社団法人　電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
TECHNICAL REPORT OF IEICE.

離散事象システムにおけるオートメーションサプライズに対する警報器の設計

梁瀬　裕行[1†]　　潮　　俊光[†]　　足立　正和[†]　　宇川　佳孝[†]

† 大阪大学大学院基礎工学研究科
〒 560–8531 豊中市待兼山町 1–3
E-mail: [1]yanase@hopf.sys.es.osaka-u.ac.jp

あらまし　人間-機械システムでは，ユーザはインタフェースを介することでマシンの部分的な情報を得てマシンを操作する．したがって，不適切なインタフェースでは，ユーザはマシンの状態を正しく追従することができず，オートメーションサプライズと呼ばれる現象が発生することがある．オートメーションサプライズの発生を避けるための，人間-機械システムの形式的な検証方法や設計方法が提案されている．そこで本論文では，離散事象システムを対象にオートメーションサプライズが発生しそうなときに警報を鳴らすシステムを状態フィードバック制御を用いて構成する．これにより，インタフェースの再設計が不要となり，かつオートメーションサプライズが存在しないような人間-機械系の構成が可能となる．

キーワード　人間-機械システム, オートメーションサプライズ, 合成モデル, 状態フィードバック制御

Design of Alarm for Automation Surprises Avoidance in Discrete Event Systems

Yuki YANASE[1†], Toshimitsu USHIO[†], Masakazu ADACHI[†], and Yoshitaka UKAWA[†]

† Graduate School of Engineering Science, Osaka University
Machikaneyama 1–3, Toyonaka-shi, 560–8531 Japan
E-mail: [1]yanase@hopf.sys.es.osaka-u.ac.jp

Abstract　In human-machine systems, a user operates a machine with machine's partial information through an interface. Therefore, due to the inadequate interface, the user can not follow correct states of the machine, and phenomena called automation surprises may arise. To avoid automation surprises, formal approach for verifying and designing a human-machine system have been proposed. In this paper, we propose a system which alarms to the user before automation surprises occur. The proposed system is based on the state feedback control of discrete event systems. By adding the system to the existing human-machine systems, redesigning of the user-interface is not needed and nonexistence of automation surprises is assured.

Key words　human-machine systems, automation surprises, composite model, state feedback control

1. ま え が き

人間-機械システムはマシン，インタフェース，ユーザモデルの合成によって表現できる [8]．また，マシンの操作方法はマニュアルによってユーザに提示される．ユーザは，インタフェースの表示を見ながらマニュアルに基づいて操作する．大規模なシステムにおいては，全てのセンサ情報をインタフェースで表示することはかえってユーザの操作を困難にし，ヒューマンエラーを引き起こす原因になることがある．また，マニュアルが不完全であったり，インタフェースが情報を抽象化しすぎると，適切な操作をするために十分な情報をインタフェース自身が提示できなくなる．このとき，実際のシステムの振る舞いとユーザが意図した振る舞いとの間に誤認識が生じ，ユーザはシステムから予期せぬ応答を受け取ることがある．このような望ましくない状況をオートメーションサプライズ [1] と呼び，ヒューマンエラーを引き起こす原因として最近注目されている．これまでにも実システムにおけるオートメーションサプライズが原因でヒューマンエラーが発生し，その結果重大な事故につながった例が報告されている [2]．

オートメーションサプライズを避けるために，与えられたイ

ンタフェース，ユーザモデルで正しくシステムを操作できるかどうかを検証する必要があるが，近年この問題に対して工学的な観点から様々なアプローチがなされている [3], [4], [5].

しかし，既に設計されたインタフェースを作り変えるには多大な時間とコストを必要とし，インタフェースの再設計に伴いユーザに与えられるマニュアルや資料も再構成しなくてはいけないことを考えると必ずしも有益であるとは言えない.

本論文では，ユーザと相互に作用するマシンとユーザの振る舞いは離散事象システムで表現されるものとする．オートメーションサプライズは先にも述べたようにマシンの振る舞いとユーザの意図との間の一貫性がなくなったときに生じるため，マシンとユーザモデルの状態の対として人間-機械システムの状態は定義することができる．このような場合，制御仕様はオートメーションサプライズを持たないという状態上の述語として与えることができるため，状態フィードバック制御 [9] を応用することができる.

