SWEST15 S2b
実践！機能安全
～Safety Conceptを作ろう！（ソフトウェア編）～

2012年8月23日（金） 9:00～10:20

武井 千春（名古屋大学 NCES）
松原 豊（名古屋大学 NCES）
水口 大知（アトリエ）
森川 聡久（ヴィッツ）

本セッションの目的・概要

- 機能安全において、すべての前提となる最も重要な活動は「Safety Concept作り」。その内「安全分析」が最も重要な作業です。
- 目的: Safety Concept構築のためのエッセンスを習得する。（今回はソフトウェアにフォーカス）
- 概要:
  - 例題システムのソフトウェアについて、故障モードを分析、安全対策の検討
  - 数人のグループでブレーンストーミング＆発表

本セッションの狙い

- ソフトウェアエンジニアへの期待
  - ソフトウェアの安全分析手法を体験する
  - ソフトウェアによる安全対策の実例を学ぶ
    - 防御プログラミング
    - 実行シーケンス監視
    - 変数2重化
    - etc

タイムテーブル

時間	実施内容
9:00～9:10	イントロダクション、グループ分け **※同じ会社の方はなるべくバラバラに座ってください**
9:10～9:20	「例題システムの説明」
9:20～10:00	グループワーク: **「ソフトウェアの安全分析」**
10:00～10:20	成果発表、まとめ

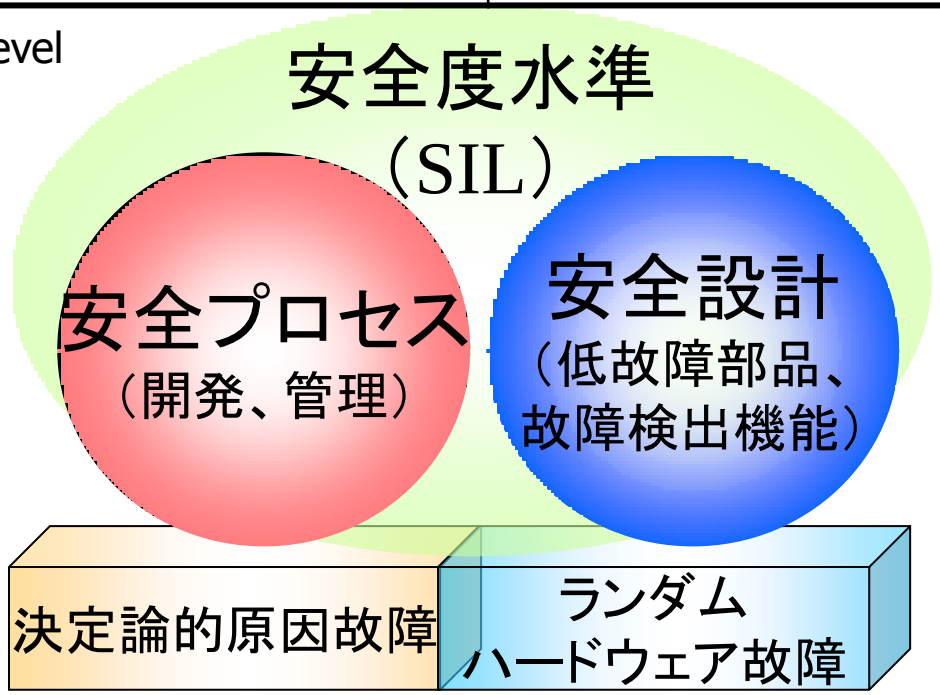
Safety Conceptの構築方法について

作成：森川 聡久（ヴィッツ）

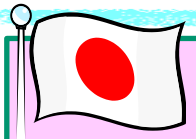
機能安全の大枠

IEC 61508		
SIL	**低頻度作動モード** 作動失敗確率（1／回）	**高頻度作動モード、連続モード** 故障率（1／時間）
4	10^{-5}以上10^{-4}未満 数万回に1度	10^{-9}以上10^{-8}未満 数万年に1度
3	10^{-4}以上10^{-3}未満 数千回に1度	10^{-8}以上10^{-7}未満 数千年に1度
2	10^{-3}以上10^{-2}未満 数百回に1度	10^{-7}以上10^{-6}未満 数百年に1度
1	10^{-2}以上10^{-1}未満 数十回に1度	10^{-6}以上10^{-5}未満 数十年に1度

