G-12

アナログ・ディジタル併用の異種冗長な計測系によるデータ完全性と可用性の保護の検討

下田 康世†　　小谷 大祐‡　　岡部 寿男‡

Kosei Shimoda　Daisuke Kotani　Yasuo Okabe

1. はじめに

実世界のセンシングを入力とする制御システムが正常に動作するためには、制御コンピュータへの入力が実世界を正しく反映していることが必要不可欠である[1]。しかしヒューマンエラー、自然災害といった偶発的な事象に加え、悪意あるサイバー攻撃者による攻撃といった外的要因でセンサの計測値が改竄・偽造・妨害されると、誤ったセンサの計測値から不適切なアクチュエーションが行われる可能性がある。したがって、それらの要因からセンサの計測値を保護し、信頼できる計測系を構築するという情報セキュリティが非常に重要である。

ある計測系において異常や故障が発生した場合でも計測系の信頼性を保つ方法として一般的に用いられるのは冗長化である。可用性の観点からは、いずれかのセンサからのデータが断絶した際も他のセンサのデータを参照することができる。完全性の観点からは、正常時は全てのセンサからのデータが要求される精度の範囲内で一致していることが想定されるが、全てのセンサからのデータが一致していないときには何らかの異常や故障があることを検出できる。

冗長化は、同型な冗長化と異種冗長化に分類される[2,3]。一般に計測系を構成する機器の自然故障を想定する場合、センサを多重に取り付けて同型の冗長化を行う。しかし、同一の機器、同一のソフトウェア、同一の測定法による同型の冗長化では単一の脆弱性が全ての系統に複製されてしまう。そのため、外部からの攻撃に対しては必ずしも有効な対抗策とならない。そこで、ヒューマンエラー、自然災害といった偶発的な事象や、悪意あるサイバー攻撃などにより引き起こされる攻撃からセンサの計測値を保護するための異種冗長化の必要性が指摘されている[4]。

しかし異種冗長な計測系を構成する際に、新規にセンサを取り付けるのが困難な場合がある。測定する対象が稼働中の機器の場合、新たなセンサの取り付けには運用の一時停止やメンテナンスによる停止まで待つ必要がある。また、安全性や性能への影響から新たなセンサを加える改修を行うことができない場合も考えられる。したがって、測定対象に直接変更を加えず、制御システムに内在する冗長性を利用して計測系を構成する手法が必要である。

また、そのような異種冗長な計測系がセンサの計測値の保護にどのように寄与するかを評価する必要がある。異種冗長構成による耐故障設計およびサイバーセキュリティの評価については先行研究が存在するが、計測系を想定したものではない、検討している攻撃の種類や性質について限定的であるなどの問題がある。

本研究では、制御システムに内在する異種冗長性としてアナログ表示の計器とディジタルセンサが併存する場合を利用し、アナログ計器の自動読み取り技術を用いることで異種冗長な計測系を構成する手法に着目する。電子的な計測系が使えなくなる電気断などのトラブルへの備えやアナログ計器のみの運用から計測系のディジタル化が進んだ場合など、運用上や歴史上の理由から、アナログ表示の計器とディジタル化されたセンサが併存することがある。それらを用いることで、測定対象に直接変更を加えず異種冗長な計測系を付加的に構成する。

アナログ計器は計測した値を指針の回転など連続的な物理量で表示する測定計器であり、ディジタルな通信インターフェースを持たない。そのため、アナログ計器表示の自動読み取りにより利便性を高めることを目的に多くのアプローチが提案されている[5,6,7]。

本研究の達成として、独立したアナログ計器とディジタル化されたセンサを併用した異種冗長な計測系のモデルを示した。このモデルによって、上述の異種冗長化がセンサの計測値の完全性及び可用性の保護においてどのような攻撃に対して優れるかの定性的な議論が可能となる。このモデルではアナログ計器の種類およびその自動読み取り方法を一般化した。加えて、攻撃を検出するための系統間の整合性確認で、アナログ計器系統とディジタルセンサ系統の比較形式について一般的に整理した。

また、温度を測定対象としたアナログな温度計とディジタルセンサによる異種冗長な計測系の単純な実装に対し、提案したモデルに基づいて攻撃検出能力の評価を行うことでモデルの有効性を確認した。この計測系では、機器の自然故障などとサイバー攻撃とを識別することは原理的にできないが、計測系統間で計測値が一致しない事象を検出することができる。

