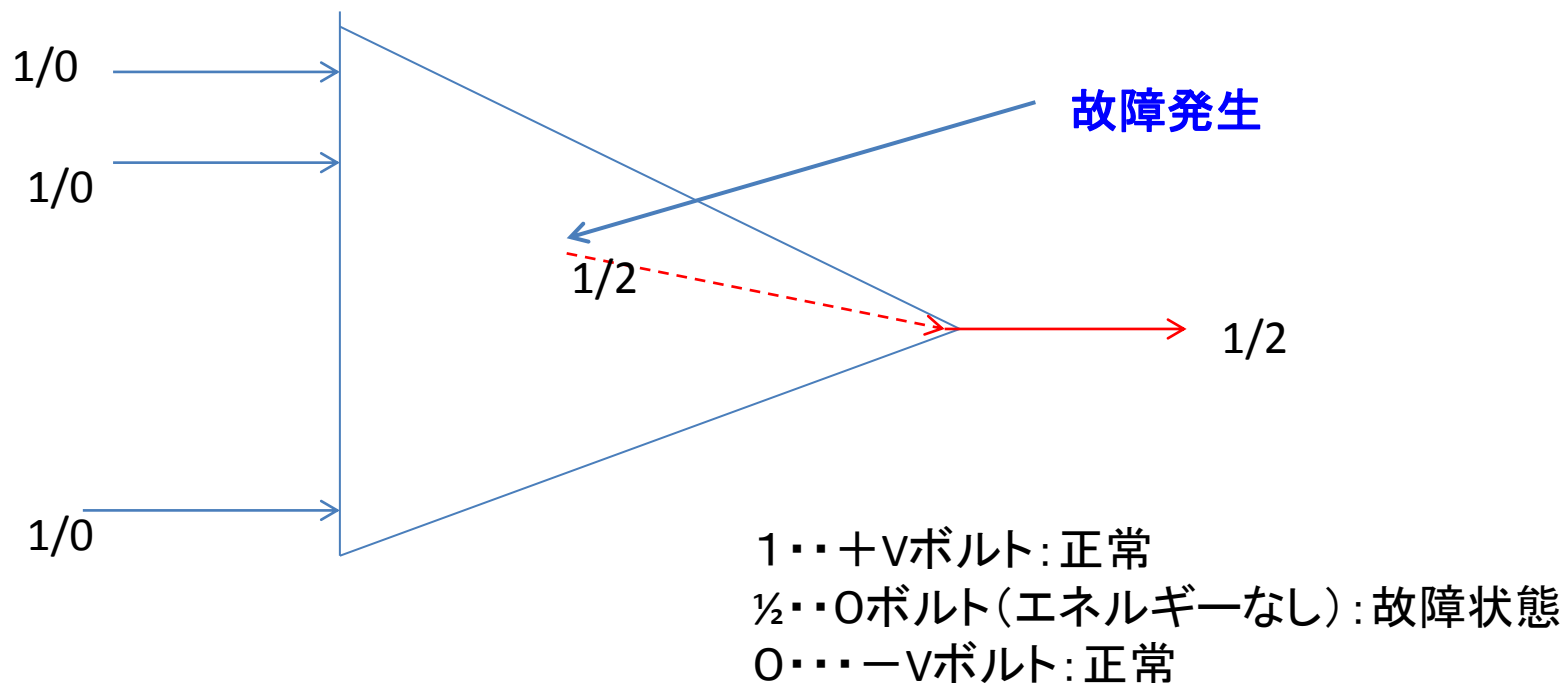
Fail-safe and fault detectable

a	0	1/2	1
$\sim a$	1	1/2	0

NOT $\sim a = 1 - a$

フェールセーフ3値論理システム

システム内に故障が発生すると出力は1/2となり、どこが故障したかがすぐ分かる：**C型フェールセーフ論理**



B型フェールセーフ論理

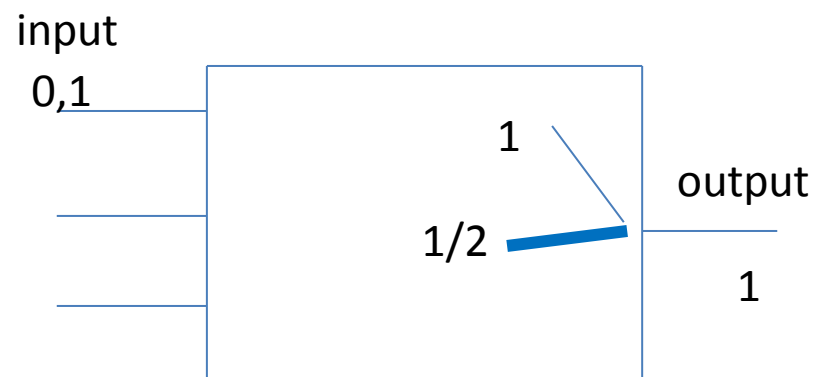
b \ a	0	1/2	1
0	0	0	0
1/2	0	1/2	1/2
1	0	1/2	1

B fail safe AND: $a \cdot b = \min(a, b)$

b \ a	0	1/2	1
0	0	1/2	1
1/2	1/2	1/2	1
1	1	1	1

B fail safe OR: $a \vee b = \max(a, b)$

B-type Fail-safe logic systems



Fail-safe and fault correctable

a	0	1/2	1
$\sim a$	1	1/2	0

NOT $\sim a = 1 - a$

多値論理研究の経歴

- C-3値論理・・・フェールセーフ論理・・・検出能力あり
- B-3値論理・・・訂正能力あり
- A-3値論理(正則3値論理)・・・入力禁止も取り扱える・・・あいまいさを取り扱う論理
- 正則3値論理関数
- 正則多値論理関数(クリーネ多値論関数)
- クリーネ論理の公理系