※SIL：Safety Integrity Level
※ASIL：Automotive SIL



従来開発と機能安全開発



従来開発

- **信頼性（壊れないこと）重視**
- 自己努力によってバグゼロが目標
- 担当者間のすり合わせ開発
- 開発文書の出来栄えは不十分
- **効率的だが説明力が乏しい**

機能安全開発

- **故障を前提とした安全担保**
- 高品質の証拠を積み重ねた開発によってバグゼロが目標
- 構成部品が**故障しても危険にならない仕組み**が必要
- 安全を**客観的に説明できる開発文書**の作成が必要

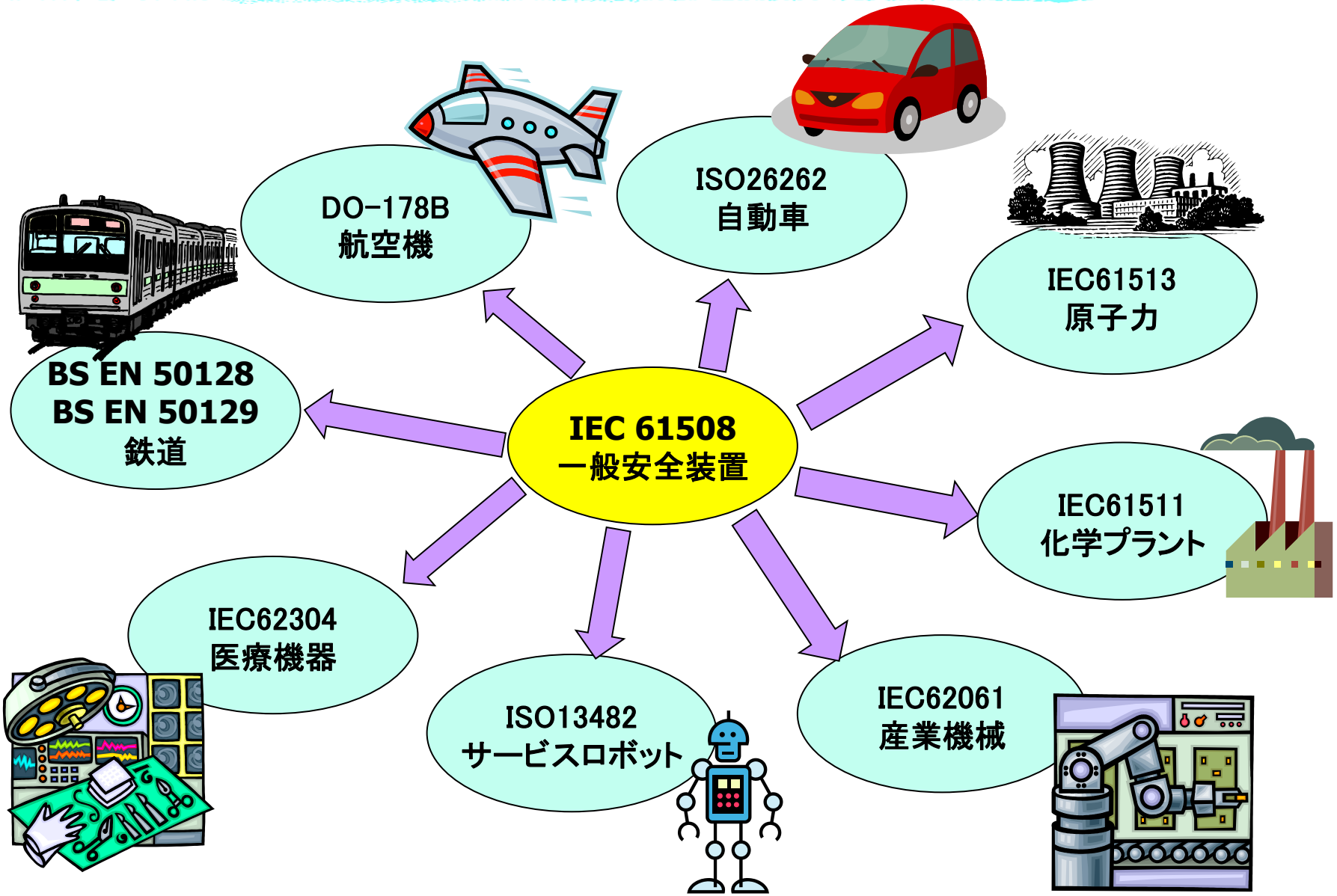
- もし緊急停止スイッチが（マイコンが・・・）**壊れたら → ”危険”**
  → アクチュエータを停止し、故障したことがわかるようにする

