A Uniform Framework for Diagnosis of Discrete-Event Systems With Unreliable Sensors Using Linear Temporal Logic

Weijie Dong, *Student Member, IEEE*, Xiang Yin, *Member, IEEE*, and Shaoyuan Li, *Senior Member, IEEE*

***Abstract*—In this article, we investigate the diagnosability verification problem of partially-observed discrete-event systems (DES) subject to unreliable sensors. In this setting, upon the occurrence of each event, the sensor reading may be nondeterministic due to measurement noises or possible sensor failures. Existing works on this topic mainly consider specific types of unreliable sensors such as the cases of intermittent sensors failures, permanent sensor failures or their combinations. In this work, we propose a novel *uniform framework* for diagnosability of DES subject to, not only sensor failures, but also a very general class of unreliable sensors. Our approach is to use linear temporal logic (LTL) with semantics on infinite traces to describe the possible behaviors of the sensors. A new notion of φ-diagnosability is proposed as the necessary and sufficient condition for the existence of a diagnoser, when the behaviors of sensors satisfy the LTL formula φ. An effective approach is provided to verify this notion. We show that, our new notion of φ-diagnosability subsumes all existing notions of robust diagnosability of DES subject to sensor failures. Furthermore, the proposed framework is user-friendly and flexible since it supports an arbitrary user-defined unreliable sensor type based on the specific scenario of the application. As examples, we provide two new notions of diagnosability, which have never been investigated in the literature, using our uniform framework.**

***Index Terms*—Diagnosability, discrete-event systems, fault diagnosis, linear temporal logic, sensor failure.**

I. Introduction

A. Backgrounds and Motivations

ENGINEERING cyber-physical systems (CPSs), such as flexible manufacturing systems and intelligent transportation systems, are very complex due to their intricate operation logic and hybrid dynamics. For such large-scale systems, *failures* during their operations are very common as millions of their components or subsystems are working in parallel under uncertain environments. Therefore, *failure diagnosis and detection* are crucial but challenging tasks in order to monitor the operation conditions and to ensure safety for safety-critical CPSs.

In this article, we investigate the fault diagnosis problem in the framework of discrete-event systems (DES), which is a class of systems widely used in modeling the high-level logical behaviors of CPSs [1]. In the context of DES, the problem of fault diagnosis was initiated by [2] and [3], where the notion of *diagnosability* was proposed. It is assumed that some events in the system are observable, and a system is said to be diagnosable if the occurrence of fault event can always be detected within a finite delay based on the observation sequence. In the past years, fault diagnosis of DES remains a hot topic due to its importance; see, e.g., some recent works [4], [5], [6], [7], [8], [9], [10], [11], [12], [13], [14]. The reader is referred to the comprehensive survey paper and textbook [15], [16], [17] for more details on this topic.

In the modeling of DES, the occurrences of events are essentially detected by the corresponding *sensors*. In practice, however, due to measurement noises, sensor failures, communication losses, or even malicious attacks, the sensor readings can be *unreliable* or *nondeterministic* so that the occurrences of events, which can be detected perfectly in the ideal case, may not always be observed correctly. For example, the sensor for an observable event may *fail* in the sense that the occurrence of the underlying event cannot be detected. The failures of the sensors can be either intermittent or permanent depending on whether or not the failures can be recovered. Also, in the networked setting, even when the sensors can always detect their underlying events, their readings still need to be transmitted from the sensors to the diagnoser via communication channels, in which packet losses are possible. Therefore, the unreliability of sensors are practical and nonnegligible issues in the analysis of diagnosability.

B. Literature Review on Diagnosis With Unreliable Sensors

In the context of DES, robust fault diagnosis for systems subject to unreliable sensors (or subject to sensor failures) has been studied by many researchers. The reader is referred to the very

Manuscript received 28 November 2022; accepted 24 March 2023. Date of publication 10 April 2023; date of current version 29 December 2023. This work was supported by the National Natural Science Foundation of China under Grant 62061136004, Grant 62173226, and Grant 61833012. Recommended by Associate Editor K. Cai. *(Corresponding author: Xiang Yin.)*

The authors are with the Department of Automation and Key Lab of System Control and Information Processing, Shanghai Jiao Tong University, Shanghai 200240, China (e-mail: wjd_dollar@sjtu.edu.cn; yinxiang@sjtu.edu.cn; syli@sjtu.edu.cn).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TAC.2023.3266021.

Digital Object Identifier 10.1109/TAC.2023.3266021

recent comprehensive survey papers [18], [19] for more details on this topic. For example, in [20], the authors investigated the verification of diagnosability for systems subject to *intermittent sensor failures*, where for the sensor of each observable event may fail or recover freely at each time instant. The scenario of intermittent sensor failures can be considered as an instance of *nondeterministic observations* [21], [22], [23]. For example, in [23], the authors proposed to use Mealy automata with nondeterministic output function to capture multiple possible observations for the same transition.

Diagnosability analysis for systems subject to *permanent sensor failures* were studied in [24], [25], [26], and [27]. In this context, once a sensor fails, it will never recover. In [24], the authors investigated the notion robust diagnosability by assuming that permanent sensor failures happen only before the first occurrence of underlying events. This assumption was relaxed by [25]. The results in [24] and [25] have been extended to the decentralized setting by [26] and [27], respectively.

More recently, attempts have been made to unify the notions of diagnosability for systems subject to intermittent sensor failures and permanent sensor failures. For example, it was showed in [19] that diagnosability for systems subject to both intermittent and permanent sensor failures can be transferred to the notion of general robust diagnosability under model uncertainty [28]. In practice, different sensors in the system may belong to different failure types: Some may recover after the failure but some may not. To address this issue, in [29], the author proposed a general framework for robust diagnosability analysis which supports both the case of intermittent sensor failures and the case of permanent sensor failures uniformly.

The effects of unreliable sensors are also closely related to the topic of *networked DES*; see, e.g., [30], [31], [32], and[33]. In this setting, packet delays or losses in the communication channels may also result in nondeterministic observations, which is very similar to the effect of unreliable sensors. For example, in [34], the authors studied the verification of K-loss diagnosability by assuming that the communication channel can only have a bounded number of consecutive observation losses. Besides diagnosability analysis, the effects of unreliable sensors have also been studied for other state estimation problems [35], [36] as well as the supervisory control problem [37], [38], [39], [40].

C. Our Approach and Contributions

In the aforementioned existing works on diagnosability analysis for DES subject to unreliable sensors, one needs to develop customized techniques for different types of sensor failures or sensor modes. For example, in [29], where intermittent and permanent sensor failures are unified, one needs to build the sensor automaton that captures all possible switching between the normal mode and the failure mode. Here, we observe that, each type of sensor failures is actually a *constraint* on how the behaviors of the sensors can change. Such a sensor constraint is essentially a *linear-time property* on the sequence of the sensor modes. For example, the case of permanent sensor failures is actually a safety property requiring that once the sensor goes to a failure mode, it should not recover anymore.

Motivated by the above observation, in this article, we propose a new *uniform framework* for fault diagnosis of DES subject to unreliable sensors. Mathematically, sensors can be modeled as a mapping from internal events to external events. By "unreliable," we mean that either the value of mapping or the mapping itself may change (details about unreliable sensors are provided in Section II-B). In contrast to existing works, our approach does not rely on any pre-specified type of sensors. Instead, we propose to use linear temporal logic (LTL) formulae as a general tool to describe an arbitrary type of unreliable sensors. To this end, we first adopt the model of Mealy automata with nondeterministic output functions proposed in [23] and [38] as the *unconstrained observation space* of the sensors. Then, we further use an LTL formula φ, which is referred to as the *sensor constraint* and its specific form is scenario dependent, to describe how sensors can behave within the unconstrained space. We propose a new diagnosability condition, called φ-diagnosability, following an *assumption based* type of reasoning. That is, whenever the sensors behave following the assumption φ, the diagnoser should be able to detect the fault within a finite number of steps. We provide an effective procedure for verifying this new condition. In particular, the complexity of the verification procedure is exponential in the number of operators in LTL formula φ, but is only polynomial in the size of the plant model.

Our uniform framework is developed based on an arbitrary LTL formula φ without its specific meaning. To show the generality of our framework, we further show how the proposed notion of φ-diagnosability subsumes existing notions of robust diagnosability by explicitly writing down φ for different scenarios of unreliable sensors. In particular, we show that existing notions of diagnosability for DES subject to 1) intermittent sensor failures [20], [21], [23]; 2) permanent sensor failures [24], [25]; and 3) bounded sensor losses [34], can all be captured within our framework in a uniform manner.

Furthermore, since our notion of φ-diagnosability is very generic and LTL is a very expressive and human language-like approach for presenting linear-time properties; our framework, in fact, provides a general and user-friendly way to study diagnosability under arbitrary user-defined or scenario-specified unreliable sensors. As examples, we further introduce two practical scenarios of unreliable sensors, which have never been studied in the literature. One is the scenario of *minimum dwell-time* of sensor modes, i.e., whenever a sensor fails, it cannot recover immediately. Another is the scenario of *output fairness* in the setting of nondeterministic observations, where each fair observation symbol will eventually be observed if it has infinite chances to be observed.

We note that using linear temporal logic in diagnosability analysis has been investigated in the literature. For example, [41], [42], and [43] investigated how to detect faults specified by the violations of LTL formulae. In [44], [45], [46], and [14], the verification of standard diagnosability was solved using LTL model checking techniques. However, here, we *do not* aim to detect fault described by LTL or to solve diagnosability verification using LTL model checking. The role of LTL in our framework is very different from existing purposes. We use LTL formulae as a general and systematic way to describe different

types of unreliable sensors, which, to the best of our knowledge, has never been used in the literature.

D. Organizations

The rest of this article is organized as follows. Section II presents some basic preliminaries. In Section III, we describe how to use LTL formulae to model unreliable sensors. In Section IV, we introduce the notion of φ-diagnosability and its verification algorithm is developed in Section V. In Section VI, we show explicitly how our uniform framework subsumes many existing notions as well as supports new types of unreliable sensors that have not been considered. Finally, Section VII concludes the article. Our preliminary idea of using LTL formulae to described sensor behaviors was initially presented in [47]. However, the framework in the present article is much more general, where the result in [47] is a now very special instance as described in Section VI-D.

II. Preliminaries

A. Partially-Observed Discrete Event Systems

Let Σ be a finite set. A string $s = \sigma_1\sigma_2\cdots\sigma_n(\cdots)$ is a finite (or infinite) sequence over Σ if $\sigma_i \in \Sigma$ for all $i = 0, 1, \ldots$. For a finite string s, we denote by $|s|$ the length of s, which is the number of components in it. We denote by Σ^* and Σ^ω the set of all finite and infinite strings over Σ, respectively. We write $\Sigma^+ = \Sigma^* \cup \Sigma^\omega$ as the set of finite or infinite strings. Note that Σ^* includes the empty string ε. A $*$-language $L \subseteq \Sigma^*$ is a set of finite strings and an ω-language $L \subseteq \Sigma^\omega$ is a set of infinite strings. For any $*$-language $L \subseteq \Sigma^*$, its *prefix-closure* is a $*$-language $\overline{L} = \{s \in \Sigma^* : \exists t \in \Sigma^* \text{ s.t. } st \in L\}$. For any ω-language $L \subseteq \Sigma^\omega$, its prefix-closure is defined as the set of all its finite prefixes, which is $*$-language $\overline{L} = \{s \in \Sigma^* : \exists t \in \Sigma^\omega \text{ s.t. } st \in L\}$. For infinite string $s \in \Sigma^\omega$, $\mathsf{Inf}(s)$ denotes the set of components appearing infinite number of times in s.

In this work, we consider a DES modeled by a deterministic finite-state automaton

$$G = (Q, \Sigma, \delta, q_0)$$

where Q is the finite set of states, Σ is the finite set of events, $\delta : Q \times \Sigma \to Q$ is the partial deterministic transition function such that: For any $q, q' \in Q, \sigma \in \Sigma$, $\delta(q, \sigma) = q'$ means that there exists a transition from state q to state q' labeled by event σ, and $q_0 \in Q$ is the initial state. Note that, we do not consider marked states in the system model since it is irrelevant to our purpose of diagnosability verification. The transition function δ is also extended to $\delta : Q \times \Sigma^* \to Q$ recursively by: For any $q \in Q, s \in \Sigma^*$ and $\sigma \in \Sigma$, we have $\delta(q, \varepsilon) = q$ and $\delta(q, s\sigma) = \delta(\delta(q, s), \sigma)$. Then, the $*$-language generated by G is defined by $\mathcal{L}(G) = \{s \in \Sigma^* : \delta(q_0, s)!\}$, where "!" means "is defined," and the ω-language generated by G is defined by $\mathcal{L}^\omega(G) = \{s \in \Sigma^\omega : \forall s' \in \overline{\{s\}}, \delta(q_0, s')!\}$. We assume that system G is live, i.e., for any state $q \in Q$, there exists an event $\sigma \in \Sigma$ such that $\delta(q, \sigma)!$.

In the partial observation setting, the occurrence of each event may not be perfectly observed. The limited sensor capability is usually modeled by an observation mask

$$O : \Sigma \to \Delta \dot{\cup} \{\varepsilon\} \tag{1}$$

where Δ is a new set of observation symbols. That is, we observe $O(\sigma)$ upon the occurrence of event $\sigma \in \Sigma$. We say event $\sigma \in \Sigma$ is observable if $O(\sigma) \in \Delta$ and unobservable if $O(\sigma) = \varepsilon$. The observation mask is also extended to $O : \Sigma^+ \to \Delta^+$ by: For any $s \in \Sigma^+$, $O(s)$ is obtained by replacing each event σ in string s as $O(\sigma)$.

B. Observations Under Unreliable Sensors

The observation mask as defined in (1) corresponds to the case of *reliable sensors*. That is, if event $\sigma \in \Sigma$ is observable, then the sensor reading will always be $O(\sigma)$ whenever it occurs. In many real-world scenarios, however, sensors may be *unreliable* due to multiple reasons. To capture the observations under unreliable sensors, [23], [38] proposed to use the following state-dependent (or transition-based) nondeterministic observation mapping:

$$\mathcal{O} : Q \times \Sigma \to 2^{\Delta \cup \{\varepsilon\}}. \tag{2}$$

Specifically, Δ is the set of all possible observation symbols. For any state $q \in Q$ and event $\sigma \in \Sigma$, $\mathcal{O}(q, \sigma)$ denotes *the set of all possible observations* if event σ occurs at state q, i.e., the sensor reading may be any symbol $o \in \Delta$ or ε in $\mathcal{O}(q, \sigma)$ nondeterministically.

The observation mapping $\mathcal{O}$ can also be extended to $\mathcal{O} : Q \times \Sigma^+ \to 2^{\Delta^+}$ by: for any state $q \in Q$ and string $s = \sigma_1\sigma_2\cdots \in \Sigma^+$, we have $o_1o_2\cdots \in \mathcal{O}(q, s)$ if

$$\forall i = 1, 2, \cdots : o_i \in \mathcal{O}(f(q, \sigma_1 \ldots \sigma_{i-1}), \sigma_i) \tag{3}$$

where $\sigma_0 := \varepsilon$. Since the observations are nondeterministic, in general, $\mathcal{O}(q, s) \subseteq \Delta^+$ is not a singleton and each sequence in $\mathcal{O}(q, s)$ is called an *observation realization* of string s. For the sake of brevity, we use $\mathcal{O}(s)$ to denote $\mathcal{O}(q, s)$ if the state q is the initial state, i.e., $q = q_0$.