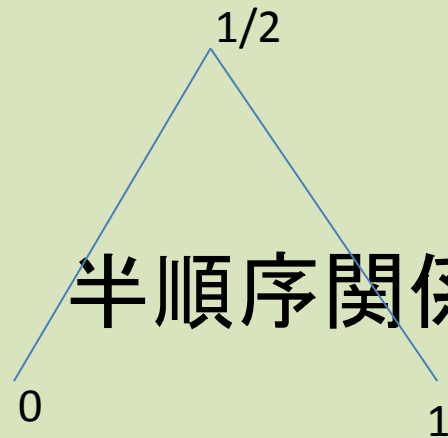
3値論理における正則性

～ Regularity ～

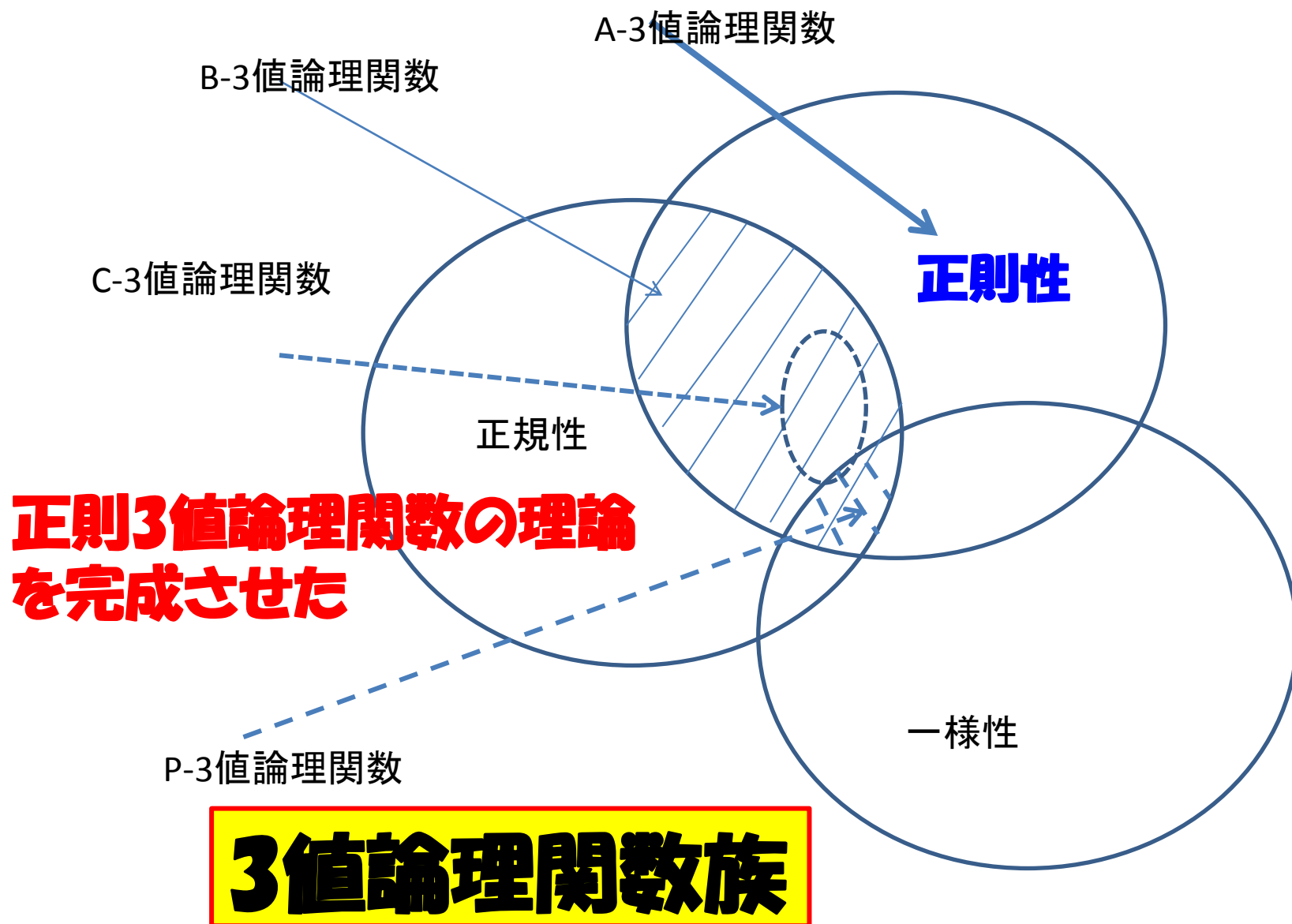
- (**正則性**: Regularity) : あいまいさの単調性

$$a > b \Rightarrow f(a) > f(b)$$

$1/2 > 0, 1/2 > 1, i > i$ 半順序関係 $>$



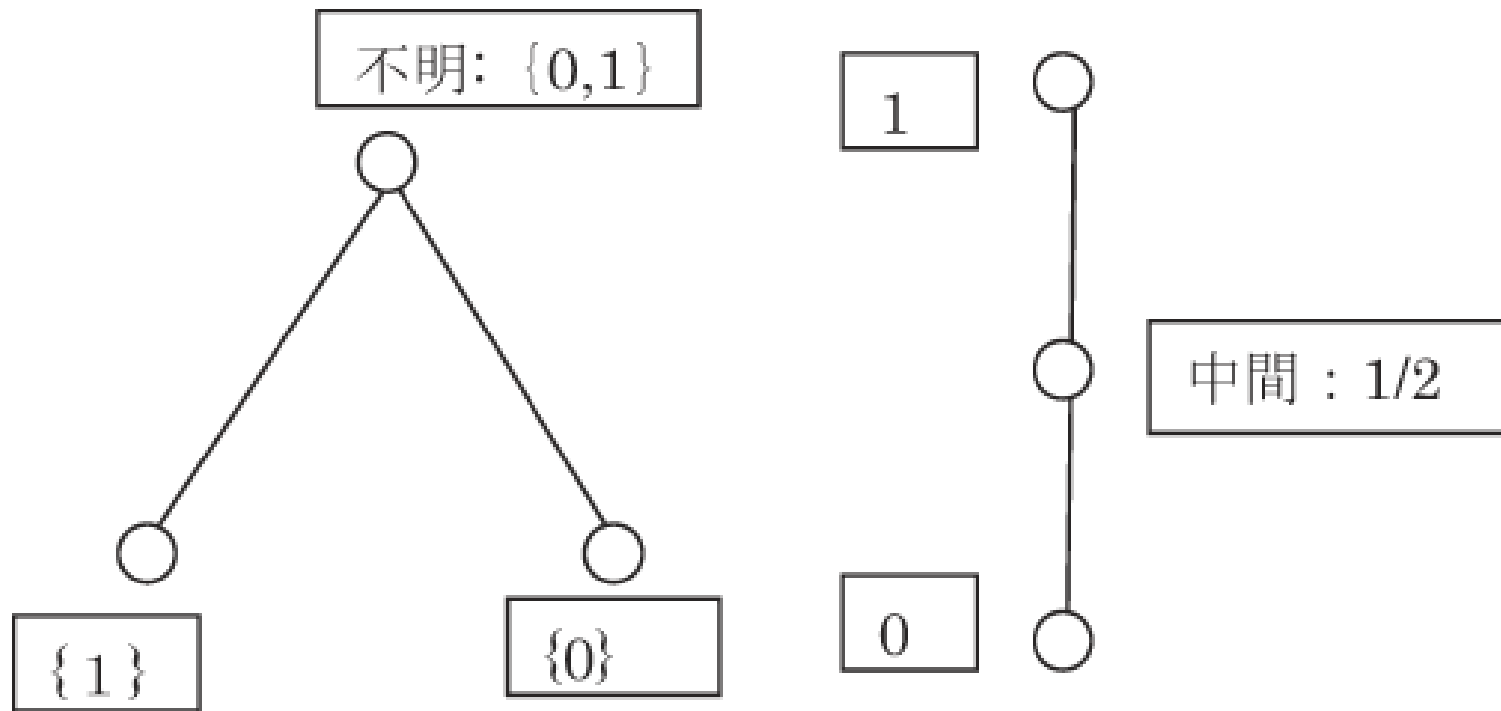
- [定理] $\{0, 1, 1/2, \text{変数}, \cdot, \vee, \sim\}$ で構成された論理式で表現される論理関数であるための必要十分条件は、正則性を満たすことである。



3. ファジィ理論の研究

多値論理からファジィ論理へ

U, Φ , 1/2: $\Leftrightarrow$ 分からない、未定、不明確、不定、故障、
矛盾、振動、止まらない、....

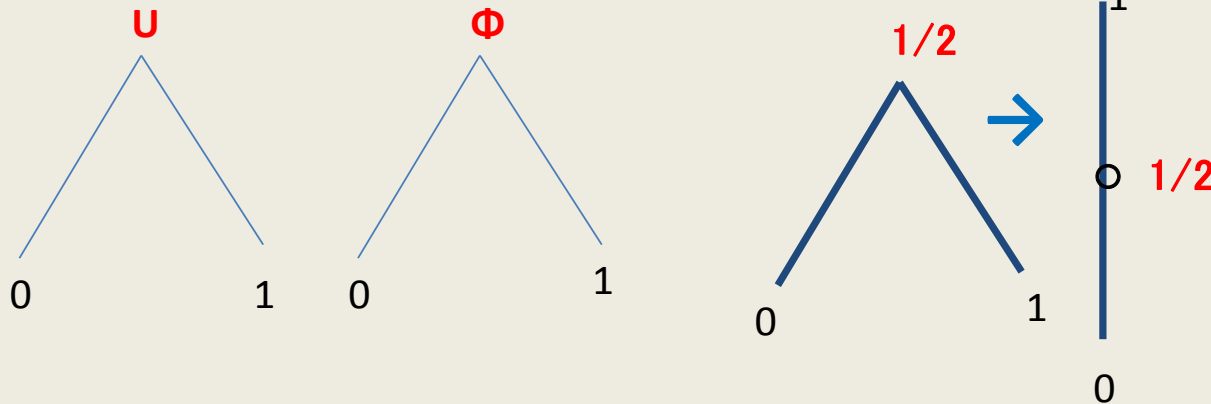


(a) 1 (真) か 0 (偽) か不明 (b) 1 (真) と 0 (偽) の中間

不明確を表す真理値をどう記すか？

1/2の割り当てがファジィ論理へ

- Symbols of the fault state in Fail Safe Logic



- Fuzzy Logic