2. 関連研究

2.1 異種冗長構成によるシステム保護

故障が発生する制御システムについて長谷川[2]は、安全制御システムを対象に、同型な冗長化構成で共通故障要因が安全度水準を支配していることを明らかにしている。また Aizpurua ら[8]はシステムに内在する異種冗長性を利用し、より信頼性の高いシステムへと再構成を行う方法を提案している。しかしこれらの研究は、各コンポーネントの故障要因を確率的に表現しており、故障要因の定性的な検討ができない。また、悪意あるサイバー攻撃者は特定の目標を達成するために計画的な攻撃を行うこともあり、故障要因として単純な確率分布で表現するのは難しい。

サイバーセキュリティの観点からは、Hu ら[9]が異種冗長な複数のコンポーネントを動的に配置することで未知の脆弱性を突いた攻撃を防ぐ DHR フレームワークを提案している。Wang[10]らは、異種冗長な機能を持つ複数の系による多数決を行うシステムについて、それぞれの系で共通する攻撃表面を元にした攻撃可能性のメトリックを提案している。しかしこれらは異種冗長性の具体的な実装方法を示すものではなく、計測系のシステム全体を評価することができない。また、Erhan ら[16]はセンサの計測値データからサイバー攻撃も含めた異常検知を行う具体的なアルゴリズムについて多くの手法と関連する先行研究をまとめている。

†京都大学情報学研究科通信情報システムコース

‡ 京都大学学術情報メディアセンター

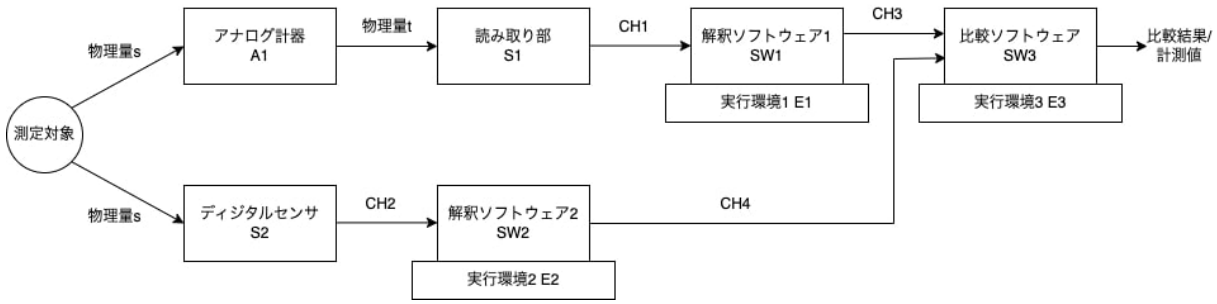


図１：アナログ・ディジタル併用の異種冗長計測系のモデル

具体的なアプリケーションを対象とした研究として、梨本ら[11]は加速度センサ、ジャイロセンサ、地磁気センサを組み合わせた異種冗長な計測系を持つドローンの姿勢推定において、攻撃可能性を評価・実証するとともに計測誤差から攻撃を検出する対策を示した。しかし、この研究で扱っているのはセンサへの物理的な信号注入攻撃のみであり、システム内のディジタル空間に対する攻撃については検討されていない。

2.2 アナログ計器の自動読み取り

アナログ計器の自動読み取りの多くはコンピュータビジョン及び画像処理に基づいている。初期の研究の１つである Algeria ら[5]は、回転式の指針を持つ計器で指針の位置が異なる２枚の異なる画像から指針の回転中心を決定し、ノイズ除去やエッジ検出といった画像処理技術を用いて値を読み取る手法を提案している。Zheng ら[6]はコンピュータビジョン分野の複数技術を適用し、明るさの変化とカメラアングルの変化に対して頑健性を持つ認識システムを提案している。Zuo ら[7]は、畳み込みニューラルネットワークに基づいたアルゴリズムにより、特に回転式の指針を持つ計器を精度よく読み取る手法を提案している。

また、画像処理によらない読み取り手法として、回転式の指針を持つ計器において指針の回転中心に磁石を貼り付け、その回転量を読み取る方法も存在する[12]。

これらの研究はアナログ計器の自動読み取りという課題として独立したものであり、ディジタルセンサとの組み合わせによる計測系の構成手法は提案されていない。

3. アナログ・ディジタル併用の計測系

本章ではアナログ計器とディジタルセンサを併用した異種冗長な計測系のモデルと攻撃者のモデルを示す。このモデルはそれぞれのセンサ、計器、センサと通信するソフトウェアおよびその実行環境という機能ごとの要素から構成される。実装された計測系においてこのモデルに基づいて攻撃経路、脆弱性などの分析を行うことで、どのような攻撃に対して検出可能か、同型な冗長化に対して優れているかの議論を行う