To incorporate the actual observation into the internal execution of the system, it is convenient to define

$$\Sigma_e = Q \times \Sigma \times (\Delta \cup \{\varepsilon\})$$

as the set of *extended events*. Then, an extended string is a finite or infinite sequence of extended events. We say an extended string $s = (q_0, \sigma_0, o_0)(q_1, \sigma_1, o_1)\cdots \in \Sigma_e^+$ is generated by G if for any $i = 1, 2, \ldots$, we have $f(q_i, \sigma_i) = q_{i+1}$ and $o_i \in \mathcal{O}(q_i, \sigma_i)$. We denote by $\mathcal{L}_e(G)$ and $\mathcal{L}_e^\omega(G)$ the set of all finite and infinite extended strings generated by G, respectively. Essentially, an extended string contains three parts of information: 1) the state sequence visited; 2) the event sequence generated; and 3) the output sequence observed. Then, for any extended string $s = (q_0, \sigma_0, o_0)(q_1, \sigma_1, o_1)\cdots \in \Sigma_e^+$, we define $\Theta_Q(s) = q_0q_1\cdots \in Q^+$, $\Theta_\Sigma(s) = \sigma_0\sigma_1\cdots \in \Sigma^+$, and $\Theta_\Delta(s) = o_0o_1\cdots \in (\Delta \cup \{\varepsilon\})^+$ as its corresponding state sequence, (internal) event string and output string, respectively. Clearly, for any $s \in \Sigma_e^+$, we have $\Theta_\Delta(s) \in \mathcal{O}(\Theta_\Sigma(s))$ because $\Theta_\Delta(s)$ is a specific observation realization of $\Theta_\Sigma(s)$.

Example 1: Let us consider system G_1 shown in Fig. 1, where $\Sigma = \{a, b, c, f, u\}$ and $\Delta = \Sigma$. The output function $\mathcal{O}$:

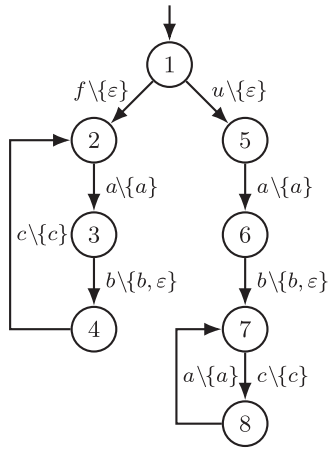

Fig. 1. System G_1.

$Q \times \Sigma \to 2^{\Delta \cup \{\varepsilon\}}$ is specified by the label of each transition, where the LHS of "\" denotes the internal event and the RHS of "\" denotes the set of all possible output symbols. For example, $b \setminus \{b, \varepsilon\}$ from state 3 to state 4 means that at state 3, upon the occurrence of event b, the system moves to state 4, i.e., $\delta(3, b) = 4$, and we may observe either b or nothing, i.e., $\mathcal{O}(3, b) = \{b, \varepsilon\}$. Then, for finite string $fab \in \mathcal{L}(G_1)$, the set of all possible observation realizations is $\mathcal{O}(fab) = \{ab, a\}$. These two different observations lead to the following two extended strings $(1, f, \varepsilon)(2, a, a)(3, b, b) \in \mathcal{L}_e(G)$ and $(1, f, \varepsilon)(2, a, a)(3, b, \varepsilon) \in \mathcal{L}_e(G)$, respectively. □

Remark 1: The nondeterministic observation mapping $Q \times \Sigma \to 2^{\Delta \cup \{\varepsilon\}}$ is quite general and subsumes many observation models in the literature. For example, for the standard natural projection, we assume that $\Sigma_o \subseteq \Sigma$ is the set of observable events and let $\Delta = \Sigma_o$. Then, one can define $\mathcal{O}$ by: $\mathcal{O}(q, \sigma) = \{\sigma\}$ for all $\sigma \in \Sigma_o$ and $\mathcal{O}(q, \sigma) = \{\varepsilon\}$ for all $\sigma \notin \Sigma_o$. Also, it captures the so-called *intermittent loss of observations* [20], [30]. In this setting, the event set is usually partitioned as $\Sigma = \Sigma_r \dot{\cup} \Sigma_{ur} \dot{\cup} \Sigma_{uo}$, where Σ_r is the set of reliable events whose occurrences can always be observed directly, Σ_{ur} is the set of unreliable events whose occurrences may be observed but can also be lost, and Σ_{uo} is the set of unobservable events whose occurrences can never be observed. This setting can be captured by considering $\mathcal{O}$ such that $\Delta = \Sigma_r \cup \Sigma_{ur}$ and for any $q \in Q$ and $\sigma \in \Sigma$, we have

$$\mathcal{O}(q, \sigma) = \begin{cases} \{\sigma\} & \text{if } \sigma \in \Sigma_r \\ \{\sigma, \varepsilon\} & \text{if } \sigma \in \Sigma_{ur} \\ \{\varepsilon\} & \text{if } \sigma \in \Sigma_{uo} \end{cases}. \tag{4}$$

Note that, for the general case we consider here, the output symbols Δ can be different from the original event set Σ.

C. Fault Diagnosis

In the context of fault diagnosis of DES, it is assumed that the system is subject to faults, which are modeled by a set of fault events $\Sigma_F \subset \Sigma$. For the sake of simplicity, we do not distinguish among different fault types in this work. We say a string $s \in \Sigma^+$ is faulty if it contains a fault event in Σ_F and we write $\Sigma_F \in s$ with a slight abuse of notation; otherwise, we call string s a normal string. We denote by $\mathcal{L}_F(G)$ and $\mathcal{L}_F^\omega(G)$ as the sets of all finite and infinite faulty strings generated by G, respectively. Similarly, we define $\Sigma_{e,F} = Q \times \Sigma_F \times (\Delta \cup \{\varepsilon\}) \subset \Sigma_e$ as the set of extended fault events and we denote by $\mathcal{L}_{e,F}(G)$ and $\mathcal{L}_{e,F}^\omega(G)$ as the sets of all finite and infinite extended faulty strings generated by G, respectively. Finally, we define $\Psi_e(G)$ as the set of all finite extended faulty strings in which extended fault events occur *for the first time*, i.e.,

$$\Psi_e(G) = \{s \in \mathcal{L}_{e,F}(G) : \forall t \in \overline{\{s\}} \setminus \{s\}, \Sigma_{e,F} \notin t\}.$$

To capture whether or not the occurrences of fault events can be always detected within a finite number of steps, the notion of diagnosability (under nondeterministic observations) has been proposed in the literature [23].

Definition 1 (Diagnosability): System G is said to be *diagnosable* w.r.t. mapping $\mathcal{O}$ and fault events Σ_F if

$$(\forall s \in \Psi_e(G))(\exists n \in \mathbb{N})(\forall st \in \mathcal{L}_e(G))[|t| \geq n \Rightarrow \mathsf{diag}] \tag{5}$$

where the diagnostic condition diag is

$$(\forall v \in \mathcal{L}_e(G))[\Theta_\Delta(v) = \Theta_\Delta(st) \Rightarrow \Sigma_{e,F} \in v].$$

Intuitively, the above definition says that, for any faulty extended string in which fault events appear for the first time, there exists a finite detection bound such that, for any of its continuation longer than the detection bound, any other extended strings having the same observation must also contain fault events, which means we can claim for sure that fault events have occurred. Note that we consider extended strings $\mathcal{L}_e(G)$ rather than the internal strings $\mathcal{L}(G)$ in order to capture the issue of nondeterministic observations. Also, we note that, for finite-state automata, "$\forall s \in \Psi_e(G)$" and "$\exists n \in \mathbb{N}$" in Definition 1 can be swapped [48], which means that if the system is diagnosable, then there exists a *uniform detection bound* for all fault strings.

Example 2: Again, we consider system G_1 depicted in Fig. 1 and we assume $\Sigma_F = \{f\}$. Let us consider faulty extended string $(1, f, \varepsilon) \in \Psi_e(G)$, which can be extended arbitrarily long as $s_F = (1, f, \varepsilon)[(2, a, a)(3, b, \varepsilon)(4, c, c)]^n$. However, for any n, we can find a normal extended string $s_N = (1, u, \varepsilon)(5, a, a)(6, b, \varepsilon)[(7, c, c)(8, a, a)]^{n-1}(7, c, c)$ such that $\Theta_\Delta(s_F) = \Theta_\Delta(s_N) = (ac)^n$. Therefore, system G_1 is not diagnosable with respect to $\mathcal{O}$ and Σ_F. □

D. Linear Temporal Logic

Let $\mathcal{AP}$ be a finite set of atomic propositions. An LTL formula φ is constructed based on a set of atomic propositions $\mathcal{AP}$, Boolean operators, and temporal operators as follows:

$$\varphi ::= \mathtt{true} \mid p \mid \neg\varphi \mid \varphi_1 \wedge \varphi_2 \mid \bigcirc\varphi \mid \varphi_1 \, U \varphi_2$$

where $p \in \mathcal{AP}$ is an atomic proposition, $\neg$ and $\wedge$ stand for logical negation and disjunction, respectively, while $\bigcirc$ and U denote "next" and "until," respectively. Note that other Boolean operators can be induced by $\wedge$ and $\neg$, e.g., $\varphi_1 \vee \varphi_2 = \neg(\neg\varphi_1 \wedge \neg\varphi_2)$ and $\varphi_1 \to \varphi_2 = \neg\varphi_1 \vee \varphi_2$. It is convenient to define temporal operators $\Diamond$ "eventually" by $\Diamond\varphi = \mathtt{true} U \varphi$ and $\Box$ "always" by $\Box\varphi = \neg\Diamond\neg\varphi$.

LTL formulae are evaluated over infinite strings of atomic proposition sets, which are also referred to as infinite *words*. For any infinite word $s \in (2^{\mathcal{AP}})^\omega$, we denote by $s \models \varphi$ if it satisfies LTL formula φ and use $\mathsf{word}(\varphi)$ to denote all strings satisfying φ, i.e., $\mathsf{word}(\varphi) = \{s \in (2^{\mathcal{AP}})^\omega : s \models \varphi\}$. The reader is referred to [49] for more details on the semantics of LTL. For example, let $s = A_0 A_1 \cdots \in (2^{\mathcal{AP}})^\omega$ be an infinite word and ϕ be a Boolean formula without temporal operators. Then, $s \models \Box\Diamond\phi$ means that proposition ϕ holds *infinitely often* in s, i.e., $\forall i \geq 0, \exists j > i : \phi(A_j) = \texttt{true}$, while $s \models \Diamond\Box\phi$ means that proposition ϕ holds *forever after some finite delays* in s, i.e., $\exists i \geq 0, \forall j > i : \phi(A_j) = \texttt{true}$.

To capture all infinite words satisfying φ, we introduce the nondeterministic Büchi automaton (NBA) as follows.

Definition 2 (Nondeterministic Büchi automaton): An NBA is a five-tuple $\mathcal{B} = (X, X_0, \Sigma_B, \xi, X_m)$, where X is a finite set of states, $X_0 \subseteq X$ is the set of initial states, Σ_B is an alphabet, $\xi : X \times \Sigma_B \to 2^X$ is a nondeterministic transition function and $X_m \subseteq X$ is the set of accepting states.

Given an infinite word $s = \sigma_0 \sigma_1 \cdots \in \Sigma_B^\omega$, an infinite path of $\mathcal{B}$ induced by s is an infinite state sequence $\rho = x_0 x_1 \cdots \in X^\omega$ such that $x_0 \in X_0$ and $x_{i+1} \in \xi(x_i, \sigma_i)$ for any $i = 0, 1, \cdots$. An infinite path ρ is said to be *accepted* by NBA $\mathcal{B}$ if it visits accepting states X_m infinitely often, i.e., $\mathsf{inf}(\rho) \cap X_m \neq \emptyset$. We say an infinite word s is accepted by $\mathcal{B}$ if it induces an infinite path accepted by $\mathcal{B}$. We denote by $\mathcal{L}_m^\omega(\mathcal{B})$ the set of strings accepted by NBA $\mathcal{B}$. The nondeterministic transition function ξ can also be extended to $\xi : X \times \Sigma_B^* \to 2^X$ recursively in the usual manner. Also, we use notation $\mathcal{L}(\mathcal{B}) \subseteq \Sigma_B^*$ to denote the set of all finite strings generated by $\mathcal{B}$, i.e., $\mathcal{L}(\mathcal{B}) = \{s \in \Sigma_B^* : \exists x_0 \in X_0 \text{ s.t. } \xi(x_0, s) \neq \emptyset\}$.

It is well known that [49], for any LTL formula φ, we can translate φ to an NBA $\mathcal{B}$ over event set $\Sigma_B = 2^{\mathcal{AP}}$, such that $\mathcal{L}_m^\omega(\mathcal{B}) = \mathsf{word}(\varphi)$, and we say such an NBA $\mathcal{B}$ is associated with φ. There are efficient tools in the literature to translate an LTL formula to an NBA such as `LTL2BA` [50].

III. LTL-Based Description of Unreliable Sensors

A. Motivation and Main Idea

In the previous section, we use nondeterministic observation mapping $\mathcal{O} : Q \times \Sigma \to 2^{\Delta \cup \{\varepsilon\}}$ to capture all possible observations. However, this model essentially provides the *possible observation space* for the purpose of worst-case analysis. When the observation nondeterminism has a concrete physical meaning, the extended language $\mathcal{L}_e(G)$ may contain observation realizations that are not feasible in practice.

To motivate our developments, we take the scenario of *permanent sensor failures* as an example. As we have discussed in Remark 1, the nondeterministic observation mapping specified in (4) can capture the scenario of intermittent sensor failures, i.e., for each event $\sigma \in \Sigma_{ur}$, we may observe σ when the sensor is normal or ε when the sensor fails. However, in the context of permanent sensor failures, once an unreliable sensor fails, it will not be normal forever. Then, for system G_1 in Fig. 1, in the context of permanent sensor failures, the following extended string in $\mathcal{L}_e(G)$ will no longer be feasible:

$$s_F = (1, f, \varepsilon)(2, a, a)(3, b, \varepsilon)(4, c, c)(2, a, a)(3, b, b)$$

because the occurrence of extended event $(3, b, \varepsilon)$ means that the sensor corresponding to event b has already failed and it is not possible to have extended event $(3, b, b)$ thereafter.

Such a simple scenario of permanent sensor failures cannot be modeled by nondeterministic mapping in the form of (2) directly. To describe this scenario, different approaches have been developed in the literature [24], [25], [27] and the basic idea is to use additional states to capture the failure/normal status of unreliable sensors.

One of the motivations of our work is to provide a general framework that unifies the scenarios of intermittent and permanent sensors failures. However, our approach goes much beyond this basic objective and supports arbitrary *user-specified* sensor behaviors. Specifically, the basic idea of our approach is as follows.

1) First, we use observation mapping $\mathcal{O} : Q \times \Sigma \to 2^{\Delta \cup \{\varepsilon\}}$ to generate the *unconstrained* observation space $\mathcal{L}_e(G)$ without considering the specific setting of each sensor.
2) Then, by incorporating how each sensor should behave, which is referred to as the *sensor constraint* throughout the article, we further restrict the unconstrained observation space by eliminating those observations that are not feasible in the concrete setting.