three truth values $\{0, \frac{1}{2}, 1\} \rightarrow$ infinite truth values
the closed interval $[0, 1]$

3値論理から無限多値論理へ

ファジィ論理の研究

(L.A.Zadeh教授との出会い)

- ・ **ファジィ論理関数の研究を完成させた**

AND: $a \cdot b = \min(a, b)$

OR: $a \vee b = \max(a, b)$

NOT: $\sim a = 1 - a$, $a, b \in [0, 1]$

- ・ 数学的性質の解明
- ・ 論理式による表現方法: 標準形の発見
- ・ ファジィ論理関数の数え上げ
- ・ 代数的公理系の発見
- ・ 各種の応用

ファジィ論理研究と仲間1

- ファジィ論理関数の数え上げ: J.Berman、巽久行
- ファジィ導出系とファジィProlog: 増沢秀穂、Zuliang Shen、Liya Ding
- 半順序関係 $\succ$ の拡張: I.G.Rosenberg
- クリーネ代数系の拡張: G.Epstein
- クリーネ代数の公理系の解明: 二宮智子
- ファジィ代数への拡張: M.Mashinchi
- 正則3値論理関数の拡張: 山本喜則
- クリーネ多値論理: 高木昇
- ファジィ論理関数の性質: 荒木智行
- ファジィ条件付き確率: Rolly Intan

