Delay-incorporating observability and predictability analysis of safety-critical continuous-time systems

Neda Eskandari, Guy A. Dumont, Z. Jane Wang

Department of Electrical and Computer Engineering, University of British Columbia, Vancouver, BC, Canada
E-mail: nedae@ece.ubc.ca

Abstract: The authors suggest a framework for human–automation interaction in safety-critical continuous systems under shared control and consider continuous-time linear time-invariant (LTI) dynamics to formalise our physical models mathematically. Their goal is to determine whether or not a given user-interface provides the information required for a certain task, under the assumption that the user does not have access to any information beyond what is provided in the display. They identify observability-based conditions under which a user-interface provides the user with necessary information to accomplish a given task, formulated as a subset of the state space. They, therefore formulate the novel delay-incorporating user-observable subspace, and the delay-incorporating user-predictable subspace and compare them with the space spanned by the combination of the states which create the task. They assume the user is a special type of observer, with capabilities corresponding to different levels of knowledge regarding the current user’s input and its derivatives. In addition, they consider that state reconstruction and prediction incorporate a processing delay.

1 Introduction

As interfaces and their underlying systems become more complex, information beyond what is contained in the interface may not be accessible. We aim to identify tools that assess the correctness of a user-interface for a given task, an especially relevant problem in systems for which intuition and simulation may not be enough to assure that an interface is effective. While in many systems, such as a human-driven car, the user has access to information beyond what is simply contained in the interface, we focus here solely on information contained in the interface, for example, a remotely controlled car or a pilot performing a task in high altitude.

Human-factors researchers have frequently pointed out the importance of incorporating human-factors into traditional control theory, which can result in better human–automation interaction [1, 2]. Many researchers have suggested frameworks for human–automation interaction in order to come up with more effective interaction between the elements of the system [1–3]. Attaining situation awareness (SA) is a human-factor concept which is known to be necessary for the user to have correct interaction with the automation [4, 5]. Attaining SA includes three levels of processing the information, (i) perception of the information, (ii) comprehension of the information and (iii) projection or prediction of the information [4, 6]. Lack of SA can lead to a faulty control action by the operator because of bad decisions. As we have already assumed that the display is the only source of information for the user, it has to be designed to allow the user perceive, comprehend and predict the desired information to attain correct SA. Hence, the display design procedure requires a careful selection and clear presentation of the information for the user to perform the desired tasks correctly.

Some examples which are available in the literature about incorporating human-factors into traditional control theory are (i) modelling the human operator as a controller for systems without [7–10] or with uncertainties [11, 12], (ii) modelling the user as an estimator and Kalman filter [13, 14] and (iii) modelling the user as an observer-based fault detector with the focus on modelling the decision making process [15, 16]. Rather than modelling the user as a full-order Kalman-filter/observer, in [17] we modelled the user as a customised functional observer which could be personalised based on the capabilities of the operator.

In [18], we suggested a method to analyse user-interfaces of a particular type of system under shared control. We obtained subspaces based on observability and predictability requirements of the user and limitations of the user regarding input signals. In [18], in order to model the shared control systems, we only took into account the low-level control inputs from the human and the automation – that is, the input by human or automation which directly affects the control surfaces. In addition, in order to evaluate the states which are predictable by the user, we simply evaluated the observability of the states and their first derivative.

The results of [18] are acceptable for the systems in which a small amount of delay in comprehension and prediction of the task vector does not affect the safety of the system. However, for safety-critical systems which have to follow a precise trajectory of the altimeter, targets cases where the human is a part of the system and partially modify our previous results in [18], we suggested a method to analyse user-interfaces of a system under shared control and consider continuous-time linear time-invariant (LTI) dynamics to formalise our physical models mathematically. Their goal is to determine whether or not a given user-interface provides the information required for a certain task, under the assumption that the user does not have access to any information beyond what is provided in the display. They identify observability-based conditions under which a user-interface provides the user with necessary information to accomplish a given task, formulated as a subset of the state space. They, therefore formulate the novel delay-incorporating user-observable subspace, and the delay-incorporating user-predictable subspace and compare them with the space spanned by the combination of the states which create the task. They assume the user is a special type of observer, with capabilities corresponding to different levels of knowledge regarding the current user’s input and its derivatives. In addition, they consider that state reconstruction and prediction incorporate a processing delay.
of the estimation and the prediction which we simply ignored in the previous work. In addition, in [18] we assumed that a subsequent value of a functional of the states is known if the current functional and its first derivative are known. Here, we relax this assumption and consider the actual evolution of the states of the system which depends on the current functional, the inputs and the input derivatives. By relaxing these assumptions, we will be able to modify our tool so that it can be used for the analyses of the displayed information in safety-critical systems. In addition, in this work, we suggest a framework for systems under shared control and consider the system to be affected by low-level input as well as the reference trajectory. Overall, we can briefly summarise our contributions as (i) incorporating the information processing delay, (ii) considering a more realistic pattern of states’ prediction and (iii) considering a more practical model of our physical system. The results of this paper are applicable to safety critical systems, such as surgical robots under shared control and fighter aircrafts. We, however, do all our analysis based on the assumption that these systems can be presented by deterministic LTI dynamics with no noise and uncertainty. Further research is required to resolve this limitation of our purposed method.

In Section 2, we introduce a framework for systems under shared control and present the proposed mathematical framework. We determine formulas for the delay-incorporating user-observable subspace, and the delay-incorporating user-predictable subspace of shared control systems in Section 3. An example on a remotely driven car is provided in Section 4.

1.1 Common notations

In the following, $\oplus$ indicates the summation of subspaces, $\mathcal{N}(\cdot)$ is the null space and $\mathcal{R}(\cdot)$ is the range space.

