安全性と制御性能のトレードオフを考慮した制御系設計*

陶山 貢市[†]・瀬部 昇[‡]

Control System Synthesis Based on Trade-off between Safety and Control Performance*

Koichi SUYAMA[†] and Noboru SEBE[‡]

This paper presents control system synthesis of providing a balance between safety and control performance according to the international standard on safety, IEC 61508. As a result, the existence of a trade-off between them is established quantitatively for the first time ever.

1. はじめに

本論文では、制御則で安全性と制御性能のバランスを定量的にとるというまったく新しい手法を国際規格に準拠した形で確立する。結果として、安全性と制御性能のトレードオフの関係をはじめて定量的に明確にする。

たとえば、「制御性能は落ちるが、ゆるやかに変化させればモータなどにかかる負担も小さく、より安全」というような安全性と制御性能のトレードオフに関する意識は様々な制御の現場などで従来から漠然と意識され、共有されている。また、安全性と制御、両分野間の関係に関しては、制御則の伝達関数行列としてのランクに関連した議論もなされている [9–11]。しかし、安全性と制御性能（目標追従誤差や耐ノイズ特性など）のトレードオフは漠然と意識されるものの、現在に至るまで定量的かつ明確には示されていない。高い制御性能だけを追求すると制御デバイス故障に対して脆弱になる数値例が与えられている程度である [14]。

一方、電気・電子・プログラマブル電子（電気技術及び/又は電子技術及び/又はプログラマブル電子技術を用いた）安全関連系に対する国際規格 IEC 61508[5]（翻訳

規格 JIS C 0508[7]）はプロセス産業、航空機、鉄道など、分野を問わずに適用され、今後産業界においてその重要性が飛躍的に高まることは確実視されている。近年、この IEC 61508 に準拠して、制御則の安全性を定量的かつ確率的に評価する枠組みが整備されつつある [15–17]。

本論文では、その安全性評価の枠組みを基礎として、制御則により安全性と制御性能のバランスを定量的にとるまったく新しい体系的手法を確立する。すなわち、制御の分野、さらにはより広くシステム理論の分野で、安全性と制御性能のトレードオフの関係をはじめて体系的かつ定量的に議論する。

制御の分野で他分野の指標とのトレードオフのバランスをとる手法としては、「エネルギー消費量」とレギュレーション性能の間の最適制御が代表的である。ただし、この「エネルギー消費量」も、状況によっては、他分野からまったく異議なく認められるとは限らない。本論文では、国際規格に準拠した形で安全性と制御性能のバランスをとる手法を提案する。

様々な分野の安全計装においては、従来、制御性能とはまったく別に、安全性は制御系の外側の安全関連系で確保するという考え方が支配的である。安全性と制御性能のバランスを制御則というロジックのレベルで定量的にとるという本論文の考え方・具体的手法は斬新である。安全性確保の点で従来の考え方・手法を補完できる可能性もあり、IEC 61508 への準拠という観点に限らず、少なからぬ影響を与えようと考えられる。

2. コントローラと制御則

一般に、コントローラは、後出の Fig.1 のように、

* 原稿受付 2007 年 8 月 29 日

[†] 東京海洋大学 海洋工学部 海事システム工学科 Department of Maritime Systems Engineering, Tokyo University of Marine Science and Technology; 2-1-6 Etchujima, Koto-ku, Tokyo 135-8533, JAPAN

[‡] 九州工業大学 情報工学部 知能情報工学科 Department of Artificial Intelligence, Kyushu Institute of Technology; 680-4 Kawazu, Iizuka, Fukuoka 820-8502, JAPAN

Key Words: safety, trade-off, control performance, control system synthesis.

- ハードウェアとしてのロジックソルバ[5,7,12]
- ソフトウェアとしての制御則

からなり、センサ・アクチュエータといった他のハードウェアを介して、制御対象を制御する。通常、制御理論ではコントローラの設計と制御則の設計とは区別されることはほとんどない。一方、安全性を議論する際には両者の区別は重要である。ロジックソルバに対してはそのランダムハードウェア故障の影響を考慮する必要がある(注意1参照)。本論文で議論の対象とするのは(センサ・アクチュエータのランダムハードウェア故障に対する)ソフトウェアとしての制御則の安全性である。通常、制御則は制御性能を考慮して決められるが、本論文ではこれに加えて上記の安全性をも考慮し、制御則により安全性と制御性能のバランスを定量的にとる手法を提案する。

3. 制御則の安全機能とその評価

3.1 条件設定

Figs. 1, 2 は IEC 61508 で考えるシステム全体とそのリスク軽減の概略を示したものである。

- EUC (Equipment Under Control): あらゆる分野の機器、設備、機械、プラントなどの制御対象
- BCS (Basic Control System): EUC を操作・制御するためのシステム

これら二つからなる制御系は初期リスク (EUC+BCS risk) をもっている。IEC 61508 は、必要が生じた場合、EUC を安全な状態に保つ、あるいは安全な状態へ移行させる電気・電子・プログラマブル電子 (Electrical/Electronic/Programmable Electronic; E/E/PE) 安全関連系 (Safety-Related Systems; SRSs) や他技術 SRSs (安全弁など)、さらには ERRFs (External Risk Reduction Facilities; 防火壁、堤防など) といった安全措置を施してリスクを軽減し、システム全体としての残存リスクを許容リスクより小さくすることを求める (Fig. 2) [15]。

BCS には Sensor 1, Sensor 2, ..., Sensor N_s と Actuator 1, Actuator 2, ..., Actuator N_a の制御デバイスが使われている。これらをあわせて Device 1, Device 2, ..., Device N ($N = N_s + N_a$) とする。

ここでは、以下の仮定1-3を設ける。

(仮定 1) Device k ($k = 1, 2, \dots, N$) には機能停止故障が故障率 λ_k の指数分布に従って独立に発生する。その修復は平均修復時間 $MTTR_k$ ¹ の指数分布に従う。□
Device k の修復率は次式で求められる。

$$\mu_k = \frac{1}{MTTR_k} \quad (k = 1, 2, \dots, N) \quad (1)$$

(仮定 2) 制御系が不安定な状態に陥ると安全措置に対してただちに作動要求が発生する。□

¹IEC 61508 では、修復率ではなく、MTTR で修復過程を定量的に扱う。

Fig. 1 Control system and safety measures

Fig. 2 Risk reduction

(仮定 3) 制御デバイス故障が原因で制御系が不安定となる頻度に比べ、それ以外の要因は無視できる。□

(注意 1) 仮定 1 において、ロジックソルバは、通常、故障率が十分小さい。まずはセンサやアクチュエータの故障を考慮した安全性評価を行い、その結果との比較において、ロジックソルバ故障の影響が無視できることを確認する、あるいは(無視できなければ)冗長化などの安全対策を講じることを想定している。□

