HITACHI
Inspire the Next

制御システムセキュリティカンファレンス2019

Connected時代のセキュア機能安全

2019/02/15

株式会社 日立製作所 研究開発グループ
システムイノベーションセンタ　セキュリティ研究部

甲斐　賢 CISSP, 情報学博士

HITACHI
Inspire the Next

Contents

HITACHI
Inspire the Next

1. 章　背景と前提知識：機能安全とは

1-1 安全とは？機能安全とは？

HITACHI
Inspire the Next

安全性とは、システムが規定された条件の下で、人の生命、健康、財産またはその環境を危険にさらす状態に移行しない期待度合(JIS X 0134:1999)

リスク

■危険な兆候の生起確率と、生起による不利な結末の関数

➢例：電車が人をはねる

本質安全

■リスクの原因を根源から排除する

➢例：電車と人を構造的に分ける

機能安全

■リスクの発生確率を機能的な工夫により**許容可能なレベル**にまで低減する

➢例：電車と人を踏み切りで分ける

1-2 ALARPの原則

ALARP: As Low As Reasonably Practicable
SIL: Safety Integrity Level

HITACHI
Inspire the Next

許容できないリスク、広く許容されるリスクを定め、その間のリスクを合理的に実行可能な限り低減する

何をやっても危険

例：近すぎる

現実的な実践手法
＋
リスク軽減手法
＋
リスクとコストが均衡

例：十分に遠い

何もやらなくても安全

許容可能な領域（ALARP）

リスクを低減する要求レベル

SIL1
SIL2
SIL3
SIL4

1-3 求められる安全度水準の例

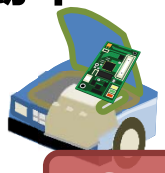
SIL: Safety Integrity Level
ASIL: Automotive SIL

HITACHI
Inspire the Next

人を危険にさらすほど、高い安全度水準 (SIL) が目安として要求される

自動車

ISO26262



エンジン ASIL B

ブレーキ ASIL D

鉄道システム

IEC62278
EN50126

運行管理 SIL 2

信号 SIL 4

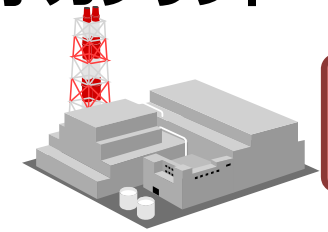
建設機械

ISO15998

操作 SIL 2

操舵(公道) SIL 3

原子力プラント

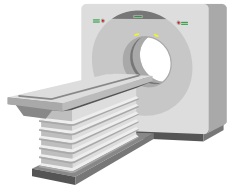


IEC61513
SIL3

生活支援ロボット

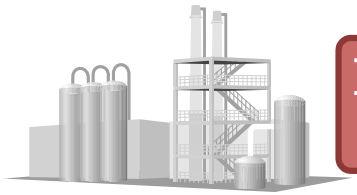
ISO13482
SIL3

医療装置



IEC62304
IEC60601
SIL 2

プロセス産業



IEC61511
SIL 2

エレベータ

ISO22201
SIL2

電化製品

ドリル

芝刈り機

IEC60335-1
Annex R
SIL 2

1-4 ランダム故障とシステマティック故障

HITACHI
Inspire the Next

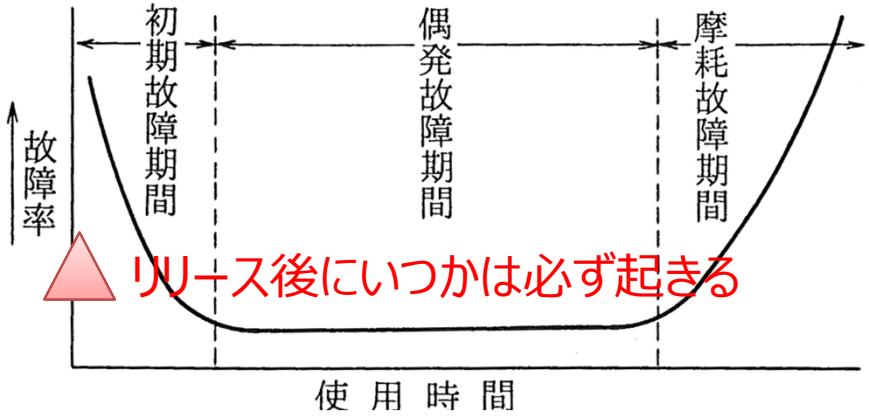
ランダム故障は、その予知は不可能であり、いつかは必ず起きる
システマティック故障は、何らかの原因があれば確定的に起きる(原因を除去できれば起きない)

故障 (failure)
要求を実行する能力が、そのアイテムになくなること。(ISO 13489-1)

以降「ランダム故障」と呼ぶ

以降「システマティック故障」と呼ぶ

偶発的HW故障 (random HW failure)
HWの劣化機構に伴う偶発的故障。(IEC 61508-4)



系統的故障 (systematic failure)
設計変更、製造工程、運転手順、文書の変更によってのみ除去できる決定的故障。(IEC 61508-4)

1-5 故障に対する“Avoidance”と“Control”

HITACHI
Inspire the Next

ランダム故障に対して、Avoidanceは無意味、Controlのみで対処
システマティック故障に対して、AvoidanceとControlの両方で対処

発生源	ランダム故障	システマティック故障
対処方策	× Avoidance	スライド#1-7 Fault Avoidance 故障が起きないように、事前に回避するための方策・技法を用いる
	スライド#1-6 Fault Control 何らかの故障が発生しても、安全機能が喪失しないか、あるいは危険な状態にならないようにする	Fault Control 同左