そこで，インタフェースとユーザモデルが適切でないときに，インタフェースを再設計せずに，オートメーションサプライズを生じる状態に至るようなイベントを禁止する機構を付加する（警報を鳴らす）ことを考える．このような機構を付加することは，インタフェースの再設計を不要とし，ユーザに与える情報もそのまま利用できるので有効であるといえる.

2. 状態フィードバック制御

本章では，離散事象システムの状態フィードバック制御 [9] について述べる．対象システム G がオートマトンでモデル化されているとする.

$$G = (X,\ \Sigma,\ \delta,\ x_0)$$

ただし，X は状態集合，Σ は事象集合，$\delta : X \times \Sigma \to X$ は状態遷移関数，x_0 は初期状態である.

生起を禁止する事象の集合を制御パターンといい，これを Γ とすると

$$\Gamma = \{\gamma\ ;\ \gamma \subseteqq \Sigma^c\}$$

である．G の各状態 $x \in X$ において制御パターン $\gamma \in \Gamma$ を決定する規則は，X から Γ への写像 $f \in \Gamma^X$ として表わされる．ここで Γ^X は X から Γ への写像の集合を表わす．$x \in X$ において，$\sigma \in f(x)$ なる事象 $\sigma \in \Sigma^c$ はその生起が禁止される．そして，$\sigma \notin f(x)$ を満たすとき，事象 σ は f によって生起が許容される.

状態フィードバック f を施した閉ループシステムを $G|f$ とすると，以下のようになる.

$$G|f = (X,\ \Sigma,\ \delta^f,\ x_0)$$

ただし，遷移関数 $\delta^f : X \times \Sigma \to X$ は次式で定義される.

$$\delta^f(x,\sigma) = \begin{cases} \delta(x,\sigma) & \text{if} \quad \sigma \notin f(x) \\ \text{undefined} & \text{otherwise} \end{cases}$$

制御仕様は状態の集合上の述語 Q で与えられているとする．さらに，X 上の述語の集合を $\mathcal{Q}$ とおく．状態 $x \in X$ において，述語 $Q \in \mathcal{Q}$ が真であるとき $Q(x) = 1$, 偽であるとき $Q(x) = 0$ と定義する.

$\mathcal{Q}$ 上の演算である $\sim$ (否定)，$\wedge$ (交わり)，$\vee$ (結び) をそれぞれ次のように定義する.
任意の $x \in X$ に対して，

$$\sim Q_1(x) = 1 \Longleftrightarrow Q_1(x) = 0$$

$$(Q_1(x) \wedge Q_2(x)) = 1 \Longleftrightarrow Q_1(x) = 1 \text{ and } Q_2(x) = 1$$

$$Q_1(x) \vee Q_2(x) = \sim ((\sim Q_1) \wedge (\sim Q_2))$$

次に $\mathcal{Q}$ 上の半順序関係 $\leqq$ を次のように定義する.

$$Q_1 \leqq Q_2 \Longleftrightarrow Q_1 \wedge Q_2 = Q_1$$

各 $\sigma \in \Sigma$ に対して，述語 D_σ を次のように定義する.

$$D_\sigma(x) = \begin{cases} 1 & \text{if} \quad \delta(x,\sigma)! \\ 0 & \text{otherwise} \end{cases}$$

各 $\sigma \in \Sigma$ に対して，$\mathcal{Q}$ 上の変換 wp_σ と wlp_σ を次のように定義する.

$$wp_\sigma(Q)(x) =$$

$$\begin{cases} 1 & \text{if} \quad \delta(x,\sigma)! \text{ and } Q(\delta(x,\sigma)) = 1 \\ 0 & \text{otherwise} \end{cases}$$

$$wlp_\sigma(Q) = wp_\sigma(Q) \vee \sim D_\sigma$$

ただし，$\sigma \in \Sigma$ と $x \in X$ に対して $\delta(x,\sigma)$ が定義されるとき $\delta(x,\sigma)!$ と書くとする．また，定義されないとき $\neg\delta(x,\sigma)!$ と書くとする.

事象 σ の生起により，状態 x から Q が真となる状態に遷移するとき，$wp_\sigma(Q)(x)$ は 1, そうでないとき 0 となる．また，状態 x において，σ は生起不可能であるか，もしくは σ の生起後の状態で Q が真であるとき，$wlp_\sigma(Q)(x)$ は 1, そうでないとき 0 となる.

