Bounded Sensor Failure Tolerant Supervisory Control [⋆]

Kurt Rohloff [*]

[*] *Raytheon BBN Technologies, 10 Moulton St., Cambridge, MA 02138, USA (e-mail: krohloff@bbn.com)*

Abstract: This paper discusses problems related to partial observation supervisory controllers with possibly faulty sensors in the framework of discrete-event systems. At initialization all controller sensors are operational such that all sensors correctly communicate their event observations to the controller. Sensor failures are unobservable. After a sensor fails, it sends no signals to the controller. Depending on the sensor failure dynamics, the controlled system could exhibit a bounded range of behaviors. We define languages that respectively define the minimal and maximal sets of behaviors that could be exhibited by a controlled system with faulty sensors. We introduce bounded discrete-event supervisory control problems for faulty-sensor control systems. We use a construction to test for the existence of controllers with faulty sensors for two different control scenarios. We discuss how to synthesize these controllers using standard supervisory control methods.

Keywords: Supervisory control, discrete-event systems, fault tolerance, partial observation, sensor failure.

1. INTRODUCTION

When designing a controller for a system to match a given specification it is generally desirable in safety-critical applications for the controller to be fault tolerant. That is, it is desirable to design controllers in a redundant manner such that even if the controller fails partially, it will still be able to achieve its control objective, or at least not fail catastrophically. This area of research, called Fault Tolerant Control (FTC), has been active in several branches of control theory (Blanke et al. (2003); Patton (1997)).

There has been some research in fault-tolerant control for discrete-event systems (Blanke et al. (2003); Dumitrescu et al. (2004); Girault and Rutten (2004); Jensen (2003)). However, partial-observation supervisory controllers, as introduced in Lin and Wonham (1988), have traditionally been designed with the assumption that the controllers are fault-free. The standard assumption of controller (and controller sensor) infallibility may not be reasonable over the full life-cycle of a control system due to the natural deterioration of control systems over time. For instance, control circuitry may degenerate as a control system ages, a control actuator may become stuck, or sensors may fail. These partial control system failures may alter the abilities of the control system.

Our work in this paper builds off our previous work in Rohloff (2005) where we introduced the concept of faulty-sensor control, a version of observability for systems with faulty sensors called sensor failure observability. and introduced the $\overrightarrow{G}$ construction to test sensor failure observability. There has been some related work including Sanchez and Montoya (2006); Ushio and Takai (2009); Xu and Kumar (2009) which investigate other approaches to control with faulty sensors. Also relevant is the prior work in Paoli et al. (2011) which looks at issues related to diagnosis with faulty sensors.

In Sanchez and Montoya (2006) a formal method is proposed based on the parallel operation of multiple supervisory controllers to avoid "disaster" states under observability failure where single event sensors may fail. Blocking is only considered in Sanchez and Montoya (2006) before sensor failures occur.

In this paper, we apply existing supervisory control techniques to the problem of supervisory control with sensor failure. This is stated as being an open problem in Sanchez and Montoya (2006). Additionally, we go beyond the safe supervisory control problem by formulating a notion of observability for faulty sensor systems and we consider control scenarios where both exact and non-blocking behavior is required. This approach to sensor failure supervisory control was originally formulated in the preliminary conference paper Rohloff (2005), which was developed independently of Sanchez and Montoya (2006).

As an illustration of the challenge of supervisory control with faulty sensors, one might think that for there to exist a supervisory control system that is tolerant to single sensor failures, one could ensure that for all $\sigma \in \Sigma_o$, $\mathcal{L}_m(H)$ is observable with respect to $\mathcal{L}(G)$, $\Sigma_o \setminus \{\sigma\}$ and Σ_c. That is, one might expect that if for a specification H and system G that if any one event $\sigma \in \Sigma_o$ is made unobservable during control operation, but the specification $\mathcal{L}_m(H)$ is always observable with respect to any $\Sigma_o \setminus \{\sigma\}$, then there would exist a nonblocking controller S tolerant to single sensor failures such that

[⋆] This research was supported in part by the NSF grant CCR 00-85917 ITR.

the controller behavior matches $\mathcal{L}_m(H)$. This would be a valid statement if one could ensure that sensors fail only at initialization and one has foreknowledge about which sensor fails. Unfortunately, this is generally not the case. Consider the following example.

Example 1. Consider the system automaton G and the specification automaton H seen in Figure 1.

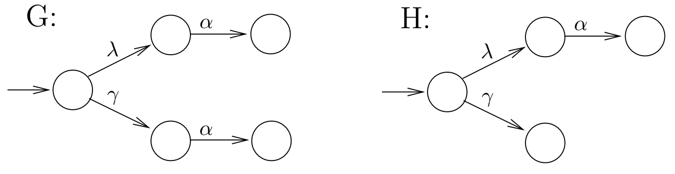

Fig. 1. The system automaton G and the specification automaton H for Example 1.

Let $\Sigma_c = \{\alpha\}$. If $\Sigma_o = \{\lambda\}$, the proper control action at initialization would be to disable α. Similarly, if $\Sigma_o = \{\gamma\}$, then the proper control action would be to enable α at initialization. However, if $\Sigma_o = \{\gamma, \lambda\}$, and if either the sensor for γ or λ may fail at initialization, and the controller can have no direct observations of sensor failure, then there is no correct initial control action. Therefore, it is not possible to synthesize a controller with possibly faulty sensors for this example when $\Sigma_o = \{\gamma, \lambda\}$ to match the specification $\mathcal{L}(H)$ even though for all $\sigma \in \Sigma_o$, $\mathcal{L}(H)$ is observable with respect to $\mathcal{L}(G)$, $\Sigma_o \setminus \{\sigma\}$ and Σ_c.