(注意 2) 仮定 1 において、安全機能の喪失につながる危険側故障のすべてを考慮する必要があるが、どの故障モードが危険側となるかは個々の事例に依存する。できるだけ汎用性の高い安全性評価を考えるため、本論文ではもっとも基本的な機能停止(いわゆる“fail zero”)を考える。この故障モードの定式化では、デバイス故障を扱った従来の reliable control theory[13] 同様、フォールト状態にあるセンサやアクチュエータの出力はその入力と無関係になる、すなわち伝達関数が 0 であることが本質的である。すなわち、スタック故障[12]やレンジの上下限值へのトラップ[12]など、そのような定式化が可能な故障モードはすべてこの機能停止の故障モードに含めて扱う。なお、たとえば航空機の飛行制御系など、機能停止とスタックや上下限值へのトラップとの間に安全性上の大きな違いがある場合には、本論文の議論の中で外乱抑制性能を制御性能評価に組み込む、別途の安全対策を講じるなどの工夫が必要となることもある。□

(注意 3) 仮定 2 は、制御則の安全機能と制御系の外側の安全措置を、目標危険事象頻度や E/E/PE SRSs の安全度水準 (SIL) に基づいて、直接結び付けるためのものである (7.1 の冒頭部参照)。一般には、EUC が頑丈な場合、BCS がオーバーライドなどの制御の切り替え機能を安全機能として有している場合など、制御系が不安定な状態に陥ってもただちに作動要求が発生するとは限らない。しかし、それらの部分で確保される安全性 (具体的には、制御系が不安定な状態に陥ったという条件のもとで作動要求が発生する確率や頻度) を考慮に入れたうえで、本論文の議論が適用可能である。□

(注意 4) 仮定 3 において、制御系が不安定な状態に陥る原因は、外的要因など様々であり、個々の事例に依存する。ここではそのような依存性は避け、原因を制御系の内部要因である制御デバイス故障に限定する。外的要因に対しては安全措置を別途講じることも多い。□

3.2 制御則の安全機能

3.2.1 デバイスコンテキスト

Device k ($k=1,2,\dots,N$) は正常、あるいは仮定 1 によるフォールトのどちらかの状態をとり、それを

$$\delta_k = \begin{cases} 0, & \text{Device } k: \text{正常} \\ 1, & \text{Device } k: \text{フォールト} \end{cases} \quad (k=1,2,\dots,N)$$

で表す。($\delta_1, \delta_2, \dots, \delta_N$) で制御系全体のデバイスの状況を統合して表し、それをデバイスコンテキストとよぶことにする。たとえば、(1,0,0,0,...,0) は Device 1 だけがフォールトとなっているデバイスコンテキスト、(0,1,1,0,...,0) は Device 2 と Device 3 だけが同時にフォールトとなっているデバイスコンテキストを表す。なお、デバイスコンテキストの総数は 2^N 個である。

3.2.2 安全機能の実体

制御則の安全機能の実体は、すべてのデバイスが正常であるコンテキスト ((0,...,0): Normal) を除く、制御系が安定であるデバイスコンテキストの集合である [17]。たとえば、{(1,0,0,0,...,0), (0,0,1,0,...,0), (1,0,1,0,...,0)} というデバイスコンテキストの集合に対応する安全機能は、正常時に加えて、Device 1, Device 3 のうち一方あるいは両方がフォールトでも、制御系の安定性を保つ。

IEC 61508 が求めるシステム全体としてのリスク軽減の観点から見れば、この制御則の安全機能は、制御系が不安定になって E/E/PE SRSs などの安全措置全体に作動要求が発生する頻度、したがって、制御系が不安定になることに端を発する危険事象によって危害が生じるリスクを軽減する。すなわち、E/E/PE SRSs などによるリスク軽減を補完することができる [17]。

3.2.3 安全機能の表現

本論文で提案する安全性と制御性能のバランスを制御則で定量的にとる手法では、安全性評価の対象となる制御則の安全機能の集合を考える必要がある (6. 参照)。

しかし、安全機能の表現としてデバイスコンテキストの集合をそのまま書き下す場合、 $2^N - 1$ 個 (N はデバイス数) のデバイスコンテキストが入る/入らないで、 $2^{2^N - 1} - 1$ 個の安全機能が考えられるが、その中から到達可能という観点で意味のあるものだけを抜き出さなければならない。たとえば、{(1,1,0,0,...), (0,0,1,0,...)} という安全機能は、(1,1,0,0,...) が Normal から (必要であれば他の要素 (この場合は (0,0,1,0,...)) だけを経由して) 到達不可能なので、除外しなければならない。しかし、 $2^{2^N - 1} - 1$ 個という膨大な個数を考慮すれば、単純にこのような抜き出しを行うことは非実用的である。

本論文では

- (m 番目の) n 個デバイスグループ $G_{(n,m)}$
- 安全機能 $[i_1, i_2, \dots, i_N]$
- 安全機能のクラス $\langle j_1, j_2, \dots, j_N \rangle$

を導入することを提案し、安全機能の機械的な列挙を可能にする。詳細は付録 1. 参照。

3.3 制御則の安全性評価

制御系が不安定になることに端を発する危険事象によって危害が生じるリスクを軽減するため、制御則の安全機能は制御系が不安定になって E/E/PE SRSs などの安全措置全体に作動要求が発生する頻度を低減する。その作動要求頻度 (demand frequency) [5,7,12] を指標とした制御則の確率的安全性評価を行う (6.2 参照)。

危険事象頻度は作動要求頻度と E/E/PE SRSs などの安全措置の作動要求時機能失敗平均確率 (作動要求に対して安全機能の遂行に失敗する平均確率) の積で求まる [5]。作動要求頻度が低い制御則ほど、制御系単独としての安全性はより高く、その分、目標危険事象頻度を達成するのに必要な E/E/PE SRSs などの安全措置にかかる負担も小さい。すなわち、作動要求時機能失敗平均確率がそれほど小さくない (高性能でない)、より低コストの安全措置で安全目標を達成できる。