Q に対して，述語 $\mathrm{Re}(G,Q)$ を次のように帰納的に定義する [11].

(i) $\mathrm{Re}(G,Q)(x_0) = 1$

(ii) $\mathrm{Re}(G,Q)(x) = 1$ であり，$\delta(x,\sigma)!$ なる $\sigma \in \Sigma$ に対して $Q(\delta(x,\sigma)) = 1$ ならば，$\mathrm{Re}(G,Q)(\delta(x,\sigma)) = 1$ である.

(iii) $\mathrm{Re}(G,Q)(x)$ を満たす全ての状態は上の (a), (b) より得られる.

【定義 1】

$Q(x_0) = 1$ なる述語 $Q \in \mathcal{Q}$ が任意の $\sigma \in \Sigma^{uc}$ に対して，

$$Q \leqq \mathrm{Re}(G,Q) \wedge wlp_\sigma(Q)$$

を満たすとき，Q は G に関して可制御であるという.

2.1 最大可制御部分述語

一般に，与えられた述語が可制御であるとは限らない．このとき，Q の部分述語の中で，集合の包含関係に関して最大となる可制御述語に対して，状態フィードバックを設計することになる．

今，$Q(x_0)=1$ なる述語 $Q\in\mathcal{Q}$ に対して，Q の全ての可制御部分述語の集合 $C(Q)\subseteqq\mathcal{Q}$ を次式で定義する．

$$\underline{C}(Q)=\{Q'\in\mathcal{Q}\,;\,Q'(x_0)=1,\quad Q'\leqq Q \text{ かつ } Q' \text{ は可制御 }\}$$

述語 $[Q]\in\mathcal{Q}$ を次式のように定義する．

$$[Q](x)=\begin{cases}1 & \text{if } x \text{ が次の条件 (A1) を満たす}\\ 0 & \text{otherwise}\end{cases}$$

(A1)　任意の事象列 $s\in\Sigma^{uc,*}$ に対して

$$\delta(x,s)!\Longrightarrow Q(\delta(x,s))=1$$

ここで，$\Sigma^{uc,*}$ は空列 ε を含む，Σ^{uc} の要素の全ての有限列の集合である．

$[Q](x_0)=1$ のとき，$\underline{C}(Q)$ の最大の述語は

$$\sup\underline{C}(Q)=\mathrm{Re}(G,[Q])$$

で与えられる．

3. 人間-機械システム

人間-機械システムはマシンモデル，インタフェース，およびユーザモデルの 3 つの要素からから構成される．まず，これらの 3 つの要素の数理モデルを与える．

3.1 マシンモデル

本論文では，マシンは離散事象システムとしてモデル化されるものとする．今，マシンモデルを以下のオートマトンで表現する．

$$G_M=(X_M,\,\Sigma_M,\,\delta_M,\,x_{M,0}) \tag{1}$$

ただし，X_M は状態集合，Σ_M は事象集合，$\delta_M:X_M\times\Sigma_M\to X_M$ は状態遷移関数，$x_{M,0}$ は初期状態である．ここで，

$\Sigma_M=\Sigma_M^o\cup\Sigma_M^{uo}$ $(\Sigma_M^o\cap\Sigma_M^{uo}=\emptyset)$

Σ_M^o ： ユーザが引き起こすマシンの事象集合，すなわちコマンドの集合．

Σ_M^{uo} ： マシン内部で自動的に生起する事象集合，すなわち内部事象の集合．

である．状態遷移関数 δ_M はマシンが決定的であることを意味している．つまり，ユーザからのコマンドや内部信号による動作はマシンのどの状態でも，一意に決まる．

システムで事象が生起していない状況を空列 ε で表わす．

3.2 インタフェース

インタフェースはマシンの状態を表示するためのディスプレイ装置である．そして，ユーザはマシンの内部状態をすべて知る必要はなく，操作するために十分な情報を持てばよいので，インタフェースはマシンの情報を抽出して設計している．よって，インタフェースは写像 $I:X_M\to X_U$ で表現できる．ただし，X_U はインタフェース表示の集合である．また内部事象の生起は観測されないので，射影操作 $\Pi:\Sigma_M\to\Sigma_M^o\cup\{\varepsilon\}$ を以下のように定義する．

$$\Pi(\sigma)=\begin{cases}\sigma & \text{if}\quad \sigma\in\Sigma_M^o\\ \varepsilon & \text{if}\quad \sigma\in\Sigma_M^{uo}\end{cases} \tag{2}$$