この計測系では、アナログ計器の読み取り値とディジタルセンサの計測値を比較することで、２つの計測系の一致性を確認しながら計測を行う。図１に、モデルを図示する。

この計測系は、計測アナログ計器 A1 及び読み取り部 S1 による系統と、ディジタルセンサ S2 による系統の２つの系統を持つ。２つの系統に整合性があるか、および計測対象の計測値を出力する。整合性については、SW1 および SW2 からデータを受け取り、両者が一致しているか比較する。比較結果は"一致"または"不一致"であり、不一致の場合、いずれかの計測系に第三者による攻撃の可能性を含む異常が発生していると考えられる。

本研究で想定するアナログ計器は、以下のような性質を持つものとする。

・動作はパッシブであり、測定対象からの物理的入力のみに依存する

・ネットワークに接続されていない

以下では提案するモデルの各構成要素についてそれぞれ説明する。

測定対象

実世界の物理対象。特定の物理量 s がアナログ計器 A1 とディジタルセンサ S2 によって測定される。物理量の例は、温度、圧力、電流などである。

アナログ計器

入力された物理量 s を測定し、連続的な物理量で表示する測定計器。表示方法には指針の回転量や目盛に対する高低、ランプの点灯・消灯などがある。その表示は読み取り部 S1 によって物理量 t を介して読み取られる。

読み取り部

アナログ計器 A1 の表示を、物理量 t を介して読み取る。読み取った物理量 t の値を SW1 へ出力する。実装の例としては、光学的に表示を読み取るカメラ[5,6,7]や、指針に固定された磁石の回転から回転量を測定する磁気センサ[12]などがある。

ディジタルセンサ

入力された物理量 s を測定し、離散的な計測値として解釈ソフトウェア SW2 へ出力する測定計器。IC センサであれば、入力 s の値はまずセンサ内の回路によって電気的な量に変換される。その電気的な量は A/D 変換器(Analogue Digital Converter；ADC)による量子化およびサンプリングによってディジタル化され、出力される。そのため、実装によってそれらの要素に更に分割できる。

解釈ソフトウェア 1,2

SW1 は通信路 CH1 を介して S1 の測定した物理量 t の情報を受け取る。SW2 は通信路 CH2 を介してディジタルセンサ S2 と通信し、受け取ったデータをデコードして物理量 s の値を得る。また、それぞれ SW3 へ、両系統の一致性を比較するためのデータと物理量 s の計測値を出力する。物理量 s の計測値について、SW1 は物理量 t の値から求め、SW2 は通信路 CH2 で用いられる通信プロトコルに準じてデータをデコードして得る。

両系統の一致性を比較するためのデータは、比較ソフトウェアで比較を行う形式で出力される。

例として、物理量 s の形式で比較する場合、SW1 は読み取った物理量 t の値を元に求めたアナログ計器 A1 への入力 s の計測値を出力する。s と t の変換は A1 および S1 の実装によって異なる。S1 がカメラの場合、A1 の表示方法に応じた画像処理により、目的の値を読み取る。

比較ソフトウェア

SW1 および SW2 から、物理量 s の計測値と、両系統の整合性を比較するためのデータを受け取る。計測対象の計測値および、2 つの系統に整合性があるかを出力する。

出力する計測値は SW1 および SW2 から得られた s の計測値に基づいて決定する。出力値は、両者のうち一方を採用するか、両者を組み合わせて決定される。

整合性については、SW1 および SW2 から整合性確認のためのデータを受け取り、両者が一致しているかを比較する。比較結果として"一致"または"不一致"を出力する。比較の方法は以下に分類することができる。

・物理量 s の形式で比較する
・物理量 t の形式で比較する
・それ以外の形式で比較する

方法 1 の場合、解釈ソフトウェア SW1 において物理量 t から物理量 s を得る変換を行う。方法 2 の場合、解釈ソフトウェア SW2 において物理量 s から物理量 t を得る変換を行う。方法 3 の場合、SW1,2 双方において s とも t とも異なる形式 u への変換を行う。

一致しているかどうかを判定する手法は、検知精度、リアルタイム性、利用可能なリソースの要件などに基づき選択する。選択した手法において、S1 および S2 の計測精度、および比較するための形式変換の精度を考慮して判定を行うことができる。

実行環境 1,2,3

SW1、2、3 が実行される環境であり、以下を含む。

・実行されるハードウェア
・実行される OS
・参照する外部のデータファイル

通信路 CH1,2,3,4

ディジタル化された情報を通信し、各コンポーネント間を結ぶ通信路。通信路上のネットワーク機器および通信プロトコルを含む。

3.2 攻撃者モデル

梨本らの研究[11]では、センサへの実世界における信号注入攻撃の攻撃能力を、計測値の任意な制御、計測値の取得妨害、攻撃能力無しという 3 つのクラスに分類している。その分類をもとにすると、3.1 節のモデルのコンポーネントおよび通信路に対する攻撃は、以下の 3 つのクラスのいずれかに属する。