In Rohloff (2005) we exclusively focused on the use of the $\overrightarrow{G}$ and $\overrightarrow{H}$ constructions to identify controller existence properties with respect to the maximal behavior permitted by a controller under faulty sensor scenarios. (We now define this maximal behavior the exclusive language $\mathcal{L}^{\cup}(S\phi G)$.) The major contribution of this work are controller existence tests and controller synthesis methods for scenarios when the controlled behavior should be bound between minimal and maximal behaviors despite the existence of faulty sensors. Additionally, we use our previous $\overrightarrow{G}$ and $\overrightarrow{H}$ constructions from Rohloff (2005) and the standard framework and mechanisms from discrete-event supervisory control theory. Although we focus on a particular sensor failure model that we identified in our previous work in Rohloff (2005), our approaches generalize to other approaches by appropriately modifying the $\overrightarrow{G}$ and $\overrightarrow{H}$ constructions to match the assumed sensor failure dynamics.

The paper is structured as follows. Section 2 formalizes the behavioral properties and notations of control systems with faulty sensors. Section 3 formalizes the faulty sensor control scenarios that are analyzed in this paper. Section 4 presents an observability property for systems with faulty sensors. Section 5 discusses approaches to testing controller existence and performing controller synthesis for the bounded and matched faulty controller problems. Section 6 closes the paper with a review of the results contained herein and a brief discussion of how to generalize the identified results for other sensor failure dynamics.

2. FAULTY SENSOR SYSTEM DYNAMICS

As in Rohloff (2005), we assume that after a sensor fails, the sensor halts sending signals to the controller. Sensor failures are assumed to be sufficiently uncommon that it is valid to assume only one sensor will be failed at any given time.

We generalize the deterministic projection operation (originally $P : \Sigma^* \to \Sigma_o^*$) to the faulty sensor projection operation $P^f : \Sigma^* \to {\Sigma_o}^*$ where if a string $s \in \Sigma^*$ occurs in the system, the set $P^f(s)$ represents all strings that could be observed due to the occurrence of s.

Before formally defining $P^f(\cdot)$, let the projection $P_\sigma : \Sigma^* \to (\Sigma_o \setminus \{\sigma\})^*$ be defined the same as $P(\cdot)$ except that events in $\Sigma_o \setminus \{\sigma\}$ are retained in the projection instead of events in Σ_o. That is, for the empty event ϵ, $P_\sigma(\epsilon) = \epsilon$, and for a string of events s and an event γ,

$$P_\sigma(s\gamma) = \begin{cases} P_\sigma(s)\gamma & \text{if } \gamma \in \Sigma_o \setminus \{\sigma\} \\ P_\sigma(s) & \text{otherwise} \end{cases} .$$

Then, for a string $s \in \Sigma^*$, we define the set $P^f(s)$ as follows:

$$P^f(s) = \{P(s_1)P_\sigma(s_2) | s_1 s_2 = s, \sigma \in \Sigma_o.\} \tag{1}$$

For a controller $S(\cdot)$ with faulty sensors, any string in $P^f(s) \subseteq 2^{\Sigma_o^*}$ could be observed by the controller due to the occurrence of s. Suppose $t \in P^f(s)$ is the string nondeterministically observed by the controller due to the occurrence of s. Then, $S(t) \in 2^{\Sigma_c} \cup \Sigma_{uc}$ is the control action enforced by the controller due to the observation of t after s occurs in the system. As alluded to in prior work (Rohloff (2005); Sanchez and Montoya (2006); Ushio and Takai (2009); Xu and Kumar (2009)), even though a faulty-sensor supervisory controller may deterministically map observations to control actions, nondeterministic sensor failures cause the controller to operate in a nondeterministic manner due to the nondeterministic mapping of event occurrences to observations and the deterministic mapping of observations to control actions. As we show in this paper, we can use deterministic controllers to satisfy control objectives even if we have imperfect information about unobserved sensor failures and event occurrences due to these unobserved sensor failures.

The basis of our approach to controller existence testing and synthesis for faulty-sensor systems is to more explicitly account for faulty sensor dynamics which lead to nondeterministic mapping of event occurrences to control actions with a deterministic controller. To reinforce the fact that, due to different observation projections, the coupling of S with G under the assumption of faulty sensors is inherently different from the control coupling under the assumption of fault-free sensors denoted by S/G, we use $S\phi G$ to denote the composed system of a supervisory controller S with faulty sensors operating on G.

Unfortunately, due to the nondeterministic observation behavior of a faulty-sensor controller, the generated language of $S\phi G$ cannot be defined in the usual manner. For a string $s \in \mathcal{L}(G)$ there may be multiple possible control actions by the controller due to a nondeterministic observation of an occurrence of s. That is, if for two strings $t, t' \in P^f(s)$ such that $(\sigma \in S(t)) \wedge (\sigma \notin S(t'))$ and s is in the language generated by $S\phi G$, should $s\sigma$ be in the language generated by $S\phi G$?

This uncertainty motivates the need to define two classes of languages for faulty-sensor systems. We define *inclusive* languages to be the set of strings where there exists some faulty sensor observation that causes the controller to allow the string. Conversely, we define *exclusive* languages to be the set of strings accepted where all possible observations due to a string cause the controller to allow the string.

Definition 1. The *inclusive language generated by* $S\not\phi G$ and denoted by $\mathcal{L}^{\cup}(S\not\phi G)$ is defined recursively as follows:

- $\epsilon \in \mathcal{L}^{\cup}(S\not\phi G)$.
- $s\sigma \in \mathcal{L}^{\cup}(S\not\phi G)$ if and only if $s \in \mathcal{L}^{\cup}(S\not\phi G)$, $s\sigma \in \mathcal{L}(G)$ and $\exists t \in P^f(s)$ such that $\sigma \in S(t)$.

The *inclusive language marked by* $S\not\phi G$, denoted by $\mathcal{L}^{\cup}_m(S\not\phi G)$, is $\mathcal{L}^{\cup}(S\not\phi G) \cap \mathcal{L}_m(G)$.