ファジィ論理研究と仲間2

- ファジィ論理における類似性尺度 : Hassan Rezaei
- ファジィ区間真理値 : 菊池浩明、安井浩之、大塚和彦
- ファジィ真理値の拡張 : 江本全志、Vladik Kreinovich
- ファジィ論理演算の性質 : 畑豊
- ファジィ推論 : 野島 和行
- ファジィ推論と確率推論 : 山内ゆかり
- ファジィフリップフロップ : 森 雄一郎
- B-3値PLAの応用 : 井口幸洋、長田康敬
- ファジィクラスタリングとその応用 : Rui-Ping 、宮本定明
- ファジィアブダクション : 山田耕一
- ファジィルールの応用 : 江原義郎、A.Bastian

ファジィという概念

～あいまいの2大分類～

- ランダムネス

- 確率論・統計学で扱っているあいまいさ
 - まだ分らないが、分ってしまえば、白(1)か 黒(0)
 - 灰色を認めない:排中律が成立する, 矛盾は認めない(2値論理に基づく)
 - (例)サイコロの目

- ファジィネス

- ファジィ理論で扱っているあいまいさ
 - 境界のあいまいさ:分っても白(1)か 黒(0)か はいえない。
 - 両極端ではなく, その中間に意味がある.
 - 灰色を認める:排中律の不成立, ある程度の矛盾を許容する(多値論理に基づく)。
 - (例)私はいいい男だ

ファジィという概念

- ファジィ(FUZZY)とは・・・
 - 本来，“あいまい”を意味するが、
いい加減ではなく、丁度“良い”加減を意味する。
- 「0」と「1」の中間、反対・対立するものを融合、
丁度良いところを探そう
- 世の中は実は曖昧が真実であって、数理は近似である
- 曖昧なものの存在を認め、議論する態度は合理的にしよう
- 人間の感性，主観，言葉の意味，等々，厳密に定義は不可能
- 東洋的な思想と西欧的な合理的思想の融合

4. 安全の研究

ファジィ論理から再び安全へ

信頼性研究から再び安全性研究へ

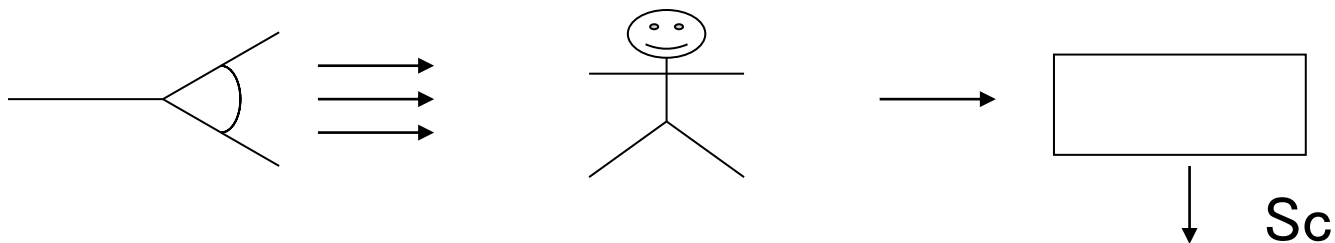
- 信頼性と安全性は、基本的には異なった概念
- 信頼性：如何に機能を維持するか
 - フォールトトレランス（多重系）の研究
 - 確率を重視
- 安全性：機能を失った後を問題にする
 - フェールセーフ、フルプルーフの研究
 - 構造を重視

危険検出型と安全確認型

(蓮原弘一、杉本旭、向殿政男)

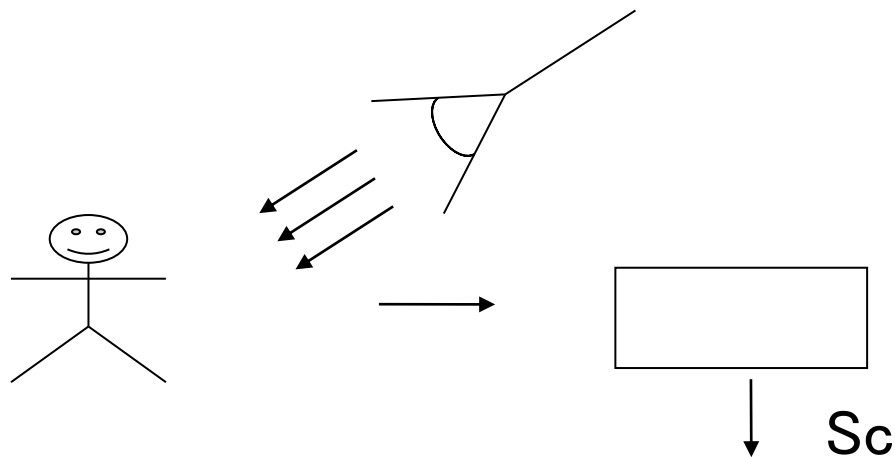
- 1. 危険検出型** 危険であることを検出して、この危険情報により作業を止める／回避する(危険情報がない時は続行)
- 2. 安全確認型** 安全であることを確認して、安全情報を受けているときだけ作業を続行する(安全情報がない時は止める)