To realize the above idea, the key question is how to describe the behaviors of unreliable sensors for different contexts. Our novelty here is that the user does not need to hand-code the feasible behaviors of the sensors. Instead, we provide a very generic and user-friendly way to describe the sensor constraints using LTL formulae.

B. Sensor Constraints as LTL Formulae

To capture the sensor constraints using LTL formulae, we define a labeling function

$$\mathsf{label} : \Sigma_e \to 2^{\mathcal{AP}} \tag{6}$$

that assigns each extended event a set of atomic propositions. For any infinite extended string $s = \sigma_1 \sigma_2 \cdots \in \Sigma_e^\omega$, its *trace* is defined by $\mathsf{trace}(s) = \mathsf{label}(\sigma_1)\mathsf{label}(\sigma_2) \cdots \in (2^{\mathcal{AP}})^\omega$. Let φ be an LTL formula specifying the sensor constraint. We say an infinite extended string $s \in \Sigma_e^\omega$ is *φ-compatible*, if $\mathsf{trace}(s) \models \varphi$. For simplicity, with a slight abuse of notation, we also write $s \models \varphi$ whenever $\mathsf{trace}(s) \models \varphi$. We define

$$\mathcal{L}_e^\varphi(G) = \{s \in \mathcal{L}_e^\omega(G) : s \models \varphi\}$$

as the set of all φ-compatible infinite extended strings in G.

Intuitively, the above definition says that if we assume that the behaviors of the sensors satisfy LTL formula φ, then only infinite observations in $\mathcal{L}_e^\varphi(G)$ are feasible in practice. Note that, we use infinite observation in order to match the semantic of LTL. For the purpose of online diagnosis, we only observe finite observations in $\overline{\mathcal{L}_e^\varphi(G)}$. In other words, it is impossible to observe finite extended strings in $\mathcal{L}_e(G) \setminus \overline{\mathcal{L}_e^\varphi(G)}$ since they cannot be extended to infinite strings in $\mathcal{L}_e^\varphi(G)$. Finally, we

also define $\mathcal{L}^{\varphi}_{e,F}(G) = \mathcal{L}^{\varphi}_{e}(G) \cap \mathcal{L}^{\omega}_{e,F}(G)$ as the set of infinite extended faulty strings that are φ-compatible.

Note that, how to select atomic propositions $\mathcal{AP}$, labeling function $\mathsf{label} : \Sigma_e \to 2^{\mathcal{AP}}$ and LTL formula φ is application dependent. In Section VI, we will elaborate on how they are selected for different practical scenarios. Here, we consider the scenario of permanent sensor failures to illustrate the choices of $\mathcal{AP}$, label and φ, and use this scenario as a running example for the latter developments.

Example 3 (Sensor constraints for permanent sensor failures): We still consider system G_1 shown in Fig. 1. However, now we further assume that the reason why event b may become unobservable is due to a *permanent sensor failure*. This scenario can be described as follows. First, we choose the set of atomic propositions as $\mathcal{AP} = \{m_0, m_1\}$, where m_0 and m_1 represent that the sensor for event b is normal and faulty, respectively. Then, we define the labeling function $\mathsf{label} : \Sigma_e \to 2^{\mathcal{AP}}$ by: for any $\sigma_e = (q, \sigma, o) \in \Sigma_e$

$$\mathsf{label}(\sigma_e) = \begin{cases} \{m_0\}, & \text{if } \sigma = b \wedge o = b \\ \{m_1\}, & \text{if } \sigma = b \wedge o = \varepsilon \\ \emptyset, & \text{otherwise} \end{cases}. \tag{7}$$

Then, the sensor constraint can be written as

$$\varphi_{\mathsf{per}} = \Box(m_1 \to \Box\neg m_0). \tag{8}$$

Intuitively, formula φ_{per} says that whenever atomic proposition m_1 holds, which means that sensor for event b fails, atomic proposition m_0, which means that sensor reads the occurrence of b normally, cannot hold anymore.

Then, under the above described sensor constraint φ_{per}, we know that the following extended string is not φ_{per}-compatible:

$$s_F = (1, f, \varepsilon)(2, a, a)(3, b, \varepsilon)((4, c, c)(2, a, a)(3, b, b))^{\omega}$$

because $\mathsf{trace}(s_F) = \emptyset\emptyset\{m_1\}(\emptyset\emptyset\{m_0\})^{\omega} \not\models \varphi_{\mathsf{per}}$. Therefore, with sensor constraint φ_{per}, it is impossible to observe finite sequence $acab$ because

$$(1, f, \varepsilon)(2, a, a)(3, b, \varepsilon)(4, c, c)(2, a, a)(3, b, b) \notin \overline{\mathcal{L}^{\varphi}_{e}(G)}.$$

□

IV. Diagnosability Under Sensor Constraints

In this section, we investigate diagnosability under sensor constraints. Specifically, we formally propose the notion of φ-diagnosability as the necessary and sufficient condition of the existence of a diagnoser working correctly for DES subject to sensors constrained by specification φ.

A. Definition of φ-Diagnosability

First, we modify the existing definition of diagnosability in Definition 1 to a new notion of diagnosability, called φ-*diagnosability*, by taking the issues of the LTL sensor constraint φ into account.

Definition 3 (φ-Diagnosability): System G is said to be φ-diagnosable w.r.t. output function $\mathcal{O}$, fault events Σ_F and sensor constraint φ, if and only if

$$(\forall s \in \mathcal{L}^{\varphi}_{e,F}(G))(\exists t \in \overline{\{s\}})[\varphi\text{-}\mathsf{diag}] \tag{9}$$

where the φ-diagnostic condition φ-diag is

$$(\forall v \in \overline{\mathcal{L}^{\varphi}_{e}(G)})[\Theta_{\Delta}(v) = \Theta_{\Delta}(t) \Rightarrow \Sigma_{e,F} \in v].$$

The above definition says that, for any infinite faulty extended string s satisfying sensor constraint φ, there is a finite prefix t such that for any finite extended string v that are possible as a prefix of some infinite string satisfying the sensor constraint, if the outputs of v and t are equivalent, then the extended string v must also be faulty. Intuitively, φ-diagnosability modifies the standard diagnosability by restricting our attention only to those infinite extended strings satisfying the sensor constraint φ. Clearly, by setting $\varphi = \mathtt{true}$, our φ-diagnosability becomes to the standard diagnosability in Definition 1.

Example 4: Again, let us consider system G_1 shown in Fig. 1 with the same setting in Example 3. Note that there exists an infinite faulty extended string

$$s_F = (1, f, \varepsilon)((2, a, a)(3, b, \varepsilon)(4, c, c))^{\omega}$$

with $\mathsf{trace}(s_F) = \emptyset(\emptyset\{m_1\}\emptyset)^{\omega} \models \varphi_{\mathsf{per}}$, i.e., $s_F \in \mathcal{L}^{\varphi}_{e,F}(G)$. However, there exists an infinite normal extended string

$$s_N = (1, u, \varepsilon)(5, a, a)(6, b, \varepsilon)((7, c, c)(8, a, a))^{\omega}$$

whose trace is $\mathsf{trace}(s_N) = \emptyset\emptyset\{m_1\}(\emptyset\emptyset)^{\omega} \models \varphi_{\mathsf{per}}$, i.e., $s_N \in \mathcal{L}^{\varphi}_{e}(G)$, such that the output of s_F and s_N are the same, i.e., $\Theta_{\Delta}(s_F) = \Theta_{\Delta}(s_N) = (ac)^{\omega}$. Therefore, for any finite prefix $t \in \overline{\{s_F\}}$, there exists a normal extended string $v \in \overline{\{s_N\}}$, such that $\Theta_{\Delta}(t) = \Theta_{\Delta}(v)$. Namely, there exists an infinite faulty extended string compatible to the sensor constraint φ_{per} such that for each of its prefix, there exists a normal extended string having the same output with the prefix. By Definition 3, system G_1 is not φ_{per}-diagnosable. □

Next, we show that the proposed notion of φ-diagnosability indeed provides the necessary and sufficient condition for the existence of a diagnoser that works "correctly" under sensor constraint φ. Formally, a diagnoser is a function

$$D : \{\Theta_{\Delta}(v) \in \mathcal{O}(\mathcal{L}(G)) : v \in \overline{\mathcal{L}^{\varphi}_{e}(G)}\} \to \{0, 1\}$$

that decides whether a fault has happened (by issuing "1") or not (by issuing "0") based on the output string. We say that a diagnoser works correctly under the sensor constraint φ if it satisfies the following conditions.

C1) The diagnoser will eventually issue a fault alarm for any occurrence of fault events, i.e.,

$$(\forall s \in \mathcal{L}^{\varphi}_{e,F}(G))(\exists t \in \overline{\{s\}})[D(\Theta_{\Delta}(t)) = 1].$$

C2) The diagnoser will not issue a false alarm if the execution is still normal, i.e.,

$$(\forall s \in \overline{\mathcal{L}^{\varphi}_{e}(G)} : \Sigma_{e,F} \notin s)[D(\Theta_{\Delta}(s)) = 0].$$

The following theorem says that there exists a diagnoser which works "correctly" under sensor constraint φ, if and only if the system is φ-diagnosable. All proofs hereafter are provided in the Appendix.

Theorem 1: There exists a diagnoser satisfying conditions 1 and 2, if and only if G is φ-diagnosable w.r.t. fault events Σ_F, output function $\mathcal{O}$, and sensor constraint φ.

B. Existence of Uniform Bound

In the definition of φ-diagnosability, since the assumption of LTL sensor constraint is imposed on infinite strings, we can only guarantee that for any infinite faulty string, there exists a finite detection bound. However, this does not imply that there exists a uniform detection bound for all faulty strings. For example, suppose that there is an indicator event that will occur infinite number of times after fault events. If we assume that the sensor constraint φ for the indicator event is that it will *not always fail*, i.e., its occurrence will *eventually* be observed correctly, then the system is φ-diagnosable. However, this condition does not ensure when it will be observed since the satisfaction instant of "eventually" can be arbitrarily late.

Here, we identify a condition under which a uniform detection bound exists. Formally, we define $\Psi_e^{\varphi}(G)$ as all prefixes of φ-compatible infinite extended strings in which extended fault events occur for the first time, i.e.,

$$\Psi_e^{\varphi}(G)=\{s\in\overline{\mathcal{L}_e^{\varphi}(G)}:\forall t\in\overline{\{s\}}\setminus\{s\},\Sigma_{e,F}\notin t\wedge\Sigma_{e,F}\in s\}.$$

Then, we introduce the notion of finite φ-diagnosability.

Definition 4 (Finite φ-diagnosability): System G is said to be *finite φ-diagnosable* w.r.t. mapping $\mathcal{O}$, fault events Σ_F, and sensor constraint φ if

$$(\exists n\in\mathbb{N})(\forall s\in\Psi_e^{\varphi}(G))(\forall st\in\overline{\mathcal{L}_e^{\varphi}(G)})[|t|\geq n\Rightarrow\varphi_F\text{-diag}]$$

where the finite φ-diagnostic condition φ_F-diag is

$$(\forall v\in\overline{\mathcal{L}_e^{\varphi}(G)})[\Theta_\Delta(v)=\Theta_\Delta(st)\Rightarrow\Sigma_{e,F}\in v].$$

Clearly, finite φ-diagnosability implies φ-diagnosability, but the converse direction is not true in general. Here, we show that these two notions coincide when φ is a safety property [51]. Formally, a linear-time property $P\subseteq(2^{\mathcal{AP}})^\omega$ is called a *safety property* if, for any $s\in(2^{\mathcal{AP}})^\omega\setminus P$, there exists a prefix $s_1\in\overline{\{s\}}$, such that $P\cap\{s'\in(2^{\mathcal{AP}})^\omega:s_1\in\overline{\{s'\}}\}=\emptyset$. Intuitively, the violation of a safety property can always be determined in a finite horizon. We say φ is a safety LTL formula if word(φ) is a safety property. Then, we have the following result.

Theorem 2: Suppose that φ is a safety LTL formula. Then a system is finite φ-diagnosable, if and only if it is φ-diagnosable.

V. Verification of φ-Diagnosability

In this section, we provide a verifiable necessary and sufficient condition for the verification of φ-diagnosability based on the verification system.

A. Augmented Systems

To verify φ-diagnosability, our first step is to augment both the state-space and the event-space of G such that:

- the information of whether or not a fault event has occurred is encoded in the *augmented state-space*; and
- the information of which state the event is enabled from and which specific output is observed are encoded in the *augmented event-space*.

Definition 5 (Augmented systems): Given system $G=(Q,q_0,\Sigma,\delta)$, fault events Σ_F, and output function $\mathcal{O}$, we define the *augmented system* as a new-tuple

$$\tilde{G}=(\tilde{Q},\tilde{q}_0,\Sigma_e,\tilde{\delta}) \tag{10}$$

where the variables are defined as follows:

- $\tilde{Q}\subseteq Q\times\{F,N\}$ is the set of augmented states;
- $\tilde{q}_0=(q_0,N)$ is the initial augmented state;
- Σ_e is the set of extended events;
- $\tilde{\delta}:\tilde{Q}\times\Sigma_e\to\tilde{Q}$ is the transition function defined by: for any $\tilde{q}=(q,l)\in\tilde{Q}$ and $\tilde{\sigma}=(q,\sigma,o)\in\Sigma_e$, we have $\tilde{\delta}(\tilde{q},\tilde{\sigma})!$ whenever $\delta(q,\sigma)!$ and $o\in\mathcal{O}(q,\sigma)$. Furthermore, when $\tilde{\delta}(\tilde{q},\tilde{\sigma})!$, we have

$$\tilde{\delta}(\tilde{q},\tilde{\sigma})=\begin{cases}(\delta(q,\sigma),N) & \text{if } l=N\wedge\tilde{\sigma}\notin\Sigma_{e,F}\\ (\delta(q,\sigma),F) & \text{otherwise}\end{cases}.$$

The above constructed augmented system $\tilde{G}$ has the following properties.

- First, the augmented system $\tilde{G}$ generates extended strings. Essentially, it still tracks the original dynamic of the system by putting both the output realization and the current state information together with the internal event. Therefore, we have $\mathcal{L}(\tilde{G})=\mathcal{L}_e(G)$.
- Second, each augmented state $(q,l)\in\tilde{Q}\subseteq Q\times\{F,N\}$ has two components. The first component q is the actual state in the original system G and the second component $l\in\{N,F\}$ is a label denoting whether fault events have occurred. By the construction, the label will change from N to F only when an extended fault event occurs and once the label becomes F, it will be F forever. We denote by $\tilde{Q}_N=\{(q,l)\in\tilde{Q}:l=N\}$ the set of normal augmented states and the set of faulty states $\tilde{Q}_F$ is defined analogously.

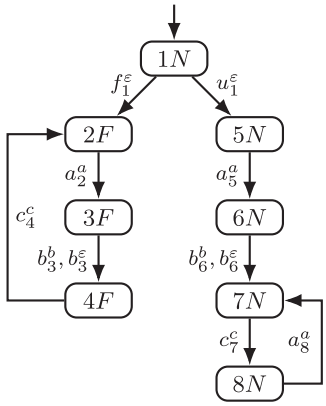

Fig. 2. Augment system $\tilde{G}_1$ of system G_1. For simplicity, we also use σ_q^o to denote the extended event $(q,\sigma,o)\in\Sigma_e$.