4. 制御則の制御性能評価

従来の H_∞ 制御系設計においては、制御系の性能は、与えられた一般化プラントの伝達関数行列 G 、すなわち

$$\begin{bmatrix} z \\ y \end{bmatrix} = G \begin{bmatrix} w \\ u \end{bmatrix} \quad (2)$$

(u, y は制御対象の制御入力、観測出力、 w, z は外部入力、制御出力) に対して、

$$\|T_{zw}\|_\infty = \|\mathcal{F}_l(G, K)\|_\infty \quad (3)$$

により評価される。ただし、 K は制御則の伝達関数行列を表し、 $\mathcal{F}_l$ は lower LFT を表す (Fig. 3 参照)。

なお、制御デバイス故障を考えた制御系設計の際には、故障状況に応じて一般化制御対象を修正する必要がある。その詳細は 6.3 で述べる。

Fig. 3 Control performance

本論文では H_∞ ノルムによる制御性能評価 (3) 式を考えているが、たとえば H_2 ノルムや減衰率などの他の制御性能評価に対しても本論文と同様の議論が可能である。

5. 安全性と制御性能のバランスのとり方

本論文で提案する安全性と制御性能のバランスを制御則で定量的にとる手法は以下のようなものである。

ステップ1: 安全性評価の対象となる制御則の安全機能 (3.2 参照) の集合を把握する。

ステップ2: 作動要求頻度 (DF, 3.3 参照) の目標値 DF_{tar} を設定することで、安全要求 $DF < DF_{tar}$ を考える。この安全要求を満たす安全機能は一般に複数個存在するため、その集合を把握する。

ステップ3: ステップ2の集合に属する安全機能の一つを実現する制御則の中で、すなわち安全要求を満たしたうえで、制御性能指標が最適となる制御則を求める (6.3 参照)。

その具体的なアルゴリズムは 6. で示される。

DF_{tar} を小さく (大きく) 設定すれば安全要求は高く (低く) なる。7.3 の数値例においても、高い安全要求を満たそうとすれば最終的に設計によって達成が保証される制御性能は低くならざるを得ない、逆に、満たすべき安全要求が低いほどより高い制御性能の達成が保証される、という直観的なトレードオフが明らかになるが、この DF_{tar} を可変と考えることにより、安全性と制御性能のバランスをとることが可能である。

6. 安全要求を満たして制御性能指標を最適化する制御則設計

本章では、作動要求頻度の目標値により設定される安全要求を満たしたうえで、制御性能指標が最適となる制御則を求めるアルゴリズムを与える。

6.1 ステップ1: 安全性評価の対象となる安全機能

制御デバイス数 N の情報を用いて、考えられる安全機能をクラスごとに機械的に列挙し、次のステップ2における安全性評価の対象となる安全機能の集合を求める。以下、これを安全機能の一次候補とよぶことにする。

後出の Table 2 に、 $N=6$ の場合について、列挙されるクラスごとの安全機能 (一次候補) の数を示す。機械的に列挙する様子は 7.1.1 のステップ1の例参照。

(注意 5) 一次候補の中には

$$i_1 = i_2 = \dots = i_{N_s} \geq N_s \quad (4)$$

あるいは

$$i_{N_s+1} = i_{N_s+2} = \dots = i_N \geq N_a \quad (5)$$

を満たす安全機能 $[i_1, i_2, \dots, i_N]$ も含まれる。条件 (4) 式を満たす安全機能は、すべてのセンサが同時にフォールトとなっているデバイスコンテキストにおいても制御系の安定性を求める。しかし、そのデバイスコンテキストでの制御は無意味である。アクチュエータの場合 (条件 (5) 式) とあわせて、このような安全機能はステップ3の制御則設計の段階で、制御対象が不安定な場合は、そのデバイスコンテキストでの安定化不可能性により解とはなり得ない。また、制御対象が安定な場合でも、安全機能を実現したうえでの最適化制御性能指標値の観点から、最終的な解とはまずなり得ない。以上より、この段階で条件 (4), (5) 式を満たす安全機能を一次候補から除外しても実用上問題ないと考えられる。□

6.2 ステップ2: 安全性評価

すべてのデバイスの故障率, MTTR のデータ (λ_k , $MTTR_k$ ($k=1, 2, \dots, N$))¹を用いて、ステップ1で得られた安全機能の一次候補それぞれについて、以下のアルゴリズム1により作動要求頻度 DF を求める。そして、システム全体のリスク軽減戦略に基づいて別途与えられる作動要求頻度の目標値 DF_{tar} と比較し、安全要求 $DF < DF_{tar}$ を満たす安全機能だけを最終候補とする。この最終候補の集合が次のステップ3において制御則設計の対象となる。

[アルゴリズム1]²

(i) 以下のルールにより、安全機能 $[i_1, i_2, \dots, i_N]$ に含まれるデバイスグループ $G_{(n,m)}$ ($n, m=1, 2, 3, \dots$) を求める。

- $i_{k_1} = i_{k_2} = \dots = i_{k_l} = \dots = 1$ ($k_1 < k_2 < \dots < k_l < \dots$) であれば1個デバイスグループ $G_{(1,l)} = \{\text{Device } k_l\}$ 。
- $i_{k_1} = i_{k_2} = \dots = i_{k_n} = n' = n + 1 - (1/2)^{m-1}$ であれば m 番目の n 個デバイスグループは $G_{(n,m)} = \{\text{Device } k_1, \text{Device } k_2, \dots, \text{Device } k_n\}$ 。ただし、 n は n' を超えない最大の自然数。

(ii)

$$\lambda_{total} = \sum_{k=1}^N \lambda_k \quad (6)$$

とし、各 $G_{(n,m)} = \{\text{Device } k_{n,m,1}, \text{Device } k_{n,m,2}, \dots, \text{Device } k_{n,m,n}\}$ ($n, m=1, 2, 3, \dots$) について、以下を計算する。