光センサーの構造



Safety : Absence of human

(a) Transmission type

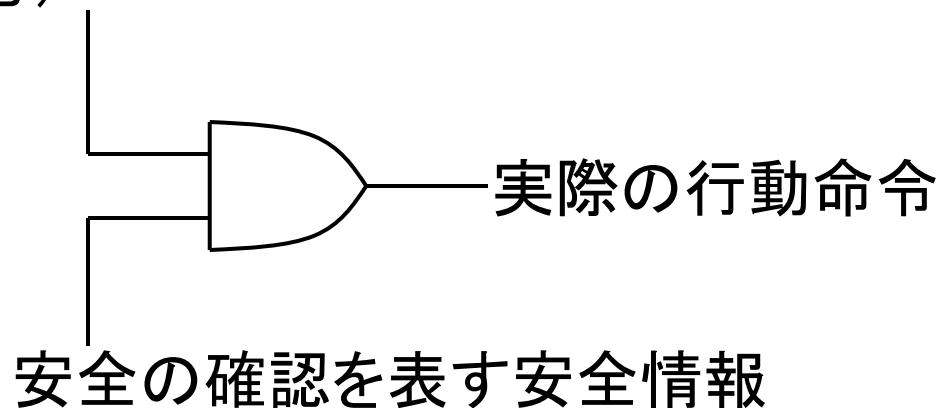


Safety : Presence of human

(b) Radar type

安全確認型フェールセーフシステム

危険を伴う行動命令
(誤りを含む)



- * 安全情報は、非対称誤り
- * AND回路は、非対称誤り
- * 実際の行動は、“止まれば安全”でなければならない——無条件安全(停止安全)

機械安全の世界

- 機械類の安全性: ISO/TC199
日本機械工業連合会から派遣されて国際会議に参加する
- ISO/IECガイド51・・・安全設計の基本概念を知る
- ISO12100・・・安全設計の原則、規格の階層化を知る
- 安全の世界的な流れを知る・・・リスクに基づく安全

安全という概念

～安全(Safety)の定義～

- 「人への**危害**または損傷の危険性が、**許容可能**な水準に抑えられている状態」
- 「受け入れ不可能な**リスク**が存在しないこと」
- 「受け入れることの出来ない**リスク**からの解放」(ISO/IECガイド51)

* リスク: 危害の発生する確率とひどさの組合せ

許容可能なリスク (Tolerable risk) の定義

- その時代の社会の価値観に基づく所与の状況下で、受け入れられるリスク
- 無視可能なリスク
- 広く受け入れられるリスク(Acceptable Risk)
- 適切に低減されたリスク

リスクアセスメントとは？

- 機械・設備の使用条件を明確にして(合理的に予見可能な誤使用も含む)
- すべての危険源(ハザード)を見出しておき
- 各ハザードごとにその危険性(リスク)の大きさを見積り
- 大きなリスクを持つ危険源から,そのリスクが受け入れ可能になるまで安全対策を施し
- 残った残留リスクの情報を開示し
- リスクアセスメントの結果を文書化しておくこと

事故の未然防止のための科学的、体系的、論理的、網羅的な手法である

リスク低減の順番

～スリーステップメソッド～

(設計者側)