Example 5: Still, we consider system G_1 in Fig. 1, which has been discussed in Example 3. The augmented system $\tilde{G}_1$ of G_1 is depicted in Fig. 2 , where all states reachable via extended fault event $(1,f,\varepsilon)$ are augmented with label F and we denote every extended event $(q,\sigma,o)\in\Sigma_e$ by σ_q^o. Furthermore, the transitions of $\tilde{G}_1$ are defined according to the actual transitions and the underlying observations of the original system G_1. For example,

because $\delta(3,b)=4$ and $\mathcal{O}(3,b)=\{b,\varepsilon\}$, we have two new transitions in $\tilde{G}_1$: $\tilde{\delta}(3F,(3,b,b))=4F$ and $\tilde{\delta}(3F,(3,b,\varepsilon))=4F$; each for them represents a different observation realization. □

B. Observation Constrained System

Recall that for any LTL formula φ, there exists an NBA $\mathcal{B}=(X,X_0,2^{\mathcal{AP}},\xi,X_m)$ such that $\mathcal{L}^{\omega}_m(\mathcal{B})=\mathsf{word}(\varphi)$. In order to capture all possible extended strings that can be observed under sensor constraint φ, we construct the observation constrained system.

Definition 6 (Observation constrained system): Given augmented system $\tilde{G}=(\tilde{Q},\tilde{q}_0,\Sigma_e,\tilde{\delta})$ and NBA $\mathcal{B}=(X,X_0,2^{\mathcal{AP}},\xi,X_m)$ associated with LTL formula φ, the *observation constrained system* is defined as a new-tuple

$$T=(Q_T,\Sigma_e,\delta_T,Q_{0,T},Q_{m,T}) \tag{11}$$

where the variables are defined as follows:

- $Q_T\subseteq\tilde{Q}\times X$ is the set of states;
- Σ_e is still the set of extended events;
- $\delta_T: Q_T\times\Sigma_e\to 2^{Q_T}$ is the nondeterministic transition function defined by: for any $q_T=(\tilde{q},x)\in Q_T$ and $\sigma_e\in\Sigma_e$, we have

$$\delta_T(q_T,\sigma_e)=\left\{(\tilde{q}',x'):\ \begin{array}{c}\tilde{q}'=\tilde{\delta}(\tilde{q},\sigma_e)\text{ and}\\ x'\in\xi(x,\mathsf{label}(\sigma_e))\end{array}\right\};$$

- $Q_{0,T}=\{\tilde{q}_0\}\times X_0$ is the set of initial states;
- $Q_{m,T}=\{(\tilde{q},x)\in Q_T: x\in X_m\}$ is the set of accepting states.

Intuitively, the observation constrained system T is constructed by synchronizing the augmented system $\tilde{G}$ with the NBA $\mathcal{B}$ associated with φ according to the atomic propositions. Specifically, for any states $q_T=(\tilde{q},x),q'_T=(\tilde{q}',x')\in\tilde{Q}\times X$ and extended event $\sigma_e\in\Sigma_e$, we have $q'_T\in\delta_T(q_T,\sigma_e)$ whenever (i) in the first (plant model) component, the event itself satisfies the dynamic of the system, i.e., $\tilde{q}'=\tilde{\delta}(\tilde{q},\sigma_e)$; and (ii) in the second (LTL formula) component, the atomic propositions of the event satisfies the transition rules of the Büchi automaton, i.e., $x'\in\xi(x,\mathsf{label}(\sigma_e))$. Therefore, for any string $s=\sigma_1\sigma_2\cdots\sigma_n\in\mathcal{L}(T)$, we have $s\in\mathcal{L}_e(G)=\mathcal{L}(\tilde{G})$ and $\mathsf{trace}(s)\in\mathcal{L}(\mathcal{B})$. Furthermore, by construction, a state $(\tilde{q},x)\in Q_T$ is accepting if its second component $x\in X_m$ is an accepting state in NBA $\mathcal{B}$. Therefore, T essentially recognizes all infinite strings in G satisfying the sensor constraint φ, i.e.,

$$\mathcal{L}^{\omega}_m(T)=\mathcal{L}^{\varphi}_e(G). \tag{12}$$

In Definition 3, we need to compare the observations of prefixes of those strings in $\mathcal{L}^{\varphi}_{e,F}(G)$ with finite strings in $\overline{\mathcal{L}^{\varphi}_e(G)}$. Using observation constrained system T, we know that finite string $s\in\overline{\mathcal{L}^{\varphi}_e(G)}$ if its trace can reach a state in T from which accepting states can be visited infinitely often. To this end, we say a state $q\in Q_T$ in T is *feasible* if $\mathcal{L}^{\omega}_m(T_q)\neq\emptyset$, where $T_q=(Q_T,\Sigma_e,\delta_T,\{q\},Q_{m,T})$ is the NBA by setting the initial state of T as state q. We denote by $Q_{\text{feas},T}\subseteq Q_T$ the set of feasible states. Then, we have the following equivalence

$$s\in\overline{\mathcal{L}^{\varphi}_e(G)}\Leftrightarrow\exists q_0\in Q_{0,T},\delta_T(q_0,s)\cap Q_{\text{feas},T}\neq\emptyset. \tag{13}$$

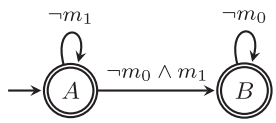

Fig. 3. NBA $\mathcal{B}_{\text{per}}$ for specification $\varphi_{\text{per}}=\Box(m_1\to\Box\neg m_0)$ with $\mathcal{AP}=\{m_0,m_1\}$, where accepting states are highlighted by double circles. Here, we follow the standard abbreviation for drawing NBA over alphabet $2^{\mathcal{AP}}$. For example, transition $\neg m_1$ is the abbreviation of $\{\emptyset,\{m_0\}\}$ and transition $\neg m_0\wedge m_1$ is the abbreviation of $\{\{m_1\}\}$.

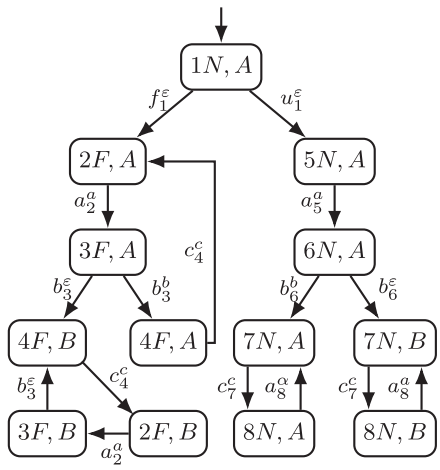

Fig. 4. Observation constrained system T_1 for system $\tilde{G}_1$ with sensor constraint φ_{per}, where all states are accepting.

Also, we denote by $Q_{N,T}=\{(q,N,x)\in Q_T\}$ and $Q_{F,T}=\{(q,F,x)\in Q_T\}$ as the set of normal and faulty states in T, respectively. Then, for any $s\in\overline{\mathcal{L}^{\varphi}_e(G)}$, we also have the following equivalence:

$$\Sigma_{e,F}\in s\Leftrightarrow\exists q_0\in Q_{0,T},\delta_T(q_0,s)\cap Q_{F,T}\neq\emptyset. \tag{14}$$

We illustrate the above concepts by the following example.

Example 6: Let us still consider system G_1 in Fig. 1, whose augmented system $\tilde{G}_1$ has been given in Fig. 2. We still consider sensor constraint φ_{per} in (8), which can be translated to NBA $\mathcal{B}_{\text{per}}$ as shown in Fig. 3. Based on $\tilde{G}_1$ and $\mathcal{B}_{\text{per}}$, we construct the observation constrained system T_1 as shown in Fig. 4, where we omit double circles as all states are accepting. Since all states are accepting and the system is live, we know that all states in T_1 are feasible. For example, finite string $s=(1,f,\varepsilon)(2,a,a)(3,b,\varepsilon)(4,c,c)(2,a,a)(3,b,b)\in\mathcal{L}(\tilde{G})$, we have $s\notin\mathcal{L}(T)$ since proposition m_1 has already been satisfied by $(3,b,\varepsilon)$ and proposition m_0 cannot hold thereafter; i.e., extended event $(3,b,b)$ cannot be synchronized with $\mathcal{B}_{\text{per}}$ when constructing T_1. Hence, we know that $s\notin\overline{\mathcal{L}^{\varphi}_e(G)}$. □

C. Verification Structure

According to Definition 3, a system is *not* φ-diagnosable if there exists an infinite extended faulty string $s\in\mathcal{L}^{\varphi}_{e,F}(G)$ such that for any prefix $t\in\overline{\{s\}}$, there is an extended normal string $v\in\overline{\mathcal{L}^{\varphi}_e(G)}$ having the same output with t. Motivated by this

observation, we construct the verification system to capture all pairs of extended faulty strings and extended normal strings that have the same outputs and both satisfy the sensor constraint.

Definition 7 (Verification system): Given system G and sensor constraint φ, its verification system is a new tuple

$$V = (Q_V, \Sigma_V, \delta_V, Q_{0,V}, Q_{m,V}) \tag{15}$$

where the variables are defined as follows:

- $Q_V \subseteq Q_T \times Q_T$ is the finite set of states;
- $\Sigma_V = \Sigma_V^o \cup \Sigma_V^{uo}$ is the finite set of events, where
  - $\Sigma_V^o = \{(\sigma_1, \sigma_2) \in \Sigma_e \times \Sigma_e : \Theta_\Delta(\sigma_1) = \Theta_\Delta(\sigma_2) \neq \varepsilon\}$;
  - $\Sigma_V^{uo} = \{(\sigma_1, \varepsilon) \in \Sigma_e \times \{\varepsilon\} : \Theta_\Delta(\sigma_1) = \varepsilon\} \cup \{(\varepsilon, \sigma_2) \in \{\varepsilon\} \times \Sigma_e : \Theta_\Delta(\sigma_2) = \varepsilon\}$;
- $\delta_V : Q_V \times \Sigma_V \to 2^{Q_V}$ is the nondeterministic transition function defined by: for any $q_V = (q_1, q_2) \in Q_V$ and $\sigma_V = (\sigma_1, \sigma_2) \in \Sigma_V$, we have

$$\delta_V(q_V, \sigma_V) = \delta_T(q_1, \sigma_1) \times \delta_T(q_2, \sigma_2);$$

- $Q_{0,V} = Q_{0,T} \times Q_{0,T}$ is the set of initial states;
- $Q_{m,V} \subseteq Q_V$ is the set of accepting states defined by

$$Q_{m,V} = \left\{ (q_1, q_2) \in Q_V : \begin{array}{c} q_1 \in Q_{m,T} \cap Q_{F,T} \\ \text{and } q_2 \in Q_{\text{feas},T} \cap Q_{N,T} \end{array} \right\}.$$

Intuitively, each state $q_V = (q_1, q_2)$ in the verification system V is a pair of states in system T. The event set Σ_V is divided into two categories: $\Sigma_V = \Sigma_V^o \cup \Sigma_V^{uo}$, event (σ_1, σ_2) is in Σ_V^o if both σ_1 and σ_2 have the same nonempty output, and event (σ_1, σ_2) is in Σ_V^{uo} if the output of $\sigma_1(\sigma_2)$ is empty and $\sigma_2(\sigma_1)$ is empty. Essentially, V is obtained by synchronizing T with its copy according to their outputs. Then, for event $\sigma_V = (\sigma_1, \sigma_2)$, we denote by $\theta_1(\sigma_V) = \sigma_1$ and $\theta_2(\sigma_V) = \sigma_2$ its first and second components, respectively; the notation is also extended to a string $s = \sigma_V^1 \sigma_V^2 \cdots \in \Sigma_V^* \cup \Sigma_V^\omega$ by $\theta_1(s) = \theta_1(\sigma_V^1)\theta_1(\sigma_V^2)\cdots$ and $\theta_2(s) = \theta_2(\sigma_V^1)\theta_2(\sigma_V^2)\cdots$. By the construction, T has the following properties.

1) For any $s \in \mathcal{L}(V)$, we have $s_1 = \theta_1(s), s_2 = \theta_2(s) \in \mathcal{L}(T)$ and $\Theta_\Delta(s_1) = \Theta_\Delta(s_2)$.
2) For any pair of extended strings $s_1, s_2 \in \mathcal{L}(T)$ such that $\Theta_\Delta(s_1) = \Theta_\Delta(s_2)$, there exists a string $s \in \mathcal{L}(V)$ such that $\theta_1(s) = s_1$ and $\theta_2(s) = s_2$.

Regarding the accepting conditions $Q_{m,V}$, intuitively, a state $q_V = (q_1, q_2)$ is accepting if: 1) its first component q_1 is a faulty accepting state in T; and 2) its second component q_2 is normal and feasible. The first condition says that by repeatedly visiting state $q_V \in Q_{m,V}$, the first component of the string will be an infinite faulty string satisfying φ. The second condition says that for any finite string reaching $q_V \in Q_{m,V}$, the second component of the string is a normal string in $\overline{\mathcal{L}_e^\varphi(G)}$.

D. Checking φ-Diagnosability

Now, we present how to verify φ-diagnosability using the verification system V. To this end, we first introduce some concepts. A *run* in V is a finite sequence $\pi = q_V^1 \xrightarrow{\sigma_V^1} q_V^2 \xrightarrow{\sigma_V^2} \cdots \xrightarrow{\sigma_V^{n-1}} q_V^n$, where $q_V^i \in Q_V, \sigma_V^i \in \Sigma_V$ and $q_V^{i+1} \in \delta_V(q_V^i, \sigma_V^i)$. A run π is called a *cycle* if $q_V^1 = q_V^n$; a cycle π is said to be *reachable* if there exists a finite string $s \in \mathcal{L}(V)$ and $q_{0,V} \in Q_{0,V}$ such that $q_V^1 \in \delta_V(q_{0,V}, s)$.

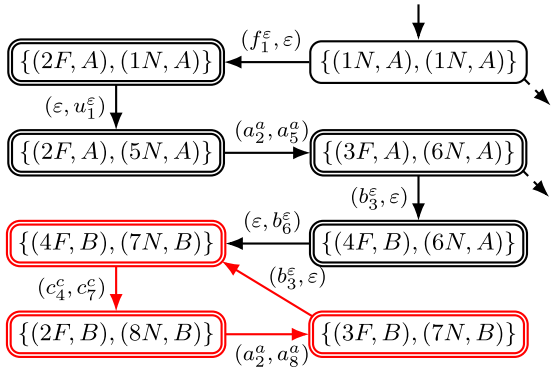

Fig. 5. Verification system V_1.

We are now ready to present the main theorem.

Theorem 3: System G is not φ-diagnosable w.r.t. fault events Σ_F, output function $\mathcal{O}$, and sensor constraint φ, if and only if in the verification system V, there exists a reachable cycle

$$\pi = q_V^1 \xrightarrow{\sigma_V^1} q_V^2 \xrightarrow{\sigma_V^2} \cdots \xrightarrow{\sigma_V^{n-1}} q_V^n$$

such that

1) $\theta_1(\sigma_V^i) \neq \varepsilon$ for some $i = 1, \ldots, n$; and
2) $q_V^j \in Q_{m,V}$ for some $j = 1, \ldots, n$.