¹さらに (1) 式により得られる Device k の修復率 μ_k 。

²本論文で導入した安全機能の表現 (付録 1. 参照) と文献 [17] の安全性評価手法の本質的な部分を組み合わせた。

$$\lambda_{(n,m)} = \sum_{l=1}^n \lambda_{k_{n,m},l} \quad (7)$$

$$\lambda'_{(n,m)} = \lambda_{\text{total}} - \lambda_{(n,m)} \quad (8)$$

(iii) 近似のため、おのおのの $G_{(n,m)}$ ($n, m = 1, 2, 3, \dots$) 内のデバイスのフォールトは、その数によらず、修復率

$$\mu_{(n,m)} = \min_{l=1, \dots, n} \mu_{k_{n,m},l} \quad (9)$$

の指数分布に従って同時に修復されるとする。

(iv) 以下により、DF を求める。

$$\text{DF} = \frac{1}{q_0 + \sum_{n,m} q_{(n,m)}} \quad (10)$$

ただし

$$q_0 = \left[\lambda_{\text{total}} - \sum_{n,m} \frac{\lambda_{(n,m)} \mu_{(n,m)}}{\mu_{(n,m)} + \lambda'_{(n,m)}} \right]^{-1}$$

$$q_{(n,m)} = \frac{\lambda_{(n,m)}}{\mu_{(n,m)} + \lambda'_{(n,m)}} q_0 \quad (n, m = 1, 2, 3, \dots)$$

である。

(注意 6) 近似 (iii) は、デバイスグループ内で修復にもっとも時間がかかるデバイスでそのグループ内のあらゆる（同時）修復を保守的に評価する。これにより、デバイス数 N が数十、あるいはそれ以上になっても安全機能の安全性評価を (10) 式で容易に行うことができる。この近似により生じる誤差はたかだか 0.1% 程度ときわめて小さく、精度という点においては問題ない [17]。□

6.3 ステップ 3：制御則設計

(2) 式で与えられた一般化プラント G に対し、ステップ 2 で得られた安全機能の最終候補それぞれについて、その安全機能を実現したうえで、制御性能評価 (3) 式を最適化する制御則、およびそのときの最適化指標値を以下のようにロバストパフォーマンス問題へ帰着することで求める。そして、最終候補すべてにわたって最小の最適化指標値を与える安全機能、制御則を最終的な解とする。

まず、一般化プラント G から Fig. 4(a) のように新たな一般化プラント G' を作り、Fig. 4(b) のようなロバストパフォーマンス問題の枠組みを考える。制御対象と制御デバイス（センサとアクチュエータ）をあわせた部分の Normal における特性をノミナルと考える。各デバイスコンテキストは何らかのデバイス故障を含む状況であり、それによるこの部分のノミナルからの特性変化をロバスト制御における不確かさとして扱う。 Δ はデバイスコンテキストを表現する不確かさであり、その取り得る値の集合 Δ ($\ni \Delta$) は実現しようとする安全機能 $[i_1, i_2, \dots, i_N]$ に応じて次のように定まる。

$$\Delta = \left\{ \text{diag}\{\delta_1, \delta_2, \dots, \delta_N\} \mid (\delta_1, \delta_2, \dots, \delta_N) \right.$$

(a)

(b)

Fig. 4 Robust performance problem

$$\in \left(\text{Normal} \cup \left(\bigcup_{n,m} S_{(n,m)} \right) \right) \quad (11)$$

ただし、Fig. 4 で、 $\delta_k = 1$ は Device k がフォールトになっていてその伝達関数が 0 である状況を表す。また、 $S_{(n,m)}$ は、安全機能に含まれるデバイスグループ $G_{(n,m)}$ ($n, m = 1, 2, 3, \dots$)¹ に対応するデバイスコンテキストの集合である。この不確かさの集合 Δ と一般化プラント G' によって定められるロバストパフォーマンス問題を解くことで、安全機能を実現する制御則とその制御則が達成する制御性能指標値が得られる。制御性能指標値は、正常時およびその安全機能が対応するすべてのデバイスコンテキストに対して、設計された制御則が制御性能評価 (3) 式の意味で性能を達成することを保証する、その保証性能値である。

デバイスコンテキストを表現する不確かさ Δ は対角行列であり、構造化特異値 [2] の枠組みでロバストパフォーマンス問題として形式的には定式化できる。しかし、通常の構造化特異値の枠組みでは、故障を想定したデバイスすべてが故障する場合も（つまり不要なデバイスコンテキストも）集合に含めるような不確かさのモデリングしかできないため、結果として非常に保守的な制御則設計しかできない。これに対して文献 [9, 11] では、離散的な不確かさをすべて含む不確かさの集合のモデル化と H_∞ 制御性能を満たす制御則設計を同時に行う文献 [1] の方法を用い、デバイスコンテキストの集合 Δ に対して性能を考慮した制御則設計ができることを示している。

なお、出力フィードバックの場合、解くべきロバストパフォーマンス問題は双線形行列不等式として定式化されるため、大域的最適解を求めるのは一般に困難である。これに対して、文献 [1, 6] の提案している双対反復 (dual

¹ アルゴリズム 1 の (i) により求められる。

iteration) とよばれる方法を適用することで、最適性の保証はないものの、保守性の少ない制御則設計が行える。

7. 数値例

7.1 基本的設計

本節では、前章のアルゴリズムの数値例を与える。次の一般化プラントを考える。

$$\begin{bmatrix} z \\ y \end{bmatrix} = \begin{bmatrix} -2 & 1 & 1 & 1 & | & 1 & 0 & 0 & 0 \\ 3 & 0 & 0 & 2 & | & 0 & 1 & 0 & 0 \\ -1 & 0 & -2 & -3 & | & 1 & 0 & 0 & 1 \\ -2 & -1 & 2 & -1 & | & 0 & 0 & 1 & 0 \\ \hline 1 & 2 & -1 & 0 & | & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & | & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & | & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 2 & | & 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} w \\ u \end{bmatrix} \quad (12)$$

$\begin{bmatrix} A & B \\ C & D \end{bmatrix}$ は伝達関数行列 $C(sI - A)^{-1}B + D$ を表す ((13) 式も同様)。制御対象は 3 出力 3 入力 ($N_s = 3, N_a = 3$) で、したがって $N = 6$ である。各デバイスの故障率と MTTR を Table 1 に示す。

Table 1 Failure rate and MTTR

Device	Failure rate [/h]	MTTR [h]
Device 1	4×10^{-5}	200
Device 2	9×10^{-6}	1000
Device 3	2×10^{-5}	500
Device 4	3×10^{-5}	200
Device 5	6×10^{-6}	1000
Device 6	9×10^{-6}	1000