・C (Controllable)：攻撃者は、対象のコンポーネントから次の通信路への出力を任意に決定できる。あるいは、攻撃者は対象の通信路から次のコンポーネントへの入力を任意に決定できる。

・D (Disruptive)：攻撃者は、対象のコンポーネントから次の通信路への出力を妨害することができるが、値を制御することはできない。あるいは、攻撃者は対象の通信路から次のコンポーネントへの入力を妨害することはできるが、値を制御することはできない。

・U (Uncontrollable)：攻撃者は、対象のコンポーネントに介入することはできない。あるいは、攻撃者は対象の通信路に介入することはできない。

クラス C に属する攻撃はデータの完全性に対する攻撃であり、データの改竄または偽装を行う。また、クラス D に属する攻撃はデータの可用性に対する攻撃であり、データが正常に得られないよう妨害を行う。ただしクラス D に属する攻撃の中でも計測値が一点に固定されてしまうようなものの場合、攻撃を受けた次のコンポーネントにおいて妨害されていることに気づけないこともある。クラス C の攻撃能力を持つ攻撃者は、無効なデータを用いることでクラス D の攻撃を行うことができる可能性がある。したがって、クラス C の攻撃能力を持つ攻撃者は、クラス D の攻撃を行うことができるとする。

各ソフトウェアおよびその実行環境については、それぞれの実装および実行環境における脆弱性を突いた攻撃を受ける可能性がある。デジタル出力のセンサでは、センサの出力したアナログの電圧/電流値を A/D 変換器によりデジタル表現へ変換する。そのため、アナログの電圧/電流値に対する攻撃や、A/D 変換に対する攻撃の可能性などがある。実際、A/D 変換器の参照電圧端子への入力を操作することで、デジタル表現の出力を改竄できることが示されている[13]。

通信路上ではネットワーク機器に対する攻撃や通信プロトコルに対する攻撃などが考えられる。特に、産業用の通信プロトコルは暗号化や認証を含んだセキュリティ機能を備えていないものが多く、改竄、偽造及び妨害の方法が示されているものもある[14,15]。また、A1 と S1 間の物理量 t の読み取りについてもある種の通信路として捉えることができる。例としてカメラを使った読み取りの場合、偽の計器表示の写真を用いることで計測値を任意に操作するクラス C の攻撃が考えられる。また、強い光の照射や、光源を奪うことで計器表示を読み取れなくするクラス D の攻撃が考えられる。

4. 温度を例にした実装

本章では、単純な計測系の実装において前章のモデルに基づき攻撃検出能力を議論することでモデルの有効性を示す。室内の温度を測定対象として、アナログな計器としての温度計とディジタルセンサによる異種冗長な計測系を実装した。

4.1 計測系の概要

本実装は、独立した温度計とカメラによるアナログ計器系統と、IC 温度センサによるディジタルセンサ系統を持つ。それら 2 系統における温度の計測値を比較し、その差の絶対値が一定の値より大きい場合は系統間に不一致があると判定する。計測値の解釈および比較ソフトウェアについて、Raspberry Pi 上に Python で実装した。また、実装上の便宜のため、SW１、２、３は集約して単一のプログラムとして実装されている。