2 Problem statement

While performing a desired task, a human controller might make mistakes because of different factors, including lack of understanding about the system’s dynamics and the indeterministic behaviour of the automation. These problems can be solved by providing the user with sufficient training and by designing a deterministic plant, respectively. In addition, lack of correct displayed information is a safety threat to the system. Our goal, here, is to address this safety aspect for the system by analysing the displays and rejecting those which do not let the users attain the required understanding about the desired states of the system. Clearly, if a user does not have access to the necessary information about the desired states of the system, making correct decisions is not possible for them, hence, their actions may result in unwanted or even hazardous outcomes.

In this work, in order to analyse the correctness of the displayed information in safety-critical systems, we will come up with an inclusion which has to be satisfied, otherwise the interface is rejected.

The importance of having a complete and correct understanding about the situation, that is, the desired combination of the states of the system, has been pointed out by various human-factors researchers [4, 35–37]. The process of information acquisition and analysis was formally named the SA process by Endsley [4] and is mentioned to be the foundation of correct decision making and action. SA which is defined as ‘the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the near future’ [4], incorporates three levels which are perception of information, comprehension of information and projection (prediction) of information.

In this work, we assume that the information processing only occurs in the working memory – that is, we simply ignore the effect of pattern matching which can help the user with state estimation and prediction without loading the working memory. In addition, we assume that the only role of the mental model is to provide the user with adequate understanding about the system’s dynamics.

On the basis of the above discussion, we assume that the comprehension of the non-measured part of the task functional (i.e. the portion of the task which is not measured in the display) and also the prediction the task functional have to take place within the working memory which is associated with certain amount of processing delay [38]. We limit our work to systems with only visual cues available in their displays. From [39], the perception delay of visual cues can be seen to be smaller than the processing delay. Hence, by focusing on the processing delay and assuming the perception delay to be negligible, we build our technique on the following assumption.

Assumption 1: Comprehension of the directly measured combination of the states of the system does not incorporate delay. However, prediction of all combinations of the states and also comprehension of the non-measured functionals of the states are associated with a delay, $\tau_1$.

2.1 Framework for human–automation interaction

For analysing the human-automation interaction, several researchers have developed various frameworks [1–3]. In [40], we suggested a framework for shared-control continuous-time systems, such that through providing a low-level control input as well as a reference trajectory, the user-interacts with an automated system. For this work, we consider a similar model as in [40] with a slightly different representations to make the model more proper for our current case. The model is provided in Fig. 1 and shows a human who interacts with an automated plant through a user-interface.

Deriving the model for the specific cases of a human-driven system and a fully automated system from Model 1 is straightforward.

In Model 1, we consider the user to be a function that maps display information to the user input. This mapping involves different stages of processing the information which we have earlier discussed. In our framework, we similarly consider the user to first obtain situation awareness, then decide on the required action, and finally act on the system. As was pointed out earlier, our focus is on the stage of attaining situation awareness and our purpose is to evaluate the understanding of the user from the available information in the display. This helps us to understand whether or not the user has access to the necessary information.

We also assume to have a trained user who is fully experienced with the given dynamics of the automation. It is worth mentioning that the amount of training and the experience to attain the required level of user’s proficiency depends on the complexity of the automation which the user is controlling or monitoring [41] (e.g. the difference between the amount of training and experience of the user and the automation). In this work, we assume that the information processing only occurs in the working memory – that is, we simply ignore the effect of pattern matching which can help the user with state estimation and prediction without loading the working memory. In addition, we assume that the only role of the mental model is to provide the user with adequate understanding about the system’s dynamics.

![Fig. 1](image.png)

This model presents an automation and a human interacting with each other through a user-interface.
required for a driver and a pilot). In this paper, a trained and an experienced user is the one who can make use of the input and output signals and some of their derivatives to reconstruct the current and upcoming values of a desired functional.

The automation shown in Fig. 1 consists of a plant, actuators and a computer. Although, in general the role of the computer is to determine the required movement in the control surfaces corresponding to the desired reference trajectory, in this model, we partially combine the computer with the plant. Hence, we simplify this role to generating the final reference trajectory and model our plant as a set of differential equations which is designed to have both the low-level inputs and the reference-trajectory as its input

\[
\dot{x}(t) = Ax(t) + Bu(t) + Fr
\]

with \( x(t) \in \mathbb{R}^n \) is the state vector, \( u(t) \in \mathbb{R}^m \) is the low-level input from the control effort of the human, \( r \in \mathbb{R}^n \) is the time-invariant reference trajectory and matrices \( A, B \) and \( F \) have compatible dimensions. We also assume that no poles of the system have a zero real part.

**Assumption 2:** Matrix \( A \) has no eigenvalues on the imaginary axis.

The actuators shown in Fig. 1 are devices which translate the low-level input to the movement of the control surfaces. As a result of a possible saturation or rate limiting, the actuator behaviour is not necessarily deterministic. However, we consider the operating conditions in which actuators behave deterministically. Our focus here is not on the mathematical model of the actuator, but, as we considered to have a deterministic actuator, in order to analyse the displayed information, it is enough for us to know how much knowledge the users have about their own input to the system.

**Assumption 3:** The user knows up to \( \lambda \) derivatives of the user’s low-level input to the system. For the users who do not know about their own input to the system, \( \lambda = -1 \).

One of the main elements of the system represented in Fig. 1 is the user-interface. The user-interface is an instrument through which the user-interacts with the automation. This device consists of a display and controls. The display is providing the user with abstract information about the states and inputs of the automation. The user on the other hand acts on the system through the control.