安全要求は $DF_{tar} = 1.1416 \times 10^{-5}$ [/h] とする。これは、目標危険事象頻度 10^{-3} [/yr] (1000 年に 1 回) が低頻度作動要求モードの SIL2 の E/E/PE SRS だけで達成可能であるための作動要求頻度の許容最大値である [15]。

制御則 K の制御性能評価は、この一般化プラント (12) に基づいて、(3) 式に従って行う。

7.1.1 ステップ 1

$N = 6$ なので、Table A1 より安全機能のクラスは 11 個。さらにおおのこのクラスに属する安全機能の数は (A3) 式で求められ、Table 2 にその数を示す。

たとえば、 $n(\geq 2)$ 個デバイスグループを含まないクラス $<1, 0, 0, 0, 0, 0>$ には、 $[1, 0, 0, 0, 0, 0]$, $[0, 1, 0, 0, 0, 0]$, $[1, 1, 0, 0, 0, 0]$ など、二進数を利用して機械的に列挙される 63 個の安全機能が含まれる。また、 $n(\geq 2)$ 個デバイスグループとして 4 個グループを一つだけ含むクラス $<1, 0, 0, 1, 0, 0>$ には、

$[4, 4, 4, 4, 0, 0]$, $[4, 4, 4, 4, 1, 0]$, $[4, 4, 4, 4, 0, 1]$, $[4, 4, 4, 4, 1, 1]$,
 $[4, 4, 4, 0, 4, 0]$, $[4, 4, 4, 1, 4, 0]$, $[4, 4, 4, 0, 4, 1]$, $[4, 4, 4, 1, 4, 1]$,

$[4, 4, 4, 0, 0, 4]$, $[4, 4, 4, 1, 0, 4]$, $[4, 4, 4, 0, 1, 4]$, $[4, 4, 4, 1, 1, 4]$ など、 $i_1, \dots, i_6$ から 4 個の '4' を選ぶことを通じて機械的に列挙される 60 個の安全機能が含まれる。

11 個のクラスすべてでは合計 876 個の安全機能があり、これらが一次候補となる。

なお、たとえば、安全機能 $[4, 4, 4, 4, 1, 0]$ の実体は安定性が確保される 16 個のデバイスコンテキストの集合、 $\{(1, 0, 0, 0, 0, 0), (0, 1, 0, 0, 0, 0), (0, 0, 1, 0, 0, 0), (0, 0, 0, 1, 0, 0), (1, 1, 0, 0, 0, 0), (1, 0, 1, 0, 0, 0), (1, 0, 0, 1, 0, 0), (0, 1, 1, 0, 0, 0), (0, 1, 0, 1, 0, 0), (0, 0, 1, 1, 0, 0), (1, 1, 1, 0, 0, 0), (1, 1, 0, 1, 0, 0), (1, 0, 1, 1, 0, 0), (0, 1, 1, 1, 0, 0), (1, 1, 1, 1, 0, 0), (0, 0, 0, 0, 1, 0)\}$ である。このようなデバイスコンテキストの集合をそのまま安全機能の表現とすれば、データ構造・容量の点で実用上望ましくないばかりではなく、安全機能の間の比較や到達可能性という観点で意味のある安全機能の列挙に困難が生じる (3.2.3 参照)。本論文で安全機能の表現 (付録 1. 参照) を導入し、その表現のうえで上述した二進数や 4 個の '4' を選ぶことなどを通じて、比較や機械的列挙が容易になったことの意味は大きい。

7.1.2 ステップ 2

Table 3 参照。一次候補 876 個の安全機能それぞれについて 6.2 の方法により安全性評価を行った結果、265 個の安全機能が安全要求 ($DF < DF_{tar}$) を満たす最終候補となった。

7.1.3 ステップ 3

ステップ 2 で得られた 265 個の安全機能の最終候補それぞれについて、その安全機能を満たしたうえで制御性能指標を最適化する制御則設計を行った。スペースの都合上、最適化制御性能指標値が 1.7 未満となる 13 個の安全機能だけを Table 3 に示す。中でも指標値が最小 (1.5558) となる安全機能 $[1, 1, 1, 1, 0, 1]$ およびそれらを達成する以下の制御則が求める解である。

$$K = \begin{bmatrix} -69.05 & -287.3 & -251.8 & 1.369 \times 10^5 \\ 2.11 & -9.476 & -5.485 & 2730 \\ -6.041 & -36.74 & -33.57 & 1.641 \times 10^4 \\ 436.8 & -1673 & 2490 & -3.656 \times 10^6 \\ \hline 0.5733 & -1.437 & -0.3474 & -928.5 \\ 74.58 & 313 & 275 & -1.499 \times 10^5 \\ \hline 0.1285 & -0.7374 & -0.9788 & -502.9 \\ \hline 34.04 & 30.11 & 2.647 \\ 1.708 & 1.635 & -0.1548 \\ 4.269 & 4.046 & 0.3535 \\ 3860 & 3435 & -169.9 \\ \hline 0.4981 & 0.5697 & 0.08769 \\ -36.88 & -33.02 & -2.942 \\ -0.6163 & 0.4417 & -0.07587 \end{bmatrix} \quad (13)$$

なお、本章で扱った制御対象は不安定 (極は $-1.3160 \pm 2.9194j$, -2.2559 , 0.1906) である。すべてのセンサあ

Table 2 Initial candidates of safety function obtained in Step 1

Class	Corresponding partition	Number of initial candidates
$\langle 1,0,0,0,0,0 \rangle$	$1+1+1+1+1+1$	63
$\langle 1,1,0,0,0,0 \rangle$	$2+1+1+1+1$	240
$\langle 1,2,0,0,0,0 \rangle$	$2+2+1+1$	180
$\langle 0,3,0,0,0,0 \rangle$	$2+2+2$	15
$\langle 1,0,1,0,0,0 \rangle$	$3+1+1+1$	160
$\langle 1,1,1,0,0,0 \rangle$	$3+2+1$	120
$\langle 0,0,2,0,0,0 \rangle$	$3+3$	10
$\langle 1,0,0,1,0,0 \rangle$	$4+1+1$	60
$\langle 0,1,0,1,0,0 \rangle$	$4+2$	15
$\langle 1,0,0,0,1,0 \rangle$	$5+1$	12
$\langle 0,0,0,0,0,1 \rangle$	6	1
Total		876