参考：https://apac.tuv.com/jpblog/iec615081-1

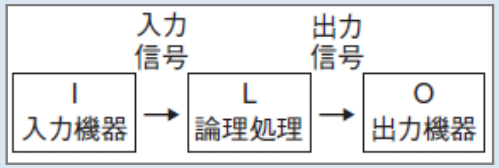
1-6 ハードウェアに対するFault Control

HITACHI
Inspire the Next

冗長性、多様性によって、発生確率を「論理的」に下げることができる

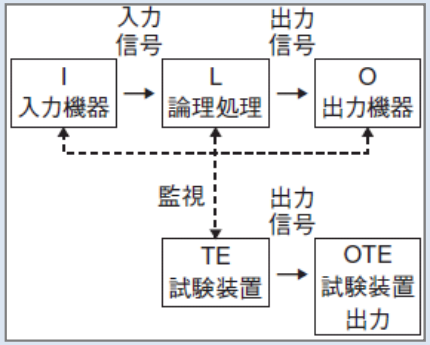
■コンポーネントとして発生確率を下げる（ISO 13849参考）

パフォーマンスレベル
カテゴリB,1



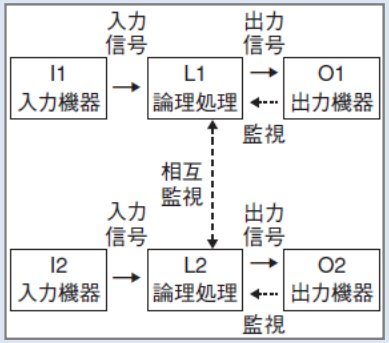
発生
頻度
＞

カテゴリ2



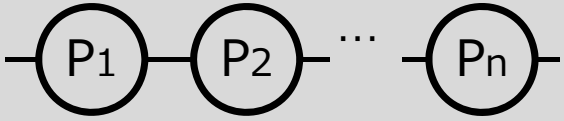
発生
頻度
＞

カテゴリ3,4



■システムとして発生確率を下げる

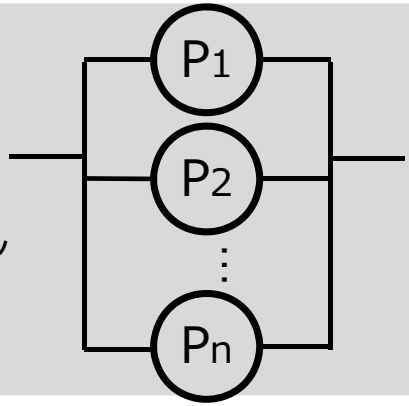
直列システム



1箇所でも故障すれば
全体が障害になる

発生
頻度
＞

並列システム

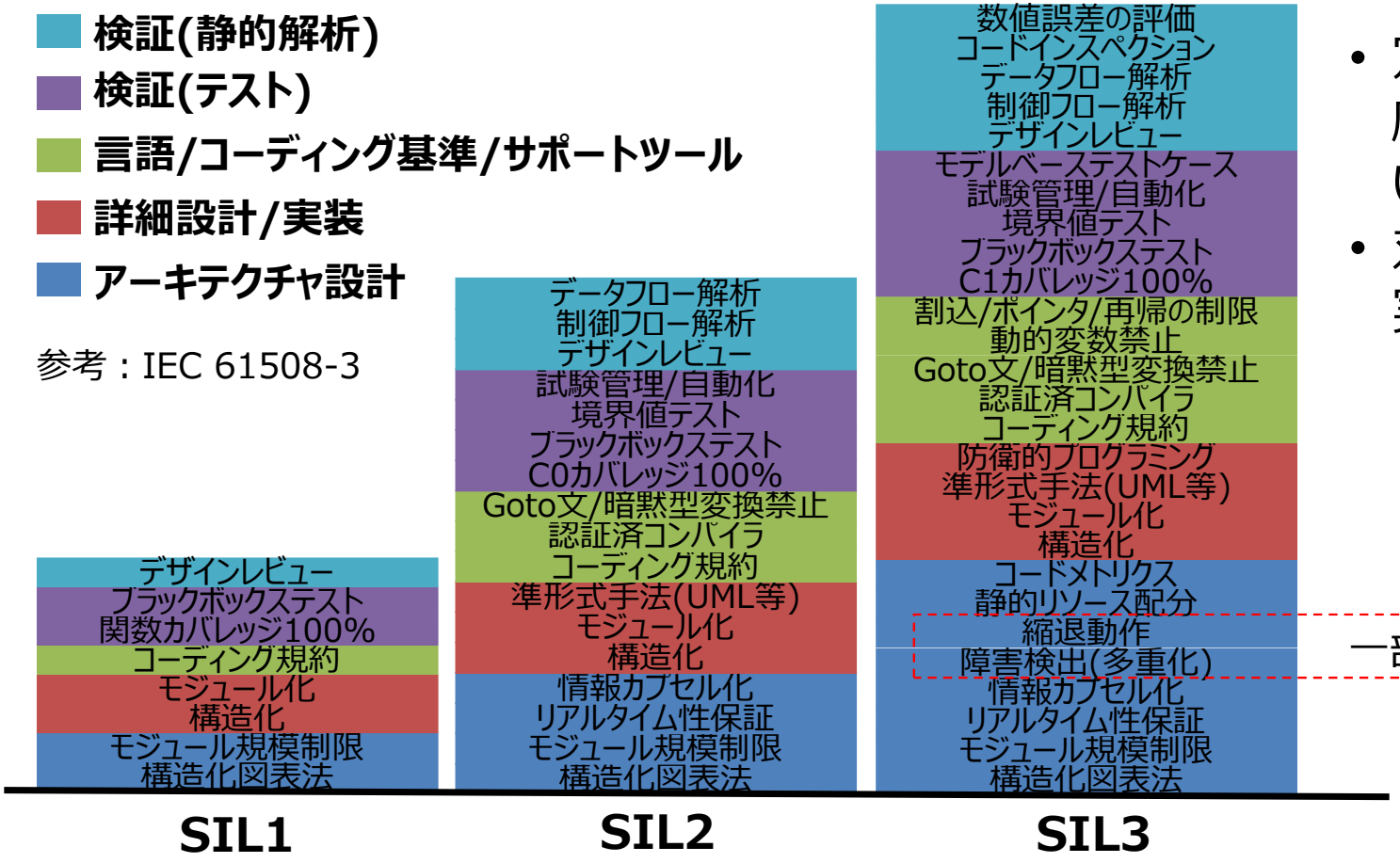


全箇所が故障し
なければ全体は
障害にならない

1-7 ソフトウェアに対するFault Avoidance

HITACHI
Inspire the Next

SILに応じてふさわしいAvoidanceが「経験的」に定められている



- 定量的なSILにふさわしい厳しさの技法が選択されている。
- 対応するSILレベルに応じて実施すべき技法が増える。

SILが上がるほど
対応は困難

一部Fault Controlあり

HITACHI
Inspire the Next

2. 章　機能安全の体系でサイバーセキュリティを扱うときの課題

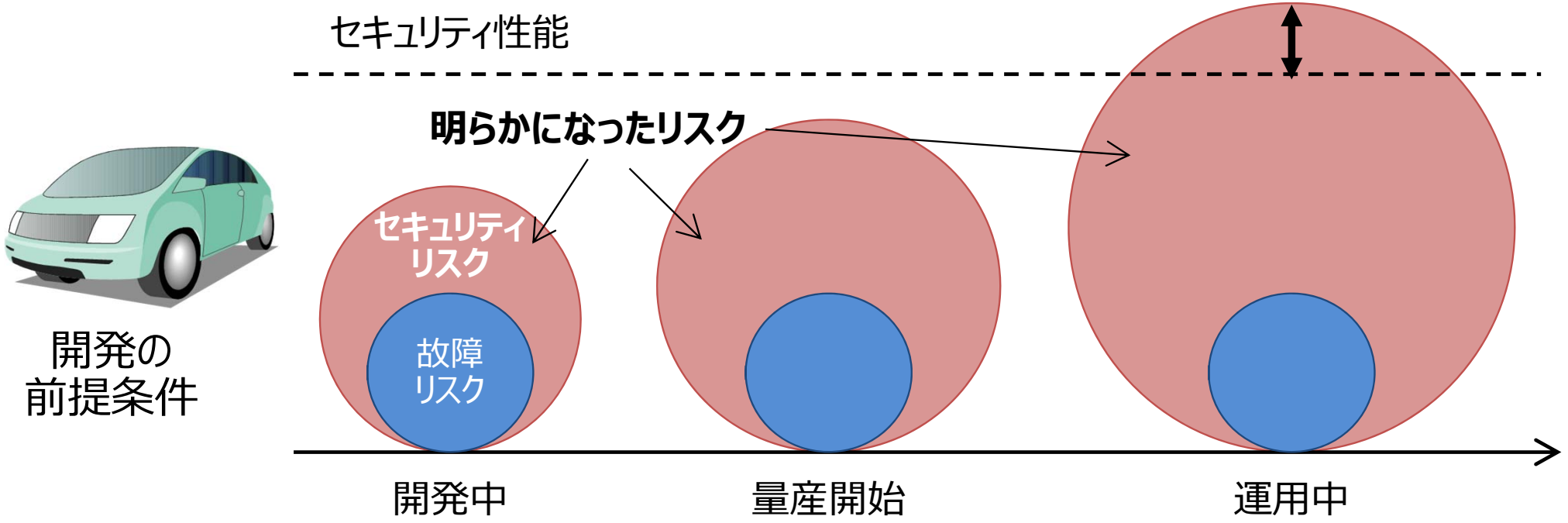