Definition 2. The *exclusive language generated by* $S\not\phi G$ and denoted by $\mathcal{L}^{\cap}(S\not\phi G)$ is defined recursively as follows:

- $\epsilon \in \mathcal{L}^{\cap}(S\not\phi G)$.
- $s\sigma \in \mathcal{L}^{\cap}(S\not\phi G)$ if and only if $s \in \mathcal{L}^{\cap}(S\not\phi G)$, $s\sigma \in \mathcal{L}(G)$ and $\forall t \in P^f(s)$, $\sigma \in S(t)$.

The *exclusive language marked by* $S\not\phi G$, denoted by $\mathcal{L}^{\cap}_m(S\not\phi G)$, is $\mathcal{L}^{\cap}(S\not\phi G) \cap \mathcal{L}_m(G)$.

As may be intuitive, the exclusive language $\mathcal{L}^{\cap}(S\not\phi G)$ is always contained in the inclusive language $\mathcal{L}^{\cup}(S\not\phi G)$.

3. SENSOR FAILURE CONTROL SCENARIOS

Inclusive and exclusive languages are useful for specifying the maximum and minimum sets of behavior that could occur in a faulty sensor system despite the non-deterministic control dynamics due to sensor failures. This motivates us to define two faulty sensor supervisory control scenarios. The more general scenario, called the *Bounded Faulty-Sensor Supervisory Control Problem*, focuses on ensuring that the behavior of the controlled system with faulty sensors ($S\not\phi G$) is contained between lower and upper boundary languages, J and L respectively, no matter the failure dynamics.

Problem 1. The Bounded Faulty-Sensor Supervisory Control Problem: For a system G, a set of controllable events Σ_c, a set of observable events Σ_o and two languages $J = \overline{J}$, $L = \overline{L}$ such that $J \subseteq L \subseteq \mathcal{L}(G)$, find a supervisor S such that

$$\begin{aligned} J &\subseteq \mathcal{L}^{\cap}(S\not\phi G) \\ \mathcal{L}^{\cup}(S\not\phi G) &\subseteq L. \end{aligned} \tag{2}$$

A second control scenario is a special case of the bounded control scenario, called the *Matched Faulty-Sensor Supervisory Control Problem*, ensures that the behavior of the controlled system with faulty sensors ($S\not\phi G$) always matches the behavior of a language K no matter the failure dynamics, so that no deviance away from the specification behavior K is permitted.

Problem 2. The Matched Faulty-Sensor Supervisory Control Problem: For a system G, a set of controllable events Σ_c, a set of observable events Σ_o and a language $K = \overline{K} \subseteq \mathcal{L}(G)$, find a supervisor S such that

$$\mathcal{L}^{\cap}(S\not\phi G) = \mathcal{L}^{\cup}(S\not\phi G) = K. \tag{3}$$

Although Problems 1 and 2 are presented only in terms of generated languages, marked language versions of these problems exist where the faulty-sensor controllers should be non-blocking. We present results on the generated language bounded control problem and the marked non-blocking matched control problem in Section 5.

4. SENSOR FAILURE OBSERVABILITY

Due to the insufficiency of observability as a necessary and sufficient condition for fault-tolerant controller existence, we previously introduced an alternative version of observability called *observability with respect to sensor failure*, or *sensor failure observability* for short in Rohloff (2005). This property is useful to solve faulty sensor controller existence problems for the control scenarios in Section 3.

Definition 3. Rohloff (2005) Consider the set of controllable events Σ_c, the set of observable events Σ_o and the languages K and M such that $M = \overline{M}$. The language K is *sensor failure observable* with respect to M, $P^f(\cdot)$ and Σ_c if for all $t \in \overline{K}$ and for all $\sigma \in \Sigma_c$,

$$\begin{aligned} &\left[(t\sigma \notin \overline{K}) \wedge (t\sigma \in M)\right] \Rightarrow \\ &\qquad \left[{P^f}^{-1}\left[P^f(t)\right]\sigma \cap \overline{K} = \emptyset\right]. \end{aligned} \tag{4}$$

Similar to observability for standard supervisory control, the concept of sensor failure observability is part of the set of necessary and sufficient conditions for faulty-sensor controller existence for the matched faulty sensor control problem. The following theorem is a generalization a result previously shown in Rohloff (2005) to account for the newly define inclusive and exclusive languages.

Theorem 1. For a finite state automaton system G, a finite state automaton specification H such that $\mathcal{L}_m(H) \subseteq \mathcal{L}(G)$, a set of controllable events Σ_c and a set of observable events Σ_o with sensors that may fail there exists a non-blocking partial observation faulty sensor controller S such that $\mathcal{L}^{\cap}_m(S\not\phi G) = \mathcal{L}^{\cup}_m(S\not\phi G) = \mathcal{L}_m(H)$ and $\mathcal{L}^{\cap}(S\not\phi G) = \mathcal{L}^{\cup}(S\not\phi G) = \overline{\mathcal{L}_m(H)}$ if and only if the following conditions hold:

1. $\mathcal{L}_m(H)$ is controllable with respect to $\mathcal{L}(G)$ and Σ_{uc}.
2. $\mathcal{L}_m(H)$ is sensor failure observable with respect to $\mathcal{L}(G)$, Σ_o and Σ_c.
3. $\mathcal{L}_m(H)$ is $\mathcal{L}_m(G)$-closed.

The proof of this theorem is a variation on the proof of the controllability and observability theorem as originally discussed in Lin and Wonham (1988). For the sake of brevity, we do not show this proof here.

5. FAULTY SENSOR CONTROL EXISTENCE AND SYNTHESIS

This section focuses on properties of controller existence and synthesis to solve faulty sensor control problems. In Rohloff (2005) we introduced the $\overrightarrow{G}$ and $\overrightarrow{H}$ constructions from G and H to test sensor failure observability. We can use these constructions to test controller existence and synthesize controllers that solve variations of the faulty-sensor supervisory control Problems 1 and 2.