In the real world, displays usually provide the user with information through multi channels—that is, there are multiple sources of information in any realistic system which interact with each other. For instance, when the user is provided with too much information, multiple sensory channels could be used to reduce the workload and increase the capability of the user in processing the information [42]. In the suggested framework, we, however, consider having a uni-modal display and assume that all information in that display is of equal weight. We formulate the display as

\[
y = \begin{bmatrix} y_1 \\ y_2 \end{bmatrix}
\]

where \( y_1 = Cx \) and \( y_2 = Dr \) with \( C \in \mathbb{R}^{r \times n} \) and \( D \in \{0, 1\} \).

Our focus in this paper is on systems in which the user does not have access to any information beyond what is provided in the display. For instance, for a remotely driven car, the user cannot have any access to the information from the environment. In addition, the information that a pilot gets from the environment in higher altitudes, may not be what exactly he relies on to accomplish what he wants. In most systems, however, a part of information is provided through the environment. Consider a driver who has access to position information from the windscreen. Having direct measurements from the environment reduces his need for GPS which provides similar information as what already is available to him. A careful combination of information from the display and environment together with a powerful presentation of information helps the user to perceive information much better, for example, heads-up displays.

We also impose the following assumption about the user.

**Assumption 4:** The user knows up to \( \gamma \) derivatives of the measured output.

### 2.2 Task formulation

Another important notion that should be specified in order to reliably evaluate the interaction between the user and the automation is task.

Degani and Heymann [43] introduced a schematic diagram to define the desired relationship between the elements of system which are the user model, task and the user-interface during human–automation interaction. Using their suggested model, they could describe the interrelation between these elements of the system [43]. When user’s capabilities, information from the display, and task requirements are aligned, the correct interaction between the elements of the system is possible. As an extension to their model, we suggest Fig. 2 which presents the necessary relationship between the elements of the system.

From Fig. 2, the human–automation interaction is not correct for all tasks unless the task requirements is entirely included in the intersection of user model and user-interface—that is, to have a correct human–automation interaction, it is necessary for the user-interface to provide the user with information related to any feasible task.

In our previous work [18], we defined the task as ‘conditions that must always be met or must be eventually met’. Hence, we formulated the task as ‘a function \( f : \mathbb{R}^l \rightarrow \mathbb{R} \) with \( s \) subtasks, such that

\[
\mathcal{F} = \{ x \mid f(Tx) \geq 0 \}, \quad T \in \mathbb{R}^{l \times n_{aug}}
\]

with task matrix \( T \) comprised of \( l \) linear combinations of the state. For ‘always \( \mathcal{F} \)’, the state trajectory must lie in \( \mathcal{F} \) for all time in order for the task to be successfully completed. For ‘eventually \( \mathcal{F} \)’, when the state enters the set \( \mathcal{F} \) at some finite time, the task has been successfully completed’. Denote the ‘task space’ \( \mathcal{T} \) by the row space of \( T \), that is, \( \mathcal{T} = \mathbb{R}^r(T^1) \). We impose some assumptions on the task.

Note that for fully automated systems, by task accomplishment we essentially mean monitoring the accomplishment of a desired task.

**Assumption 5:** To assure the feasibility of the task, let \( \mathcal{T} \subseteq \mathcal{C} \), the controllable subspace of (1).

Having developed a framework for shared control systems and having formulated the task physically and mathematically, we are ready to come-up with a mathematical criterion for evaluating the information content of the display for the system presented in Fig. 1 to meet the requirements of a task formulated in (3). Hence, we should evaluate whether the user has access to the required information to attain situation awareness regarding the task. We therefore impose the following assumption.

![Fig. 2 Required relationship between the elements of a system](image-url)
Assumption 6: In order to accomplish or monitor a desired task, all rows of \( T \) should be mathematically observable and predictable by the user.

Oftentimes, it might be acceptable for the user to reconstruct and predict the task functional with a small amount of processing delay, for example, to maintain the velocity of a car in a desired bound. However, for safety-critical systems, it is necessary that the user has precise information about the current and the upcoming task functionals. Therefore even very small processing delays may be hazardous.

Under Assumption 6, the user-interface of a safety-critical system under shared control must provide the user with information that results in a delay-incorporating user-observable and a delay-incorporating user-predictable which we define them as below.

**Definition 1**: The delay-incorporating user-observable subspace, \( O^u_H(t) \), is a space which is spanned by the combination of current states, \( x(t) \), which are known to the user at current time, \( t \).

**Definition 2**: The delay-incorporating user-predictable subspace, \( P^u_H(t) \), is a space which is spanned by the combination of upcoming states, \( x(t + \tau) \), which are known to the user at current time, \( t \).

To make this more clear, consider a user who aims to reconstruct a combination of the states \( x(t) \) given \( u(t) \) and \( y(t) \). Although this reconstruction might be feasible for the user, because of the processing delay, the desired combination of \( x(t) \) will become available to the user at time \( t + \tau \). For a safety critical system, this late understanding about the states of the system can be unacceptable. Hence, in order to determine a necessary condition for having a ‘good’ user-interface in an LTI system under shared control, we impose the following problem:

**Problem 1**: Find delay-incorporating user-observable and delay-incorporating user-predictable subspaces of the mentioned system.

**Subproblem 1**: Find the combinations of states \( x(t) \) and \( x(t + \tau) \) which can be known to the user at time \( t \), that is, the combination of the states \( x(t) \) and \( x(t + \tau) \) which can be reconstructed from \( u(t - \tau) \), \( y(t - \tau) \)), and their available derivatives.

We obtain \( O^u_H \) and \( P^u_H \) using projection matrices to remove the automation input and human input derivative which are unknown, from the derivatives of the state and output equations.

### 3 Methodology

Under Definitions 1 and 2, for system (1), we formulate the delay-incorporating user-observable subspace, and the delay-incorporating user-predictable subspace.