2-1 発生確率を見積る難しさ

HITACHI
Inspire the Next

発生確率を見積もる開発時に、運用時の発生確率を見積もれない

サイバーセキュリティは「開発の前提条件」に対して
明らかになるリスクが次第に増える
ところが、故障リスクと違う

機能・性能に影響ある場合、
追加の対応が必要



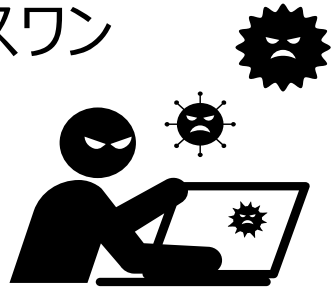
2-2 ゼロデイ脆弱性というブラックスワン（※）

※めったに起こらないが、壊滅的被害をもたらす事象のこと。

HITACHI
Inspire the Next

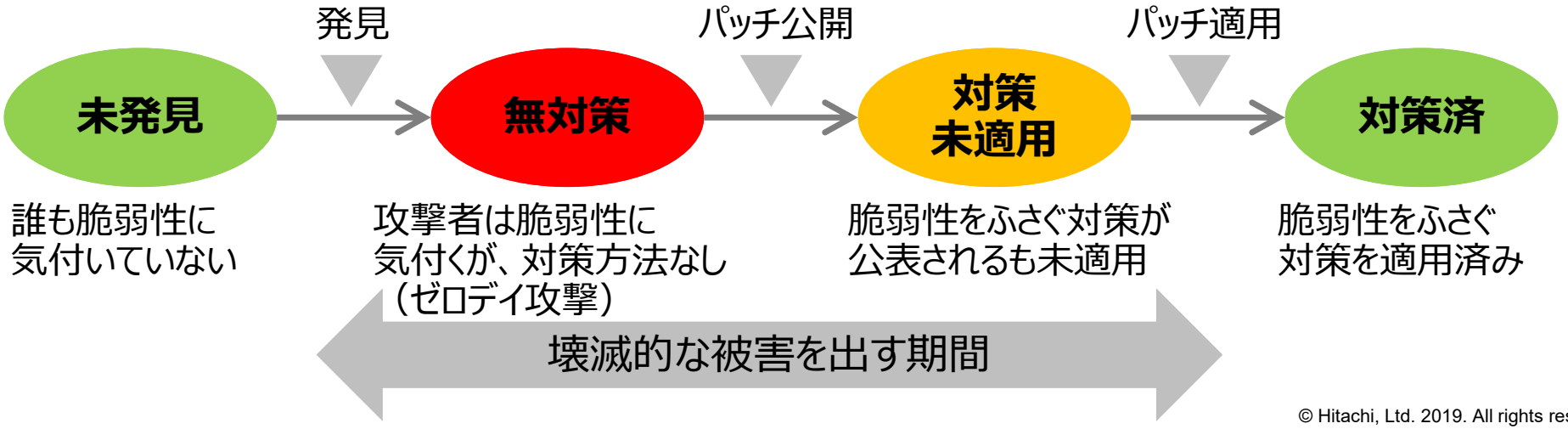
いつ、誰が、あらたな脆弱性を見つけるのかは、誰にも分からない

最近のブラックスワン



- Heartbleed（OpenSSL脆弱性）
- EternalBlue（Windows脆弱性）
- Shellshock（Bash脆弱性）
- Meltdown/Spectre（Intel CPU脆弱性）

脆弱性のライフサイクル



2-3 安全のなかでサイバーセキュリティをどこまで考えているか

HITACHI
Inspire the Next

安全を脅かす原因・脅威のひとつではあるが、サイバー攻撃は「見て見ぬふり」

安全を脅かす原因、脅威

- 機器のハード故障・劣化、ソフトウェアのバグ
- 地震、雷、台風
- **破壊、ハッカー（厳密にはクラッカー）、テロ、なりすまし、盗聴、などの人間の悪意ある行動**
- 設計外の負荷、通信の輻輳などの過負荷
- 大規模化、複雑化、ブラックボックス化などの複雑性
- 時代（年代ギャップ、バージョンアップによるギャップ）、文化（異文化ギャップ）、などに起因するコミュニケーション不足
- 環境変化（景気の変化、社会の変化、時代の変化など）