つまり，マシンの内部事象はユーザには観測されず空動作となる．そして，マシンの内部事象の生起は以下のような 2 つの場合が存在する．

(C1)　マシンの内部事象の生起がインタフェースの状態を変化させない場合．ユーザは事象の生起に関して何も分からない．

(C2)　マシンの内部事象の生起がインタフェースの状態を変化させる場合．ユーザは何らかの不可観測な事象の生起を認識する．

(C1) のケースは通常マニュアル等に記載する必要はないが，(C2) のケースは適切に記載される必要がある．もし，空動作によりインタフェースの状態が変化するような状況がユーザモデルで定義されていない場合，ユーザは空動作によってインタフェースの状態が変化する可能性があることを知らず，実際にそのような遷移が生じたときに混乱を招く恐れがある．以下では，インタフェースの状態を変化させない内部事象の生起（ユーザモデルにおける ε による明示的な自己ループ）の表記を省略する．

3.3 ユーザモデル

マシンの操作のためにユーザが知っている知識は実際のマシンのふるまいを簡単化したものである．そして，それはマニュアル，訓練資料などで与えられる．したがって，ユーザモデルはインタフェース，与えられるマニュアルに基づいて構築されることになる．

ユーザモデルはインタフェース表示の集合 X_U が状態集合となり，オートマトン G_U で表わされる．

$$G_U=(X_U,\,\Sigma_M^o\cup\{\varepsilon\},\,\delta_U,\,x_{U,0}) \tag{3}$$

ただし，$\Sigma_M^o\subseteqq\Sigma_M$ はユーザが出すコマンドの集合である．状態遷移関数 $\delta_U:X_U\times(\Sigma_M^o\cup\{\varepsilon\})\to 2^{X_U}$ は一般に非決定的であるが，コマンドを出したことによるモード遷移は決定的にわかると仮定する．すなわち，$\forall x\in X_U$ と $\forall\sigma\in\Sigma_M^o$ に対し，

$$|\delta_U(x,\sigma)|\leqq 1$$

である．ただし，$|\cdot|$ は要素数を表わす．

3.4 合成モデル

以上説明した 3 つの要素はすでに与えられているとする．しかし，マシンモデルとユーザモデルの合成モデルを考えるこ

とにより，与えられたインタフェースとユーザモデルにおいてオートメーションサプライズの存在を検証する方法が提案されている [4], [5], [7]．本節では，警報システムの設計に適したマシンモデルとユーザモデルの同期合成の規則を定義する．

マシンが状態 x_M にあり，事象 $\sigma \in \Sigma_M$ の生起により状態 x'_M に遷移するとする．これを

$$x_M \xrightarrow{\sigma} x'_M$$

と表す．また，マシンが状態 x_M にいるとき，ユーザモデルで対応する状態 x_U にいるとし，事象 $\Pi(\sigma) \in \Sigma_U$ の生起により状態 x'_U に遷移するとする．これを

$$x_U \xrightarrow{\Pi(\sigma)} x'_U$$

とする．このとき，合成遷移を

$$(x_M,\ x_U) \xrightarrow{\sigma} (x'_M,\ x'_U)$$

と定義する．

このとき，合成遷移には以下のような状況が存在する．

マシンモデルの状態 x_M と対応するユーザモデルの状態 x_U に対して

(a) $\delta_M(x_M,\sigma)!$ かつ $\delta_U(x_U,\Pi(\sigma))!$

(a)-1 $I(x'_M) = x'_U$

マシンモデル，ユーザモデルの両方で遷移が定義されており，かつ遷移後の状態も整合性がとれているので，オートメーションサプライズは発生しない．つまり，望ましい遷移が起こったことになる．

(a)-2 $I(x'_M) \neq x'_U$

マシンモデル，ユーザモデルの両方で遷移が定義されているが，遷移後の状態でユーザの予測とマシンの実際の振る舞いとの間に整合性が取れておらず，ユーザは予期せぬ結果を受け取ることになる．このときオートメーションサプライズが生じる．

(b) $\neg\delta_M(x_M,\sigma)!$ かつ $\delta_U(x_U,\Pi(\sigma))!$

ユーザの命令に対して，マシンモデルに対応する遷移がなく命令が受け入れられない．このとき，ユーザは意図したとおりにマシンを操作することができず，オートメーションサプライズが生じる．