The intuition of the above theorem is as follows. Since π is a reachable cycle, we know that we can find an infinite string $s = t(\sigma_V^1 \cdots \sigma_V^N)^\omega$ in V, where t is some string entering the cycle. Then the two conditions ensure that: 1) its first component $\theta_1(s)$ is indeed an infinite extended string in $\mathcal{L}^\omega(\tilde{G})$ that is both faulty and satisfying φ; and 2) its second component $\theta_2(s)$ is an extended string such that any of its finite prefix is normal and can be extended to an infinite string satisfying φ, i.e., $\theta_2(s) \in \overline{\mathcal{L}_e^\varphi(G)}$. Moreover, the construction of V ensures that $\theta_1(s)$ and $\theta_2(s)$ have the same output. Therefore, the existence of such a cycle falsifies φ-diagnosability. The detailed proof is provided in the Appendix. Here we illustrate this theorem by the following example.

Example 7: Let us still consider the running example G_1 in Fig. 1 with the same setting in Example 3. As we have discussed in Example 4, this system is not φ_{per}-diagnosable. Here, we analyze this more formally by Theorem 3. Based on its observation constrained system T_1, we construct the verification system V_1, which is partially shown in Fig. 5, where accepting states are marked by double circles, e.g., state $\{(4F, B), (7N, B)\}$ is in $Q_{m,V}$ as $(4F, B) \in Q_{m,T} \cap Q_{F,T}$ and $(7N, B) \in Q_{\text{feas},T} \cap Q_{N,T}$. Here, we only focus on the reachable cycle satisfying conditions in Theorem 3 and omit other parts without loss of generality for the purpose of verification. Specifically, we consider the cycle as highlighted with red lines in the Fig. 3, i.e.,

$$\{(4F, B), (7N, B)\} \xrightarrow{(c_4^c, c_7^c)} \{(2F, B), (8N, B)\} \xrightarrow{(a_2^a, a_8^a)} \{(3F, B), (7N, B)\} \xrightarrow{(b_3^\varepsilon, \varepsilon)} \{(4F, B), (7N, B)\}.$$

Note that all states in the cycle are accepting states and there exist events (c_4^c, c_7^c) and (a_2^a, a_8^a) such that $\theta_1((c_4^c, c_7^c)) \neq \varepsilon$ and $\theta_1((a_2^a, a_8^a)) \neq \varepsilon$. Thus, system G_1 is not φ_{per}-diagnosable according to Theorem 3. □

Remark 2: We conclude this section by discussing the complexity of checking φ-diagnosability. First, we note that the augmented system $\tilde{G}$ consists of at most $2|Q|$ states, where $|Q|$ denotes the number of states in system G. Second, we obtain the observation constrained system T by composing augmented system $\tilde{G}$ with Büchi automaton $\mathcal{B}$ that is translated from the LTL formula φ. Therefore, T has at most $2 \cdot |Q| \cdot |X|$ states, where $|X|$ is the number of states in the Büchi automaton. In general, for any LTL formula φ, the NBA $\mathcal{B}$ associated with φ has at most $2^{|\varphi|} \cdot |\varphi|$ number of states, where $|\varphi|$ is the number of operators in formula φ [49]. Then, the verification system V has at most $4 \cdot |Q|^2 \cdot |X|^2$ states. Finally, checking the existence of the particular cycle in Theorem 3 is simply a cycle search problem which can be done in polynomial-time in the size of V [52]. Overall, our approach is polynomial in the size of the system model G and exponential in the length of the sensor constraint formula φ.

VI. Applications of the Uniform Framework

Our framework consists of the following four steps:

1) Choose atomic propositions $\mathcal{AP}$ and labeling function $\mathsf{label} : \Sigma_e \to 2^{\mathcal{AP}}$;
2) Describe the sensor constraint by LTL formula φ;
3) Construct the observation constrained system T and the verification system V;
4) Check φ-diagnosability based on V by Theorem 3.

In the previous sections, we have shown how to implement Steps 3 and 4. However, Steps 1 and 2 are more application-dependent, i.e., one needs to carefully choose $\mathcal{AP}$ and label, and write down φ based on the specific scenario of the system. In this section, we show explicitly how the proposed new notion of φ-diagnosability subsumes existing notions of 1) diagnosability under intermittent sensor failures; 2) diagnosability under permanent sensor failures; and 3) K-loss diagnosability. Furthermore, we introduce two new types of diangsability called 1) diagnosability under output fairness; and 2) diagnosability under unreliable sensors with minimum dwell-time, using the general notion of φ-diagnosability.

A. Diagnosability Subject to Sensor Failures

In Remark 1, we have discussed how to capture the notion of robust diagnosability subject to *intermittent sensor failures* in our framework. Furthermore, we have shown, by the running example, that how to model the notion of robust diagnosability subject to *permanent sensor failures* in our framework for the special case of a single failure sensor. Here we formally present a unified way that supports both intermittent and permanent sensor failures using our framework.

Let $G = (Q, \Sigma, \delta, q_0)$ be the system model. We assume that transitions $\mathbb{T} \subseteq Q \times \Sigma$ are partitioned as follows:

$$\mathbb{T} = \mathbb{T}_{uo} \dot{\cup} \mathbb{T}_o \dot{\cup} \mathbb{T}_{\mathsf{int}} \dot{\cup} \mathbb{T}_{\mathsf{per}}$$

where the variables are defined as follows:

1) $\mathbb{T}_{uo}$ are transitions that can never be observed;
2) $\mathbb{T}_o$ are transitions that can always be observed;
3) $\mathbb{T}_{\mathsf{int}}$ are transitions subject to intermittent sensor failures;
4) $\mathbb{T}_{\mathsf{per}}$ are transitions subject to permanent sensor failures.

Similar to (4), we define an observation mapping $\mathcal{O} : Q \times \Sigma \to 2^{\Sigma \cup \{\varepsilon\}}$ by: for any $q \in Q$ and $\sigma \in \Sigma$, we have

$$\mathcal{O}(q, \sigma) = \begin{cases} \{\varepsilon\} & \text{if } (q, \sigma) \in \mathbb{T}_{uo} \\ \{\sigma\} & \text{if } (q, \sigma) \in \mathbb{T}_o \\ \{\sigma, \varepsilon\} & \text{if } (q, \sigma) \in \mathbb{T}_{\mathsf{int}} \cup \mathbb{T}_{\mathsf{per}} \end{cases}. \tag{16}$$

Note that, for those transitions subject to intermittent sensor failures, there is no need to put additional sensor constraints since they are freely to fail or recover. However, we need to use LTL formula to constrain the behavior of those sensors subject to permanent sensor failures. To this end, we choose the following set of of atomic propositions

$$\mathcal{AP}_{\mathsf{per}} = \{m_i^{(q,\sigma)} : i \in \{0, 1\}, (q, \sigma) \in \mathbb{T}_{\mathsf{per}}\} \tag{17}$$

where $m_0^{(q,\sigma)}$ means that the sensor observes event σ successfully for transition (q, σ), i.e., the corresponding sensor is normal, while $m_1^{(q,\sigma)}$ means that the sensor misses the observation for transition (q, σ), i.e., the corresponding sensor is faulty. Then, the labeling function $\mathsf{label}_{\mathsf{per}} : \Sigma_e \to 2^{\mathcal{AP}_{\mathsf{per}}}$ is defined by: for any $\sigma_e = (q, \sigma, o) \in \Sigma_e$, we have

$$\mathsf{label}_{\mathsf{per}}(\sigma_e) = \begin{cases} \{m_0^{(q,\sigma)}\}, & \text{if } (q, \sigma) \in \mathbb{T}_{\mathsf{per}} \wedge o = \sigma \\ \{m_1^{(q,\sigma)}\}, & \text{if } (q, \sigma) \in \mathbb{T}_{\mathsf{per}} \wedge o = \varepsilon \\ \emptyset, & \text{otherwise.} \end{cases} \tag{18}$$

Then, the sensor constraint for the scenario of intermittent/permanent failures can be written as

$$\varphi_{\mathsf{int} \wedge \mathsf{per}} = \bigwedge_{(q,\sigma) \in \mathbb{T}_{\mathsf{per}}} \Box(m_1^{(q,\sigma)} \to \Box \neg m_0^{(q,\sigma)}). \tag{19}$$

Remark 3: If we only consider the case of intermittent sensor failures, i.e., $\mathbb{T}_{\mathsf{per}} = \emptyset$, then the above formulation becomes $\mathcal{AP}_{\mathsf{per}} = \emptyset$, $\mathsf{label}_{\mathsf{per}}(\sigma_e) = \emptyset, \forall \sigma_e \in \Sigma_e$ and $\varphi_{\mathsf{int} \wedge \mathsf{per}} = \mathtt{true}$. Then, the Büchi automaton $\mathcal{B}_{\mathsf{int} \wedge \mathsf{per}}$ associated with $\varphi_{\mathsf{int} \wedge \mathsf{per}}$ only contains a single state with a self-loop labeled with $\mathtt{true}$. Therefore, such an NBA $\mathcal{B}_{\mathsf{int} \wedge \mathsf{per}}$ will not restrict the behavior of $\tilde{G}$ at all, and the verification system V essentially becomes to the standard structures in [20].

Remark 4: An approach for the unification of diagnosability of DES subject to both intermittent and permanent sensor failures has been recently proposed by [29]. The above presented proposed further generalized the result in [29] by supporting state-dependent (or transition-based) observations. Furthermore, the result in [29] is an instance of our general framework, which, as we will further show later, supports much more user-specified scenarios.

B. K-Loss Robust Diagnosability

Recently, in [34], the authors proposed a new notion of K-loss diagnosability in order to capture the scenario of bounded

losses in observation channels. In this setting,[1] it is assumed that the event set is partitioned as $\Sigma = \Sigma_o \cup \Sigma_{uo}$. Observable events in Σ_o are transmitted from the sensors to the diagnoser via $n \leq |\Sigma_o|$ communication channels. To this end, the set of observable events Σ_o is further partitioned as

$$\Sigma_o = \Sigma_{o,1} \dot{\cup} \Sigma_{o,2} \dot{\cup} \cdots \dot{\cup} \Sigma_{o,n}$$

where for each $i \in \{1, \ldots, n\}$, $\Sigma_{o,i}$ is the set of events whose observations are transmitted via the ith communication channel. Furthermore, it is assumed that for each observation channel $i \in \{1, \ldots, n\}$, integer $k_i \in \mathbb{N}$ is the maximum number of *consecutive losses of observations*. That is, if event $\sigma \in \Sigma_{o,i}$ occurs $k_i + 1$ times consecutively and the diagnoser does not receive its first k_i occurrences due to losses in the observation channel, then its $k_i + 1$th occurrence will be received by the diagnoser for sure. We denote by $K = (k_1, \ldots, k_n)$ the tuple of all maximum numbers of consecutive loss for all channels. The notion of K-loss (co)diagnosability was introduced in [34] as the necessary and sufficient condition for the existence of a diagnoser under such a setting.

Now, we discuss how to formulate K-loss diagnosability in terms of our general notion of φ-diagnosability. For system $G = (Q, \Sigma, f, q_0)$, we define observation mapping $\mathcal{O} : Q \times \Sigma \to 2^{\Sigma_o \cup \{\varepsilon\}}$ by: For any $q \in Q$ and $\sigma \in \Sigma$, we have

$$\mathcal{O}(q, \sigma) = \begin{cases} \{\varepsilon\} & \text{if } (q, \sigma) \in \Sigma_{uo} \\ \{\sigma, \varepsilon\} & \text{if } (q, \sigma) \in \Sigma_o \end{cases}. \tag{20}$$

Then, we choose the set of atomic propositions by

$$\mathcal{AP}_{\text{K-loss}} = \{m_i^j : i \in \{0, 1\}, j \in \{1, \ldots, n\}\} \tag{21}$$

where m_0^j means that an event $\sigma \in \Sigma_{o,j}$ occurs and it is transmitted successfully in the jth channel and m_1^j means that an event transmission in the jth channel is lost. To capture the above meanings, we define a labeling function $\mathsf{label}_{\text{K-loss}}$ by: for any $\sigma_e = (q, \sigma, o) \in \Sigma_e$, we have

$$\mathsf{label}_{\text{K-loss}}(\sigma_e) = \begin{cases} \{m_0^j\}, & \text{if } \sigma \in \Sigma_{o,j} \wedge o \neq \varepsilon \\ \{m_1^j\}, & \text{if } \sigma \in \Sigma_{o,j} \wedge o = \varepsilon \\ \emptyset, & \text{otherwise} \end{cases} \tag{22}$$

where $j \in \{1, \ldots, n\}$.

To formalize the sensor constraint for K-loss diagnosability, we need to exclude the scenario, where there are more than k_j consecutive observation losses for some channel $j \in \{1, \ldots, n\}$. To this end, for each $j \in \{1, \ldots, n\}$, we define a sequence of LTL formulae $\Phi^j(0), \ldots, \Phi^j(k_j)$ as follows:

$$\begin{cases} \Phi^j(0) = m_1^j, \\ \Phi^j(k) = m_1^j \wedge \bigcirc(\neg m_0^j U \Phi^j(k-1)) \end{cases} \tag{23}$$

where $k \geq 1$. Intuitively, $\Phi^j(0) = m_1^j$ means that the current observation in the jth channel is lost. Then $\Phi^j(1) = m_1^j \wedge \bigcirc(\neg m_0^j U m_1^j)$ means that the current observation in the jth channel is lost and the no event $\Sigma_{o,j}$ in the jth channel can be observed until the next observation loss in the jth channel, which means that the jth channel will have two consecutive losses. Therefore, by induction, $\Phi^j(k)$ means that the observations in the jth channel will have $k+1$ consecutive losses. Then, the requirement that "starting from any instant, the jth observation channel cannot have $k_j + 1$ consecutive losses" can be captured by the LTL formula $\Box\neg\Phi^j(k_j) = \neg\Diamond\Phi^j(k_j)$.Since we require that all n channels satisfy the K-loss assumption, the sensor constraint for this scenario is given by

$$\varphi_{\text{K-loss}} = \bigwedge_{j \in \{1, \ldots, n\}} \Box\neg\Phi^j(k_j). \tag{24}$$

We use the following example to illustrate this scenario.