Table 3 Final candidates of safety function obtained in Step 2 and achieved performances in Step 3

Class	Number of final candidates	Safety function with performance index < 1.7		
		Safety function	DF [/h]	Performance index
$\langle 1,0,0,0,0,0 \rangle$	2	$[1,1,1,1,0,1]$	9.318×10^{-6}	1.5558
$\langle 1,1,0,0,0,0 \rangle$	25	$[2,1,2,1,0,1]$	9.305×10^{-6}	1.5599
		$[2,1,1,1,0,2]$	1.051×10^{-5}	1.5635
		$[1,2,2,1,0,1]$	9.733×10^{-6}	1.5648
		$[1,2,1,1,0,2]$	9.188×10^{-6}	1.6775
		$[1,1,2,2,0,2]$	9.390×10^{-6}	1.5647
		$[1,1,2,1,0,2]$	9.733×10^{-6}	1.5619
$\langle 1,2,0,0,0,0 \rangle$	58	$[2,2^{1/2},2,1,0,2^{1/2}]$	9.177×10^{-6}	1.6782
		$[2,2^{1/2},2^{1/2},1,0,2]$	1.090×10^{-5}	1.5736
		$[2,1,2^{1/2},2^{1/2},0,2]$	1.057×10^{-5}	1.5732
		$[1,2,2^{1/2},2^{1/2},0,2]$	9.261×10^{-6}	1.6802
$\langle 0,3,0,0,0,0 \rangle$	15	—		
$\langle 1,0,1,0,0,0 \rangle$	32	$[3,1,3,1,0,3]$	9.557×10^{-6}	1.5738
		$[1,3,3,1,0,3]$	9.306×10^{-6}	1.6924
$\langle 1,1,1,0,0,0 \rangle$	72	—		
$\langle 0,0,2,0,0,0 \rangle$	10	—		
$\langle 1,0,0,1,0,0 \rangle$	26	—		
$\langle 0,1,0,1,0,0 \rangle$	15	—		
$\langle 1,0,0,0,1,0 \rangle$	9	—		
$\langle 0,0,0,0,0,1 \rangle$	1	—		
Total	265			

るいはアクチュエータが同時にフォールトとなっているデバイスコンテキストでの安定化は不可能であり、注意 5 で指摘した安全機能を実現する制御則は存在しない。そのため、たとえそれが安全要求を満たしていたとしても、最終的な解とはなり得ない。

(注意 7) $\langle 1, 0, 0, 0, 0 \rangle$ (2 個以上のデバイスグループがない), $\langle 1, 1, 0, 0, 0 \rangle$ (2 個デバイスグループが 1 個のみ), $\langle 1, 2, 0, 0, 0 \rangle$ (2 個デバイスグループが 2 個のみ) などのクラスに属する安全機能は対応するデバイスコンテキストの数も少なく、一般に安全要求を満たしにくい。反面、制御則設計に際しての制約条件がゆるいので、最適化制御性能指標値はより小さくなる。このことは Table 3 から読み取ることができるが、 $\langle 1, 0, 0, \dots, 0 \rangle$ や $\langle 1, 1, 0, \dots, 0 \rangle$ などのクラスで安全要求を満たす安全機能があればそれらが最終的な解になりやすいという実用上重要な指針を与えている。□

7.2 制御則以外の制御系内部の安全機能

本節では、注意 3 で述べた、ECU の頑丈さや BCS のオーバーライドなど、制御則以外の制御系内部の安全機能を 6. のアルゴリズムの中で考慮に入れる例を与える。

たとえば、その部分が低頻度作動要求モードの SIL1 のリスク軽減を行っている場合、実際に作動要求が発生する回数は、制御系が不安定な状態に陥った回数の 1/10 未満 1/100 以上となる。7.1 同様に目標危険事象頻度 $10^{-3}[\text{yr}]$ (1000 年に 1 回) が低頻度作動要求モードでの SIL2 の E/E/PE SRS だけで達成可能であるためには、その部分によるリスク軽減の下限值 (1/10) を考慮して、安全要求を 7.1 での $DF_{\text{tar}} = 1.1416 \times 10^{-5}[\text{h}]$ から $DF_{\text{tar}} = 1.1416 \times 10^{-5}[\text{h}] \times 10 = 1.1416 \times 10^{-4}[\text{h}]$ に変更する。以下、この DF_{tar} の値を用いて、前章で与えたアルゴリズムを適用すればよい。

7.3 安全性と制御性能のトレードオフとそれらのバランスをとる手法

一般化プラント (12) に関して、安全要求を設定する作動要求頻度の目標値 DF_{tar} と、それを満たしたうえで 6. のアルゴリズムにより求められる、制御性能指標の最適値 (最終的に設計によって達成が保証される制御性能) の関係を、Fig. 5 に示す。

7.1 で示したように、安全要求を $DF_{\text{tar}} = 1.1416 \times 10^{-5}[\text{h}]$ にとると、達成可能な制御性能指標の最適値は 1.5558 であった。たとえば、2 倍の $DF_{\text{tar}} = 2.2832 \times 10^{-5}[\text{h}]$, 5 倍の $DF_{\text{tar}} = 5.7080 \times 10^{-5}[\text{h}]$ と、 DF_{tar} をより大きく設定して満たすべき安全要求を低くしていくと、達成可能な制御性能指標の最適値は 0.6599, 0.0409 となり、より高い制御性能が保証されることがわかる。逆に、1/2 倍の $DF_{\text{tar}} = 5.7080 \times 10^{-6}[\text{h}]$ と、 DF_{tar} をより小さく設定して安全要求を高くすれば、達成可能な制御性能指標の最適値は 2.0998 となり、最終的に保証される制御性能は低くならざるを得ないことが

わかる。

Fig. 5 はこのようなきわめて直観的な安全性と制御性能のトレードオフの関係を示している。制御の分野でその存在をはじめて定量的に明確に示す例である。

このトレードオフを背景として、 DF_{tar} を可変と考えることにより、安全性と制御性能のバランスを制御則で定量的にとることが可能である。すなわち、 DF_{tar} を小さく (大きく) 設定すれば、安全要求は高く (低く) なり、最終的に保証される制御性能は低くなる (高くなる)。安全性 (制御性能) をより重視する際には DF_{tar} をより小さく (大きく) することによって、安全性と制御性能のバランスを調節することができる。