(c) $\delta_M(x_M,\sigma)!$ かつ $\neg\delta_U(x_U,\Pi(\sigma))!$

マシンモデルでなんらかの事象が生起しているにも関わらず，ユーザモデルに対応する遷移が定義されておらず，ユーザはマシンの動作に追従できなくなる．このような場合も結果としてマシンとユーザとの間に誤認識が生まれ，オートメーションサプライズが生じる．

オートメーションサプライズを状況ごとにさらに細かく分類した場合，(a)-2 は Mode confusion [8]，(b) は Refusal state [5]，(c) は Blocking state [6], [7] とそれぞれ呼ばれているが，本報告ではこれらを分類せず，単にオートメーションサプライズと呼ぶ．

以上よりマシンモデル G_M とユーザモデル G_U の合成モデル G_{com} は以下のようになる．

$$G_{com} = ((X_M \times X_U) \cup \{AS\},\ \Sigma_M,\ \delta_{com},\ (x_{M,0},\ x_{U,0})) \qquad (4)$$

ただし，AS はオートメーションサプライズである状態を表わす．状態遷移関数 δ_{com} は次式で定義される [12]．

$$\delta_{com}((x_M,x_U),\ \sigma) = \begin{cases} (x'_M,x'_U) & \text{if } \delta_M(x_M,\sigma)!\ ,\ \delta_U(x_U,\Pi(\sigma))!, \\ & \text{and } I(x'_M) = x'_U \\ AS & \text{if } \delta_M(x_M,\sigma)!\ ,\ \delta_U(x_U,\Pi(\sigma))!, \\ & \text{and } I(x'_M) \neq x'_U \\ AS & \text{if } \neg\delta_M(x_M,\sigma)! \text{ and } \delta_U(x_U,\Pi(\sigma))! \\ AS & \text{if } \delta_M(x_M,\sigma)! \text{ and } \neg\delta_U(x_U,\Pi(\sigma))! \\ \text{undefined} & \text{otherwise} \end{cases} \qquad (5)$$

ただし，$\delta_M(x_M,\sigma) = x'_M$, $\delta_U(x_U,\Pi(\sigma)) \ni x'_U$ である．そして $(X_M \times X_U) = X_{com}, (x_{M,0},\ x_{U,0}) = x_{com,0}$ とする．

合成モデルにおいて AS に可到達でないならば，ユーザはマシンを予想通りに正しく操作できるが，AS に可到達であるならば正しく操作することができない．そこで，状態フィードバック制御を用いて，ユーザがオートメーションサプライズを起こす前に警報を鳴らして，オートメーションサプライズが起きないようにコマンドの生起を制御するシステムの構成法を次章で提案する．

4. 警報システム

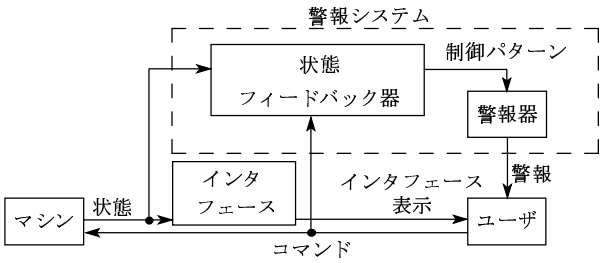

図 1 警報システムのブロック線図

Fig. 1 Block diagram of alarm system

本論文で提案する警報システムは，図 1 に示すように状態フィードバック器と警報器からなる．オートメーションサプライズはマシンとユーザモデルの状態の対に対して定義することができる．マシンの状態はマシンをセンシングすることにより得ることができ，ユーザモデルの状態はユーザコマンドにより状態が決定的に次の状態に遷移するので，コマンドをセンシングすることで得ることができる．制御仕様を状態上の述語として与えることができるため，状態フィードバック制御 [11] を応用する．

オートメーションサプライズが生じない状態で真，オートメーションサプライズが生じる状態で偽となる述語 Q_{AS} を考えると以下のようになる．

$$Q_{AS}(x_{com}) = \begin{cases} 1 & \text{if} \quad x_{com} \neq AS \\ 0 & \text{if} \quad x_{com} = AS \end{cases} \tag{6}$$