The goal of the constructions of $\overrightarrow{G}$ and $\overrightarrow{H}$ is that if there are two strings $t_1, t_2 \in \mathcal{L}(G) \cap \overline{\mathcal{L}_m(H)}$ and an event $\sigma \in \Sigma_c$ such that $t_1\sigma \in \overline{\mathcal{L}_m(H)}$ then we know that the properties $t_2\sigma \in \mathcal{L}(G) \setminus \overline{\mathcal{L}_m(H)}$ and $P^f(t_1) \cap P^f(t_2) \neq \emptyset$ hold. This example is a violation of sensor failure observability with respect to $\mathcal{L}(G)$, Σ_o and Σ_c. When $P^f(t_1) \cap P^f(t_2) \neq \emptyset$, it is possible for the sensors of the controllers to fail in such a way that the observation generated by t_1 in G and the observation generated by t_2 in G are identical. Further, because there is an event $\sigma \in \Sigma_c$ such that $t_1\sigma \in \overline{\mathcal{L}_m(H)}$ and $t_2\sigma \in \mathcal{L}(G) \setminus \overline{\mathcal{L}_m(H)}$, then it is possible that the correct control action after t_2 cannot be known due to possible observations of t_1 and t_2 with respect to sensor failure.

The basis of the $\overrightarrow{G}$ construction from G is to model how sensor failure dynamics affect the observations of a supervisory controller operating on G. For every string $s \in \mathcal{L}(G)$, there is a corresponding set of strings $P^f(s)$ that represent possible observations due to faulty sensors that could be generated from s. For a system G and a set of events Σ_o, the automaton $\overrightarrow{G}$ is constructed such that every string $\overrightarrow{s} \in \mathcal{L}(\overrightarrow{G})$ encodes both the underlying behavior of the system G that generates s and the sensor failure dynamics that would generate an observation $s^f \in P^f(s)$.

If there are n observable events $\Sigma_o = \{\sigma^1, \ldots, \sigma^n\}$, the $\overrightarrow{G}$ model of the system G has $n+1$ modes of operation with respect to sensor failure. In the initial mode of operation, mode 0, all sensors for observable events are operational. However, when the sensor for event $\sigma^i \in \{\sigma^1, \ldots, \sigma^n\}$ fails, the system then enters one of the other modes of operation where σ^i event occurrences are no longer observable. The underlying state transition behavior in G does not change despite any sensor failures, but the observability properties of events occurrences are altered between various modes of operation.

To model the sensor failure dynamics in $\overrightarrow{G}$, two sets of events $F^{\Sigma_o} = \{f^{\sigma^1}, \ldots, f^{\sigma^n}\}$ and $\Sigma_o^f = \{\sigma^{1f}, \ldots, \sigma^{nf}\}$ are defined where every observable event $\sigma^i \in \Sigma_o$ has the corresponding events $f^{\sigma^i} \in F^{\Sigma_o}$ and $\sigma^{if} \in \Sigma_o^f$. In the set F^{Σ_o}, f^{σ^i} models the failure of the sensor for event σ^i which drives a transition from mode 0 to mode i. When in mode i, σ^{if} events are used in place of σ^i events in order to model the altered observability of σ_i due to the mode switch.

We restrict our analysis and discussion to the scenario where sensor failures (i.e., events in F^{Σ_o}) are unobservable. However, it is feasible to generalize the our approaches to scenarios where some or all of the sensor failures are observable by making the corresponding events in F^{Σ_o} observable.

Taken together, the automata $\overrightarrow{G}$ and $\overrightarrow{H}$ are constructed to be augmented copies of G and H such that there exists a faulty-observation equivalent pair t_1, t_2 in G and H such that $P^f(t_1) \cap P^f(t_2) \neq \emptyset$ if and only if there are two strings $\overrightarrow{t}_1, \overrightarrow{t}_2 \in \overline{\mathcal{L}_m(\overrightarrow{G})}$ and $\overrightarrow{t}_1, \overrightarrow{t}_2 \in \overline{\mathcal{L}_m(\overrightarrow{H})}$ such that $P(\overrightarrow{t}_1) = P(\overrightarrow{t}_2)$. Furthermore, there are additional states d and d_m in $\overrightarrow{G}$ and $\overrightarrow{H}$ such that $t_1\sigma \in \overline{\mathcal{L}_m(H)}$ if and only if $\overrightarrow{t}_1\sigma \in \overline{\mathcal{L}_m(\overrightarrow{H})}$ and $t_2\sigma \in \mathcal{L}(G) \setminus \overline{\mathcal{L}_m(H)}$ if and only if $\overrightarrow{t}_2\sigma \in \mathcal{L}(\overrightarrow{G}) \setminus \overline{\mathcal{L}_m(\overrightarrow{H})}$ if $P(t) = P(\overrightarrow{t})$. This construction converts the sensor failure observability test of $\mathcal{L}_m(H)$ with respect to $\mathcal{L}(G)$, Σ_o and Σ_c into an observability test of $\mathcal{L}_m(\overrightarrow{H})$ with respect to $\mathcal{L}(\overrightarrow{G})$, $\overrightarrow{\Sigma}_o$ and $\overrightarrow{\Sigma}_c$.

If a slight abuse of notation is used to extend the definition of $P(\cdot)$ over an expanded domain such that $P : \overrightarrow{\Sigma}^* \to \Sigma_o^*$, our controller existence results rely on the result that $P^f(\mathcal{L}_m(G)) = P(\mathcal{L}_m(\overrightarrow{G}))$ which we do not show for the sake of brevity.

5.1 Bounded Faulty Sensor Control

This section focuses on how the bounded faulty sensor controller existence and synthesis problems can be solved using the $\overrightarrow{G}$ construction. Suppose a system model G and minimum and maximum behavior specification automata A and E are given such that $\mathcal{L}(A) \subseteq \mathcal{L}(E) \subseteq \mathcal{L}(G)$ and the automata $\overrightarrow{A}$, $\overrightarrow{E}$, $\overrightarrow{G}$ are constructed from them and a set of observable events Σ_o and controllable events Σ_c. For a controller $\overrightarrow{S}$, $\mathcal{L}(\overrightarrow{A}) \subseteq \mathcal{L}(\overrightarrow{S}/\overrightarrow{G}) \subseteq \mathcal{L}(\overrightarrow{E})$ implies that $\mathcal{L}(A) \subseteq \mathcal{L}^{\cap}(\overrightarrow{S}\phi G)$ and $\mathcal{L}^{\cup}(\overrightarrow{S}\phi G) \subseteq \mathcal{L}(E)$.