＜対策＞

- **バグが潜在していないことを客観的に説明可 → 安全プロセスの強化**
- **故障を発見する → 故障検出機能**
- **故障しにくくする → システムの多重化、低故障率の部品を使用**

} **安全設計**

IEC61508の派生規格



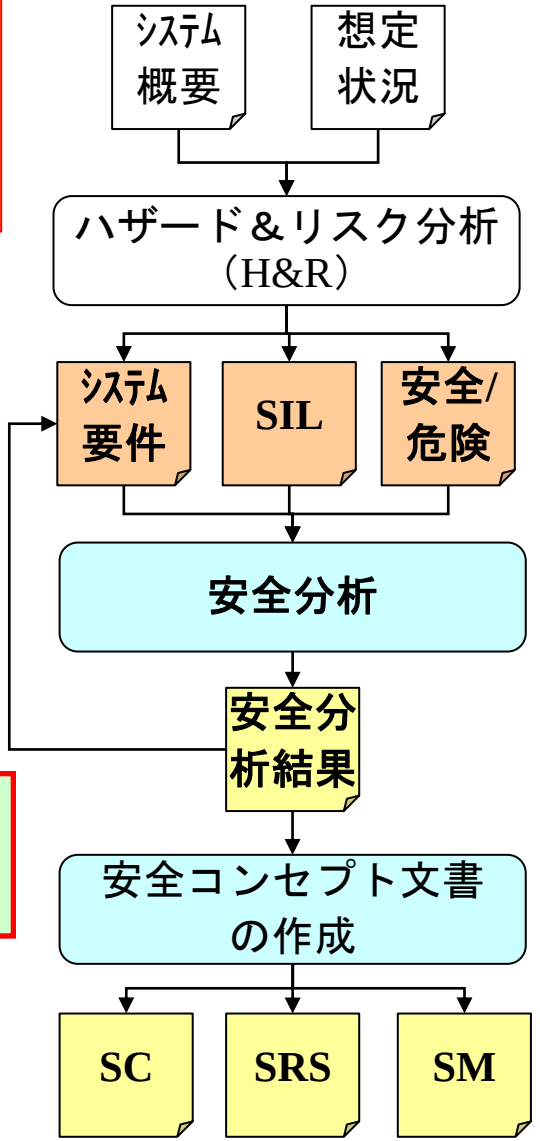
安全コンセプトの構築の流れ

いかなる故障が発生しても、必要なレベルの安全を達成できることを証明すること。
一番の肝は「安全分析」。

＜安全コンセプト4文書＞

・安全分析結果
　故障を網羅的に洗い出すことと、安全対策が重要
・SRS：Safety Requirement Specification：安全要求仕様書
　安全関連機能について記載した仕様書
・SC：Safety Concept：安全コンセプト
　コンセプトレベルで安全を証明（説明）できる資料
・SM：Safety Manual：安全マニュアル
　ユーザやハードへの制約条件

目標とするSILの達成を証明できるまで繰り返し実施



SILと安全策の関係

・IEC61508ではSFFの達成が必要！
・SILとN重化によって、要求SFFが決まる。

Safe failure fraction of an element	Hardware fault tolerance		
	0	1	2
<60 %	Not Allowed	SIL 1	SIL 2
60 % – <90 %	SIL 1	SIL 2	SIL 3
90 % – <99 %	SIL 2	SIL 3	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4

IEC61508:2010-2より抜粋

SFF＝安全側故障率／全故障率

⇒ 故障検出率（DC）を上げることで、安全側故障率を上げる必要あり。
⇒ 最悪ケースを想定すると、SFF相当のDCを目指すことを推奨する。

DCの決定方法

IEC61508:2010-2 Table.A に記載あり。
検出可能な故障によって、DC=High（99%）／Medium（90%）／Low（60%）を判定。
それを達成するための具体的な方策についても、記載あり。
⇒ 本セッションでは、後ほど方策一覧をお配りします。