Fig. 5 Trade-off between safety and control performance

8. おわりに

国際規格 IEC 61508 に準拠して安全性と制御性能のバランスを制御則で定量的にとる手法を提案した。また、安全性と制御性能のトレードオフの関係をはじめて定量的に明確にすることができた。ステップ 3 におけるより保守性の少ない制御則設計、さらには安全性と (正常時および各安全機能が対応するすべてのデバイスコンテキストに対する保証性能でなく) 正常時の制御性能のトレードオフに関する考察は今後の重要な課題である。

安全性は、品質、環境に続く、国際規格に基づく認証の「第 3 の波」であり、産業界の将来を大きく左右するといわれている。制御理論が境界領域に新たな分野の確立を目指すパートナーとしては、現状、安全性はもっとも期待できるものの一つであろう。本論文がそのような方向性を明確にする第一歩となれば望外の喜びである。

謝 辞

本研究の一部は科学研究費補助金基盤研究 (C) (課題番号 19560438) の補助を受けた。記して謝意を表する。

参考文献

付 録

- [1] T. Asai, S. Hara and T. Iwasaki: Simultaneous parametric uncertainty modeling and robust control synthesis by LFT-scaling; *Automatica*, Vol. 36, pp. 1457–1467 (2000)
- [2] J. C. Doyle: Analysis of feedback system with structured uncertainties; *IEEE Proceedings*, Vol. 129-D, No. 6, pp. 242–250 (1982)
- [3] 濱田, 新, 瀬部: 耐故障性を有する多変数制御系の一設計法 —*l*-部分インテグリティ条件—; 計測自動制御学会論文集, Vol. 34, No. 9, pp. 1184–1190 (1998)
- [4] IEC 61165: Application of Markov techniques (2006)
- [5] IEC 61508: Functional safety of electrical/electronic/programmable electronic safety-related systems (1998–2000)
- [6] T. Iwasaki: The dual iteration for fixed-order control; *IEEE Transactions on Automatic Control*, Vol. 44, No. 4, pp. 783–788 (1999)
- [7] JIS C 0508: 電気・電子・プログラマブル電子安全関連系の機能安全 (1999–2000)
- [8] 日本数学会編, 数学辞典, 岩波書店 (1985)
- [9] N. Sebe: A study on the structure of reliable controllers; *Proceeding of the 16th International Symposium on Mathematical Theory of Networks and Systems*, 6 pages (2004)
- [10] N. Sebe: Rank deficiency of reliable controllers; *Proc. 10th IFAC/IFORS/IMACS/IFIP Symposium on Large Scale Systems: Theory and Applications*, pp. 542–547 (2004)
- [11] N. Sebe and A. Mochimaru: Structure of reliable controllers; *Systems and Human Science —For Safety, Security, and Dependability—* (T. Arai, S. Yamamoto and K. Makino, eds.), Elsevier, pp. 187–200 (2005)
- [12] 関口, 佐藤 (監修), 日本機械工業連合会, 日本電気計測器工業会編: 「機械安全 (電気装置)/機能安全」実用マニュアル, 日刊工業新聞社 (2001)
- [13] K. Suyama: Systematization of reliable control; *Proceedings of the 2002 American Control Conference*, pp. 5110–5118 (2002)
- [14] K. Suyama: Safety integrity analysis framework for a controller according to IEC 61508; *Proceedings of the 42nd IEEE Conference on Decision and Control*, pp. 2477–2483 (2003)
- [15] 陶山: 制御則の確率的安全性評価・管理 I — 機能安全に関する国際規格 IEC 61508 とその制御との接点; システム/制御/情報, Vol. 50, No. 2, pp. 55–61 (2006)
- [16] 陶山: 制御則の確率的安全性評価・管理 II — 国際規格 IEC 61508 を媒介にした制御と安全性のコラボレーション; システム/制御/情報, Vol. 50, No. 5, pp. 175–180 (2006)
- [17] 陶山: 国際規格 IEC 61508 に基づく制御則の確率的安全性評価; 電子情報通信学会論文誌, Vol. J89-A, No. 6, pp. 523–534 (2006)

付録 1. 安全機能の表現

付録 1.1 デバイスグループ

制御則の安全機能を表現するうえで、以下のような、個々の安全機能の中における制御デバイスのグループ (デバイスグループ) を考える。本論文で提案する安全性と制御性能のバランスを制御則で定量的にとる手法においては、安全性評価の対象となる安全機能の集合を考える必要があるが、デバイスグループの導入により、仮定 4 による制約はあるものの、到達可能性という観点で意味のある安全機能の列挙を困難なく行える。それは、個々のデバイスグループに対応するデバイスコンテキストの集合 (後述の $S_{(n,m)}$) は Normal から到達可能なものだけからなる、安全機能のクラスが利用できる (付録 1.3 参照), などの理由による。

n 個のデバイスからなるグループ (以下, n 個デバイスグループ) がいくつかある中で m 番目のもの $G_{(n,m)} = \{\text{Device } k_{n,m,1}, \text{Device } k_{n,m,2}, \dots, \text{Device } k_{n,m,n}\}$ を考えよう。 $G_{(n,m)}$ に属する n 個のデバイスの正常/フォールトのあらゆる組合せにより作られる $2^n - 1$ 個のデバイスコンテキスト (Normal は除く) をまとめて $S_{(n,m)}$ と書く。たとえば, 2 個デバイスグループの中で 1 番目のグループ $G_{(2,1)} = \{\text{Device } 1, \text{Device } 2\}$ に対して, $S_{(2,1)} = \{(1,0,0,\dots), (0,1,0,\dots), (1,1,0,\dots)\}$ である。

グループの集合

$$\begin{aligned} & \{G_{(n,m)} \mid (n,m=1,2,3,\dots) \mid G_{(n_1,m_1)} \cap G_{(n_2,m_2)} \\ & = \phi \mid ((n_1,m_1) \neq (n_2,m_2))\} \end{aligned} \quad (\text{A1})$$

は N 個のデバイスの一部あるいは全部をグループに分けることに相当する。どのグループにも属さないデバイスは、考えている安全機能にはその故障対策が含まれていないものであり、その集合を次のように定義する。

$$G_{\text{rest}} = \{\text{Device } 1, \text{Device } 2, \dots, \text{Device } N\} \setminus \bigcup_{n,m} G_{(n,m)} \quad (\text{A2})$$