Theorem 2. Suppose a system model G and minimum and maximum behavior specification automata A and E are given such that $\mathcal{L}(A) \subseteq \mathcal{L}(E) \subseteq \mathcal{L}(G)$ and the automata $\overrightarrow{A}$, $\overrightarrow{E}$, $\overrightarrow{G}$ are constructed from them and a set of observable events Σ_o and controllable events Σ_c. For any controller $\overrightarrow{S}$ such that $\mathcal{L}(\overrightarrow{A}) \subseteq \mathcal{L}(\overrightarrow{S}/\overrightarrow{G}) \subseteq \mathcal{L}(\overrightarrow{E})$, the same controller can be used such that $\mathcal{L}(A) \subseteq \mathcal{L}^{\cap}(\overrightarrow{S}\phi G)$ and $\mathcal{L}^{\cup}(\overrightarrow{S}\phi G) \subseteq \mathcal{L}(E)$.

Proof. We demonstrate this theorem in two parts. We start by showing through a proof by induction on the length of s that if $\mathcal{L}(\overrightarrow{A}) \subseteq \mathcal{L}(\overrightarrow{S}/\overrightarrow{G})$ then

$$(s \in \mathcal{L}(A)) \Rightarrow \left(s \in \mathcal{L}^{\cap}(\overrightarrow{S}\phi G)\right).$$

To start, suppose that $|s| = 0$. This implies that $s = \epsilon$. We assume without loss of generality that A and G are non-empty automata, so by definition $\epsilon \in \mathcal{L}(A)$ and $\epsilon \in \mathcal{L}^{\cap}(\overrightarrow{S}\phi G)$.

For the induction hypothesis, suppose that for $|s| \leq n$, $(s \in \mathcal{L}(A)) \Rightarrow \left(s \in \mathcal{L}^{\cap}(\overrightarrow{S}\phi G)\right)$.

Suppose that $|s| = n$ and for some event $\sigma \in \Sigma$, $s\sigma \in \mathcal{L}(A)$. By the definition of $\mathcal{L}(\cdot)$, $s \in \mathcal{L}(A)$, and from the induction hypothesis, $s \in \mathcal{L}^{\cap}(\overrightarrow{S}\phi G)$. Because $\mathcal{L}(A) \subseteq \mathcal{L}(G)$, $s\sigma \in \mathcal{L}(G)$.

If $\sigma \in \Sigma_{uc}$, then by the implicit assumption that $\overrightarrow{S}$ is admissible, then $s\sigma \in \mathcal{L}^{\cap}(\overrightarrow{S}\phi G)$.

If $\overrightarrow{P}(\cdot)$ is the projection that maps from events in $\overrightarrow{G}$ to $Sigma_o$, let $\overrightarrow{s}$ be any element of $\overrightarrow{P}^{-1}(s)$. If $\sigma \in \Sigma_c$, then $\overrightarrow{s}\sigma \in \mathcal{L}(\overrightarrow{A})$ by the construction of A. This implies that $\overrightarrow{s}\sigma \in \mathcal{L}(\overrightarrow{S}/\overrightarrow{G})$. Because $\overrightarrow{s}$ is any element of $\overrightarrow{P}^{-1}(s)$, then for any observation $s' \in P^f(s)$ due to the occurrence of s (which are represented by the failure dynamics encoded in the strings in $\overrightarrow{P}^{-1}(s)$), σ will be enabled after the occurrence of s. Hence, by the definition of $\mathcal{L}^{\cap}(\overrightarrow{S}\phi G)$, $s\sigma \in \mathcal{L}^{\cap}(\overrightarrow{S}\phi G)$.

We now show through a proof by induction on the length of s that if $\mathcal{L}(\overrightarrow{S}/\overrightarrow{G}) \subseteq \mathcal{L}(\overrightarrow{E})$ then

$$\Big(s \in \mathcal{L}^{\cup}(\overrightarrow{S}\phi G)\Big) \Rightarrow (s \in \mathcal{L}(E))$$

To start, suppose that $|s| = 0$. This implies that $s = \epsilon$. We assume without loss of generality that E and G are non-empty automata, so by definition $\epsilon \in \mathcal{L}(E)$ and $\epsilon \in \mathcal{L}^{\cup}(\overrightarrow{S}\phi G)$.

For the induction hypothesis, suppose that for $|s| \leq n$, $\Big(s \in \mathcal{L}^{\cup}(\overrightarrow{S}\phi G)\Big) \Rightarrow (s \in \mathcal{L}(E))$.

For the induction step, suppose that $|s| = n$ and there exists a σ such that $s\sigma \in \mathcal{L}^{\cup}(\overrightarrow{S}\phi G)$. This implies $s\sigma \in \mathcal{L}(G)$. By the control law, we know that $\overrightarrow{S}$ enables σ after observing some sensor failure observation of $t \in P^f(s)$. Because $P^f(\mathcal{L}_m(G)) = P(\mathcal{L}_m(\overrightarrow{G}))$ there exists a strings $\overrightarrow{s}$ such that $P(\overrightarrow{s}) = t \in P^f(s)$ and $\overrightarrow{s}\sigma \in \mathcal{L}(\overrightarrow{G})$. We therefore know that $\overrightarrow{S}$ enables σ after observing $t = P(\overrightarrow{s})$. Consequently, $\overrightarrow{s}\sigma \in \mathcal{L}(\overrightarrow{S}/\overrightarrow{G})$ and we therefore know that $\overrightarrow{s}\sigma \in \mathcal{L}(\overrightarrow{E})$.