実装において、実世界の環境に以下の仮定を置いた。

・温度計及び温度センサへの入力は常に一致
・温度計とカメラ位置の関係は固定されている

本実装の構成を提案したモデルに基づき示したものが図 2 である。また、本実装の外観を図 3 に示す。

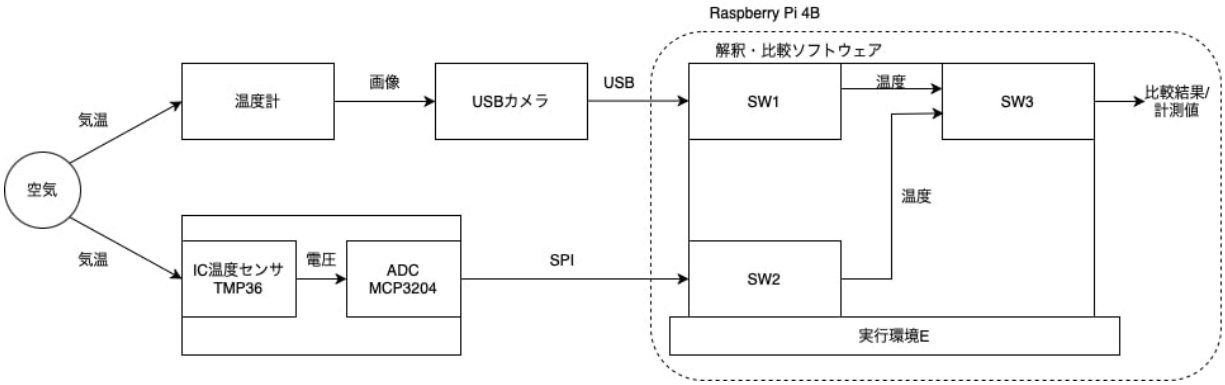
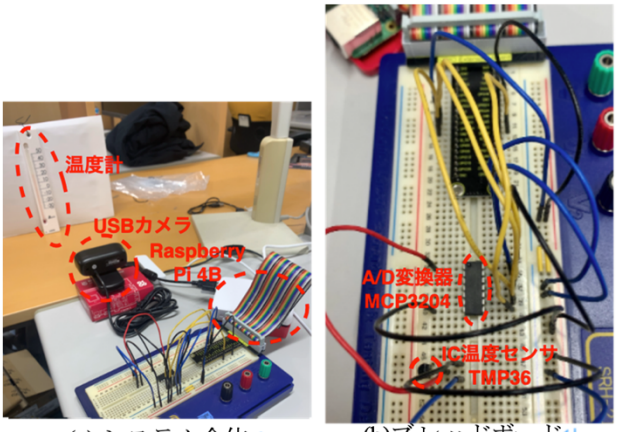
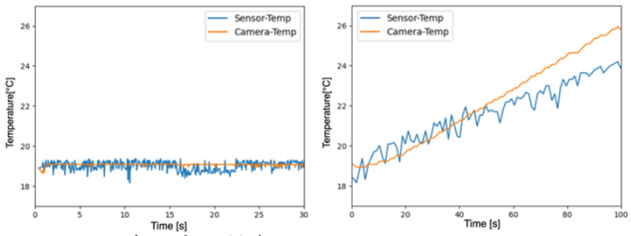


図 2 ：実装した計測系の構成



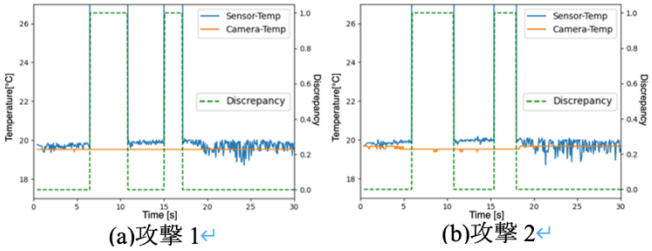
(a) システム全体　(b)ブレッドボード

図 3 ：実装した計測系の外観



(a)温度一定の環境　(b)加熱下の環境

図 4 ：平常時の計測値



(a)攻撃 1　(b)攻撃 2

図 5 ：攻撃による計測値の変化と検出

4.2　計測系の構成

アナログ計器系統は、温度計から比較・解釈ソフトウェア内の SW1 の機能に相当する部分までを含む。ディジタルセンサ系統は、IC 温度センサから比較・解釈ソフトウェア内の SW2 の機能に相当する部分を含む。

温度計系統

アナログ計器として赤液温度計(シンワ測定、プチサーモスクエア 縦 20cm ホワイト【48795】)、表示読み取り部として USB カメラ(サンワサプライ、CMS-V59BK)を用いた。SW1 では、まず OpenCV を用いてカメラの取得画像から温度計の赤色表示部分を抽出する。カメラと温度計の位置関係は固定されているので、画像内の赤色部分の上端の座標から温度計の計測値を求める。

ディジタルセンサ系統

ディジタルセンサは、アナログ電圧を出力する IC 温度センサ(Analog Instrument、TMP36)と A/D 変換器(Microchip Technology、MCP3204-CI/P)を組み合わせてブレッドボード上に構成した。

A/D 変換器では温度センサから出力される電圧値をディジタル化し、SPI 通信によって解釈・比較ソフトウェアへデータを送信する。SW2 では、温度センサ、A/D 変換器、SPI の仕様に基づき、受信した電圧データからセンサの計測した温度を求める。

SW3

ループ処理で、SW1 への計測値の要求、SW2 への計測値の要求、2 系統の計測値の比較を行う。今回使用した温度計と IC 温度センサはともに計測精度が±1℃であるから、両系統の計測値に 2℃以上の差がある時、不一致と判定する。不一致の時、Discrepancy の値として 1 を、一致している時 0 を出力する。