出典：向殿政男、安全設計の基本概念、p38、2007年

機能安全ISO 26262 2nd ed
→サイバーセキュリティ
SAE(※) J3061を参照まで
※SAE:米国自動車技術会

IEC TC65/WG20
→機能安全IEC 61508と
システムセキュリティIEC 62443
を共通に利用するガイドランを提供

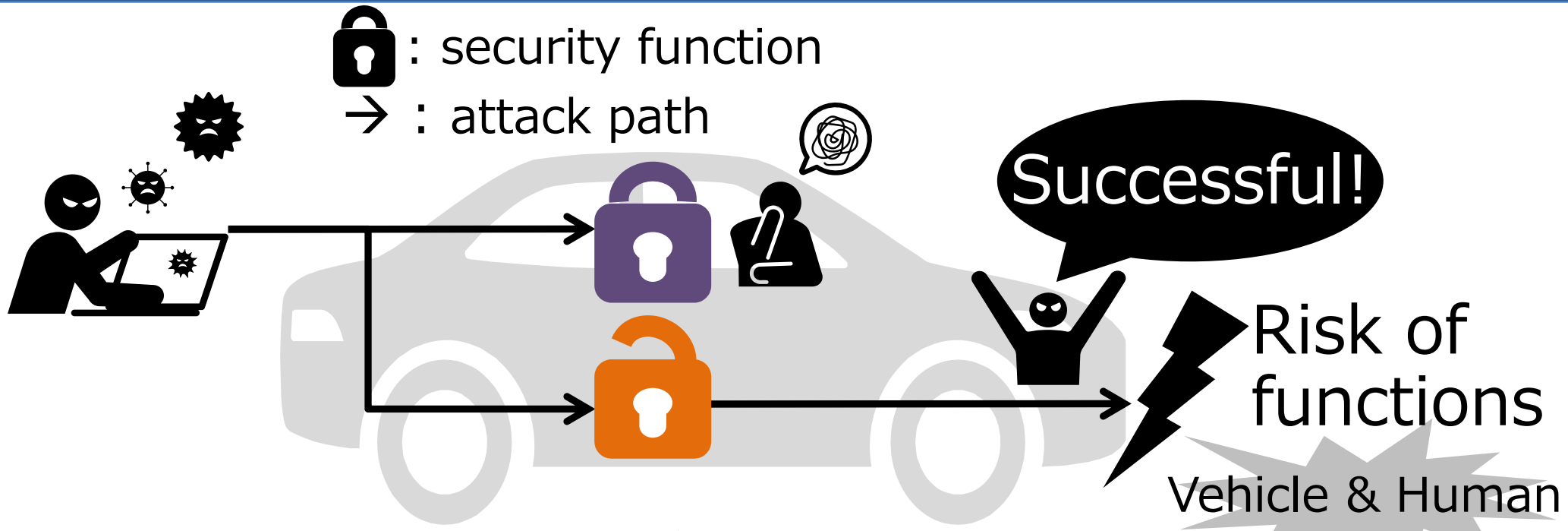
HITACHI
Inspire the Next

3. 章　機能安全のサイバーセキュリティ拡張

3-1 着目するのは、発生確率から攻撃成功確率へ

HITACHI
Inspire the Next

サイバー攻撃の発生確率は見積もれなくても、攻撃成功確率は見積もれる



発生確率 $P(Attack)$ ⇒ 攻撃成功確率 $P(Success \mid Attack)$

3-2 サイバー攻撃に対する対処方策

Se-SIL: Security enhanced SIL

HITACHI
Inspire the Next

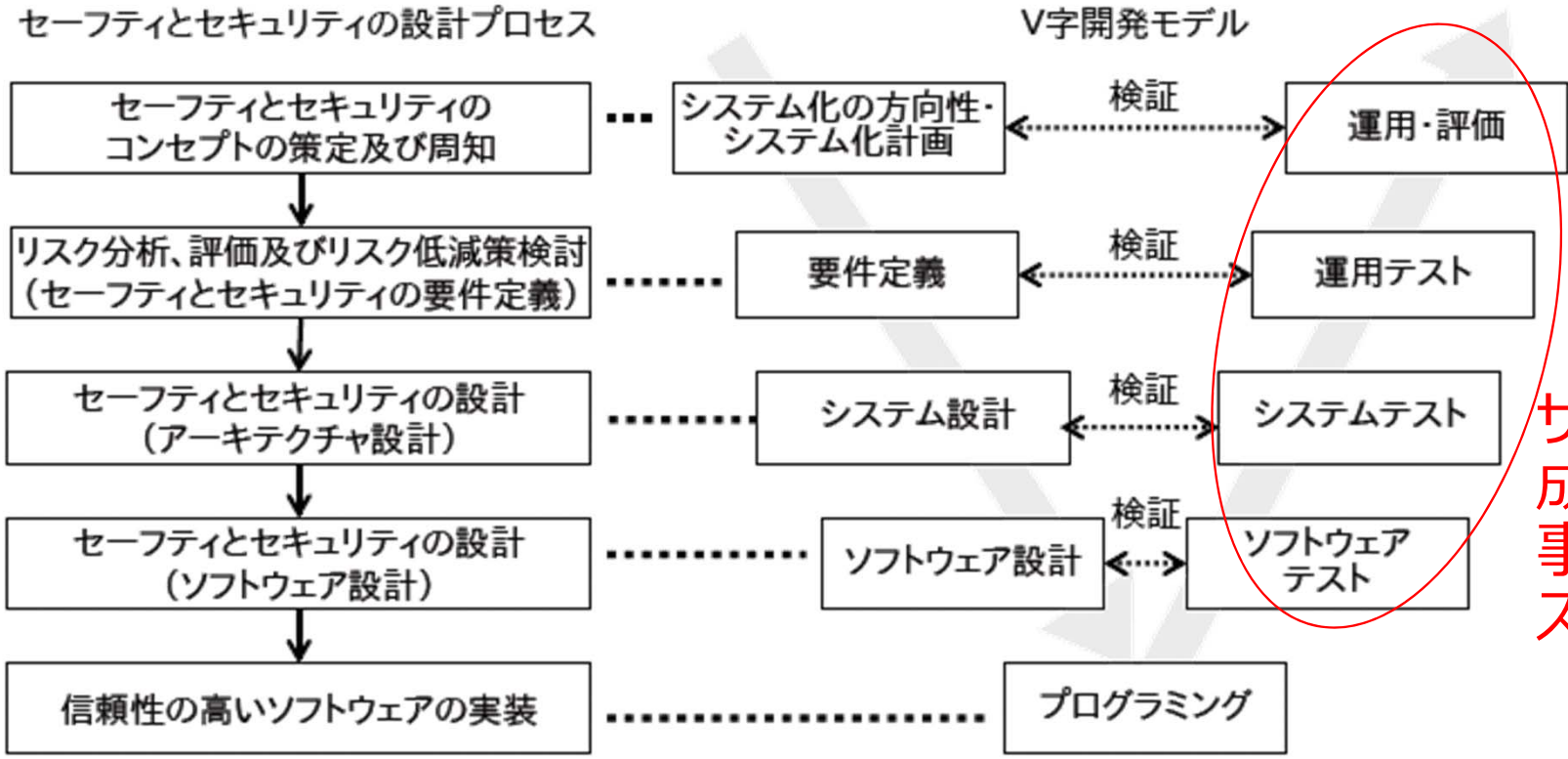
脆弱性に対するAvoidanceと、攻撃を成功させないControlとの組合せ

発生源	故障		サイバー攻撃
	ランダム故障	システマティック故障	
対処方策	× Avoidance	Fault Avoidance 故障が起きないように、事前に回避するための方策・技法を用いる	**脆弱性に対するAvoidance** サイバー攻撃が成功しないように、事前に回避するための方策・技術を用いる Se-SIL拡張 1
	Fault Control 何らかの故障が発生しても、安全機能が喪失しないか、あるいは危険な状態にならないようにする	Fault Control 同左	**攻撃を成功させないControl** サイバー攻撃が成功しても、安全機能が喪失しないか、あるいは危険な状態にならないようにする Se-SIL拡張 2
効果	P(Danger|Fault)を下げる	P(Fault)を下げる	**P(Success|Attack)を下げる**