From the construction of $\overrightarrow{E}$, $\overrightarrow{s}\sigma \in \mathcal{L}(\overrightarrow{E})$, implies that $s\sigma \in \mathcal{L}(E)$. ■

5.2 Matched Faulty Sensor Control

Given the $\overrightarrow{G}$ and $\overrightarrow{H}$ constructions, there exists a faulty sensor controller S such that $\mathcal{L}^{\cap}(S\phi G) = \mathcal{L}^{\cup}(S\phi G) = \overline{\mathcal{L}_m(H)}$ if and only if there exists a perfect sensor controller $\overrightarrow{S}$ such that $\mathcal{L}(\overrightarrow{S}/\overrightarrow{G}) = \mathcal{L}(\overrightarrow{H})$. This result is obtained with a faulty-sensor equivalent of the controllability and observability theorem developed from the results in Rohloff (2005) that:

- $\mathcal{L}_m(H)$ is controllable with respect to $\mathcal{L}(G)$ and Σ_{uc} if and only if $\mathcal{L}_m(\overrightarrow{H})$ is controllable with respect to $\mathcal{L}(\overrightarrow{G})$ and $\overrightarrow{\Sigma}_{uc}$ where $\overrightarrow{\Sigma}_{uc} = \overrightarrow{\Sigma} \setminus \overrightarrow{\Sigma}_c$.
- $\mathcal{L}_m(H)$ is $\mathcal{L}_m(G)$-closed if and only if $\mathcal{L}_m(\overrightarrow{H})$ is $\mathcal{L}_m(\overrightarrow{G})$-closed.

Matched faulty sensor existence can now be tested with the $\overrightarrow{G}$ and $\overrightarrow{H}$ constructions as a corollary of Theorem 1:

Corollary 3. Consider G and H such that $\mathcal{L}_m(H) \subseteq \mathcal{L}(G)$, a set of controllable events Σ_c and a set of observable events Σ_o. From G, H, Σ_c and Σ_o, construct $\overrightarrow{G}$, $\overrightarrow{H}$, $\overrightarrow{\Sigma}_c$ and $\overrightarrow{\Sigma}_o$ as discussed above. There exists a nonblocking faulty sensor controller S such that $\mathcal{L}_m^{\cap}(S\phi G) = \mathcal{L}_m^{\cup}(S\phi G) = \mathcal{L}_m(H)$ and $\mathcal{L}^{\cap}(S\phi G) = \mathcal{L}^{\cup}(S\phi G) = \overline{\mathcal{L}_m(H)}$ if and only if there exists a nonblocking perfect sensor controller $\overrightarrow{S}$ such that $\mathcal{L}_m(\overrightarrow{S}/\overrightarrow{G}) = \mathcal{L}_m(\overrightarrow{H})$.

An additional convenience of the $\overrightarrow{G}$ and $\overrightarrow{H}$ constructions and the constructive nature of the controllability and observability theorem is that if a nonblocking controller $\overrightarrow{S}$ is synthesized under the assumption of perfect sensors such that $\mathcal{L}_m(\overrightarrow{S}/\overrightarrow{G}) = \mathcal{L}_m(\overrightarrow{H})$, then the same controller can be used in the faulty-sensor case to ensure that $\mathcal{L}_m^{\cap}(\overrightarrow{S}\phi G) = \mathcal{L}_m^{\cup}(\overrightarrow{S}\phi G) = \mathcal{L}_m(H)$ and $\mathcal{L}^{\cap}(\overrightarrow{S}\phi G) = \mathcal{L}^{\cup}(\overrightarrow{S}\phi G) = \overline{\mathcal{L}_m(H)}$.

Theorem 4. Consider an automaton system model G, an specification automaton H such that $\mathcal{L}_m(H) \subseteq \mathcal{L}_m(G)$, a set of controllable events Σ_c and a set of observable events Σ_o corresponding to sensors that may fail. From G, H, Σ_c and Σ_o, construct $\overrightarrow{G}$, $\overrightarrow{H}$, $\overrightarrow{\Sigma}_c$ and $\overrightarrow{\Sigma}_o$ as discussed above. If a nonblocking controller $\overrightarrow{S}$ is synthesized such that $\mathcal{L}_m(\overrightarrow{S}/\overrightarrow{G}) = \mathcal{L}_m(\overrightarrow{H})$ and $\mathcal{L}(\overrightarrow{S}/\overrightarrow{G}) = \overline{\mathcal{L}_m(\overrightarrow{H})}$, then $\overrightarrow{S}$ can be used in the faulty-sensor situation such that $\mathcal{L}_m^{\cap}(\overrightarrow{S}\phi G) = \mathcal{L}_m^{\cup}(\overrightarrow{S}\phi G) = \mathcal{L}_m(H)$ and $\mathcal{L}^{\cap}(\overrightarrow{S}\phi G) = \mathcal{L}^{\cup}(\overrightarrow{S}\phi G) = \overline{\mathcal{L}_m(H)}$.

Proof. Because there exists a nonblocking controller $\overrightarrow{S}$ such that $\mathcal{L}_m(\overrightarrow{S}/\overrightarrow{G}) = \mathcal{L}_m(\overrightarrow{H})$ and $\mathcal{L}(\overrightarrow{S}/\overrightarrow{G}) = \overline{\mathcal{L}_m(\overrightarrow{H})}$, then $\mathcal{L}_m(\overrightarrow{H})$ is controllable with respect to $\mathcal{L}(\overrightarrow{G})$, and $\overrightarrow{\Sigma}_{uc}$, $\mathcal{L}_m(\overrightarrow{H})$ is observable with respect to $\mathcal{L}(\overrightarrow{G})$, $\overrightarrow{\Sigma}_o$ and $\overrightarrow{\Sigma}_c$, and $\mathcal{L}_m(\overrightarrow{H})$ is $\mathcal{L}_m(\overrightarrow{G})$-closed. Because $\mathcal{L}_m(H)$ is sensor failure observable with respect to $\mathcal{L}(G)$, Σ_o and Σ_c, $\mathcal{L}_m(H)$ is controllable with respect to $\mathcal{L}(G)$ and Σ_{uc}, and $\mathcal{L}_m(H)$ is $\mathcal{L}_m(G)$-closed.