(1) 本質的安全設計によるリスクの削減

(2) 安全防護対策によるリスクの削減

(3) 使用上の情報によるリスクの削減

(使用者) 訓練、個人用防具、体制によるリスクの削減

安全の境界はファジィである



図3 安全と危険の中間領域（ファジィ論理）

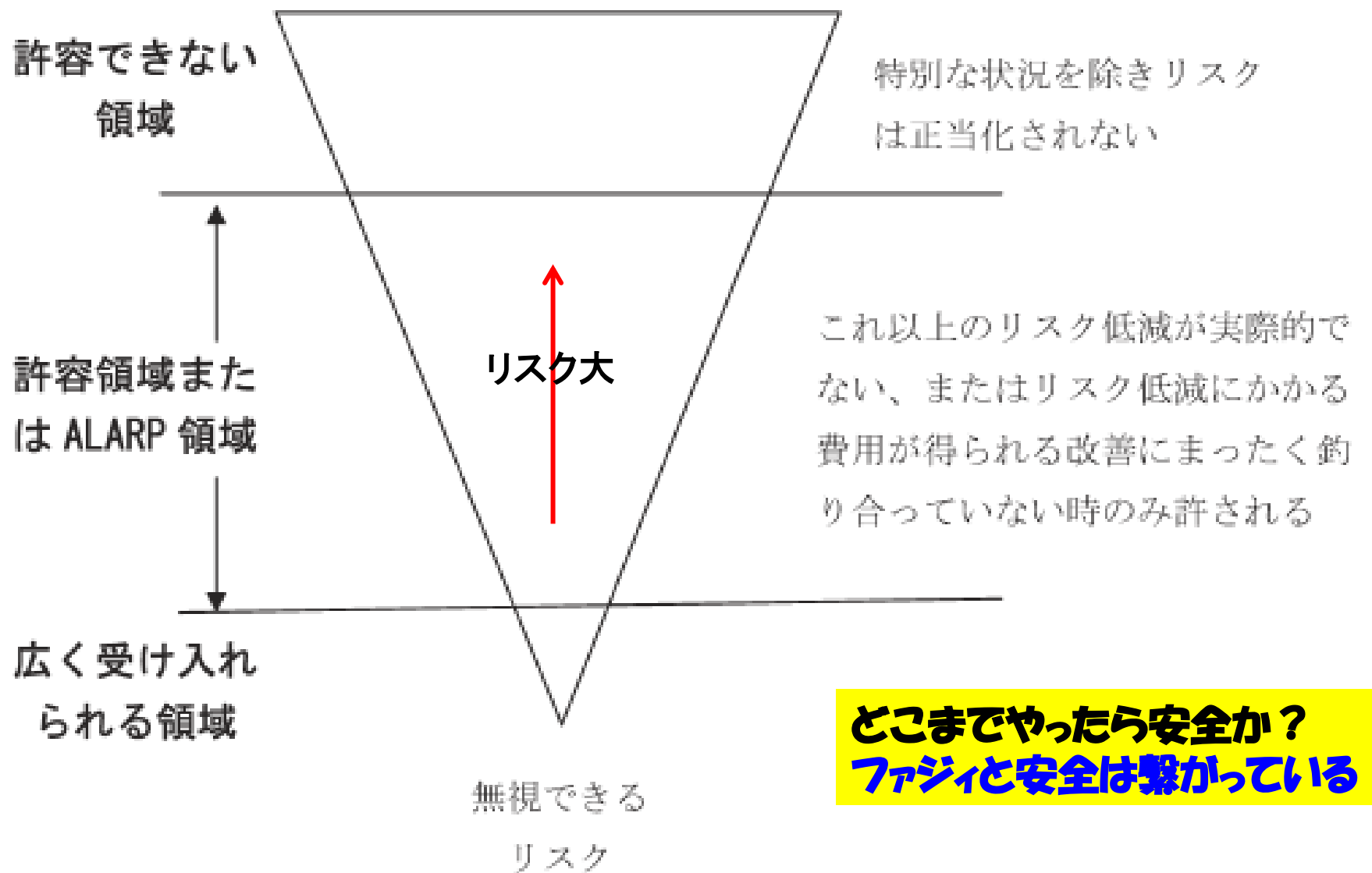


図 5 許容可能なリスクと ALARP 領域

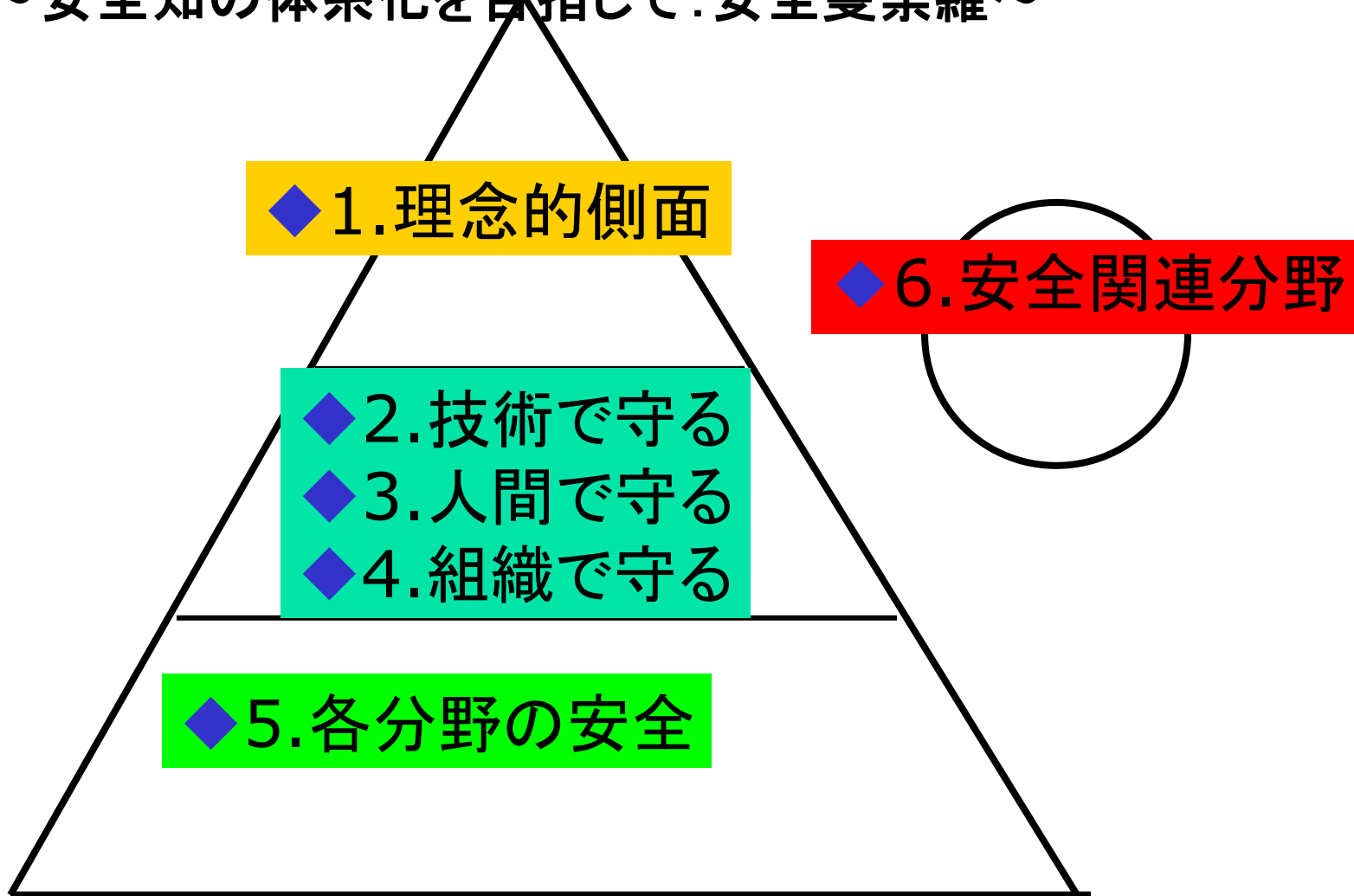
安全学の体系化に向けて

安全学の構築

- 安全は、**技術、人間、組織〔仕組み〕**を総合して初めて、実現される
- 安全に関する学問は、**技術的側面**だけでなく**人間的側面、社会的側面**を含めて、安全工学や安全科学を含んだ更に広い学問体系である**安全学**として確立
- **安全学**は、**自然科学、人文科学、社会科学を包含した文理融合型、領域横断型の学問体系**
- ただし、それを支える**理念(安全哲学)**がなくてはならない