3-3-1 脆弱性に対するAvoidance

HITACHI
Inspire the Next

V字開発プロセスを確立することによって脆弱性を作りこまない



サイバー攻撃が
成功しないように、
事前にどこまでテ
ストすれば良いか

図 3-5　V字開発モデルとセーフティとセキュリティ設計のプロセス

出典：IPA, つながる世界のセーフティ＆セキュリティ設計入門

3-3-2 現実的な値をもとめる

HITACHI
Inspire the Next

サイバー攻撃者が攻撃を成功させるまでに要する時間の相場を調べた

「10時間」の意味するところ

（原文）
71% of cyber criminals say they can breach the perimeter of a target within 10 hours.
出典：bugcrowd, INSIDE THE MIND OF A HACKER, 2018/12

（邦訳）
71%のサイバー犯罪者は、10時間あればターゲットの境界の中に侵入できると言う。

「10,000時間」の意味するところ

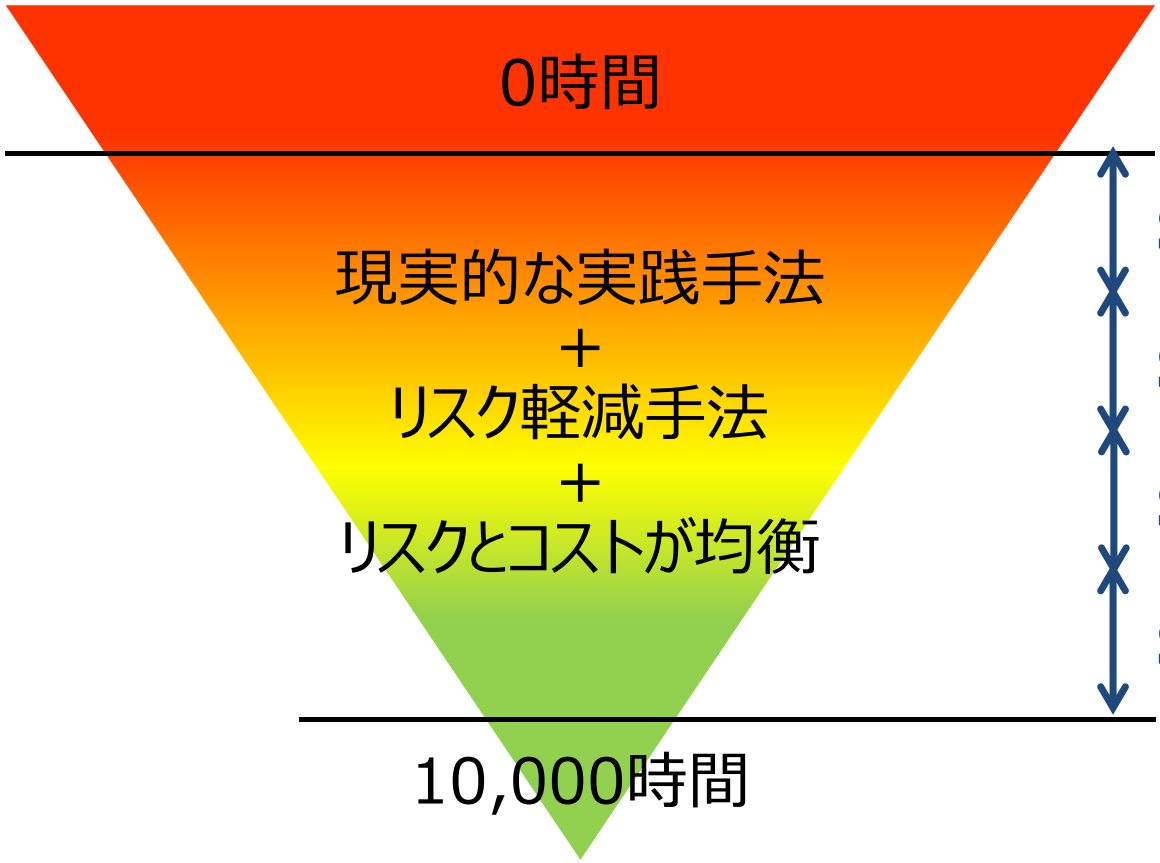
（原文）
Symantec estimates that the group developing Stuxnet would have consisted of anywhere from five to thirty people, and would have taken six months to prepare.
出典：Symantec

（邦訳）
Symantecは、Stuxnetを開発したグループは、5人から30人からなり、準備に6ヶ月はかかっただろうと見積もっている。
10人×40時間/週×25週＝10,000時間

3-3-3 ALARPにもとづくAvoidanceの程度

HITACHI
Inspire the Next

0時間は許容不可、10,000時間を広く許容されるとして、10倍ずつ長くテストする



リスクを低減する
要求レベル

Se-SIL1 : 0-10時間

Se-SIL2 : 10-100時間

Se-SIL3 : 100-1,000時間

Se-SIL4 : 1,000-10,000時間

NVD: National Vulnerability Database
CWE: Common Weakness Enumeration

HITACHI
Inspire the Next

おもにソフトウェアの脆弱性をAvoidanceするための実践手法

R: Recommended, HR: Highly Recommended

脆弱性に対するAvoidance (テスト項目は、サイバーセキュリティ試験基準UL2900を参考)		Se-SIL1	Se-SIL2	Se-SIL3	Se-SIL4
脆弱性と攻撃	既知の脆弱性テスト(例: NVD)	HR	HR	HR	HR
	マルウェアテスト	HR	HR	HR	HR
	不正な形式の入力テスト	—	HR	HR	HR
	構造化された侵入テスト(例: 設定回避、権限昇格)	—	R	HR	HR
ソフトウェア脆弱性	ソフトウェア脆弱性分析	R	HR	HR	HR
	静的ソースコード分析(例: CWE/ SANS Top25)	R	HR	HR	HR
	静的バイナリとバイトコード分析	R	HR	HR	HR