また，各 $\sigma \in \Sigma_M$ に対して，述語 D_σ と $\mathcal{Q}_{\mathcal{AS}}$ 上の変換 wp_σ と wlp_σ は同様に定義できる．

$Q_{AS}(x_{com,0}) = 1$ なる述語 $Q_{AS} \in \mathcal{Q}_{\mathcal{AS}}$ が任意の $\sigma \in \Sigma^{uc}$ に対して，

$$Q_{AS} \leqq \mathrm{Re}(G_{com}, Q_{AS}) \wedge wlp_\sigma(Q_{AS}) \tag{7}$$

を調べることにより合成モデルの可制御性がわかる．

合成モデルの事象の中で可制御な事象を Σ_M^c とし，不可制御な事象を Σ_M^{uc} とすると

$$\Sigma_M^c \cup \Sigma_M^{uc} = \Sigma_M$$
$$\Sigma_M^c \cap \Sigma_M^{uc} = \emptyset$$

である．本論文では簡単のため

$$\Sigma_M^c = \Sigma_M^o$$
$$\Sigma_M^{uc} = \Sigma_M^{uo}$$

であるとする．禁止する事象集合のベキ集合を

$$\Gamma = \{\gamma \ ; \ \gamma \subseteqq \Sigma_M^o\}$$

とおく．状態フィードバック f を施した閉ループシステムを $G_{com}|f$ とすると，以下のようになる．

$$G_{com}|f = (X_{com}, \ \Sigma_M, \ \delta_{com}^f, \ x_{com,0})$$

ただし，遷移関数 $\delta_{com}^f : X_{com} \times \Sigma_M \to X_{com}$ は次式で定義される．

$$\delta_{com}^f(x, \sigma) = \begin{cases} \delta_{com}(x, \sigma) & \text{if} \quad \sigma \notin f(x) \\ \text{undefined} & \text{otherwise} \end{cases}$$

可到達集合 $Reach(x_{com,0})$ を

$$Reach(x_{com,0}) = \{x_{com} \in X_{com} | \ \exists s \in \Sigma_M^* \\ \text{s.t. } \delta_{com}(x_{com,0}, s) = x_{com}\}$$

とおくと，以上の議論より，警報システムの設計手順は次のようになる．

Step 1 マシンモデル G_M，インタフェース I，ユーザモデル G_U を与える．

Step 2 合成モデル G_{com} を構成する．

Step 3 $AS \notin Reach(x_{com,0})$ ならば人間-機械系は適切であり，警報器を作る必要はない．$AS \in Reach(x_{com,0})$ ならば人間-機械系はオートメーションサプライズを生じるので次ステップへ．

Step 4 述語 Q_{AS} と任意の $\sigma \in \Sigma_M^{uc}$ に対して式 (7) を調べる．もし成立しないならば，最大可制御部分述語を求める．

Step 5 状態フィードバック則 $f \in \Gamma^{X_{com}}$ を決定する．

Step 6 得られた状態フィードバック則をもとに禁止する事象に対する警報のタイミングが得られ，警報を鳴らす状態からの遷移より警報解除を知らせるタイミングを求め，警報器 $alarm$ を構成する．

$\delta_{com}(x_{com}, \eta) = x'_{com}$ とおくと警報器は以下のように表現できる．

$alarm(x_{com}, x'_{com}) =$

$$\begin{cases} on(\sigma) & \text{if} \quad \sigma \notin f(x_{com}) \text{ and } \sigma \in f(x'_{com}) \\ off(\sigma) & \text{if} \quad \sigma \in f(x_{com}) \text{ and } \sigma \notin f(x'_{com}) \\ \text{nosignal} & \text{otherwise} \end{cases} \tag{8}$$

ここで，$on(\sigma)$ は事象 σ の生起を禁止するように警報を出すことを，$off(\sigma)$ は禁止されていた σ が許容されたときの警報解除の指示を，nosignal は警報の更新がないことを，それぞれ表わす．警報器 $alarm$ は x'_{com} において警報を出したり，解除したりする．