4.3　攻撃と検出の実証

測定対象の温度が一定の環境と温度が変化する環境のそれぞれにおける、2 つの計測系統の計測値を図 4 に示した。グラフ中の Sensor-Temp はディジタルセンサ系統の計測値、Camera-Temp は温度計系統の計測値を示す。ただし、図 4(a)での計測は SW3 におけるループ処理で次の計測値の取得までに遅延を与えず、図 4(b)での計測ではより長時間の計測のため 0.5 秒の遅延を与えた。温度が変化する環境については、プチサーモスクエアの球部と TMP36 にヒーターシートを接触させることで両者に同様に熱を加えた。

温度が一定の環境において、図 4(a)から、カメラによる温度計の読み取りに対してデジタルセンサの計測値が振動している。しかし、両系統の計測値の差は 2℃以上離れておらず、安定して一致している。しかし加熱下の環境では、時間の経過とともに両系統の計測値が乖離している。これ

は、プチサーモスクエアと TMP36 で温度変化への感度が異なっていることから生じていると考えられる。

本実装でセンサの計測値への攻撃が検出できることを確認するため、以下の 2 つの攻撃を行った。

・**攻撃 1**：ディジタルセンサ S2 に対するクラス D の攻撃
・**攻撃 2**：通信路 CH3 に対するクラス D の攻撃

攻撃 1 は、IC 温度センサと A/D 変換器の間のアナログ電圧に対し、3.3V の電圧を加えた。攻撃 2 は、A/D 変換器と Raspberry Pi 間の SPI 通信における MISO の通信路に対し、3.3V の電圧を加えた。いずれにおいても正常な動作範囲を上回る過剰な電圧によって本来の通信が妨害される。攻撃 1、2 とその検出の様子を図 5 に示す。図 4(a)、(b)において、それぞれ 2 回攻撃を行った。いずれも電圧を加えたことでデジタルセンサ系統の計測値は直ちに上昇しており、両系統の計測値の不一致が同時に検出されている。また、電圧を加えるのをやめると、デジタルセンサ系統の計測値は元の値の付近へ戻り、両系統の計測値は一致していると判定されている。以上から、提案したモデルに基づく計測系において、今回想定した攻撃を検出することが可能であることが実証された。

今回の実装では、攻撃検知のアルゴリズムとして 2 つの計測値が 2℃以上離れたとき攻撃と判定する単純な方式を採用した。この方式では図 4(b)のような場合も計測値の乖離が進むと攻撃と判定されるが、測定対象のシステムによっては計測値がより複雑な振る舞いをとることも考えられる。その場合は計測値の正常な挙動に応じて適切な特徴空間と攻撃検知手法を選択する必要がある。

4.4 攻撃の誤検出と検出能力

はじめに、攻撃者の存在しない環境において実装した計測系が攻撃を誤検出しないために必要な条件を整理する。まず、4.3節で示したように温度変化の速さによって、2つの計測系統の計測値に閾値以上の差が生じるような場合がある。本実装では、このような計測器ごとの温度変化への感度の違いを補正していない。したがって、測定対象の温度変化が 2 つの計測値に閾値以上の差を与えないのに十分緩やかである必要がある。

また、プチサーモスクエアと TMP36 はそれぞれ計測可能な温度の範囲が異なる。プチサーモスクエアの計測範囲は-30℃～50℃、TMP36 の計測範囲は-40℃～125℃である。双方に共通する-30℃～50℃では正しく計測できるが、それ以外の範囲では 2 つの計測値が一致しない。したがって、測定対象の温度が 2 つの系統の両方で正しく計測できる範囲にある必要がある。

最後に、計測系の各コンポーネントおよび通信路において、計測値に影響を与えるような自然故障が発生していない必要がある。計測値の振る舞いは故障ごとの特性によって異なるが、故障によって計測値が誤った値になる、または利用できなくなる可能性がある。

ここで、測定対象および計測系についてこれらの条件が満たされているとする。このとき、この計測系は SW3 に入力される 2 つの計測値が不一致と判定される攻撃について検出することができる。逆に SW3 に入力される 2 つの計測値を一致させながら改竄する攻撃や、SW3 における不一致の判定を改竄する攻撃など、2 つの計測値が不一致と判定されない攻撃は検出することができない。実装した計測系を対象とした攻撃の例を、提案したモデルに従って攻撃対象ごとに区分したものが表 1 である。また、それぞれの攻撃の例について、3.2 節で定義した攻撃能力のクラスのうちどのクラスに属する可能性があるかを示した。表 1 では図 2 に基づいて各コンポーネントと通信路とに区分している。