【今後の課題】攻撃手法のState-of-the-Artを踏まえた継続的なアップデート

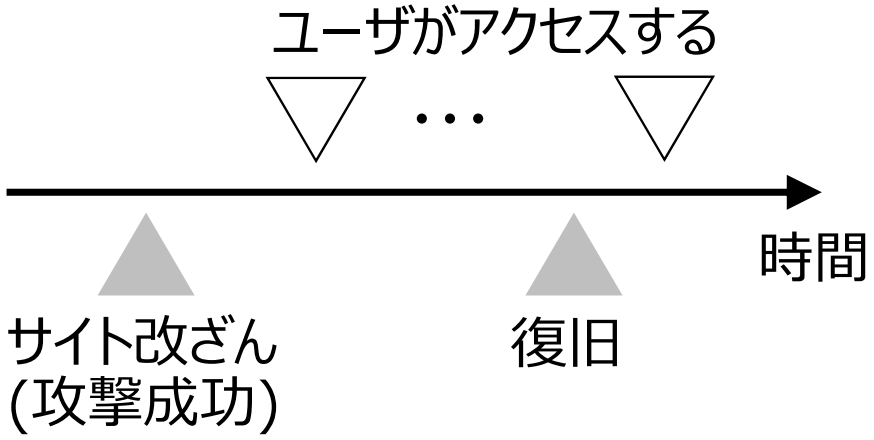
3-4-1 攻撃を成功させないControl

HITACHI
Inspire the Next

サイバー攻撃を受けても危険になる前に制御を取り戻す

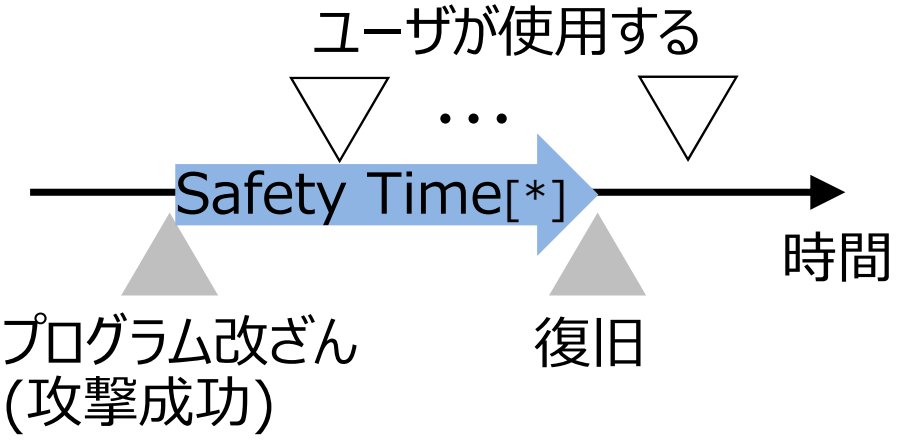
Webサイトの改ざん

サイト改ざんされても、ユーザが気付く前に元通りに直せば、改ざんにはならない



制御を乗っ取られる

サイバー攻撃を受けても、ユーザが危険になる前に元通りに直せば、成功にはならない



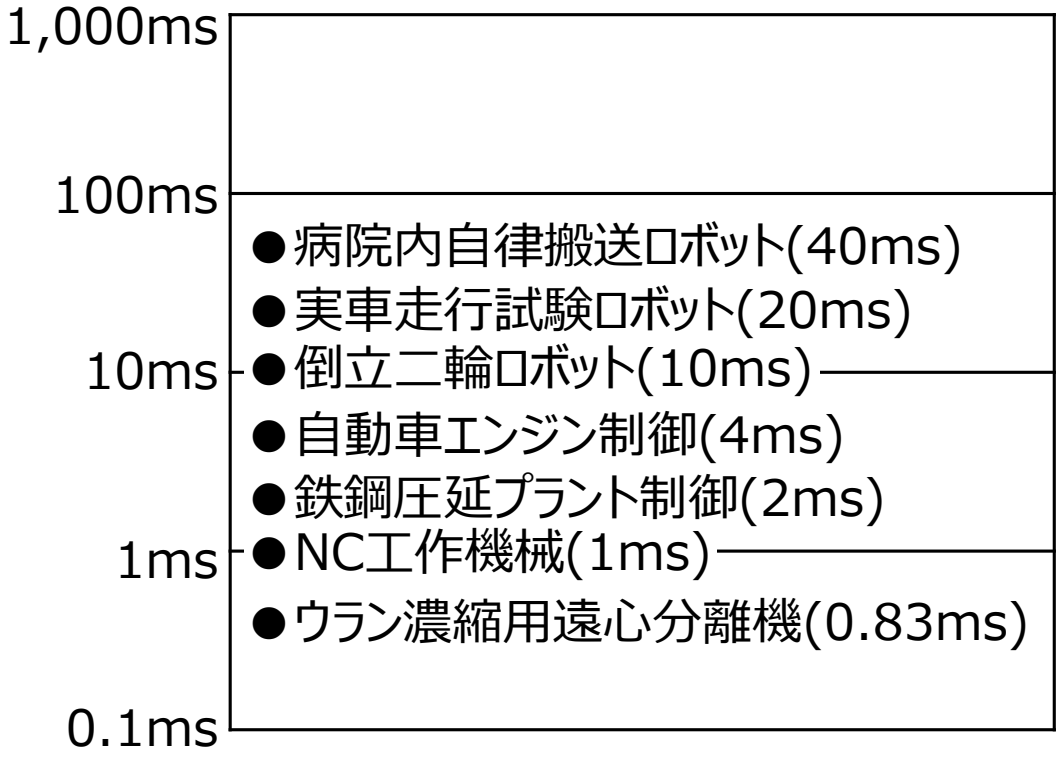
[*]それまでに元に戻れば危険にならない時間

NC: Numerically Controlled

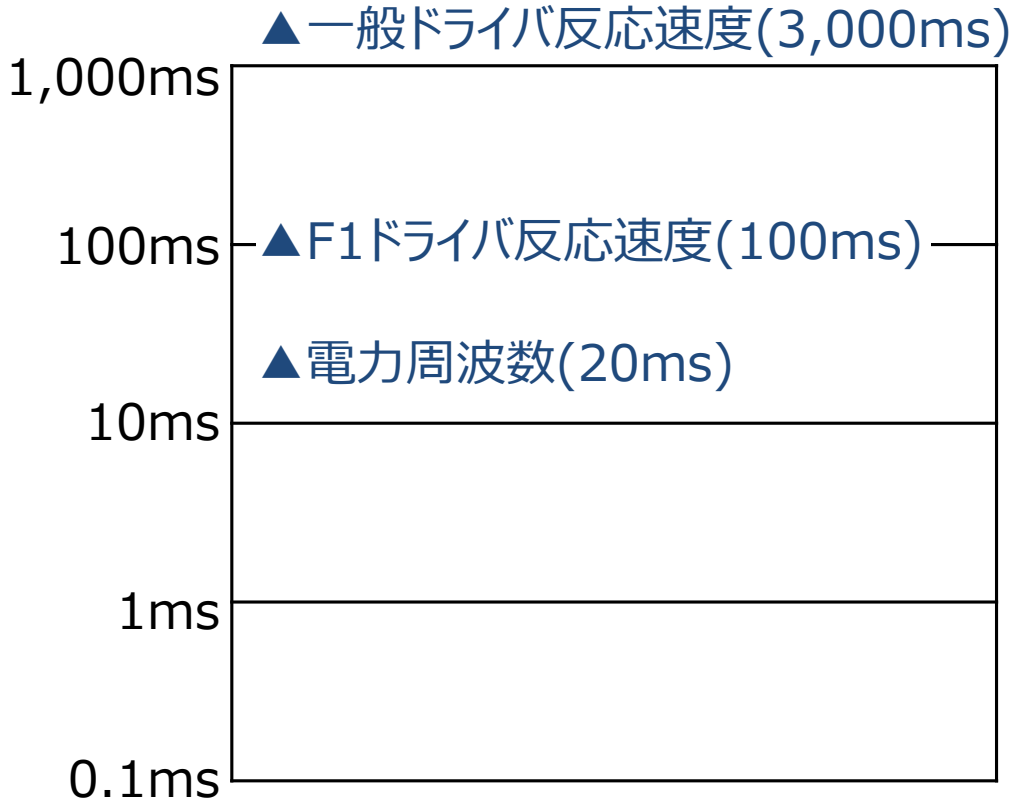
HITACHI
Inspire the Next

制御システムが制御不能にならないための制御周期を調べた

制御システムの制御周期の例



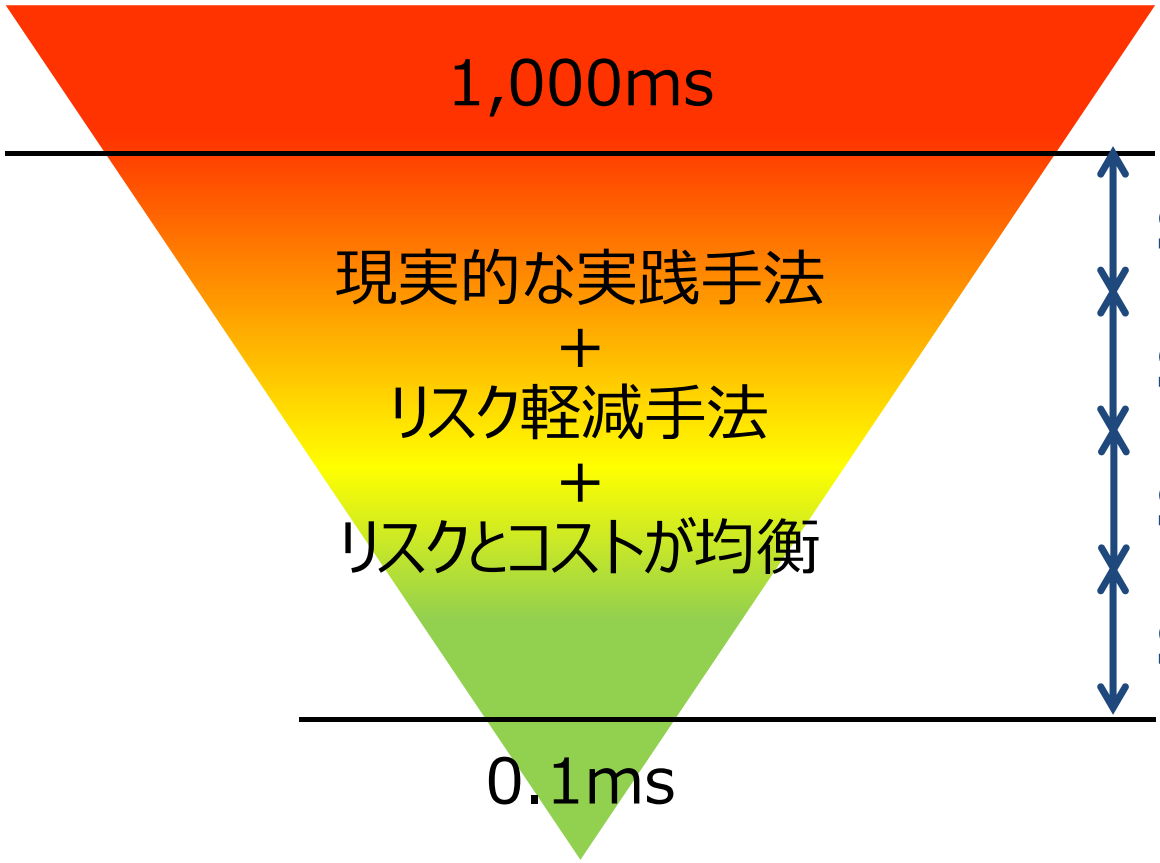
（参考）身近な制御周期の例



3-4-3 ALARPにもとづくControlの程度