From Assumption 1, we can write

\[
O^u_H = O_{H,y} \oplus O_{H,t}
\]

where \( O^u_H \) is the delay-incorporating user-observable space, \( O_{H,y} \triangleq \mathcal{R}(C^T) \) is obtained from the directly measured combinations of the states, \( y_i(t) = Cx(t) \), and \( O_{H,t} \) is the delayed observable space which is the space spanned by the non-measured functional of states which can be reconstructed given \( \tau_1 \geq \tau \) delay.

#### 3.1 Delay-incorporating user-observable subspace

In this section, we determine the combination of the states at time \( t \), that is, \( x(t) \), which can be reconstructed by time \( t \). Mathematically, this means to obtain what combination of \( x(t) \), can be reconstructed given \( y(t - \tau) \), \( u(t - \tau) \), and some of their derivatives.

Consider the output equation and its \( i \)-th derivative for \( i \in \{1, \ldots, \gamma\} \) at time \( t - \tau_1 \)

\[
y(t - \tau_1) = Cx(t - \tau_1) \\
y^{(i)}(t - \tau_1) = CA^iy(t - \tau_1) + CA^{i-1}Bu(t - \tau_1) + \cdots + CBu(t - \tau_1) + CA^{i-1}Fr
\]

(5)

If we put all the derivatives of the output equation together in a matrix form we will attain

\[
Y_{0,y}(t - \tau_1) = Ox(t - \tau_1) + Hu_0(t - \tau_1) + H_1r \tag{6}
\]

with

\[
Y_{0,y}(t - \tau_1) \triangleq \begin{bmatrix} y(t - \tau_1) \\
y^{(1)}(t - \tau_1) \\
\vdots \\
y^{(\gamma)}(t - \tau_1) \end{bmatrix} \\
U_{0,y}(t - \tau_1) \triangleq \begin{bmatrix} u(t - \tau_1) \\
u^{(1)}(t - \tau_1) \\
\vdots \\
u^{(\gamma)}(t - \tau_1) \end{bmatrix}
\]

(7)

In (6), \( O \) is the observability matrix and \( H_1 \) is the Toeplitz matrix obtained from (5). In addition, the coefficient matrix of the reference trajectory has the following form

\[
H_1 \triangleq \begin{bmatrix} Ch_1 \\
Ce^{A\tau_1} \\
\vdots \\
Ce^{A\gamma\tau_1} \\
A^{\gamma-1} \end{bmatrix}
\]

(8)

In (6), the delayed states of the system – that is, \( x(t - \tau_1) \), are formulated as a function of the input, output, their derivatives up to the \( \gamma \)-th derivative and the reference trajectory at time \( t - \tau_1 \).

From Assumption 3, only \( \lambda \) derivatives of the input is known to the user. Hence, it is not possible to directly obtain \( x(t - \tau_1) \) from (6). We, therefore, define \( P_0 = I \) and

\[
P_i = \prod_{j=0}^{\min(\lambda-1,i+1)} P_{ij} \tag{9}
\]

If we select \( P_{ij} \) and \( P_{ij} \) as follows, pre-multiplication of the \( i \)-th derivative of the output equation by \( \prod_{j=0}^{i-1} P_i \) will remove the unknown values from the \( i \)-th derivative of output.

- The matrix \( P_{ij} \) is the projection matrix onto the left null-space of \( D^*(\prod_{k=0}^{j-1} P_kCA^{i-1}F) \), where \( D^* \in \{0, I\} \) is the complement of \( D \) – that is, \( D^* + D = I \) all the time.
- For \( j \leq \lambda \), \( P_{ij} = I \) and for \( j = \lambda + 1 \) where \( i > j \), \( P_{ij} \) is the projection onto the left null-space of \( (P_{ij} \prod_{k=0}^{\lambda} P_kCA^{i-1}B) \).

Now, consider a matrix

\[
M \triangleq \begin{bmatrix} P_0 & 0 & 0 & 0 \\
0 & P_1P_0 & 0 & 0 \\
0 & 0 & \ddots & 0 \\
0 & 0 & 0 & \prod_{i=0}^{\lambda-1} P_i 
\end{bmatrix}
\]

(10)
and pre-multiply it in (6) to eliminates the unknown values of the input derivatives and the reference trajectory. Hence

\[ MY(t - \tau) = M Ox(t - \tau) + MHu_{\tau}(t - \tau) + MHr \]  

in which the only unknown value is \( x(t - \tau) \).

**Theorem 1:** In a system of form (1) and under Assumptions 3 and 4, the delay-incorporating user-observable subspace is of the form

\[ O_H^\triangle = R((e^{-\delta T}I)\gamma (MO)^T P_{T_1}) \]  

where \( M \) is from (10) and \( P_{T_1} \) is from (18).

**Proof:** Since in general the delay is small, we consider \( \tau_1^2 \) to be negligible, hence

\[ u(t) = u(t - \tau) + \tau_1 \dot{u}(t - \tau) \]  

(12)

Note that to make the results more precise, it is straightforward to model the current state as a larger series of previous states and modify the rest of the results as per need.