表 1 : 実装した計測系への攻撃例と各攻撃の属しうるクラス

温度計		IC 温度センサ	
温度計の赤色表示を偽造	C	内部の回路を改造	C/D
赤色液を抜き取る/加える	C/D	センサ故障	C/D
温度計の位置・角度変更	C	グラウンド電圧を操作	C/D
コンポーネントの破壊・取り外し	D	参照電圧を操作	C/D
		コンポーネントの破壊・取り外し	D
温度計：カメラ		IC 温度センサ：A/D 変換器	
カメラの撮影対象を偽造	C	センサの出力電圧を操作・妨害	C/D
撮影環境の操作による撮影の妨害	D		
USB カメラ		A/D 変換器	
ファームウェア改竄で画像偽造	C/D	参照電圧を操作	C/D
解像度,FPS などの設定変更	D	グラウンド電圧を操作	C/D
その他設定変更で撮影を妨害	D	ADC の電源切断	D
コンポーネントの破壊・取り外し	D	コンポーネントの破壊・取り外し	D
USB カメラ：Raspberry Pi		A/D 変換器：Raspberry Pi	
通信路上で画像データを改竄/妨害	C/D	SPI の MISO を改竄/妨害	C/D
不正なデバイスで画像データを偽造	C/D	SPI の MOSI を改竄/妨害	C/D
		不正なデバイスでデータを偽造	C/D
SW1		SW2	
画像から温度への変換を改竄	C/D	ビット列から温度への変換を改竄	C
変換に用いる定数値を改竄	C/D	変換に使う参照電圧の定数を改竄	C
・カメラ解像度		SPI の取得ビットを変更	C
・上端温度,下端温度		SPI の通信周波数を低下させる	D
・上端座標,下端座標		SPI 通信を不正に終了	D
USB 通信を不正に終了	D	不正なキーボード入力で終了	D
不正なキーボード入力で終了	D		D
比較ソフトウェア			
異常検知の閾値を改竄	C/D		
csv への書き込みデータを操作	C/D		
・計測値			
・異常検知結果			
・タイムスタンプ			
異常検知の標準出力を改竄	C/D		
不正なキーボード入力で終了	D		

本実装で検出できる実世界での攻撃の例として、温度計の位置や角度を変更するもの、温度計の設置された環境の照明を喪失させてカメラによる読み取りを阻害するものなどがある。これらの攻撃は、温度計系統の計測値を改竄・妨害しうるが、ディジタルセンサ系統の計測値へは影響を与えない。したがって、温度計系統の計測値とディジタルセンサ系統の計測値を比較することでこれらの攻撃を検出することができる。

また、サイバー攻撃の例として、SPI 通信で受け取ったビット列を温度の計測値に変換する SW2 内のメソッドの改竄や、SPI 通信を不正に終了させるものなどがある。これらの攻撃はディジタルセンサ系統の計測値を改竄・妨害しうるが、温度計系統の計測値へは影響を与えない。したがって、温度計系統の計測値とディジタルセンサ系統の計測値を比較することでこれらの攻撃を検出することができる。

5. まとめと今後の展望

本研究では、独立したアナログ計器とディジタル化されたセンサを併用した異種冗長な計測系のモデルを提案する。モデル化によって、ディジタルセンサによる同型な冗長化に比べて上述の異種冗長化が、センサの計測値の完全性及

び可用性の保護においてどのような場合に優れるかの評価が可能となる。

また、温度を測定対象とした、アナログな温度計とディジタルセンサによる異種冗長な計測系の実装について、3.1 節で提案したモデルに基づいて攻撃の検出能力という観点からセンサの計測値の保護への寄与を論じ、モデルの有効性を確認した。この計測系では、機器の自然故障などとサイバー攻撃とを識別することは原理的にできないが、計測系統間で計測値が一致しない事象を検出することができる。

本研究で想定するアナログ計器は動作がパッシブで測定対象からの物理的入力のみに依存し、ネットワークに接続されていない性質を持つものである。よって、そのような性質を満たす任意の計器は提案したモデルにおけるアナログ計器として利用することができる。4 章における温度を例にした実装では、温度によって赤色液の液面位置が変化する温度計を用いた。他の計器の例として、回転式の指針を持つものでは、温度変化による金属の伸縮性の違いを利用する温度計、湿度変化による乾湿剤の収縮率の違いを利用する湿度計、加わる圧力による内部の機構の変位を利用する圧力計、内部を流れる電流による電磁力を利用する電流計・電圧計などがある。測定対象の電流によって点灯または消灯するような LED 電球などの光による表示も前述の性質を満たす。

また、本研究で提案した計測系のモデルはディジタルセンサ系統 1 つとアナログ計器系統 1 つによる冗長化であった。しかし、ディジタルセンサ、アナログ計器が複数存在する場合や、単一のアナログ計器に複数の読み取り装置を設ける場合などは 3 重以上の冗長化が可能となる。冗長化の数についてモデルを一般的に拡張することで、これらの場合も表現することができる。