◆安全学の観点から

～安全知の体系化を目指して:安全曼荼羅～



分類	例
1. 理念的側面	安全の哲学, 安全の思想 、安全の定義, 安全目標, 安全の構造, 安全責任, 等々
2. 技術的側面	本質安全設計, フェールセーフ, 信頼性, 冗長性, 診断, 保全, 等々
3. 人間的側面	過誤, インターフェース, 人間工学, 安全意識, 訓練・教育, 等々
4. 組織的側面	マネジメントシステム, 標準化, 法律, 規則、規制, 認証・認定, 事故調査, 危機管理, 等々
5. 各分野の安全	機械安全, 交通安全, 情報安全, 原子力安全, 食品安全, 製品安全, 電気安全, 医療安全, システム安全, 化学薬品安全, プロセス安全, ロボット安全, 等々
6. 関連分野	防犯, 保険, 裁判, 等々

学問としての安全学

- 安全知の体系化
- 皆で協力をして作り上げられる体系
- 現場の知恵・工夫を吸い上げ、学問から現場の知恵を引き出せる体系
- 失敗や危険に学び、明るく前向きに、富を生み、幸せの構築に資する学問
- 安全に関する教育の体系化とカリキュラムの構成
- 家庭、教育機関、社会での安全教育

安全の思想

～安全学からの視点～

安全思想の分類

～安全学として**フラクタル構造**となっている～

0. 安全哲学

1. 作る立場の安全思想：**安全設計思想**

2. 規制・管理する立場の安全思想：**規制体系
の思想**、法理念、安全管理思想、
Regulatory Science

3. 利用する立場の安全思想（個人、消費者、
作業者、社会、国等）：安全受容思想、**安全
文化**

安全における常識

- 機械設備は劣化等でいつかは壊れるものである
- 人間はいつかは間違えるものである(時には、認知症の人、意識を失う人、悪意の人もある)
- 組織やルールに完全なものはありません

絶対安全は存在しない

- 絶対安全(リスクゼロ)は(目指すべき目標ではあっても)、実際には存在しない。
- 製造者は、如何に残留リスクを許容可能以下にまで低減するかに努力をするのが役割
- 使用者は、残留リスクの存在を自覚して、注意して使用するのが役割
- 管理者は、これらが確実に実行されているかを確認、保証するのが役割

再発防止より未然防止

・未然防止方策

↓(予防安全:設計安全)

・事故を起こさない

↓(運用安全:保守・点検・修理)

・危害のひどさを下げる

↓(衝突安全)

・再発防止対策(事後安全)
(事故調査)

・過去の歴史に学べ

・事故データを収集
せよ

・緊急時を考えて
おけ

すべてのステージを総合的に考えておく

大きなリスクから対応せよ

- 部品は劣化する・・・製品は故障をするもの
- 人間は年を取る・・・人間は間違えるもの
- ある程度、事故は避けられない
- 消費者(社会)の信用を一旦失うと企業(大学)は持続的に存続できなくなる時代に
 - * 大きな事故は起こさない(未然防止:リスクアセスメントの重要性)
 - * 事故が起きたら、迅速に対応、隠さない、逃げない、正直に、トップが対応、・・(責任問題や事故原因が不明でも)

リスクは小さいほど良いとは限らない

- リスク感覚を磨く機会、学習する機会を逸する
- コストが掛り過ぎる（製品の価格が上がる）
- 他のリスクが増大する
- 各種リスクのベストミックスが必要
- 許容可能なリスク、受け入れ可能なリスクの追及が望ましい

安全と安心は異なる

- 安全と安心は明確に分けるべきである
- 安心には価値観が関与しており、科学(安全)と価値観(安心)は分けて考えるべきである
- 科学的事実を明らかにし(安全)、それを受け入れるか否かは、民衆が判断する(安心)
- 特にリスクの高い影響の大きなシステムに関しては、安心を得られない場合には、いくら科学的に安全であっても、作らないという判断はあり得る

安全の基本は情報公開である

- 残されているリスクが最悪を考えてどのようなものであるかを事前に情報開示しておくこと
- 安全を合理的に、客観的に判断するためには必須のこと
- 良い情報も悪い情報も公開：隠さない
- 民衆がパニックに陥るだろうからとか、理解できないだろうからという理由で、残留しているリスク情報を開示しないというのは、正しくない。
- ただし、我々民衆も、冷静にリスクを判断する科学リテラシーや安全文化を身につける必要がある。それが正しく怖がるための基本である。

安全における難しさ

～安全学からの視点～

- 適切なリスクの判断は難しい(リスクは小さければ小さいほど良いというものでもない: 少しぐらいのリスクは、あった方が多い場合が多い)
- 正しく恐れるのは難しい
- 安心すると危険
- 人間は、痛い目に遭わなければ、対応しない(転んだ後の杖)
- 災害は忘れたころにやってくる(安全は風化する)
- 想定外は常にあり得る(だから、対応を考えておけ)
- 安全の責任は、事前に分かっていることを何処まで対応したかの責任

設計者の心得

- 誤使用が多いのは設計の問題
- 人間の注意による安全確保よりは、機械の安全化が先
- 機械のリスク低減の順番は本質的安全設計
⇒安全防護・安全装置⇒使用上の情報の提供を忘れるな
- 再発防止の前に未然防止が大前提
- 死に方設計を重視せよ