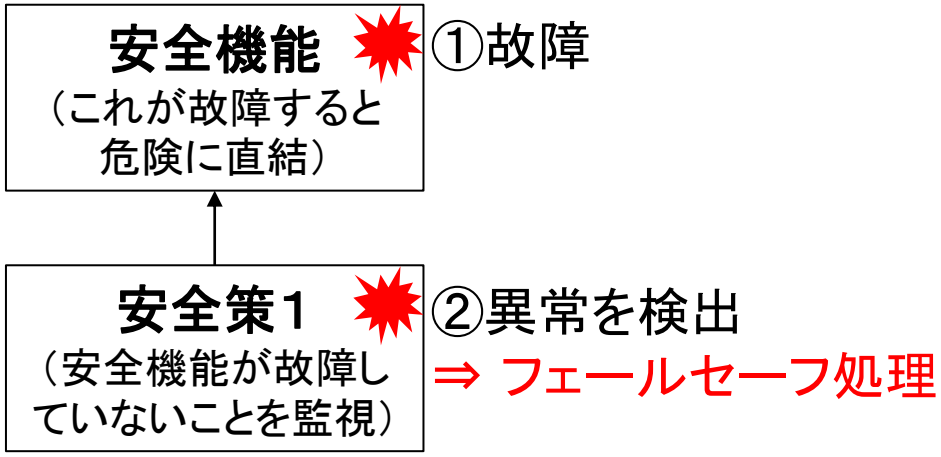
安全分析にて考慮すべき故障のパターン

- 系統的原因故障（バグ）と ランダムHW故障
- 単一故障 と 多重故障
  - IEC61508では、単一故障のみ考慮
  - ISO26262（自動車）では、２重故障まで考慮必要
  - BS EN 50129（鉄道）では、３重故障まで考慮必要
- 恒久故障 と 一時故障
  - 一時故障の例）ノイズによるメモリ化け
- 従属故障
  - ある故障が原因で、その影響を受け、別の箇所が故障する
- 共通原因故障
  - １つの原因により、複数箇所への同時故障が生じること
  - 例１）電源異常により、２マイコン共誤動作
  - 例２）ノイズの影響（環境）により、２マイコン共誤動作
  - 例３）安全系のある変数が化け、各出力系全てが誤動作
  - 例４）同一設計のソフトのため、同じ箇所にバグが存在