HITACHI
Inspire the Next

1sは許容不可、0.1msは広く許容されるとして、Safety timeを1/10ずつ短く



リスクを低減する
要求レベル

Se-SIL1 : 100-1,000ms

Se-SIL2 : 10-100ms

Se-SIL3 : 1-10ms

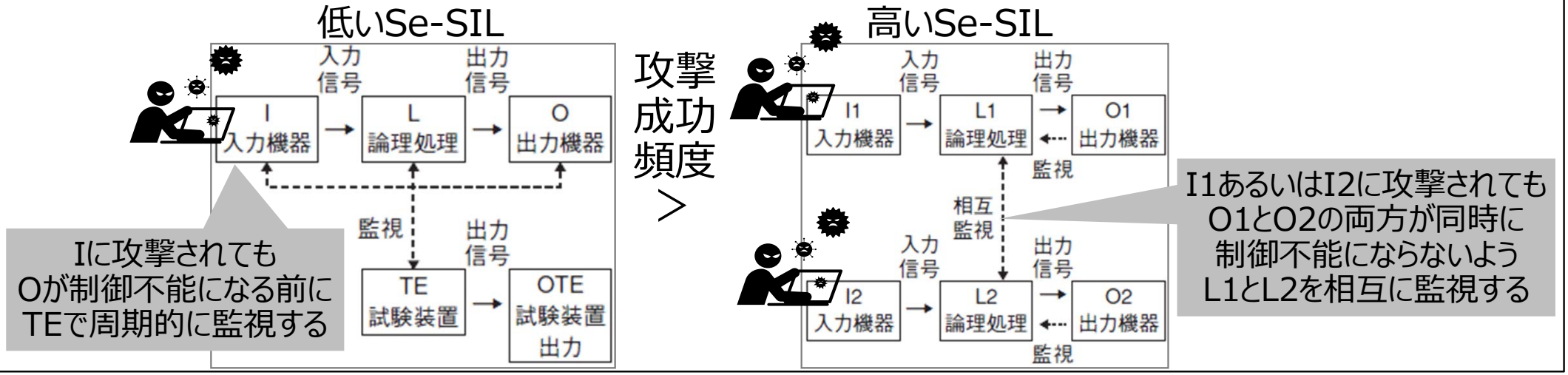
Se-SIL4 : 0.1-1ms

3-4-4 Safety Timeの実践手法

HITACHI
Inspire the Next

サイバー攻撃を成功させないControlのための実践手法

■コンポーネントとしてControlする



■システムとしてControlする

多層防御により、サイバー攻撃の到達可能性を下げ、攻撃者に許してしまう自由時間を短くする

参考: YIWEN CHEN, TAKASHI KAWAUCHI, CHINATSU YAMAUCHI, SATOSHI KAI, ERIKO ANDO, An Approach to Quantify Cybersecurity Risk in Terms of Functional Safety Requirement in Connected System, DICOMO 2018, pp.1149-1154