企業の心得

- 顧客からの苦情、事故・ヒヤリハット情報を集めて分析せよ
- 事故は、正直に、すばやく、報告・公表（オネストリー、クイックリー）
- 責任追及よりは原因究明を優先
- 安全はコストではなく投資だ
- 事後処理の負担・金額を考えれば、事前の安全投資は安上がり
- ライフサイクルコストを考えれば、上流の、早急の安全対策の方が安上がり（設計段階、製造段階）
- 安全は、設計から廃棄まで

規制側の心得

- 再発防止よりは、未然防止を重視しよう
- 事前規制よりは、事後規制を重視しよう
- 官主導よりは、民主導にしよう
- 個別規制よりは、包括規制にしよう
- 仕様規定よりは、性能規定にしよう
- 第三者による外部認証制度を確立しよう
- 責任追及よりは原因究明を優先しよう

消費者の心得12カ条

1. 製品ごとの正しい使用法を尊重しよう
2. 製品のリスクはゼロではない
3. 最終的なリスクの対応は消費者に任されている
4. 自分の身は自分で守る気概を持とう
5. 手入れ、保守点検は消費者の責任である
6. 住宅備え付けの装置も手入れをしよう
7. 製造年月日、異常(音、臭い、発熱)に注意しよう
8. 製品には寿命がある(部品・材料は劣化する)
9. 安全には適切な対価を払おう
10. 事故情報に気を配ろう
11. ヒヤリハット、気がかり情報は、発信しよう
12. 安全に真摯な企業を評価しよう

安全は全員で作る時代

- * **経営者の立場と作業・消費者の立場の融合**
- * 企業（経営者、管理者）は**安全**の達成を迫っている
- * 現場（作業・消費者）は**安心**を求めている
- * 現場のリスク、不安を最もよく知っているのは作業・消費者
- * ヒヤリハット、インシデント情報は貴重な財産＋作業とのきずな
- * 企業：愚直なまでに安全を実現する姿勢、良い情報も悪い情報もの情報開示、コミュニケーションを通じた作業・消費者との信頼関係の樹立
- * 情報の開示と透明性が信頼を生む

安全・安心の方程式

＊ **情報の公開と透明性**が信頼を生む

- ・ **リスクコミュニケーションの重要性**
- ・ **安全が実現されている＋実現している人間・組織を信頼している→**

$$\text{安全} \times \text{信頼} = \text{安心} < 1$$

新しい安全の文化創造へ

～より高度な安全の実現に向けて～

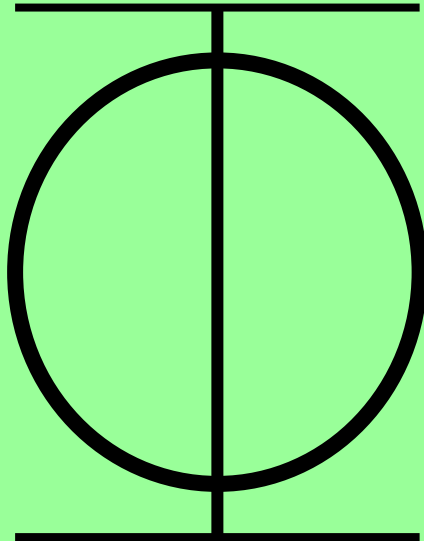
- 安全技術の発展
- 安全学の確立
- 技術者倫理の確立
- 企業トップの安全意識の向上・安全の価値を重視した経営
- 消費者力の向上
- 報道力の向上
- 安全を支援する社会制度の確立（税制・保険・認証・投資等の活用）
- 大学における安全教育・安全/保全技術者の育成と待遇改善
- 安全文化の向上
- **日本は、安全・安心を基本とした国づくりへ**

来し方と行く末を考える
～新しい人生を始めます～

これまでの生き方

- 人に喜ばれるのが好き
- お人よし、安請け合い、おっちょこちょい
- 文武両道
- 真面目、誠実、律義(?)
- 真理は中庸にあり
- **中庸とバランス感覚**
- トップダウン思考とボトムアップ思考の並立
- 基本に帰る、基本から考える
- 何をやっても同じ。面白いものがあって、それを探すのではない。今やっていること、やらなければならないことを面白くする、その中から面白味を見つけ、作っていくのです

Φ型人間の必要性



目指すべきは
Φ型人間

- ・大局的、包括的、総合的観方ができること
- ・専門分野を一つ持っていること
- ・真理は0と1の間にあり

これからの生き方

当面は、

- 明治大学への恩返し: 校友会
- 教育、情報関係への恩返し: 私立大学教育協会
- 安全関係者への恩返し: 安全技術応用会、国の各審議会等

を続ける積り。

- **しかし、運と出会いにより、行く末は分からないが……**

現在の心境

- 忙しすぎるのは止めよう！
- ただし、好きなことをやっている分には、忙しいのは楽しめるし、後悔はしないだろう。
- 少し時間をとって、今後をじっくりと考えたい
(充電期間、時には情報と仕事の鎖国も必要)
- 選択肢は狭まるのに、やりたいことは広がる→
選択と集中
- 時間を掛けて、納得できる仕事、役に立つ仕事をしたい

安全学確立の夢に向かって

- 安全学の確立：安全思想の究明と確立に向けて
- 安全の仲間と協力をしながら進めたい
- 今後も、安全に関する「**見識のある、奥の深い、常識**」を提言して行く積りである

感謝

- 恩師
- ゼミの学生諸君
- 世界中の研究仲間
- 明治大学の教職員
- 明治大学の校友
- 校友課の職員
- 明治大学に感謝
- 両親
- 家族
- 特に妻(晴美)

1991年度ゼミ卒業生



2012年度最後のゼミ合宿



健康第一！
生涯現役！
一生勉強！
～ 考える、感じる～

御清聴ありがとうございました