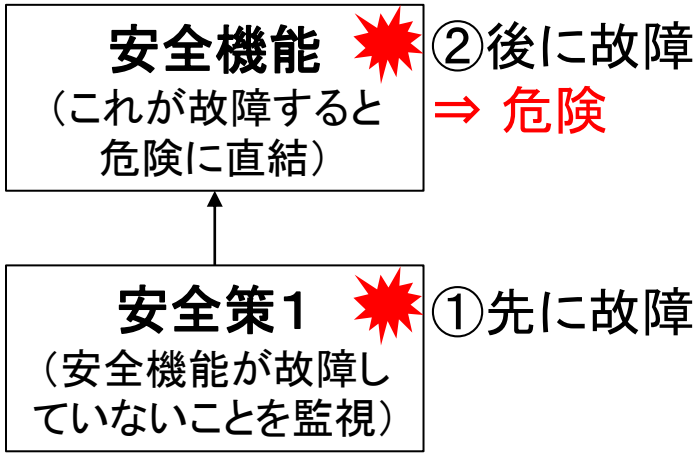
潜在故障

- 安全策（Safety Mechanism；SM）の潜在故障

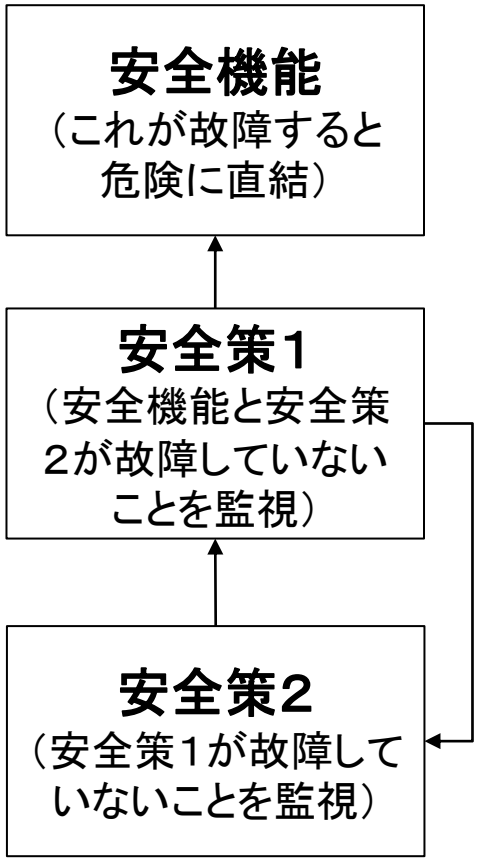
a) 安全なケース



b) 危険なケース



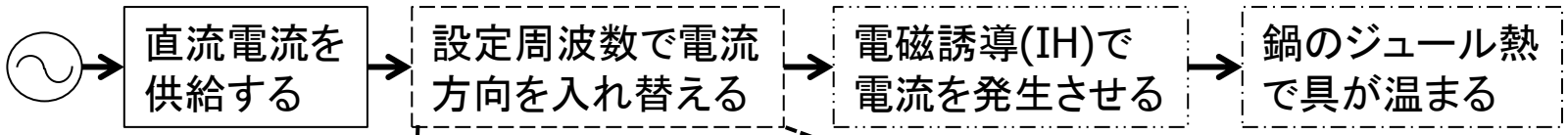
対策例



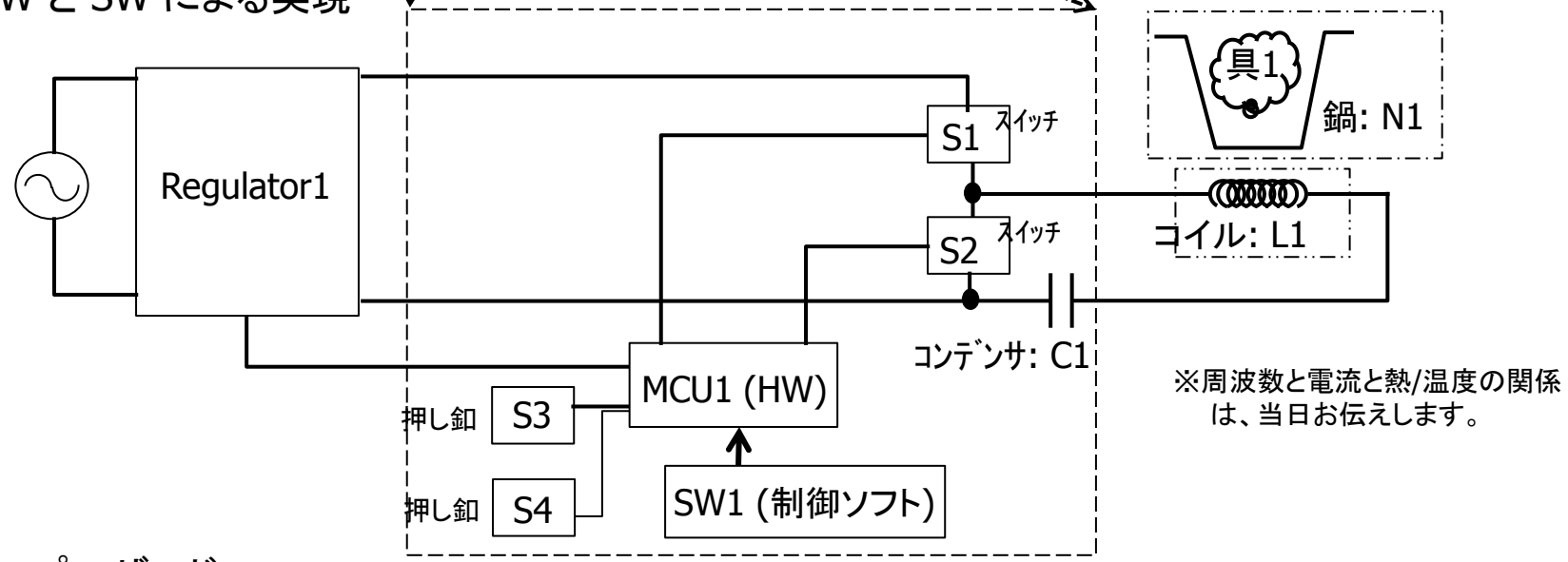
例題システムの説明

例題システム：IHクッキングヒーター

1. システムレベル (機能記述)