Under (13), the states of a continuous time system (1) evolve as

\[ x(t) = e^{At} x(t - \tau) + c \]  

where

\[ c = \int_{t-\tau}^{t} e^{A(t-r)} \begin{bmatrix} B & F \end{bmatrix} \begin{bmatrix} u(r) \\ r \end{bmatrix} \, dr \]  

(14)

By introducing the variables

\[ \theta_0 \triangleq (e^{A\tau} - I) A^{-1} B \]  

\[ \theta_1 \triangleq ((e^{A\tau} - I) A^{-1} - \tau_1 I) A^{-1} B \]  

\[ \theta_2 \triangleq (e^{A\tau} - I) A^{-1} F \]  

(15)

From (13)-(16), we can write

\[ x(t - \tau) = e^{-\delta T} x(t) - e^{-\delta T} \sum_{k=0}^{1} \theta_k u^{(k)}(t - \tau) - e^{-\delta T} \theta_2 r \]  

(17)

We can combine (11) and (17) to formulate \( x(t) \) as a function of the input, output and their derivatives at time \( t - \tau \). As, new unknown \( u(t - \tau) \), \( \dot{u}(t - \tau) \), and \( r \) may arise, we introduce

\[ P_{T_1} \triangleq \sum_{k=0}^{1} P_{T_1, k} P_{T_1, r} \]  

(18)

where \( P_{T_1, k}, P_{T_1, r} \) and \( P_{T_1, r} \) are defined as follows:

- The matrix \( P_{T_1, r} \) is a projection onto the left null-space of \( D^T (MOe^{-\delta T} \theta_1) \).
- For \( j \leq k \), \( P_{T_1, r} \) is an identity matrix and it is a projection onto the left null-space of \( \left( \bigoplus_{k=0}^{1} P_{T_1, k} P_{T_1, r} \right) (MOe^{-\delta T} \theta_2) \) otherwise.

From (17) and (18), we can rewrite (11) as

\[ P_{T_1} MY_{0,y}(t - \tau) = P_{T_1} MOe^{-\delta T} x(t) - C_{known} \]  

(19)

where

\[ C_{known} = P_{T_1} e^{-\delta T} \theta_0 u(t - \tau) + P_{T_1} e^{-\delta T} \theta_1 \dot{u}(t - \tau) + P_{T_1} e^{-\delta T} \theta_2 r \]  

(20)

Hence, the combination of \( x(t) \) which spans \( R((P_{T_1} MOe^{-\delta T} \tau)^T) \) can be reconstructed from \( Y_{0,y}(t - \tau) \) and \( U_{0,x}(t - \tau) \). Therefore, from (4), Theorem 1 is proved.

**Procedure:** The following steps are required to calculate the delay-incorporating user-observable subspace, \( O_H^\triangle \):

- Determine matrices \( O, H, \) and \( H_t \) and calculate the value of \( \theta_0 - \theta_2 \) from (16).
- Obtain \( P_t \) from (9) and \( P_{T_1} \) from (18).
- Determine \( M \) from (10).
- Determine the delay-incorporating user-observable subspace from (12).

**Corollary 1:** A delay-incorporating user-observable space is also user observable.

**Proof:** By definition, the user-observable space is the space which is spanned by the combination of the current states which are known to the user at the current time, for \( t = 0 \).

From (11), the user-observable subspace can be formulated as

\[ O_H^\triangle \triangleq R((MO)^T) \]  

We also have the equation of \( O_H^\triangle \) from (12).

Under Assumption 2, the matrix \( A \) is of full rank, hence \( R((e^{-\delta T}I)^T(MO)^TP_{T_1}^T) = R((MO)^TP_{T_1}^T) \). In addition, for random matrices \( N \) and \( Q \) of compatible dimensions, we have \( R(NQ) \subseteq R(N) \). Hence

\[ O_H^\triangle \subseteq R((MO)^T) \]  

which proves that \( O_H^\triangle \subseteq O_H \).

**3.2 Delay-incorporating user-predictable subspace**

From Definition (2), the delay-incorporating user-predictable space is the space which can be spanned at time \( t \) based on the information available on \( x(t + \tau) \). As in Section 3.1, we can write the upcoming states as a function of \( Y_{0,y}(t - \tau) \) and \( U_{0,x}(t - \tau) \).

**Theorem 2:** In a system of form (1) and under Assumption 3, the delay-incorporating user-predictable subspace is of the form

\[ P_{H}^\triangle \triangleq R((e^{-\delta T}x(t + \tau)\tau^T)(MO)^T P_{T_1} P_{T_1}^T) \]  

where \( P_{T_1} \) is from (27), \( P_{T_1} \) is from (18) and \( M \) is from (10).

**Proof:** From (19) and

\[ x(t) = e^{-\delta T} x(t + \tau) - e^{-\delta T} \sum_{i=0}^{\tau} \delta_i u(t)(n) - e^{-\delta T} \delta_0 r \]  

(21)

we can write

\[ \begin{align*}
\delta_0 & \triangleq (e^{A\tau} - I) A^{-1} B \\
\delta_1 & \triangleq ((e^{A\tau} - I) A^{-1} - \tau_1 I) A^{-1} B \\
\delta_2 & \triangleq (e^{A\tau} - I) A^{-1} F
\end{align*} \]  

(22)

where \( \delta_0, \delta_1, \delta_2 \) are defined as above.
By pre-multiplying (26) by

\[ P_j = \prod_{k=0}^{1} P_{x_j}P_{x_j} \]  

(27)

we can remove all unknown values from it. In (27),

- The matrix \( P_{x_j} \) is a projection onto the left null-space of \( D^j(P_{x_j}MO) e^{-\gamma(t+\tau)} \).
- For \( j = \lambda \), \( P_{x_j} \) is an identity matrix and it is a projection onto the left null-space of \( (\prod_{k=0}^{1} P_{x_j}P_{x_j}MO) e^{-\gamma(t+\tau)} \) otherwise.