【今後の課題】ランタイム処理のState-of-the-Artを踏まえた継続的なアップデート

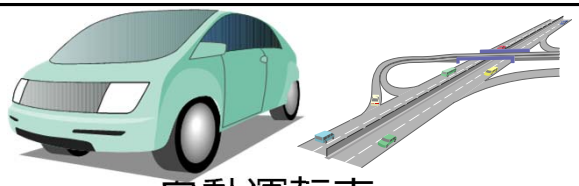
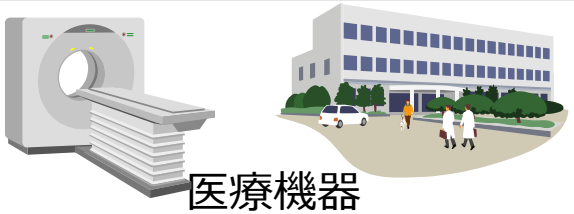
HITACHI
Inspire the Next

4. 章　おわりに

4-1 業界動向

HITACHI
Inspire the Next

安全が要求されていた分野で、サイバーセキュリティへの要求も出てきた

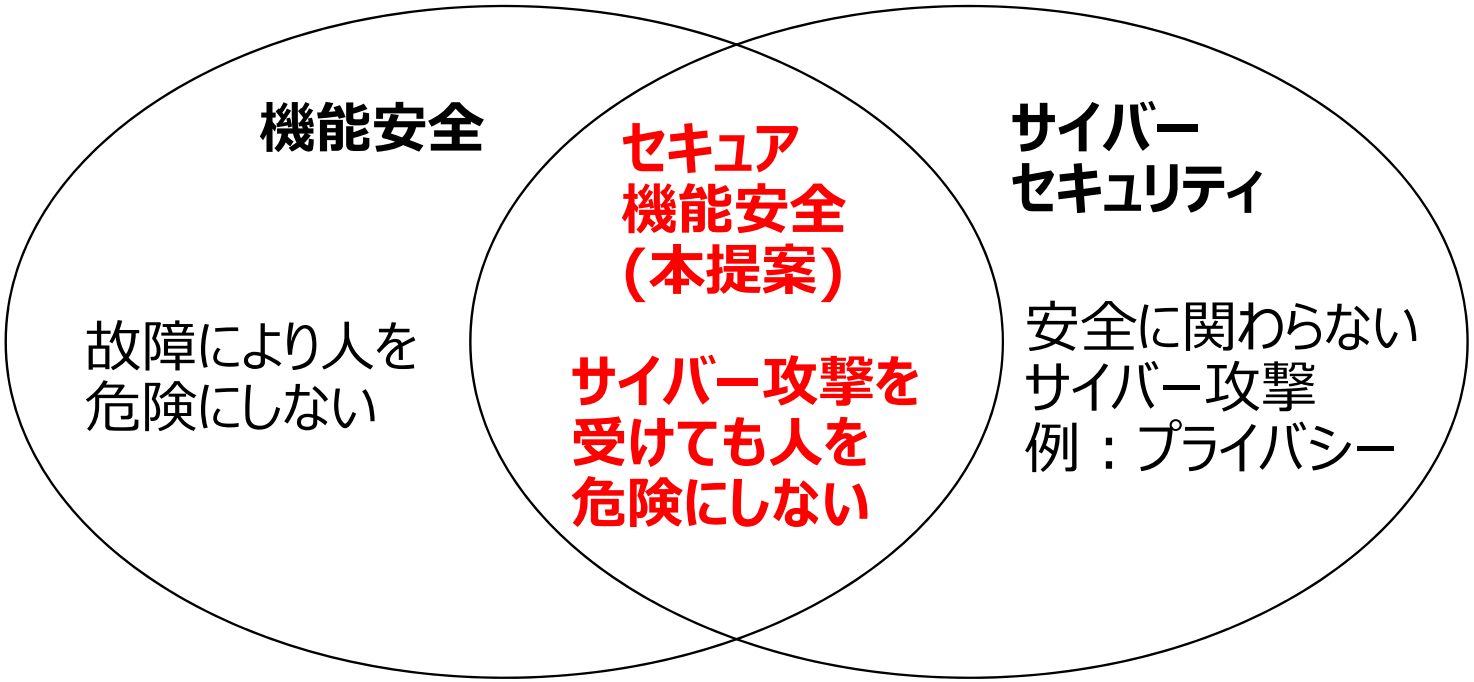
対象	 自動運転車	 農業機械	 医療機器
所轄官庁	国土交通省	農林水産省	米国食品医薬品局(FDA)
文書名	自動運転車の安全技術ガイドライン	農業機械の自動走行に関する安全性確保ガイドライン	「UL 2900-2-1」がFDAのRecognized Consensus Standardsに
公表日	2018年9月	2018年3月	2018年6月
安全の要求に見られるサイバーセキュリティの要求	• 車外NWから社内の制御NWが影響を受けないこと • システムの機能不全時の「セーフモード」を備えること • 不正操作を検知したときは、運転者に警告の上、車両を安全にコントロールすること	• ロボット農機の不正稼動やロボット農機に蓄積された情報の漏洩等のサイバー攻撃を防ぐことができるよう、サイバーセキュリティ対策を講ずること	「UL 2900-2-1」の目次 • 製品、製品設計、製品利用の文書化 • リスクコントロール • リスクマネジメント • 脆弱性と攻撃 • ソフトウェア脆弱性 • ﾗｲﾌｻｲｸﾙを通じたｾｷｭﾘﾃｨﾌﾟﾛｾｽ

4-2 めざす世界

HITACHI
Inspire the Next

機能安全に関わるサイバーセキュリティを、相場観をもって、安全と見なされるように

安全が要求される分野



ベンダがお客に示すもの

安全に関わる製品・システム

<機能安全>
SIL

<セキュア機能安全>
Se-SIL

<サイバーセキュリティ>

HITACHI
Inspire the Next

END

Connected時代のセキュア機能安全

2019/02/15

株式会社 日立製作所　研究開発グループ
システムイノベーションセンタ　セキュリティ研究部
甲斐　賢


HITACHI
Inspire the Next