It is now shown that $s \in \mathcal{L}^{\cap}(\overrightarrow{S}\phi G) \Rightarrow s \in \overline{\mathcal{L}_m(H)}$ through a proof by induction on the length of the string s.

For the induction hypothesis, suppose that $|s| = 0$ so $s = \epsilon$. Due to the definition of $\mathcal{L}^{\cap}(\overrightarrow{S}\phi G)$, $\epsilon \in \mathcal{L}^{\cap}(\overrightarrow{S}\phi G)$ and by the definition of the prefix-closure, $\epsilon \in \overline{\mathcal{L}_m(H)}$. Therefore, $\epsilon \in \mathcal{L}^{\cap}(\overrightarrow{S}\phi G) \Rightarrow \epsilon \in \overline{\mathcal{L}_m(H)}$

For the induction hypothesis it is assumed that $s \in \mathcal{L}^{\cap}(\overrightarrow{S}\phi G) \Rightarrow s \in \overline{\mathcal{L}_m(H)}$ if $|s| \leq n$.

For the induction step assume $|s| = n$. It is now shown that $s\sigma \in \mathcal{L}^{\cap}(\overrightarrow{S}\phi G) \Rightarrow s\sigma \in \overline{\mathcal{L}_m(H)}$.

First suppose that $s\sigma \in \mathcal{L}^{\cap}(\overrightarrow{S}\phi G)$ and $\sigma \in \Sigma_{uc}$. From the induction hypothesis, $s \in \overline{\mathcal{L}_m(H)}$. From the definition of controllability it must hold that $s\sigma \in \overline{\mathcal{L}_m(H)}$.

Now suppose that $s\sigma \in \mathcal{L}^{\cap}(\overrightarrow{S}\phi G)$ and $\sigma \in \Sigma_c$. This implies that $s \in \mathcal{L}^{\cap}(\overrightarrow{S}\phi G)$, $s\sigma \in \mathcal{L}(G)$ and for all $t \in P^f(s)$, $\sigma \in \overrightarrow{S}(t)$. The projection $P(s)$ is in $P^f(s)$ by definition, so $\sigma \in \overrightarrow{S}(P(s))$. Hence, $s\sigma \in \mathcal{L}(\overrightarrow{S}/\overrightarrow{G})$.

It is known that $\mathcal{L}(\overrightarrow{S}/\overrightarrow{G}) = \overline{\mathcal{L}_m(\overrightarrow{H})}$, so $s\sigma \in \overline{\mathcal{L}_m(\overrightarrow{H})}$. Because $s\sigma \in \mathcal{L}(G)$ it is known that $s\sigma \in \Sigma^*$. Therefore, by the construction of $\overrightarrow{H}$ from H and H_0, $s\sigma \in \overline{\mathcal{L}_m(\overrightarrow{H})}$ implies that $s\sigma \in \overline{\mathcal{L}_m(H)}$. Consequently $s\sigma \in \mathcal{L}^{\cap}(\overrightarrow{S}\phi G) \Rightarrow s\sigma \in \overline{\mathcal{L}_m(H)}$.

It is now shown that $s \in \overline{\mathcal{L}_m(H)} \Rightarrow s \in \mathcal{L}^{\cup}(\overrightarrow{S}\phi G)$ through a proof by induction on the length of the string s.

For the base of induction, suppose that $|s| = 0$, so $s = \epsilon$. By the definition of the prefix-closure, $\epsilon \in \overline{\mathcal{L}_m(H)}$ and due to the definition of $\mathcal{L}^{\cup}(\overrightarrow{S}\phi G)$, $\epsilon \in \mathcal{L}^{\cup}(\overrightarrow{S}\phi G)$.

For the induction hypothesis it is assumed that $s \in \overline{\mathcal{L}_m(H)} \Rightarrow s \in \mathcal{L}^{\cup}(\overrightarrow{S}\not\phi G)$ if $|s| \leq n$.

For the induction step assume $|s| = n$. Let σ be any event. It is now shown that $s\sigma \in \overline{\mathcal{L}_m(H)} \Rightarrow s\sigma \in \mathcal{L}^{\cup}(\overrightarrow{S}\not\phi G)$. From the definition of prefix-closure, $s \in \overline{\mathcal{L}_m(H)}$. From the induction hypothesis, $s \in \mathcal{L}^{\cup}(\overrightarrow{S}\not\phi G)$.

First suppose that $s\sigma \in \overline{\mathcal{L}_m(H)}$ and $\sigma \in \Sigma_{uc}$. From the implicit assumption that $\overrightarrow{S}$ is an admissible controller, it must hold that $s\sigma \in \mathcal{L}^{\cup}(\overrightarrow{S}\not\phi G)$.

Now suppose that $s\sigma \in \overline{\mathcal{L}_m(H)}$ and $\sigma \in \Sigma_c$. Due to the construction of $\overrightarrow{H}$ it is known that $s\sigma \in \overline{\mathcal{L}_m(\overrightarrow{H})}$. Because $\mathcal{L}(\overrightarrow{S}/\overrightarrow{G}) = \overline{\mathcal{L}_m(\overrightarrow{H})}$, it must hold that $s\sigma \in \mathcal{L}(\overrightarrow{S}/\overrightarrow{G})$. This implies that for some $t = \overrightarrow{P}(s)$, $\sigma \in \overrightarrow{S}(t)$. Because $s\sigma \in \mathcal{L}(\overrightarrow{G})$, then from the construction of $\overrightarrow{G}$ from G and G_0, $s\sigma \in \mathcal{L}(G)$. Hence, when s occurs in G, it is possible that the controller $\overrightarrow{S}$ observes a string t such that $\sigma \in \overrightarrow{S}(t)$. It is therefore possible for σ to be enabled after s occurs in $\overrightarrow{S}\not\phi G$. It is already known from the induction hypothesis that $s \in \mathcal{L}^{\cup}(\overrightarrow{S}\not\phi G)$, so by the definition of $\mathcal{L}^{\cup}(\cdot)$ it must be true that $s\sigma \in \mathcal{L}^{\cup}(\overrightarrow{S}\not\phi G)$.