Hence, the functional of the upcoming states of the system, \( x(t+\tau) \), which span the row space of \( P_{x_j}P_{x_j}MO e^{-\gamma(t+\tau)} \) can be reconstructed by the user by time \( t \).

\[ \square \]

Procedure: The steps that are required to calculate the delay-incorporating user-predictable subspace, \( P^*_H \), are as follows:

- Obtain all the required matrices to determine \( O^*_H \).
- Obtain \( \delta_0 - \delta_2 \) from (25).
- Obtain \( P_{x_j} \) from (27).
- Determine the delay-incorporating user-predictable subspace from (23).

\[ \square \]

Corollary 2: A delay-incorporating user-predictable space is also delay-incorporating user-observable.

\[ \square \]

Proof: As in the proof in Corollary 1, if is straightforward to show that with \( A \) being a full rank matrix

\[ P^*_H \triangleq R((e^{-\gamma(t+\tau)})^T(MO)^TP_{x_j}^TP_{\tau}^T) \]

\[ = R((e^{-\gamma(t)})^T(MO)^TP_{x_j}^TP_{\tau}^T) \]

\[ \leq R((e^{-\gamma(t)})^T(MO)^TP_{x_j}^TP_{\tau}^T) \]

which proves that \( P^*_H \subseteq O^*_H \).

Corollary 3: A delay-incorporating user-predictable space is also user predictable.

\[ \square \]

Proof: Consider \( \tau_1 = 0 \), hence \( P_{\tau_1} = I \) and from (23), \( P_H \) can be formulated as

\[ P^*_H \triangleq R((e^{-\gamma(t)})^T(MO)^TP_{\tau_1}^T) \]

As in Corollaries 1 and 2, it is trivial to show that \( P^*_H \subseteq P_H \).

3.3 Validation of the displayed information

In Section 2, we stated that for safety-critical systems under human or shared control, the user-interface must provide the user with information that results in a delay-incorporating user-observable and a delay-incorporating user-predictable tasks. Hence, we can introduce the following proposition.

Proposition 1: In order for a user to be able to accomplish a desired task in a safety-critical condition for a system of form (1) and under Assumptions 1–5, the following inclusion is necessary

\[ T \subseteq P^*_H \]

(29)

where \( P^*_H \) is the delay-incorporating user-predictable subspace, formulated in (23).

4 Example

We consider a remotely driven point mass car modelled as a double integrator and stabilised to have poles on \(-2\) and \(-3\). The system matrices are

\[ A = \begin{bmatrix} 0 & 1 \\ -2 & -3 \end{bmatrix}, \quad B = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \]

(30)

Our goal is to evaluate whether for such a system the displays (which measure the position or the velocity of the car) are effective to accomplish a desired task, when the processing delay is \( \tau_1 = 0.2 \) [39].

We consider two cases, (1) a user who controls the system via a known force with known constant rate – that is, all derivatives of the input are known and (2) a user whose input to the system is complicated and random, thus, has no knowledge about input derivatives – that is, \( \lambda = 0 \). For both cases, we consider \( \gamma = 1 \).

Our desired task is stopping at a stop sign, hence, we can define the task space as

\[ T = R \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \]

which spans \( \mathbb{R}^2 \).

4.1 Delay-incorporating user-observable subspace

It is first required to calculate the delay-incorporating user-observable subspace for different measurements of states available to the user.

From (12), for \( \lambda = \infty \), we can obtain \( M = I \) and \( P_{\tau_1} = I \). Hence

\[ O^*_H|_{\lambda=\infty} = R(C^T) \ominus R((e^{-\gamma(t)})^T O^T) \]

(31)

Also, for \( \lambda = 0 \), we can obtain \( M = I \), therefore

\[ O^*_H|_{\lambda=0} = R(C^T) \ominus R((e^{-\gamma(t)})^T O^T P_{\tau_1}^T) \]

(32)

From (31) and (32), for either of the two different displays including a GPS with \( C = [1 \ 0] \) and a speedometer with \( C = [0 \ 1] \), we can show that \( O^*_H|_{\lambda=\infty} \) spans \( \mathbb{R}^2 \).

In addition, when \( \lambda = 0 \), with either of the measurements in the display we can obtain

\[ P_{\tau_1} = \begin{bmatrix} 0.9919 & 0.0899 \\ 0.0899 & 0.0081 \end{bmatrix} \]

hence, \( O^*_H|_{\lambda=0} = \mathbb{R}^2 \).

The results state that for such a system, regardless of the type of the measurements and the complexity of users’ input, the user can reconstruct both states of the system.

4.2 Delay-incorporating user-predictable subspace

For \( \tau = 0.1 \), we calculate the delay-incorporates user-predictable subspace of this system for different measurements of states provided in the display.

From (23), for \( \lambda = \infty \), we can obtain \( P_{\tau_1} = I \), hence

\[ P^*_H|_{\lambda=\infty} = R((e^{-\gamma(t+\tau)})^T O^T) \]

(33)

Also, for \( \lambda = 0 \) from (23)

\[ P^*_H|_{\lambda=0} = R((e^{-\gamma(t+\tau)})^T O^T P_{\tau_1}^T) \]

(34)

From (33), we can obtain \( P^*_H|_{\lambda=\infty} = \mathbb{R}^2 \) with either the GPS or the speedometer.

When \( \lambda = 0 \), for either of the displays,

\[ P_{\tau_1} = \begin{bmatrix} 0.0881 & -0.0899 \\ -0.0899 & 0.9919 \end{bmatrix} \]

hence, \( P^*_H|_{\lambda=0} = \emptyset \). This states that, with a complicated input, the user can reconstruct no combination of the states \( x(t+\tau) \) at time \( t \).
The results above can help the reader understand Corollary 2 better, as it is clear that in all of the above cases, the delay-incorporating user-predictable space is a subset of the delayed incorporated user-observable space.

We now consider $\lambda = 0$ for the case of having no processing delay, $\tau_1 = 0$. We thus can obtain the user-predictable subspace to be

$$P_H = \mathbb{R} \left( \begin{pmatrix} 1.0000 \\ -0.0526 \end{pmatrix} \right)$$

for either of the displays. On the basis of Corollary 3, the delay-incorporating user-predictable space is always a subset of the user-predictable space which we also have shown it to be the case in this example.