5. 例　　題

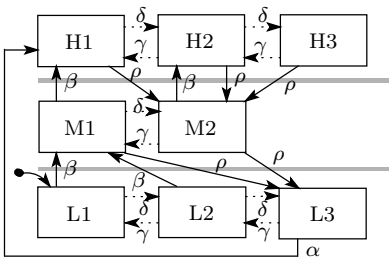

図 2　マシンモデル
Fig. 2　Machine model

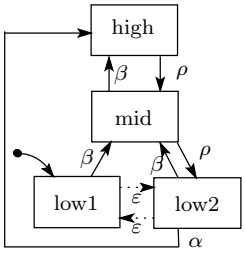

図 3　ユーザモデル
Fig. 3　User model

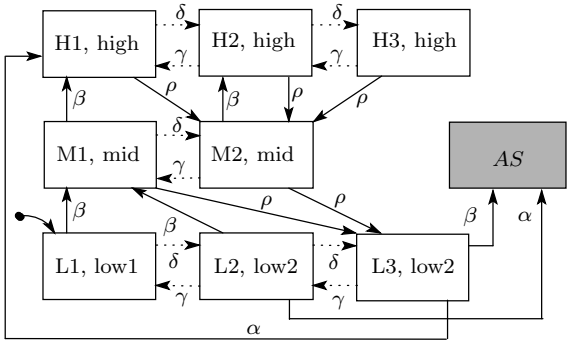

図 4　合成モデル
Fig. 4　Composite model

図 2，図 3 で示されるマシンモデルとユーザモデルを考える．図 2 のマシンモデルは 8 個の状態がある．ユーザが引き起こす遷移は実線の矢印で表し，一方，自動的な遷移は点線の矢印で表す．つまり，ユーザの手による遷移はそれぞれ α, β, ρ であり，自動的な遷移はそれぞれ δ, γ で表わされている．

マシンの事象集合 Σ_M は

$$\Sigma_M = \{\varepsilon, \ \alpha, \ \beta, \ \rho, \ \delta, \ \gamma\}$$

であり，可制御な事象 Σ_M^c と不可制御な事象 Σ_M^{uc} は

$$\Sigma_M^c = \{\alpha,\ \beta,\ \rho\}$$
$$\Sigma_M^{uc} = \{\varepsilon,\ \delta,\ \gamma\}$$

である．

初期状態は図でどの状態にも属さない所から入ってくる矢印で表す．つまり，マシンモデルの初期状態は L1 である．また，写像 I は

$$\begin{cases} I(\mathrm{L}_1) = \mathrm{low1} \\ I(\mathrm{L}_2) = I(\mathrm{L}_3) = \mathrm{low2} \\ I(\mathrm{M}_i) = \mathrm{mid} \quad (i = 1, 2) \\ I(\mathrm{H}_i) = \mathrm{high} \quad (i = 1, 2, 3) \end{cases}$$

である．マシン内部の自動的な遷移によって low1 から low2 に変わるとき，ユーザはインタフェース表示が変わることにより，何らかの内部事象が生起したことを認識でき，ユーザモデルに ε が現れる．

図 2 のマシンモデルと図 3 のユーザモデルから図 4 の合成モデルを構成し，x_0 = (L1, low1), x_1 = (L2, low2), x_2 = (L3, low2), x_3 = (M1, mid), x_4 = (M2, mid), x_5 = (H1, high), x_6 = (H2, high), x_7 = (H3, high), $x_8 = AS$ とおくと $AS \in Reach(x_{com,0})$ であるのでオートメーションサプライズが生じることが分かる．それはユーザが (L2, low2) から α で遷移させようとする場合と (L3, low2) から β で遷移させようとする場合である．

そこで，4 章の設計手順に従い，警報システムを構成する．

まず，述語 Q_{AS} は

$$Q_{AS}(x_{com}) = \begin{cases} 1 & \text{if} \quad x_{com} = x_i \quad (i = 1 \cdots 7) \\ 0 & \text{otherwise} \end{cases}$$

となり，

$$Q_{AS} = \{x_0, x_1, x_2, x_3, x_4, x_5, x_6, x_7\}$$
$$\mathrm{Re}(G_{com}, Q_{AS}) = \{x_0, x_1, x_2, x_3, x_4, x_5, x_6, x_7\}$$

であり，任意の $\sigma \in \Sigma_M^{uc} = \{\delta, \gamma\}$ に対して

$$wlp_\sigma(Q_{AS}) = \{x_0, x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8\}$$