Example 8: We consider the system G_2, shown in Fig. 6(a), where the observable events $\Sigma_o = \{a, b, c\}$ are partitioned into two observation channels with $\Sigma_{o,1} = \{a, c\}$ and $\Sigma_{o,2} = \{b\}$. We assume that $k_1 = 0$ and $k_2 = 1$, i.e., the first channel for $\Sigma_{o,1}$ is reliable without observation loss and the second channel for $\Sigma_{o,2}$ can only have at most one consecutive observation loss. Then, the set atomic propositions is $\mathcal{AP}_{\text{K-loss}} = \{m_0^1, m_1^1, m_0^2, m_1^2\}$, the labeling function is specified in (22) and the sensor constraint is

$$\varphi_{\text{K-loss}} = \Box\neg m_1^1 \wedge \Box\neg(m_1^2 \wedge \bigcirc(\neg m_0^2 U m_1^2)).$$

The Büchi automaton $\mathcal{B}_{\text{K-loss}}$ associated with $\varphi_{\text{K-loss}}$ is shown in Fig. 6(b). We construct the verification system V_2, which is partially depicted in Fig. 6(c). Due to the sensor constraint $\varphi_{\text{K-loss}}$, if the event b_3^ε or b_6^ε occurs in G_2, the next occurrence of b_3^ε or b_6^ε is possible only after b_3^b or b_6^b occurs. For example, from state 3, if the event b_3^ε occurs, we can only obtain the extended string $b_3^\varepsilon c_4^c a_2^a b_3^b$ rather than $b_3^\varepsilon c_4^c a_2^a b_3^\varepsilon$ since the latter corresponds to the case of two consecutive losses in channel $\Sigma_{o,2}$. Furthermore, for the first communication channel, since its maximum failure bound is $k_1 = 0$, i.e., if it is reliable, the extended events such as a_2^ε and c_4^ε will not be feasible. In Fig. 6(c), we see that the system is blocked at state $\{(3F, B), (7N, A)\}$. This is because that the first component $(3F, B)$ means that the second communication channel has lost an observation and, therefore, has to transit next observation successfully. However, only event b_3^b can occur from state $(3F, B)$, while only event c_7^c can occur at state $(7N, A)$. With the similar reason, one can also complete the remaining part of V_2 in which no reachable cycle satisfying the conditions in Theorem 3 can be found. Therefore, system G_2 is $\varphi_{\text{K-loss}}$-diagnosable. □

C. Unreliable Sensors With Minimum Dwell-Time

We have shown that both intermittent sensor failures and permanent sensor failures can be captured in our unified framework. Note that, in the existing framework of intermittent sensor failures, those unreliable sensors can fail and recover *arbitrarily* at any instant. Here, we show how our LTL-based approach can describe a more general scenario, where sensors may switch between failure mode and normal mode but with *minimum dwell-time* for each mode. This is motivated by the practical scenario that whenever a normal sensor breaks down, it will take some time to recover, and whenever a sensor failure is fixed, it can ensure to work normally for some periods.

[1]Results in [34] considers the decentralized setting. Here, we just review its centralized counterpart.

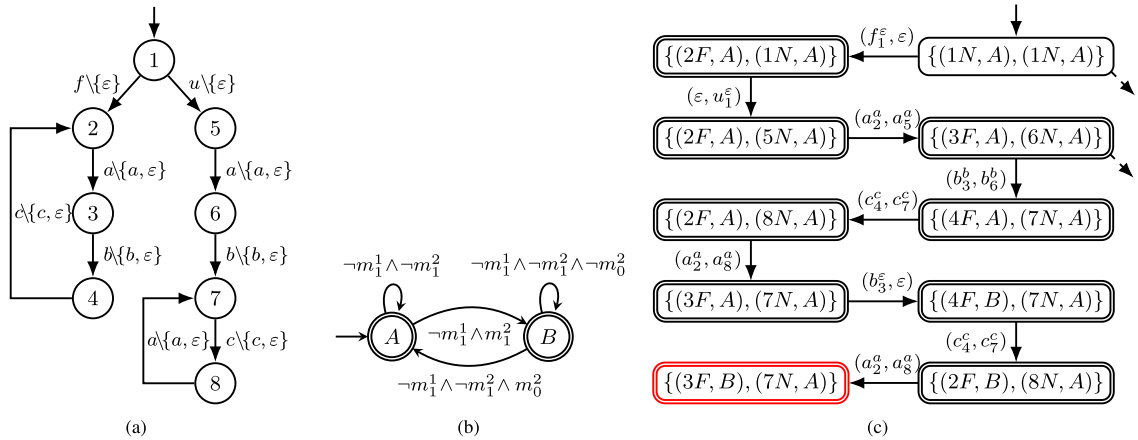

Fig. 6. Example of *K*-loss robust diagnosability. For system G_2: $\Sigma_o = \Sigma_{o,1} \cup \Sigma_{o,2}, \Sigma_{o,1} = \{a, c\}$, and $\Sigma_{o,2} = \{b\}$. (a) System G_2. (b) Büchi automaton $\mathcal{B}_{\text{K-loss}}$. (c) Verification system V_2.

Still, we consider system $G = (Q, \Sigma, \delta, q_0)$ and assume that the event set is partitioned as $\Sigma = \Sigma_o \dot{\cup} \Sigma_{uo} \dot{\cup} \Sigma_{ur}$, where Σ_{ur} is the set of events whose sensors are unreliable. We denote by $k_N \in \mathbb{N}$ the minimum dwell-time for the normal mode (or simply, *normal dwell-time*), which means that whenever a sensor recovers from failure to normal, it will remain normal at least for the next k_N uses of the sensor. Similarly, we denote by $k_F \in \mathbb{N}$ the minimum dwell-time for the failure mode (or simply, *failure dwell-time*), which means that whenever a sensor breaks down from normal to failure, it will remain failure at least for the next k_F uses of the sensor.

To formalized the above setting in our framework, we define an observation mapping $\mathcal{O} : Q \times \Sigma \to 2^{\Sigma_o \cup \Sigma_{ur} \cup \{\varepsilon\}}$ by: For any $q \in Q$ and $\sigma \in \Sigma$, we have

$$\mathcal{O}(q, \sigma) = \begin{cases} \{\varepsilon\} & \text{if } \sigma \in \Sigma_{uo} \\ \{\sigma\} & \text{if } \sigma \in \Sigma_o \\ \{\sigma, \varepsilon\} & \text{if } \sigma \in \Sigma_{ur} \end{cases}. \tag{25}$$

The set of atomic propositions is chosen as

$$\mathcal{AP}_{\mathsf{dwell}} = \{m_i^\sigma : i = 0, 1, \sigma \in \Sigma_{ur}\} \tag{26}$$

where m_0^σ means that event $\sigma \in \Sigma_{ur}$ occurs and its sensor is normal, while m_1^σ means that event $\sigma \in \Sigma_{ur}$ occurs and its sensor is failing. The labeling function $\mathsf{label}_{\mathsf{dwell}}$ is defined by: For any $\sigma_e = (q, \sigma, o) \in \Sigma_e$, we have

$$\mathsf{label}_{\mathsf{dwell}}(\sigma_e) = \begin{cases} \{m_0^\sigma\}, & \text{if } \sigma \in \Sigma_{ur} \wedge o \neq \varepsilon \\ \{m_1^\sigma\}, & \text{if } \sigma \in \Sigma_{ur} \wedge o = \varepsilon \\ \emptyset, & \text{otherwise} \end{cases}. \tag{27}$$

To capture the sensor constraint of normal dwell-time, we first need to exclude the scenarios where a sensor switches from the failure mode to the normal mode and remains normal for less than k_N uses, before the next switch back to the failure mode. To this end, we define a sequence of LTL formulae inductively as follows:

$$\begin{cases} \Phi_{\mathsf{nor}}^\sigma(1) = m_0^\sigma \wedge \bigcirc(\neg m_0^\sigma U m_1^\sigma) \\ \Phi_{\mathsf{nor}}^\sigma(k) = m_0^\sigma \wedge \bigcirc((\neg m_0^\sigma \wedge \neg m_1^\sigma) U \Phi_{\mathsf{nor}}^\sigma(k-1)) \end{cases}. \tag{28}$$

Intuitively, $\Phi_{\mathsf{nor}}^\sigma(1)$ means that, σ is observed currently with a normal sensor, and there is no occurrence of σ until its sensor fails. Therefore, this formula captures the scenario where the sensor of event σ remains normal for one time of use before switching to the failure mode. By induction, $\Phi_{\mathsf{nor}}^\sigma(k)$ means that the sensor of event σ has remained normal for k times of use before switching to the failure mode.

Since the dwell-time of normal mode is counted starting from the transition from failure mode to normal mode, we can describe the scenario where sensor switches from failure mode to normal mode and remains at normal mode for k uses before switching back to failure mode by the following formula:

$$\Phi_{\mathsf{nor,dwell}}^\sigma(k) = m_1^\sigma \wedge \bigcirc(\neg m_0^\sigma U \Phi_{\mathsf{nor}}^\sigma(k)). \tag{29}$$

However, the minimum normal dwell-time k_N requires that the above formula should not be satisfied for any $k \leq k_N - 1$; otherwise, it means that the sensor fails again when it switches back to normal for less than k_N times of uses. Therefore, the overall, normal dwell-time constraint is given by

$$\Phi_{\mathsf{nor,dwell}} = \bigwedge_{\sigma \in \Sigma_{ur}} \bigwedge_{k=1,\ldots,k_N-1} \Box \neg \Phi_{\mathsf{nor,dwell}}^\sigma(k). \tag{30}$$

Similar to the case of normal dwell-time, we can define the sensor constraint for failure dwell-time by

$$\Phi_{\mathsf{fail,dwell}} = \bigwedge_{\sigma \in \Sigma_{ur}} \bigwedge_{k=1,\ldots,k_F-1} \Box \neg \Phi_{\mathsf{fail,dwell}}^\sigma(k) \tag{31}$$

where we have

$$\begin{cases} \Phi_{\mathsf{fail,dwell}}^\sigma(k) = m_0^\sigma \wedge \bigcirc(\neg m_1^\sigma U \Phi_{\mathsf{fail}}^\sigma(k)) \\ \Phi_{\mathsf{fail}}^\sigma(1) = m_1^\sigma \wedge \bigcirc(\neg m_1^\sigma U m_0^\sigma) \\ \Phi_{\mathsf{fail}}^\sigma(k) = m_1^\sigma \wedge \bigcirc((\neg m_1^\sigma \wedge \neg m_0^\sigma) U \Phi_{\mathsf{fail}}^\sigma(k-1)) \end{cases}. \tag{32}$$

Therefore, the overall sensor constraint for both normal and failure dwell-times is given by

$$\varphi_{\mathsf{dwell}} = \Phi_{\mathsf{nor,dwell}} \wedge \Phi_{\mathsf{fail,dwell}}. \tag{33}$$

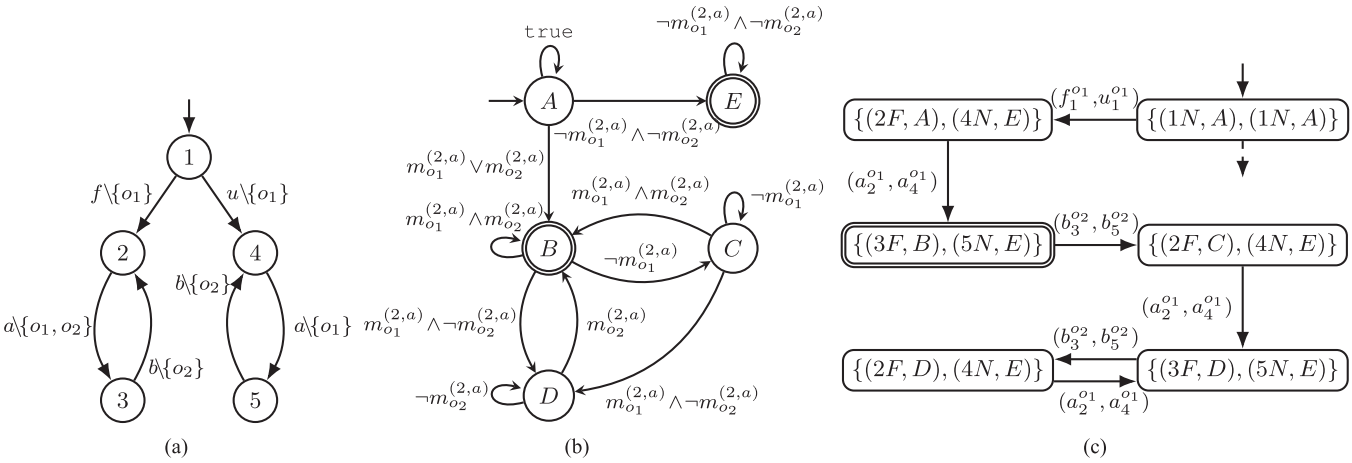

Fig. 7. Example of diagnosability with output fairness. For system G_3: $\Sigma=\{a,b,f,u\}$ and $\Delta=\{o_1,o_2\}$. (a) System G_3. (b) Büchi automaton $\mathcal{B}_{\text{fair}}$. (c) Verification system V_3.

D. Diagnosability With Output Fairness

In the previous three subsections, we have $\Delta\subseteq\Sigma$ in the observation mapping due to the specific meanings of sensor failures or observation losses. Here, we further consider the general case where Δ and Σ are different.

As a motivating example, consider system G_3 shown in Fig. 7(a) with $\Sigma=\{a,b,f,u\}$, $\Sigma_F=\{f\}$ and $\Delta=\{o_1,o_2\}$. The output function $\mathcal{O}:Q\times\Sigma\to 2^{\Delta\cup\{\varepsilon\}}$ is specified in Fig. 7(a). Without any sensor constraint, the system is not diagnosable according to Definition 1 as defined in [23]. This is because one can observe output sequence $o_1(o_1o_2)^n$ for an arbitrary large n for which we cannot determine whether the underlying internal string is faulty or normal.

However, this above issue of nondiagnosability is not very practical since it is *unfair* for output o_2 at transition $(2,a)$. Specifically, the reason why we may observe output sequence $o_1(o_1o_2)^\omega$ is that, after the occurrence of fault event f, every time the system fires transition $(2,a)$, output symbol o_2 loses its opportunity to be observed. However, if we assume that the occurrences of o_1 and o_2 are purely random with some (unknown but nonzero) probabilities, then o_2 will be observed with probability one at the system goes on and upon its occurrence, we can detect the fault.

Instead of going to a probability framework to resolve the above issue [21], [22], here we propose to use *fairness condition*, which is a widely used assumption in reactive systems, to rule out those unrealistic infinite behaviors of the sensors. Formally, still let $G=(Q,\Sigma,\delta,q_0)$ be the system model with an arbitrary output function $\mathcal{O}:Q\times\Sigma\to 2^{\Delta\cup\{\varepsilon\}}$. We assume that

$$\mathbb{T}_{\text{fair}}\subseteq Q\times\Sigma$$

is the set of transitions for which all of its outputs are *fair* in the sense that if transition $(q,\sigma)\in\mathbb{T}_{\text{fair}}$ is fired for infinite number of times, then all of its observations $o\in\mathcal{O}(q,\sigma)$ can be observed for infinite number of times. To formalize this requirement, we choose the set of atomic propositions by

$$\mathcal{AP}_{\text{fair}}=\{m_o^{(q,\sigma)}:(q,\sigma)\in\mathbb{T}_{\text{fair}},o\in\mathcal{O}(q,\sigma)\}\tag{34}$$

where $m_o^{(q,\sigma)}$ means that the output of transition $(q,\sigma)\in\mathbb{T}_{\text{fair}}$ is $o\in\mathcal{O}(q,\sigma)$. For brevity, for each transition $(q,\sigma)\in\mathbb{T}_{\text{fair}}$, we denote by $m^{(q,\sigma)}$ the proposition that transition (q,σ) occurs, i.e., $m^{(q,\sigma)}=\bigvee_{o\in\mathcal{O}(q,\sigma)}m_o^{(q,\sigma)}$.