The result of having no delay shows that not considering the processing delay can result in a larger user-predictable subspace. Overlooking this delay can mislead the designer to misjudge the capability of the user to accomplish a task; that is, by ignoring the delay, the designer might find the user capable of accomplishing the task, while, because of the existence of the processing delay, the space which is predictable by the user may not include the task space or even is empty. Thus, for safety critical systems, it is not safe to simply ignore this value as it may result in hazardous outcomes.

### 4.3 Task accomplishment

With any of the suggested displays, when $\lambda = \infty$, both the delay-incorporating user-observable and the delay-incorporating user-predictable spaces span $\mathbb{R}^2$. Hence, $T \subset P_{H} \times \lambda = \infty$. This means, regardless of the displayed information, if the pattern of changes of the user’s input is all clear to the user (i.e. the user has knowledge about his/her own input to the system and all its derivatives), it might be possible for the user to stop at a stop sign. As an example, consider a user who enters a constant value input to the system by applying a constant amount of pressure on the brake. In this case, not only the input is known to the user, it is also known that this input is not changing over time.

On the other hand, it is clear that $T \not\subset P_{H} \times \lambda = 0$ for either of the displays. Hence, under the Assumption 6, for a complicated input to the system, neither the GPS nor the speedometer are effective for a human to control the velocity of the mass.

For this example, although not having processing delay is helpful in expanding the user predictable space, it still does not help with task accomplishment.

In summary, we could show when the input and all its derivatives are known by the user, the user is capable of observing and predicting the states which are involved in the task. On the other hand, when the user does not have a knowledge about the input derivatives, he may not be able to predict the task. Hence, overall, we can see that for a car modelled as a stable point mass vehicle, acceptance or rejection of the display depends on the degree of the knowledge of the user about his own input to the system. This is due to the fact that, based on the theory of SA, this delay-incorporated user-predictability of the task is necessary for task accomplishment.

### 5 Conclusions

In this paper, we presented a framework for systems under shared control to obtain a necessary condition for evaluating the information content of the user-interfaces of the safety-critical systems. This framework incorporates both the low-level control and reference tracking. We considered systems in which the environment does not provide the user with any information. We also focused on uni-modal displays containing only visual modality.

For safety-critical LTI systems, two novel subspaces, the delay-incorporating user-observable subspace, $O^*_{H}$, and the delay-incorporating user-predictable subspace $P^*_{H}$ were formulated and were compared to the task subspace for a feasible task. If the task subspace does not lie in the relevant space, then the user-interface is incorrect, meaning that there exist a possibility that the user cannot accomplish the desired task with the given user-interface.

Furthermore, we considered a specific category of systems in which the user-interface was the only source of information for the user. Incorporating the effect of information from the environment on the required information content of the user-interface is an important work which is necessary in order to make our framework more applicable to realistic cases. Another important modification to our work can be evaluating the information content of user-interfaces in the presence of uncertainties and noisy measurements. Clearly, having uncertain measurements and noisy derivatives is very common for real systems and it is necessary that we modify our framework to become more suitable for real-world applications.

Other interesting pieces of the further research are evaluating the direct effect of mental-model on situation awareness and also extending the framework to systems with multi-modal displays by assigning proper weight to measurements from various sources. In addition, incorporating the processing delay and considering the differences between the amount of this delay for different types of the measurements is a worthy extension to the work.

### 6 Acknowledgments

This work was supported by NSERC.