Due to the two induction proofs, $s \in \overline{\mathcal{L}_m(H)} \Rightarrow s \in \mathcal{L}^{\cup}(\overrightarrow{S}\not\phi G)$ and $s \in \mathcal{L}^{\cap}(\overrightarrow{S}\not\phi G) \Rightarrow s \in \overline{\mathcal{L}_m(H)}$. Consequently, $\overline{\mathcal{L}_m(H)} \subseteq \mathcal{L}^{\cap}(\overrightarrow{S}\not\phi G)$ and $\mathcal{L}^{\cup}(\overrightarrow{S}\not\phi G) \subseteq \overline{\mathcal{L}_m(H)}$. Therefore, $\mathcal{L}^{\cap}(\overrightarrow{S}\not\phi G) = \mathcal{L}^{\cup}(\overrightarrow{S}\not\phi G) = \overline{\mathcal{L}_m(H)}$. ■

6. DISCUSSION AND GENERALIZATION

In this paper we generalized sensor-failure tolerant supervisory control to the setting of bounded ranges of permissible control behaviors. We demonstrated techniques to test for controller existence and synthesize controllers for both bounded and matched control problems.

A benefit of Theorem 4 is that it can be used to synthesize a controller $\overrightarrow{S}$ such that if $\mathcal{L}_m(H)$ is not sensor failure observable with respect to $\mathcal{L}(G)$, Σ_o and Σ_c, then, using standard supervisory control methods, one could design $\overrightarrow{S}$ using the $\overrightarrow{G}$ and $\overrightarrow{H}$ constructions such that $\mathcal{L}_m(\overrightarrow{S}/\overrightarrow{G})$ is a maximal controllable and observable sublanguage of $\mathcal{L}_m(\overrightarrow{H})$. Then, the controller $\overrightarrow{S}$ could be used in the faulty-sensor situation such that $\mathcal{L}_m^{\cap}(\overrightarrow{S}\not\phi G)$ or $\mathcal{L}_m^{\cup}(\overrightarrow{S}\not\phi G)$ are in a sense maximal.

With a slight abuse of notation, the size of $\overrightarrow{G}$ and $\overrightarrow{H}$ is in $O(|F^{\Sigma_o}|*(|G|+|H|))$. The constructions grow linearly with the product of the number of failure modes and the size of the automata G and H. It is shown in Tsitsiklis (1989) how observability can be decided in polynomial time with respect to the size of number of states and (un)observable event sets. Consequently, we can decide sensor-failure observability and use the sensor-failure control analysis procedures discussed in this paper in polynomial time with respect to the product of the number of failure modes and the size of the state spaces of G and H.

The approaches we discuss which rely on capturing sensor failure modes in the $\overrightarrow{G}$ and $\overrightarrow{H}$ models will suffer due to state explosion in the more general case of interleaved sensor failures. In particular, using the naive generalizations of the approaches presented, interleaved sensor failures force us to create interleaved state representations. The resulting state spaces grow exponentially with the number of interleaved sensor failures.

The assumption of a one-to-one correspondence between sensors and events can also be generalized using our $\overrightarrow{G}$ construction. In particular, in the $\overrightarrow{G}$ construction, instead of designing for failure modes that correspond to single sensor failures, we could design for modes that correspond to multiple failures. We could also establish transitions between modes in the $\overrightarrow{G}$ construction that corresponds to subsequent failures or even (partial) recoveries.

REFERENCES

Blanke, M., Kinnaert, M., Lunze, J., and Staroswiecki, M. (2003). *Diagnosis and Fault-Tolerant Control*. Springer-Verlag, Berlin.

Dumitrescu, E., Girault, A., and Rutten, E. (2004). Validating fault-tolerant behaviors of synchronous system specifications by discrete controller synthesis. In *Proc. 7th Workshop on Discrete Event Systems*. Reims, France.

Girault, A. and Rutten, E. (2004). Modeling fault-tolerant distributed systems for discrete controller synthesis. In *Proc. 9th International Workshop on Formal Methods for Industrial Critical Systems*.

Jensen, R. (2003). DES controller synthesis and fault tolerant control: A survey of recent advances. Technical Report TR-2003-40, The IT University of Copenhagen.

Lin, F. and Wonham, W.M. (1988). On observability of discrete-event systems. *Information Sciences*, 44, 173–198.

Paoli, A., Sartini, M., and Lafortune, S. (2011). Active fault tolerant control of discrete event systems using online diagnostics. *Automatica*, 47(4), 639–649. doi: 10.1016/j.automatica.2011.01.007.

Patton, R. (1997). Fault-tolerant control systems: The 1997 situation. In R. Patton (ed.), *IFAC Symposium on Fault Detection Supervision and Safety for Technical Processes*. Hull, UK.

Rohloff, K. (2005). Sensor failure tolerant supervisory control. In *Proc. 44nd IEEE Conf. on Decision and Control*, 3493–3498. Seville, Spain.

Sanchez, A.M. and Montoya, F.J. (2006). Safe supervisory control under observability failure. *Journal of Discrete Event Dynamical Systems: Theory and Applications*, 16, 493–525.

Tsitsiklis, J. (1989). On the control of discrete-event dynamical systems. *Mathematics of Control, Signals and Systems*, 2, 95–107.

Ushio, T. and Takai, S. (2009). Supervisory control of discrete event systems modeled by mealy automata with nondeterministic output functions. In *American Control Conference, 2009. ACC '09.*, 4260–4265.

Xu, S. and Kumar, R. (2009). Discrete event control under nondeterministic partial observation. In *Automation Science and Engineering, 2009. CASE 2009. IEEE International Conference on*, 127–132.