Based on $\mathcal{AP}_{\text{fair}}$, we define the labeling function by: For any $\sigma_e=(q,\sigma,o)\in\Sigma_e$, we have

$$\mathsf{label}_{\text{fair}}(\sigma_e)=\begin{cases}\{m_o^{(q,\sigma)}\}, & \text{if } (q,\sigma)\in\mathbb{T}_{\text{fair}}\\ \emptyset, & \text{otherwise}\end{cases}.\tag{35}$$

Then, the sensor constraint for the scenario of fairness assumption can be written as

$$\varphi_{\text{fair}}:=\bigwedge_{(q,\sigma)\in\mathbb{T}_{\text{fair}}}\left(\Box\Diamond m^{(q,\sigma)}\to\bigwedge_{o\in\mathcal{O}(\sigma,q)}\Box\Diamond m_o^{(q,\sigma)}\right).\tag{36}$$

We use the following example to illustrate this scenario.

Example 9: Still we consider system G_3, which is shown to be nondiagnosable according to Definition 1. Now we show that the system is actually φ-diagnosable under the fairness assumption for outputs. Specifically, we define $\mathbb{T}_{\text{fair}}=\{(2,a)\}$ as the set of fair transition. Then, the set of atomic propositions is $\mathcal{AP}_{\text{fair}}=\{m_{o_1}^{(2,a)},m_{o_2}^{(2,a)}\}$. Then, the sensor constraint for output fairness can be written as

$$\varphi_{\text{fair}}=\left(\Box\Diamond(m_{o_1}^{(2,a)}\vee m_{o_2}^{(2,a)})\right)\to\left((\Box\Diamond m_{o_1}^{(2,a)})\wedge(\Box\Diamond m_{o_2}^{(2,a)})\right)$$

which means that if transition $(2,a)$ occurs infinitely, then we will observe each possible output in $\mathcal{O}(2,a)=\{o_1,o_2\}$ for infinite number of times. The Büchi automaton $\mathcal{B}_{\text{fair}}$ associated with LTL formula φ_{fair} is shown in Fig. 7(b). It is worth noticing that, in contrast to Büchi automata in the previous examples, where all states are accepting, here only some states in $\mathcal{B}_{\text{fair}}$ are accepting. This is because that fairness condition φ_{fair} is an *liveness* type of property, while all previous conditions $\varphi_{\text{int}\wedge\text{per}}$, $\varphi_{\text{K-loss}}$, and φ_{dwell} belong to the category of *safety* properties. To verify φ_{fair}-diagnosability, we construct the verification system V_3 of system G_3, which is partially depicted in Fig. 7(b). Note

that, although there is a cycle $\{(3F,D),(5N,E)\} \xrightarrow{(b_3^{o2},b_5^{o2})} \{(2F,D),(4N,E)\} \xrightarrow{(a_2^{o1},a_4^{o1})} \{(3F,D),(5N,E)\}$ in V_3, it does not satisfy the conditions in Theorem 3 since the states in the cycle are not accepting. Essentially, this cycle corresponds to the unfair extended string making the system not diagnosable without fairness assumption. One can check that, in the remaining part of V_3, there is no cycle satisfying the conditions in Theorem 3, i.e., G_3 is φ_{fair}-diagnosable. □

Remark 5: We note that the verification of diagnosability of fair DES has been investigated by [45], [53], and [54]. However, the notion of fairness is different from our setting here. Specifically, existing works assume that the dynamic of the system is fair in the sense that each transition can be executed for infinite number of times whenever it is enabled infinitely. However, the observation mappings considered therein are still statically modeled as a natural projection. In contrast, we impose fairness constraint on the observation mapping rather than the internal behavior of the system the system's dynamic. Furthermore, diagnosability with output fairness has been studied in our preliminary work [47]. However, the verification algorithm in [47] is customized only to the case of output fairness. Here, we address this problem within our general framework using the unified verification procedure.

Remark 6: One can verify that the LTL formulae in Sections VI-A–C are all safety properties. Therefore, for each corresponding notion of φ-diagnosability, a uniform detection bound always exists if the system is φ-diagnosable. On the other hand, the LTL formula φ_{fair} here is not a safety property, which means that one cannot ensure the existence of a uniform detection bound.

VII. Conclusion

In this article, we developed a uniform framework for diagnosability analysis of DES subject to unreliable sensors. To this end, we used LTL formulae as a general and user-friendly tool to model unreliable sensors without restricting to specific sensor types. We proposed a new notion of φ-diagnosability as well as its effective verification procedure. Our approach leverages the automated transformation from LTL formulae to Büchi automata, which avoids hand-coding the sensor automata case-by-case. Our framework not only unifies different existing notions of robust diagnosability of DES subject to unreliable sensors, but also supports new scenarios of unreliable sensors for which the diagnosability verification problems have never been considered. In the future, we would like to extend our framework to the decentralized setting with multiple local diagnosers. Also, we would like to further investigate the active diagnosis problem for DES subject to unreliable sensors within our uniform framework.

Appendix

Proof of Theorem 1

Proof: ($\Rightarrow$) Suppose that there exists a diagnoser D satisfying conditions C1 and C2, while, for the sake of contradiction that system G is not φ-diagnosable. This means that there exists an infinite extended faulty string $s \in \mathcal{L}_{e,F}^{\varphi}(G)$ such that for any prefix $t \in \overline{\{s\}}$, there exists an extended normal string $w \in \overline{\mathcal{L}_e^{\varphi}(G)}$ having the same observation with t. Since diagnoser D satisfies condition C2, for any $t \in \overline{\{s\}}$, we have $D(\Theta_\Delta(t)) = 0$; otherwise, if $D(\Theta_\Delta(t)) = 1$, we have $D(\Theta_\Delta(v)) = D(\Theta_\Delta(t)) = 1$, which violates condition C2. Therefore, $\forall t \in \overline{\{s\}} : D(\Theta_\Delta(t)) = 0$, i.e., condition C1 does not hold for diagnoser D, which contradicts the assumption.

($\Leftarrow$) Suppose that system G is φ-diagnosable. We consider a diagnoser $D : \{\Theta_\Delta(v) \in \mathcal{O}(\mathcal{L}(G)) : v \in \overline{\mathcal{L}_e^{\varphi}(G)}\} \to \{0,1\}$ defined by: for any $o \in \{\Theta_\Delta(v) \in \mathcal{O}(\mathcal{L}(G)) : v \in \overline{\mathcal{L}_e^{\varphi}(G)}\}$

$$D(o) = \begin{cases} 1 & \text{if } \forall s \in \overline{\mathcal{L}_e^{\varphi}(G)} : o = \Theta_\Delta(s) \Rightarrow \Sigma_{e,F} \in \Theta_\Sigma(s) \\ 0 & \text{otherwise.} \end{cases}$$

We claim that diagnoser D satisfies conditions C1 and C2. We first show that the diagnoser satisfies condition C2. For any extended normal string $s \in \overline{\mathcal{L}_e^{\varphi}(G)}$ and $\Sigma_{e,F} \notin \Theta_\Sigma(s)$, we have $D(\Theta_\Delta(s)) = 0$, i.e., C2 holds. To see that C1 holds, we consider an extended faulty string $s \in \mathcal{L}_{e,F}^{\varphi}(G)$. By φ-diagnosability, there exists a finite prefix $t \in \overline{\{s\}}$ such that any finite extended string v having the same observation with t is faulty, i.e., $\Sigma_{e,F} \in \Theta_\Sigma(v)$. Then, we have $D(\Theta_\Delta(t)) = 1$, i.e., condition C1 also holds. □

Proof of Theorem 3

Proof: ($\Leftarrow$) Assume that there exists a reachable cycle $\pi' = q_V^1 \xrightarrow{\sigma_V^1} q_V^2 \xrightarrow{\sigma_V^2} \cdots \xrightarrow{\sigma_V^{n-1}} q_V^n$ in the verification system V such that $q_V^i \in Q_{m,V}$ and $\theta_1(\sigma_V^j) \neq \varepsilon$ for some $i,j \in \{1,2,\ldots,n\}$, but the system G is φ-diagnosable. Without loss of generality, let $q_V^1 = (q_1,q_2) \in Q_{m,V}$, i.e., $i = 1$, and $s_2 = \sigma_V^1\sigma_V^2\cdots\sigma_V^{n-1}$. Since cycle π' is reachable, we can find a string $s_1 \in \mathcal{L}(V)$ such that $q_V^1 \in f_V(q_{0,V}, s_1)$, where $q_{0,V} \in Q_{0,V}$. After repeating the cycle for infinite number of times, we obtain an infinite string $s = s_1(s_2)^\omega \in \mathcal{L}^\omega(V)$, over which we get a run $\pi = q_V^0 \xrightarrow{\sigma_V^0} \cdots (q_V^1 \xrightarrow{\sigma_V^1} q_V^2 \xrightarrow{\sigma_V^2} \cdots \xrightarrow{\sigma_V^{n-1}} q_V^n)^\omega$. Along run π, we can extract a path $\rho = q_V^0 \cdots (q_V^1 \cdots q_V^n)^\omega$, where accepting state $q_V^1 \in Q_{m,V}$ appears for infinite number of times, i.e., $\mathsf{Inf}(\rho) \cap Q_{m,V} \neq \emptyset$. Since there exists $i \in \{1,2,\ldots,n\}$ such that $\theta_1(\sigma_V^i) \neq \varepsilon$, the first component of sequence $s_l = \theta_1(s)$ is also an infinite extended string. By $q_V^1 = (q_1,q_2) \in Q_{m,V}$, we know that q_1 is included in $Q_{m,T} \cap Q_{F,T}$ which means infinite extended string s_l is faulty and accepting in system T, that is, $s_l \in \mathcal{L}_{e,F}^{\varphi}(G)$. On the other hand, $q_2 \in Q_{\text{feas},T} \cap Q_{N,T}$ and by (13), the second component of sequence $s_r = \theta_2(s)$ is normal and every prefix of s_r is a prefix of an accepting extended string, i.e., $\forall v \in \overline{\{s_r\}}, v \in \overline{\mathcal{L}_e^{\varphi}(G)}$ and $\Sigma_{e,F} \notin s_r$. Thus, by the first property of the verification system, for any finite prefix $t \in \overline{\{s_l\}}$, there exists $v \in \overline{\{s_r\}} \subset \overline{\mathcal{L}_e^{\varphi}(G)}$ and $\Sigma_{e,F} \notin v$ such that $\Theta_\Delta(t) = \Theta_\Delta(v)$, i.e., G is not φ-diagnosable.

($\Rightarrow$) Suppose that system G is not φ-diagnosable. That is, there exists an infinite faulty extended string $s \in \mathcal{L}_{e,F}^{\varphi}(G)$ such that for any prefix $t \in \overline{\{s\}}$, we have a normal extended string $v \in \overline{\mathcal{L}_e^{\varphi}(G)}$ with the same observation of t, i.e.,

$$(\exists s \in \mathcal{L}_{e,F}^{\varphi}(G))(\forall t \in \overline{\{s\}}) : (\exists v \in \overline{\mathcal{L}_e^{\varphi}(G)})[\Theta_\Delta(w) = \Theta_\Delta(t) \wedge \Sigma_{e,F} \notin w]. \quad (37)$$

Thus, for infinite extended faulty string $s \in \mathcal{L}^{\varphi}_{e,F}(G)$, there exists a path ρ along string s in system T such that $\mathsf{Inf}(\rho) \cap Q_{m,T} \cap Q_{F,T} \neq \emptyset$. By the accepting condition of Büchi automata, we can select a state $q_1 \in \mathsf{Inf}(\rho) \cap Q_{m,T} \cap Q_{F,T}$ such that there is a finite faulty prefix $t \in \overline{\{s\}}$, over which the path can reach state q_1 exceeding $|\Sigma_e| \times (|\Sigma_e \cup \{\varepsilon\}|) \times |Q_T|$ times. By (37), there exists a normal extended string $v \in \overline{\mathcal{L}^{\varphi}_e(G)}$ having the same observation with t. By (13), set $\delta_T(Q_{0,T}, v) \cap Q_{\text{feas},T} \cap Q_{N,T}$ is not empty. Thus, by the second property of the verification system, there exists a string $s_V \in \mathcal{L}(V)$ in verification system V such that $\theta_1(s_V) = t, \theta_2(s_V) = v$ and the run π' over s_V visits state $q_V \in \{(q_1, q_2) : q_2 \in \delta_T(Q_{0,T}, v) \cap Q_{\text{feas},T} \cap Q_{N,T}\}$ by event $\sigma \in \{(\sigma_V^1, \sigma_V^2) \in \Sigma_V : \sigma_V^1 \neq \varepsilon\}$ exceeding $|\Sigma_e| \times (|\Sigma_e \cup \{\varepsilon\}|) \times |Q_T|$ times, i.e., the structure $\xrightarrow{\sigma} q_V$ appears in π' exceeding $|\Sigma_e| \times (|\Sigma_e \cup \{\varepsilon\}|) \times |Q_T|$ times. By definition of set $Q_{m,V}$, we know that state q_V is included in $Q_{m,V}$. Since $|\{(q_1, q_2) : q_2 \in \delta_T(Q_{0,T}, v) \cap Q_{\text{feas},T} \cap Q_{N,T}\}| \leq |Q_T|$ and $|\{(\sigma_V^1, \sigma_V^2) \in \Sigma_V : \sigma_V^1 \neq \varepsilon\}| \leq |\Sigma_e| \times (|\Sigma_e \cup \{\varepsilon\}|)$, by the Pigeonhole principle, there exists a cycle $\pi = q_V^1 \xrightarrow{\sigma_V^1} q_V^2 \xrightarrow{\sigma_V^2} \cdots \xrightarrow{\sigma_V^{n-1}} q_V^n$, such that there exist $i, j \in \{1, 2, \ldots, n-1\}$ satisfying $q_V^i \in Q_{m,V}$ and $\theta_1(\sigma_V^j) \neq \varepsilon$. □

Proof of Theorem 2

Proof: Since finite φ-diagnosability implies φ-diagnosability, we focus on the other direction. Suppose that system G is not finite φ-diagnosable, i.e.,

$$(\forall n \in \mathbb{N})(\exists s \in \Psi^{\varphi}_e(G))(\exists st \in \overline{\mathcal{L}^{\varphi}_e(G)}) : [(|t| \geq n) \wedge (\exists v \in \overline{\mathcal{L}^{\varphi}_e(G)})[\Theta_\Delta(v) = \Theta_\Delta(st) \wedge \Sigma_{e,F} \notin v]]. \tag{38}$$

According to [51, Th. 1], $\mathsf{word}(\varphi)$ is a safety property, if and only if, it can be accepted by a Büchi automaton in which all states are accepting, i.e., $\mathcal{B} = (X, X_0, \Sigma_B, \xi, X_m)$, where $X_m = X$. For example, Büchi automata in Figs. 3 and 6(b) are all such automata, which means that φ_{per} and $\varphi_{\mathsf{K\text{-}loss}}$ are both safety LTL. Since $X_m = X$, we know that all states in the observation constrained system are also accepting, i.e., $Q_{m,T} = \{(\tilde{q}, x) \in Q_T : x \in X_m\} = Q_T$, and we also have $Q_{\text{feas},T} = Q_T$. In this case, accepting states in the verification system can be reduced as

$$Q_{m,V} = \left\{(q_1, q_2) \in Q_V : \begin{array}{c} q_1 \in Q_{m,T} \cap Q_{F,T} \\ \text{and } q_2 \in Q_{\text{feas},T} \cap Q_{N,T} \end{array}\right\} = \left\{(q_1, q_2) \in Q_V : \begin{array}{c} q_1 \in Q_{F,T} \\ \text{and } q_2 \in Q_{N,T} \end{array}\right\}.$$

Consider detection delay $n > |Q_{F,T}| \times |Q_{N,T}| \times |\Sigma_e| \times (|\Sigma_e \cup \{\varepsilon\}|)$ in (38). Let ρ be the path visited along extended faulty string st in T. By the axiom of choice, there is at least one state $q_1 \in Q_{F,T}$ that appears at least $|Q_{N,T}| \times |\Sigma_e| \times (|\Sigma_e \cup \{\varepsilon\}|)$ times in path ρ. By the second property of the verification system, there exists a string $s_V \in \mathcal{L}(V)$ in system V such that $\theta_1(s_V) = st, \theta_2(s_V) = v$ and the run π' over s_V visits state $q_V \in \{(q_1, q_2) : q_2 \in Q_{N,T}\}$ by event $\sigma \in \{(\sigma_V^1, \sigma_V^2) \in \Sigma_V : \sigma_V^1 \neq \varepsilon\}$ exceeding $|Q_{N,T}| \times |\Sigma_e| \times (|\Sigma_e \cup \{\varepsilon\}|)$ times. Note that, we have $q_V \in Q_{m,V}$. Furthermore, since $|\{(q_1, q_2) : q_2 \in Q_{N,T}\}| \leq |Q_{N,T}|$ and $|\{(\sigma_V^1, \sigma_V^2) \in \Sigma_V : \sigma_V^1 \neq \varepsilon\}| \leq |\Sigma_e| \times (|\Sigma_e \cup \{\varepsilon\}|)$, by the axiom of choice, there exists a cycle $\pi = q_V^1 \xrightarrow{\sigma_V^1} q_V^2 \xrightarrow{\sigma_V^2} \cdots \xrightarrow{\sigma_V^{n-1}} q_V^n$ such that there exist $i, j \in \{1, 2, \ldots, n-1\}$ satisfying $q_V^i \in Q_{m,V}$ and $\theta_1(\sigma_V^j) \neq \varepsilon$. By Theorem 2, we conclude that the system is not φ-diagnosable. □

REFERENCES

[1] C. Cassandras and S. Lafortune, *Introduction to Discrete Event Systems*. Berlin, Germany: Springer, 2021, vol. 3.

