状態フィードバック制御に基づく警報システムの設計

Design of Alarm Systems Based on State Feedback Control

大阪大学大学院基礎工学研究科　○梁瀬 裕行，潮 俊光，足立 正和，宇川 佳孝

○ Yuki YANASE, Toshimitsu USHIO, Masakazu ADACHI, and Yoshitaka UKAWA

Graduate School of Engineering Science, Osaka University

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.

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 [1]．オートメーションサプライズ [2] は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．対象を離散事象システムとし，オートメーションサプライズの発生を避けるための警報システムの構成法を提案する．

2　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から構成される．本論文では，マシンとして離散事象システム G_M を考える．

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

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．

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．G_M と G_U の間の事象における関係は射影操作 $\Pi : \Sigma_M \to \Sigma_M^o \cup \{\varepsilon\}$ により表現できる．

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．

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

ただし，$\Sigma_M^o \subseteq \Sigma_M$ 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，$|\delta_U(x,\sigma)| \leq 1$ である．ただし，$|\cdot|$ は要素数を表わす．

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．

$G_{com} =$

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

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 [3]．

$\delta_{com}((x_M, x_U),\ \sigma) =$

$$\begin{cases} (x'_M, x'_U) & \text{if} \quad \delta^{\sigma}_{x_M}!,\ \delta^{\Pi(\sigma)}_{x_U}! \text{ and } I(x'_M) = x'_U \\ AS & \text{if} \quad \delta^{\sigma}_{x_M}!,\ \delta^{\Pi(\sigma)}_{x_U}! \text{ and } I(x'_M) \neq x'_U \\ AS & \text{if} \quad \neg\delta^{\sigma}_{x_M}! \text{ and } \delta^{\Pi(\sigma)}_{x_U}! \\ AS & \text{if} \quad \delta^{\sigma}_{x_M}! \text{ and } \neg\delta^{\Pi(\sigma)}_{x_U}! \\ \text{undefined} & \text{otherwise} \end{cases}$$

ただし，$\delta_M(x_M, \sigma) = x'_M$，$\delta_U(x_U, \Pi(\sigma)) \ni x'_U$ とし，$\sigma \in \Sigma_M$ と $x \in X_M$ に対して $\delta_M(x_M, \sigma)$ が定義されるとき $\delta^{\sigma}_{x_M}!$ と書くとする (ユーザモデルも同様である)．

3　警報システム

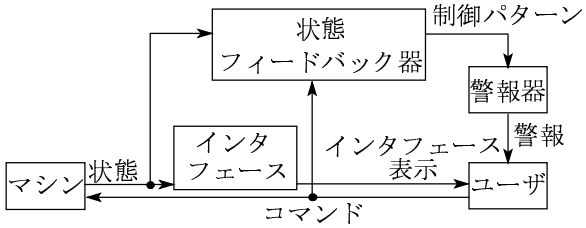

図 1: 警報システムのブロック線図

本論文で提案する警報システムのブロック線図を図 1 に示す．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 [4] を用いることができる．

禁止する事象集合の集合を $\Gamma = \{\gamma\ ;\ \gamma \subseteq \Sigma_M^o\}$ とおく．

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を Q_{AS} とおく．

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

変換 wlp_σ, 述語 $\mathrm{Re}(G_{com}, Q_{AS})$ を以下のようにおく [4].

状態 x_{com} において，σ が生起不可能であるか，σ の生起後の状態で $Q_{AS}(x_{com}) = 1$ であるとき，$wlp_\sigma(Q_{AS})(x_{com})$ は 1, そうでないとき 0 とする．

述語 $\mathrm{Re}(G_{com}, Q_{AS})$ は，$x_{com,0}$ から $Q_{AS}(x_{com}) = 1$ を満たす状態のみを遷移し，x_{com} に可到達のときのみ真とする．

また，可到達集合 $Reach(x_{com,0})$ を

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

とすると警報器の設計手順は次のようになる．

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．
2. 合成モデル G_{com} を構成する．
   (a) $AS \notin Reach(x_{com,0})$ 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．
   (b) $AS \in Reach(x_{com,0})$ 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．
3. 述語 Q_{AS} と任意の $\sigma \in \Sigma_M^{uc}$ に対して可制御性 $Q_{AS} \leq \mathrm{Re}(G_{com}, Q_{AS}) \wedge wlp_\sigma(Q_{AS})$ を調べる．(可制御でないとき，最大可制御部分述語 [4] を構成する．)
4. 状態フィードバック則 $f : X_{com} \to \Gamma$ を決定する．
5. 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．

$$alarm(x_{com}, x'_{com}) = \begin{cases} on(\sigma) & \text{if} \quad \sigma \notin f(x_{com}) \text{ and } \sigma \in f(x'_{com}) \\ off(\sigma) & \text{if} \quad \sigma \in f(x_{com}) \text{ and } \sigma \notin f(x'_{com}) \\ \text{undefined} & \text{otherwise} \end{cases}$$

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表わし，$off(\sigma)$ 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．

【例題】 図 2,3 で示されるマシンモデルとユーザモデルを考える．ただし，$I(\mathrm{L}_1) = \mathrm{low1}$, $I(\mathrm{L}_2) = I(\mathrm{L}_3) = \mathrm{low2}$, $I(\mathrm{M}_i) = \mathrm{mid}\ (i = 1, 2)$, $I(\mathrm{H}_i) = \mathrm{high}\ (i = 1, 2, 3)$ である．マシン内部の遷移で low1 から low2 に変わるとき，インタフェース表示が変わることによりユーザは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．$x_0 = (\mathrm{L1}, \mathrm{low1})$, $x_1 = (\mathrm{L2}, \mathrm{low2}), \cdots$, $x_7 = (\mathrm{H}, \mathrm{high})$, $x_8 = AS$ とおくと，図 4 の述語 Q_{AS} は可制御であることが確かめられ，警報器は次式で与えられる．

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

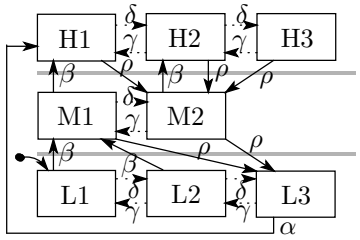

図 2: マシンモデル

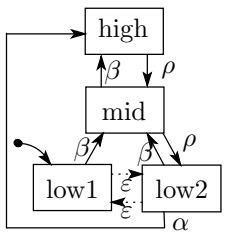

図 3: ユーザモデル

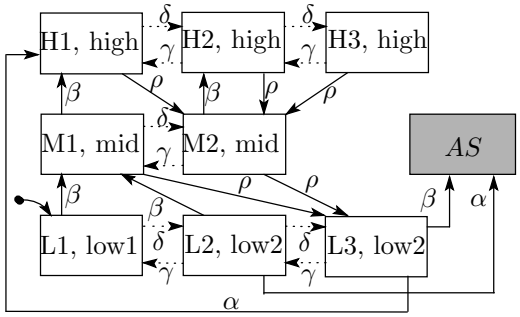

図 4: 合成モデル

4 あとがき

人間-機械システムのマシン，インタフェース，ユーザモデルを定式化した．状態フィードバック制御を用い，警報システムの構成法を提案した．今後の課題はマシンの状態が部分観測である場合への提案手法の拡張や実装などが挙げられる．

参考文献

[1] 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.

[2] 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.

[3] 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.

[4] Y. Li and W. M. Wonham, "Controllability and observability in the state feedback control of discrete event systems," in *Proc. 27th IEEE CDC*, pp. 203–208, Austin, Texas, December 1988.