2. HW と SW による実現



※周波数と電流と熱/温度の関係は、当日お伝えします。

2. トップハザード
   1) システム内部の火災
   2) 具(油等含む) の異常加熱による火災

ご協力：高野 裕之（東芝セミコンダクター＆ストレージ社）

ソフトウェアの制御

今回の安全分析対象範囲

S3
(押し釦)

S4
(押し釦)

1(下げる)/0

1(上げる)/0

ヒータ強度管理
(6段階)

ヒータ
出力強度
(0～5)

S1,S2出力時間
(t)の計算

S1,S2
出力時間
(t)

S1,S2
制御値出力

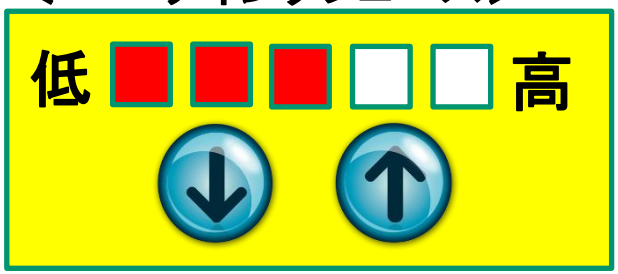
1/0

1/0

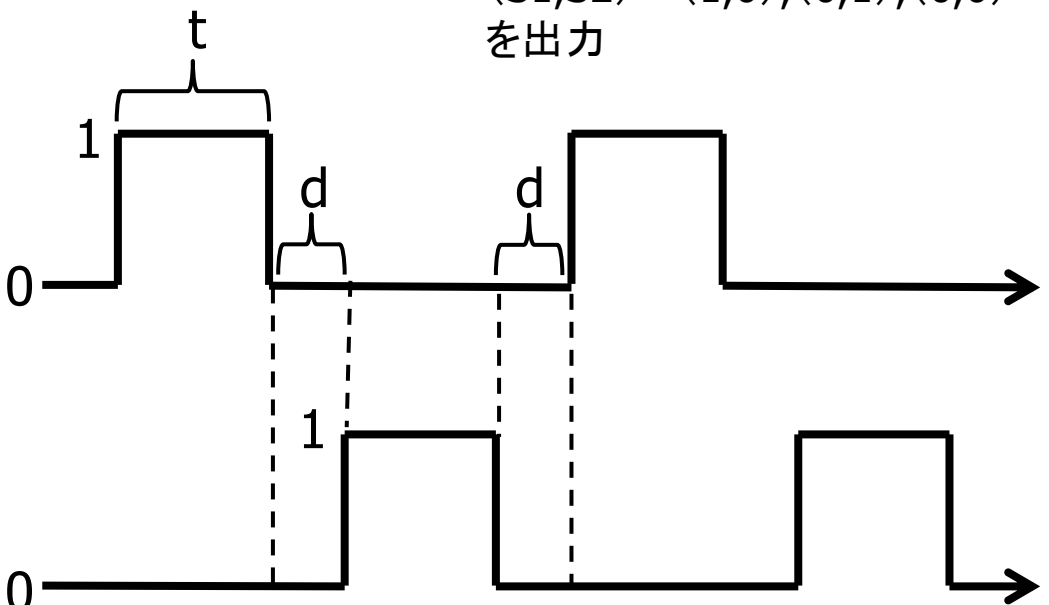
S1
(スイッチ)

S2
(スイッチ)

＜ユーザインタフェース＞



tに応じて、
(S1,S2)＝(1,0),(0,1),(0,0)
を出力



＜備考＞
今回、簡略化のため「設定値通り、時間t,dが保たれていれば、温度は一定となる」こととします。

ソフトウェアの詳細設計