## 7 References

1. Jamieson, G., Vicente, K.: ‘Designing effective human-automation-plant interfaces: a control-theoretic perspective’, Human Factors, 2005, 47, (1), pp. 12–34
2. Sheridan, T.: ‘Telerobotics, automation, and supervisory control’ (MIT Press, Cambridge, MA, 1992)
3. Cummings, M., Thornburg, K.: ‘Paying attention to the man behind the curtain’, IEEE Pervasive Comput., 2011, 10, pp. 58–62
4. Endsley, M.: ‘A theory of situation awareness in dynamic systems’, Hum. Factors, 1995, 37, (2), pp. 32–64
5. Endsley, M.: ‘Situation models: an avenue to the modeling of mental models’, 14th Triennial Congress of the Int. Ergonomics Association and the 44th Annual Meeting of the Human Factors and Ergonomics Society, Santa Monica, CA, USA, 2000
6. Endsley, M.R.: ‘Designing for situation awareness: an approach to user-centered design’ (Taylor & Francis, US, 2003)
7. McRuer, D., Weir, D.: ‘Theory of manual vehicular control’, Ergonomics, 1969, 12, (4), pp. 599–633
8. McRuer, D., Allen, R., Weir, D., Klein, R.: ‘New results in driver steering control’, Hum. Factors, 1977, 19, (4), pp. 381–397
9. Hess, R., Mohadjerladeh, A.: ‘A control theoretic model of driver steering behaviour’, IEEE Control Syst. Mag., 1990, 10, (5), pp. 3–8
10. Hess, R.: ‘Model for human and motion cues in vehicular control’, J. Guid. Control Dyn., 1990, 13, (3), pp. 476–482
11. Chen, L., Galip Ulsoy, A.: ‘Identification of a driver steering model and model uncertainty, from driving simulator data’, J. Dyn. Syst. Meas. Control, 2001, 123, (4), pp. 623–629
12. Gabibulayev, M., Ravani, B.: ‘A stochastic form of a human driver steering dynamics model’, J. Dyn. Syst. Meas. Control, 2007, 129, (3), pp. 322–336
13. Kleinman, D., Baron, S., Levison, W.: ‘An optimal control model of human response Part I: theory and validation’, Automatica, 1970, 6, (3), pp. 357–369
14. Kleinman, D., Baron, S., Levison, W.: ‘A control theoretic approach to manned-vehicle systems analysis’, IEEE Trans. Autom. Control, 1971, 16, (6), pp. 824–832
15. Gai, E.G., Curry, R.E.: ‘A model of the human observer in failure detection tasks’, IEEE Trans. Syst. Man Cybern., 1976, SMC-6, (2), pp. 85–94
16. Werewienke, P.: ‘Model of the human observer and decision-maker theory and validation’, Automatica, 1983, 19, (6), pp. 693–696
17. Eskandari, N., Wang, Z.I., Dumont, G.: ‘Modeling the user as an observer to determine display information requirements’, IEEE Int. Conf. Systems, Man Cybernetics (SMC, 2013), 2013, pp. 267–272
18. Eskandari, N., Oishi, M.: ‘Computing observable and predictable subspaces to evaluate user-interfaces of control systems under shared control’, Prog. of the IEEE Conf. on Systems, Man and Cybernetics, Tokyo, Japan, October 2011, pp. 2803–2808
19. Aboky, C., Vivaldi, J.: ‘Observability for linear systems with unknown input’, Proc. of the IEEE Conf. on Decision and Control, Sydney, Australia, December 2000, pp. 3797–3798
20. Thrun, H., Fernando, T., Nahavandi, S.: ‘Design of reduced-order functional observers for linear systems with unknown inputs’, Asian J. Control, 2004, 6, (4), pp. 514–520
21. Fernando, T., MacDougall, S., Steeram, V., Thrun, H.: ‘Existence conditions for unknown input functional observers’, Int. J. Control, 2013, 86, (1), pp. 22–28
22. Darouch, M.: ‘On the functional observers for linear descriptor systems’, Syst. Control Lett., 2012, 61, (3), pp. 427–434
23 Marx, B., Koenig, D., Ragot, J.: ‘Design of observers for Takagi-Sugeno descriptor systems with unknown inputs and application to fault diagnosis’, IET Control Theory Appl., 2007, 1 (5), pp. 1487–1495
24 Guan, Y., Saif, M.: ‘A novel approach to design of unknown-input observers’, IEEE Trans. Autom. Control, 1991, 36 (5), pp. 632–635
25 Hou, M., Muller, P.: ‘Design of observers for linear systems with unknown inputs’, IEEE Trans. Autom. Control, 1992, 37 (6), pp. 871–875
26 Boukhobza, T., Hamelin, F., Martinez, S.: ‘State and input observability for structured linear systems: a graph-theoretic approach’, Automatica, 2007, 43 (7), pp. 1204–1210
27 Hou, M., Patton, R.: ‘Input observability and input reconstruction’, Automatica, 1998, 34 (6), pp. 789–794
28 Pina, L., Botto, M.: ‘Simultaneous state and input estimation of hybrid systems with unknown inputs’, Automatica, 2006, 42 (5), pp. 755–762
29 Ortuena, R., Marx, B., Ragot, J., Maquin, D.: ‘On the simultaneous state and unknown input estimation of complex systems via a multiple model strategy’, IET Control Theory Appl., 2009, 3 (7), pp. 877–890
30 Kalman, R.: ‘On the general theory of control systems’,IRE Trans. Automat. Control, 1959, 4 (3), p. 110
31 Luenberger, D.: ‘Observing the state of a linear system’, IEEE Trans. Military Electron., 1964, 8, (2), pp. 74–80
32 Luenberger, D.: ‘An introduction to observers’, IEEE Trans. Automat. Control, 1971, 16 (6), pp. 596–602
33 Basile, G., Marro, G.: ‘On the observability of linear time-invariant systems with unknown inputs’, J. Optim. Theory Appl., 1969, 3, (6), pp. 410–415
34 Eskandari, N., Oishi, M., Wang, Z.J.: ‘Observability analysis of continuous-time LTI systems with limited derivative data’, Asian J. Control, 2014, 16 (2), pp. 623–627
35 Billings, C.: Aviation automation: the search for a human-centered approach’ (Erlbaum, Hillsdale, NJ, 1997)
36 Parasuraman, R., Sheridan, T., Wickens, C.: ‘A model for types and levels of human interaction with automation’, IEEE Trans. Syst. Man Cybern. A. Syst. Humans, 2000, 30 (3), pp. 286–297
37 Sherry, L., Feary, M., Polson, P., Palmer, E.: ‘What’s it doing now?: taking the covers off autopilot behavior’. Eleventh Int. Symp. on Aviation Psychology, Columbus, OH, USA, 2001
38 Macadam, C.C.: ‘Understanding and modeling the human driver’, Veh. Syst. Dyn., 2003, 40, (1-3), pp. 101–134
39 Hosman, R., Stassen, H.: ‘Pilot’s perception in the control of aircraft motions’, Control Eng. Pract., 1999, 7, (11), pp. 1421–1428
30 Eskandari, N., Dumont, G.A., Wang, Z.J.: ‘An observer/predictor based model of the user for attaining situation awareness’, IEEE Trans. Hum.-Mach. Syst., submitted
41 Ayres, T., Lau, E., Schmidt, R., Young, D.: ‘Operator experience and accident risk’, Proc. Human Factors Ergon. Soc. Annu. Meet., 40, (18), 1996, pp. 947–951
42 Donmez, B., Cummings, M., Graham, H.: ‘Auditory decision aiding in supervisory control of multiple unmanned aerial vehicles’, Hum. Factors, J. Hum. Factors Ergon. Soc., 2009, 51, (5), pp. 718–729
43 Degani, A., Heymann, M.: ‘Formal verification of human-automation interaction’, Hum. Factors, 2002, 44, (1), pp. 28–43