今後の課題について述べる。今回提案したモデルが対象とする異種冗長な計測系は同型な冗長化と同様に、制御の観点から導入時に検討すべき制約が複数存在する。制御システムはそれぞれ固有のリアルタイム性・精度・安定性・設置環境といった要件を持つ。それらの性能要求を満たしながら効果的に計測値の保護を可能とする実装の選択方法を検討したい。

また、本研究では異種冗長性の実現方法と異種冗長性によるデータ保護の効果について、定性的な議論にとどまっている。そこで、システムの系統間における異種性の定量的な評価、異種冗長性によるデータ保護の定量的な評価を行う方法を検討したい。具体的には、それらを評価するためのメトリックの開発や、その妥当性の検証などが必要である。

参考文献

[1] 経済産業省商務情報政策局サイバーセキュリティ課: サイバー・フィジカ ル・セキュリティ対策フレームワーク (2019)

[2] 長谷川正美: S172026 安全制御システムにおける SIL 評価について ([S172- 02] 化学装置の安全 (2)), 年次大会 2013, 一般社団法人 日本機械学会, pp. _S172026-1 (2013).

[3] 厚生労働省労働基準局: 機械の包括的な安全基準に関する指針」の解説 等 に つ い て(2007). https://www.jaish.gr.jp/anzen/hor/hombun/ hor1-48/hor1-48-37-1-0.htm. (参照 2023/7/13).

[4] 新誠一: IoT と制御システムセキュリティの概要. CSSC 編. IoT 時代のサイバーセキュリティ 制御システムの脆弱性検知と安全性・ 堅牢性確保, エヌ・ティー・エス (2018).

[5] Corra Alegria, E. and Cruz Serra, A.: Automatic calibration of analog and digital measuring instruments using computer vision, IEEE Transactions on Instrumentation and Measurement, Vol. 49, No. 1, pp. 94–99 (2000).

[6] Zheng, C., Wang, S., Zhang, Y., Zhang, P. and Zhao, Y.: A robust and automatic recognition system of analog instruments in power system by using computer vision, Measurement: journal of the International Measurement Confederation, Vol. 92, pp. 413–420 (2016).

[7] Zuo, L., He, P., Zhang, C. and Zhang, Z.: A robust approach to reading recognition of pointer meters based on improved mask-RCNN, Neurocomputing, Vol. 388, pp. 90–101 (2020).

[8] Aizpurua Unanue, J., Muxika Olasagasti, E., Manno, G. and Chiacchio, F.: Heterogeneous Redundancy Analysis based on Component Dynamic Fault Trees (2014).

[9] Hu, H., Wu, J., Wang, Z. and Cheng, G.: Mimic defense: a designed-in cybersecurity defense framework, IET Information Security, Vol. 12, No. 3, pp. 226–237 (2018).

[10] Wang, L., Zhang, Z., Li, W., Liu, Z. and Liu, H.: An attack surface metric suitable for heterogeneous redundant system with the voting mechanism, Journal of Physics: Conference Series, Vol. 1168, No. 3, IOP Publishing, p. 032079 (2019).

[11] Nashimoto, S., Suzuki, D., Sugawara, T. and Sakiyama, K.: Sensor CON- Fusion: Defeating Kalman filter in signal injection attack, Proceedings of the 2018 on Asia Conference on Computer and Communications Security, pp.511–524 (2018).

[12] SIRC: SIRC IoT 角度センサユニット PAK02 (2019). https://sirc.co.jp/cms/wp-content/uploads/2019/09/magnetic.pdf. (参照 2023/7/14).

[13] 三木拓司, 水田健人, 三浦典之, 永田真: Physical-Cyber 境界におけるア ナログ計測セキュリティ技術, 電子情報通信学会技術研究報告; 信学技報, Vol. 118, No. 3, pp. 45–48 (2018).

[14] Huitsing, P., Chandia, R., Papa, M. and Shenoi, S.: Attack taxonomies for the Modbus protocols, International Journal of Critical Infrastructure Protection, Vol. 1, pp. 37–44 (2008).

[15] Drias, Z., Serhrouchni, A. and Vogel, O.: Taxonomy of attacks on industrial control protocols, 2015 International Conference on Protocol Engineering (ICPE) and International Conference on New Technologies of Distributed Systems (NTDS), pp. 1–6 (2015).

[16] Erhan, L., Ndubuaku, M., Di Mauro, M., Song, W., Chen, M., Fortino, G., Bagdasar, O. and Liotta, A.: Smart anomaly detection in sensor systems: A multi-perspective review, Information Fusion, Vol. 67, pp. 64–79 (2021).