[2] F. Lin, "Diagnosability of discrete event systems and its applications," *Discrete Event Dyn. Syst.*, vol. 4, no. 2, pp. 197–212, 1994.

[3] M. Sampath, R. Sengupta, S. Lafortune, K. Sinnamohideen, and D. Teneketzis, "Diagnosability of discrete-event systems," *IEEE Trans. Autom. Control*, vol. 40, no. 9, pp. 1555–1575, Sep. 1995.

[4] F. Lin et al., "N-diagnosability for active on-line diagnosis in discrete event systems," *Automatica*, vol. 83, pp. 220–225, 2017.

[5] X. Yin and S. Lafortune, "On the decidability and complexity of diagnosability for labeled Petri nets," *IEEE Trans. Autom. Control*, vol. 62, no. 11, pp. 5931–5938, Nov. 2017.

[6] F. Basile, M. Cabasino, and C. Seatzu, "Diagnosability analysis of labeled time petri net systems," *IEEE Trans. Autom. Control*, vol. 62, no. 3, pp. 1384–1396, Mar. 2017.

[7] D. Lefebvre and C. Delherm, "Diagnosis of DES with petri net models," *IEEE Trans. Automat. Sci. Eng.*, vol. 4, no. 1, pp. 114–118, Jan. 2007.

[8] S. Takai and R. Kumar, "A generalized framework for inference-based diagnosis of discrete event systems capturing both disjunctive and conjunctive decision-making," *IEEE Trans. Autom. Control*, vol. 62, no. 6, pp. 2778–2793, Jun. 2017.

[9] N. Ran, H. Su, A. Giua, and C. Seatzu, "Codiagnosability analysis of bounded petri nets," *IEEE Trans. Autom. Control*, vol. 63, no. 4, pp. 1192–1199, Apr. 2018.

[10] X. Yin, J. Chen, Z. Li, and S. Li, "Robust fault diagnosis of stochastic discrete event systems," *IEEE Trans. Autom. Control*, vol. 64, no. 10, pp. 4237–4244, Oct. 2019.

[11] G. Viana and J. Basilio, "Codiagnosability of discrete event systems revisited: A new necessary and sufficient condition and its applications," *Automatica*, vol. 101, pp. 354–364, 2019.

[12] Y. Hu, Z. Ma, Z. Li, and A. Giua, "Diagnosability enforcement in labeled petri nets using supervisory control," *Automatica*, vol. 131, 2021, Art. no. 109776.

[13] Z. Ma, X. Yin, and Z. Li, "Marking diagnosability verification in labeled petri nets," *Automatica*, vol. 131, 2021, Art. no. 109713.

[14] Y. Pencolé and A. Subias, "Diagnosability of event patterns in safe labeled time petri nets: A model-checking approach," *IEEE Trans. Automat. Sci. Eng.*, vol. 19, no. 2, pp. 1151–1162, Apr. 2022.

[15] J. Zaytoon and S. Lafortune, "Overview of fault diagnosis methods for discrete event systems," *Annu. Rev. Control*, vol. 37, no. 2, pp. 308–320, 2013.

[16] S. Lafortune, F. Lin, and C. Hadjicostis, "On the history of diagnosability and opacity in discrete event systems," *Annu. Rev. Control*, vol. 45, pp. 257–266, 2018.

[17] J. Basilio, C. Hadjicostis, and R. Su, "Analysis and control for resilience of discrete event systems: Fault diagnosis, opacity and cyber security," *Foundations Trends Syst. Control*, vol. 8, no. 4, pp. 285–443, 2021.

[18] A. Boussif, M. Ghazel, and J. Basilio, "Intermittent fault diagnosability of discrete event systems: An overview of automaton-based approaches," *Discrete Event Dynamic Syst.*, vol. 31, no. 1, pp. 59–102, 2021.

[19] L. Carvalho, M. Moreira, and J. Basilio, "Comparative analysis of related notions of robust diagnosability of discrete-event systems," *Annu. Rev. Control*, vol. 51, pp. 23–36, 2021.

[20] L. Carvalho, J. Basilio, and M. Moreira, "Robust diagnosis of discrete event systems against intermittent loss of observations," *Automatica*, vol. 48, no. 9, pp. 2068–2078, 2012.

[21] D. Thorsley, T. Yoo, and H. Garcia, "Diagnosability of stochastic discrete-event systems under unreliable observations," in *Proc. Amer. Control Conf.*, 2008, pp. 1158–1165.

[22] E. Athanasopoulou, L. Li, and C. Hadjicostis, "Maximum likelihood failure diagnosis in finite state machines under unreliable observations," *IEEE Trans. Autom. Control*, vol. 55, no. 3, pp. 579–593, Mar. 2010.

[23] S. Takai and T. Ushio, "Verification of codiagnosability for discrete event systems modeled by mealy automata with nondeterministic output functions," *IEEE Trans. Autom. Control*, vol. 57, no. 3, pp. 798–804, Mar. 2012.
[24] L. Carvalho, M. Moreira, J. Basilio, and S. Lafortune, "Robust diagnosis of discrete-event systems against permanent loss of observations," *Automatica*, vol. 49, no. 1, pp. 223–231, 2013.
[25] N. Kanagawa and S. Takai, "Diagnosability of discrete event systems subject to permanent sensor failures," *Int. J. Control*, vol. 88, no. 12, pp. 2598–2610, 2015.
[26] J. Tomola, F. Cabral, L. Carvalho, and M. Moreira, "Robust disjunctive-codiagnosability of discrete-event systems against permanent loss of observations," *IEEE Trans. Autom. Control*, vol. 62, no. 11, pp. 5808–5815, Nov. 2017.
[27] A. Wada and S. Takai, "Decentralized diagnosis of discrete event systems subject to permanent sensor failures," *Discrete Event Dyn. Syst.*, pp. 1–35, 2021.
[28] L. Carvalho, M. Moreira, and J. Basilio, "Generalized robust diagnosability of discrete event systems," *IFAC Proc. Volumes*, vol. 44, no. 1, pp. 8737–8742, 2011.
[29] S. Takai, "A general framework for diagnosis of discrete event systems subject to sensor failures," *Automatica*, vol. 129, 2021, Art. no. 109669.
[30] F. Lin, "Control of networked discrete event systems: Dealing with communication delays and losses," *SIAM J. Control Optim.*, vol. 52, no. 2, pp. 1276–1298, 2014.
[31] C. Nunes, M. Moreira, M. Alves, L. Carvalho, and J. Basilio, "Codiagnosability of networked discrete event systems subject to communication delays and intermittent loss of observation," *Discrete Event Dyn. Syst.*, vol. 28, no. 2, pp. 215–246, 2018.
[32] Y. Sasi and F. Lin, "Detectability of networked discrete event systems," *Discrete Event Dyn. Syst.*, vol. 28, no. 3, pp. 449–470, 2018.
[33] R. Tai, L. Lin, Y. Zhu, and R. Su, "A new modeling framework for networked discrete-event systems," *Automatica*, vol. 138, 2022, Art. no. 110139.
[34] V. Oliveira, F. Cabral, and M. Moreira, "K-loss robust codiagnosability of discrete-event systems," *Automatica*, vol. 140, 2022, Art. no. 110222.
[35] X. Yin, "Initial-state detectability of stochastic discrete-event systems with probabilistic sensor failures," *Automatica*, vol. 80, pp. 127–134, 2017.
[36] Y. Tong, J. Luo, and C. Seatzu, "State estimation of discrete-event systems subject to intermittent and permanent loss of observations," in *Proc. IEEE 60th Conf. Decis. Control*, 2021, pp. 1048–1053.
[37] K. Rohloff, "Sensor failure tolerant supervisory control," in *Proc. IEEE 44th Conf. Decis. Control*, 2005, pp. 3493–3498.
[38] T. Ushio and S. Takai, "Nonblocking supervisory control of discrete event systems modeled by mealy automata with nondeterministic output functions," *IEEE Trans. Autom. Control*, vol. 61, no. 3, pp. 799–804, Mar. 2016.
[39] X. Yin, "Supervisor synthesis for mealy automata with output functions: A model transformation approach," *IEEE Trans. Autom. Control*, vol. 62, no. 5, pp. 2576–2581, May 2017.
[40] M. Alves, A. Cunha, L. Carvalho, M. Moreira, and J. Basilio, "Robust supervisory control of discrete event systems against intermittent loss of observations," *Int. J. Control*, vol. 94, no. 7, pp. 2008–2020, 2021.
[41] S. Jiang and R. Kumar, "Failure diagnosis of discrete-event systems with linear-time temporal logic specifications," *IEEE Trans. Autom. Control*, vol. 49, no. 6, pp. 934–945, Jun. 2004.
[42] S. Jiang and R. Kumar, "Diagnosis of repeated failures for discrete event systems with linear-time temporal-logic specifications," *IEEE Trans. Automat. Sci. Eng.*, vol. 3, no. 1, pp. 47–59, Jan. 2006.
[43] J. Chen and R. Kumar, "Fault detection of discrete-time stochastic systems subject to temporal logic correctness requirements," *IEEE Trans. Automat. Sci. Eng.*, vol. 12, no. 4, pp. 1369–1379, Oct. 2015.
[44] F. Cassez, "The complexity of codiagnosability for discrete event and timed systems," *IEEE Trans. Autom. Control*, vol. 57, no. 7, pp. 1752–1764, Jul. 2012.
[45] B. Bittner, M. Bozzano, A. Cimatti, M. Gario, S. Tonetta, and V. Vozarova, "Diagnosability of fair transition systems," *Artif. Intell.*, vol. 309, 2022, Art. no. 103725.
[46] T. Tuxi, L. Carvalho, E. Nunes, and A. da Cunha, "Diagnosability verification using LTL model checking," *Discrete Event Dyn. Syst.*, vol. 32, no. 3, pp. 399–433, 2022.
[47] W. Dong, S. Gao, X. Yin, and S. Li, "Fault diagnosis of discrete-event systems under non-deterministic observations with output fairness," in *Proc. 61th IEEE Conf. Decis. Control*, 2022, pp. 4256–4262.
[48] T. Yoo and H. Garcia, "Event diagnosis of discrete-event systems with uniformly and nonuniformly bounded diagnosis delays," in *Proc. Amer. Control Conf.*, vol. 6, 2004, pp. 5102–5107.
[49] C. Baier and J. Katoen, *Principles of Model Checking*. Cambridge, MA, USA: MIT Press, 2008.
[50] D. Giannakopoulou and F. Lerda, "From states to transitions: Improving translation of LTL formulae to büchi automata," in *Proc. Int. Conf. Formal Techn. Networked Distrib. Syst.*, Springer, 2002, pp. 308–326.
[51] B. Alpern and F. B. Schneider, "Recognizing safety and liveness," *Distrib. Comput.*, vol. 2, no. 3, pp. 117–126, 1987.
[52] R. Tarjan, "Depth-first search and linear graph algorithms," *SIAM J. Comput.*, vol. 1, no. 2, pp. 146–160, 1972.
[53] S. Biswas, D. Sarkar, S. Mukhopadhyay, and A. Patra, "Fairness of transitions in diagnosability of discrete event systems," *Discrete Event Dyn. Syst.*, vol. 20, no. 3, pp. 349–376, 2010.
[54] V. Germanos, S. Haar, V. Khomenko, and S. Schwoon, "Diagnosability under weak fairness," *ACM Trans. Embedded Comput. Syst.*, vol. 14, no. 4, pp. 1–19, 2015.

Weijie Dong (Student Member, IEEE) was born in Xinjiang, China, in 1996. He received the B.S. degree in water conservancy and hydropower engineering from Huazhong University of Science and Technology in 2019. He is currently working toward the Ph.D. degree in control science and engineering with the Department of Automation, Shanghai Jiao Tong University, Shanghai, China.

His current research interests include fault diagnosis, state estimation of discrete event systems.

Xiang Yin (Member, IEEE) was born in Anhui, China, in 1991. He received the B.Eng. degree from Zhejiang University, Zhejinag, China, in 2012, and the M.S. and Ph.D. degrees from the University of Michigan, Ann Arbor, MI, USA, in 2013 and 2017, respectively, all in electrical engineering.

Since 2017, he has been with the Department of Automation, Shanghai Jiao Tong University, Shanghai, China, where he is an Associate Professor. His research interests include formal methods, discrete-event systems, and cyber-physical systems.

Dr. Yin was the recipient of the IEEE Conference on Decision and Control (CDC) Best Student Paper Award Finalist in 2016. He is serving as the co-chair of the IEEE CSS Technical Committee on Discrete Event Systems, an Associate Editor for the *Journal of Discrete Event Dynamic Systems: Theory & Applications*, and a Member of the IEEE CSS Conference Editorial Board.

Shaoyuan Li (Senior Member, IEEE) was born in Hebei, China, in 1965. He received the B.S. and M.S. degrees in automation from the Hebei University of Technology, Tianjin, China, in 1987 and 1992, respectively, and the Ph.D. degree in control science from Nankai University, Tianjin, China, in 1997.

Since 1997, he has been with the Department of Automation, Shanghai Jiao Tong University, Shanghai, China, where he is currently a Professor. His current research interests include model predictive control, dynamic system optimization, and cyber-physical systems.

Dr. Li is the Vice President of the Chinese Association of Automation.