(仮定 4) (A1) のようなグループ分けから $\bigcup_{n,m} S_{(n,m)}$ で表現される安全機能だけを考える。 □

たとえば, $\{(1,0,0,0,\dots,0), (0,1,1,0,\dots,0)\}$ というような安全機能は考えない。

(注意 8) *l*-部分インテグリティ [3] で扱われているものも含めて, 仮定 4 の範囲を超えたより一般的な安全機能の安全性評価に際しては, 対応するデバイスコンテキストの数程度の状態を有する状態遷移図およびそれに基づく微分方程式を作成する必要がある [4]。しかし, 制御デバイス数が数十以上になるとそれらはきわめて大規模になり, 評価結果を得るにあたって非常に困難を伴う。制御則の安全性評価としては実用的ではなくなる可

能性がある．また，(そのようなより一般的な安全機能まで議論の対象を広げず) 仮定 4 の範囲，すなわちデバイスグループの組合せ (正確には $\bigcup_{n,m} S_{(n,m)}$) で表現される安全機能は，6.2 のように文献 [17] の安全性評価の枠組みをそのまま適用して，きわめて容易にその安全性を評価することができる一方，最終的に設計によって達成が保証される安全性や制御性能の観点からも十分である． □

付録 1.2 安全機能の表現

安全機能を表現するにあたって，デバイスコンテキストの集合をそのまま書き下すと，安全機能の内容によりその要素の個数は異なるので，データ長も異なり，実用上扱いづらい．そこで，本論文では，付録 1.1 で導入したデバイスグループを用いて，その安全機能の中で各デバイスが何番目の何個グループに属するかに注目して，安全機能を $[i_1, i_2, \dots, i_N]$ のように固定化されたデータ構造・データ長の中で表現する．ただし

$$i_k = \begin{cases} 1, & \text{Device } k \\ & \in 1 \text{ 個デバイスグループ} \\ n+1 - \left(\frac{1}{2}\right)^{m-1}, & \text{Device } k \in m \text{ 番目の} \\ & n(\geq 2) \text{ 個デバイスグループ} \\ 0, & \text{Device } k \in G_{\text{rest}} \end{cases}$$

2 以上の同じ値をもつデバイスは同じグループに属することに注意． $n(\geq 2)$ 個デバイスグループは順に $n, n^{1/2}, n^{3/4}, n^{7/8}, \dots$ と $[n, n+1)$ の数値で表されるが，各 n 個デバイスグループの中に含まれるもっとも番号の小さいデバイスに注目し，Device 1, Device 2, ..., Device N の順序の中でそれらが現れる順番をそのグループの n 個デバイスグループ群の中での順番 m とする．すなわち， i_k の値から n と m が一意に定まる．

付録 1.3 安全機能のクラス

安全機能を列挙するために安全機能のクラス $\langle j_1, j_2, \dots, j_N \rangle$ を導入する． j_n ($n=2, 3, \dots$) は n 個デバイスグループの個数， $j_1 (=0/1)$ は 1 個デバイスグループ，あるいはどのグループにも属さないデバイスの有 (1)/無 (0) である．最大でも N 個デバイスグループまでしか存在しないことに注意．

安全機能のクラスは整数 N の分割に対応しており，したがってクラスは分割数 [8] だけ存在する (Table A1 参照)．これは N 個のデバイスをいくつかのグループに分けるという，付録 1.2 で示した安全機能の表現上の考え方から明らかである．Table 2 は， $N=6$ の場合について，安全機能のクラス，対応する整数 N の分割などを示したものであるが，これを見ても両者の具体的な関係は明らかであろう．

また，クラス $\langle 1, 0, \dots, 0 \rangle$ には $2^N - 1$ 個，それ以外のクラス $\langle j_1, j_2, \dots, j_N \rangle$ には

Table A1 Number of partitions

N	Number of partitions
2	2
3	3
4	5
5	7
6	11
7	15
8	22
9	30
10	41
11	56
12	77

$$M = \prod_{l=0}^{N-1} T_{N-l} \quad (\text{A3})$$

個の安全機能が含まれる．ただし，

$$R_n = \begin{cases} N - \sum_{l=n+1}^N l \cdot j_l & (n=1, 2, \dots, N-1) \\ N & (n=N) \end{cases}$$

$$T_n = \begin{cases} 2^{R_1} & (n=1) \\ \frac{1}{j_n!} \prod_{l=1}^{j_n} R_{n-(l-1)n} C_n & (n \geq 2, j_n \geq 1) \\ 1 & (n \geq 2, j_n = 0) \end{cases}$$

である．

この安全機能のクラス $\langle j_1, j_2, \dots, j_N \rangle$ は，整数 N の分割との関係や各クラスに属する安全機能の数 ((A3) 式など) を参考に，安全機能を列挙するためだけに使われる (6.1 参照)．

(注意 9) j_1 は他の $j_2, \dots, j_N$ とは異なる意味をもつが，安全機能のクラスの特定には必要ない．それは，安全機能のクラスと整数 N の分割を，Table 2 のように，分かりやすく結び付けるためのものである． □

付録 1.4 例

たとえば， $[0, 2, 2^{1/2}, 2^{1/2}, 1, 2]$ で表される安全機能は，以下の (三つのデバイスグループで記述される) 計 7 個のデバイスコンテキストで制御系の安定性を保つ．

- 1 個デバイスグループ $G_{(1,1)} = \{\text{Device 5}\}$ に対応するデバイスコンテキスト $S_{(1,1)} = \{(0, 0, 0, 0, 1, 0)\}$
- 1 番目の 2 個デバイスグループ $G_{(2,1)} = \{\text{Device 2, Device 6}\}$ に対応するデバイスコンテキスト $S_{(2,1)} = \{(0, 1, 0, 0, 0, 0), (0, 0, 0, 0, 0, 1), (0, 1, 0, 0, 0, 1)\}$
- 2 番目の 2 個デバイスグループ $G_{(2,2)} = \{\text{Device 3, Device 4}\}$ に対応するデバイスコンテキスト $S_{(2,2)} = \{(0, 0, 1, 0, 0, 0), (0, 0, 0, 1, 0, 0), (0, 0, 1, 1, 0, 0)\}$

そして，2 個デバイスグループが二つと 1 個デバイスグループ，あるいはどのグループにも属さないデバイスがあるので，クラス $\langle 1, 2, 0, 0, 0, 0 \rangle$ に属する．