であるので，式 (7) が成立し，述語 Q_{AS} は可制御となる．したがって，警報器は次式で与えられる．

$$alarm(x, x') = \begin{cases} on(\alpha) & \text{if} \quad x' = x_1 \\ on(\beta) & \text{if} \quad x' = x_2 \\ off(\alpha) & \text{if} \quad \alpha \in f(x) \text{ and } \alpha \notin f(x') \\ off(\beta) & \text{if} \quad \beta \in f(x) \text{ and } \beta \notin f(x') \\ \mathrm{nosignal} & \text{otherwise} \end{cases}$$

例えば，図 3 のインタフェースが low1 から low2 へ変わったとすると，それはマシンの状態が L1 から L2 に変わったからである．すると，合成モデルでは x_0 = (L1, low1) から x_1 = (L2, low2) へ変わるので α を禁止する警報が鳴る．また，インタフェースが mid から low2 へ変わったとすると，それはマシンの状態が M1 または M2 から L3 に変わったからである．すると，合成モデルでは x_3 = (M1, mid) または x_4 = (M2, mid) から x_2 = (L3, low2) へ変わるので β を禁止する警報が出る．次に，x_2 から x_1 に変わると β の生起が許容されるので，β に対する警報は解除される．

6. あとがき

本論文では，人間-機械システムの構成要素であるマシン，インタフェース，ユーザモデルを定式化した．しかし，これらが適切でない場合，オートメーションサプライズを引き起こす可能性がある．そこで，オートメーションサプライズを起こしそうな場合，起こらないように禁止する方法として警告音を出す警報システムを提案した．提案手法では対象システムを離散事象システムと仮定し，制御仕様がオートメーションサプライズを起こさないという状態の集合上の述語として与えられるため，状態フィードバック制御を応用した．そして，ユーザに回避をさせる方法をマシンが完全観測の場合において示した．今後の課題として，マシンの状態が部分観測である場合について提案手法を拡張することや警報システム設計支援のツールの開発などが挙げられる．

文　献

[1] N. Sarter, D. Woods, and C. Billings, “Automation surprises,” in *Handbook of Human Factors and Ergonomics* (G. Salvendy, ed.), pp. 1926–1943, New York: Wiley, 1997.

[2] E. Palmer: “Oops, it didn’t arm. - a case study of two automation surprises,” in *Proceedings of the 8th International Symposium on Aviation Psychology*, Columbus, Ohio, pp. 227-232, 1995.

[3] A. Degani, *Modeling Human-Machine Systems: On Modes, Error, and Patterns of Interaction.* Ph. D. Thesis, Georgia Institute of Technology, 1996.

[4] J. Rushby, “Using model checking to help discover mode confusions and other automation surprises,” *Reliability engineering and system safety*, vol. 75, pp. 167–177, 2002.

[5] Y. Ukawa, T. Ushio, and M. Adachi, “Formal detection of mode confusion in human-machine interaction,” in *Proceedings of the 1st International Symposium on Systems & Human Science*, Osaka, Japan, pp. 309–314, November 2003.

[6] 足立 正和, 潮 俊光, 宇川 佳孝: “双模倣性を用いたオートメーションサプライズのないマン・マシンインタフェースの設計,” 第 17 回　回路とシステム（軽井沢）ワークショップ, pp. 291–296, 2004

[7] A. Degani and M. Heymann, “Formal verification of human-automation interaction,” *Human Factors*, vol. 44, no. 1, pp. 28–43, 2002.

[8] M. Heymann and A. Degani, “On abstraction and simplification in the design of human-automation interaction,” *NASA Technical Memorandum 211397, NASA Ames Research Center, Moffett Field, CA*, 2002.

[9] P. J. Ramadge and W. M. Wonham, “Modular feedback logic for discrete event systems,” *SIAM J. Control and Optimization*, vol. 25, no. 5, pp. 1202–1218, September, 1987.

[10] 高井 重昌, 潮 俊光, 児玉 慎三: “離散事象システムにおける部分観測のもとでの状態フィードバックの存在条件,” システム制御情報学会論文誌, vol. 7, no. 1, pp. 9–17, 1994.

[11] Y. Li and W. M. Wonham, “Controllability and observability in the state feedback control of discrete event systems,” in *Proceedings of the 27th IEEE Conference on Decision and Control*, pp. 203–208, Austin, Texas, December 1988.

[12] 梁瀬 裕行: “離散事象システムにおける状態フィードバック制御を用いた警報の設計方法,” 特別研究報告, 大阪大学, 2004.