UNIVERSIDADE DO ESTADO DE SANTA CATARINA – UDESC
CENTRO DE CIÊNCIAS TECNOLÓGICAS – CCT
PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA ELÉTRICA – PPGEEL

THALYS EDUARDO FERREIRA REZENDE

CONTROLABILIDADE SEGURA PELA DIAGNOSE OU PROGNOSE DE FALHAS EM SISTEMAS A EVENTOS DISCRETOS MODELADOS POR AUTÔMATOS ESTOCÁSTICOS

JOINVILLE
2023

THALYS EDUARDO FERREIRA REZENDE

CONTROLABILIDADE SEGURA PELA DIAGNOSE OU PROGNOSE DE FALHAS EM SISTEMAS A EVENTOS DISCRETOS MODELADOS POR AUTÔMATOS ESTOCÁSTICOS

Tese apresentada ao Programa de Pós–Graduação em Engenharia Elétrica do Centro de Ciências Tecnológicas da Universidade do Estado de Santa Catarina, como requisito parcial para a obtenção do grau de Doutor em Engenharia Elétrica.

Orientador: André Bittencourt Leal

JOINVILLE
2023

Ficha catalográfica elaborada pelo programa de geração automática da

Biblioteca Setorial do CCT/UDESC,

com os dados fornecidos pelo(a) autor(a)

Rezende, Thalys Eduardo Ferreira
CONTROLABILIDADE SEGURA PELA DIAGNOSE OU PROGNOSE DE FALHAS EM SISTEMAS A EVENTOS DISCRETOS MODELADOS POR AUTÔMATOS ESTOCÁSTICOS / Thalys Eduardo Ferreira Rezende. -- 2023.
127 p.

Orientador: André Bittencourt Leal
Tese (doutorado) -- Universidade do Estado de Santa Catarina, Centro de Ciências Tecnológicas, Programa de Pós-Graduação em Engenharia Elétrica, Joinville, 2023.

1. Diagnose de Falhas. 2. Prognose de Falhas. 3. Controlabilidade Segura. 4. Sistemas a Eventos Discretos. 5. Autômatos Estocásticos. I. Leal, André Bittencourt. II. Universidade do Estado de Santa Catarina, Centro de Ciências Tecnológicas, Programa de Pós-Graduação em Engenharia Elétrica. III. Título.

THALYS EDUARDO FERREIRA REZENDE

CONTROLABILIDADE SEGURA PELA DIAGNOSE OU PROGNOSE DE FALHAS EM SISTEMAS A EVENTOS DISCRETOS MODELADOS POR AUTÔMATOS ESTOCÁSTICOS

Tese apresentada ao Programa de Pós–Graduação em Engenharia Elétrica do Centro de Ciências Tecnológicas da Universidade do Estado de Santa Catarina, como requisito parcial para a obtenção do grau de Doutor em Engenharia Elétrica.

Orientador: André Bittencourt Leal

BANCA EXAMINADORA:

Prof. Dr. André Bittencourt Leal
Universidade do Estado de Santa Catarina

Membros:

Prof. Dr. Felipe Gomes de Oliveira Cabral
Universidade Federal de Santa Catarina

Prof. Dr. Marcos Vicente de Brito Moreira
Universidade Federal do Rio de Janeiro

Prof. Dr. Ricardo Ferreira Martins
Universidade do Estado de Santa Catarina

Prof. Dr. Yuri Kaszubowski Lopes
Universidade do Estado de Santa Catarina

Joinville, 02 de maio de 2023

A Deus, que me criou e foi criativo nesta tarefa. Seu fôlego de vida em mim foi sustento e encorajou-me para questionar realidades e propor sempre um novo mundo de possibilidades.

AGRADECIMENTOS

A Deus, que nem sempre deu-me tudo o que eu queria, mas sempre proveu-me de tudo o que precisava, na hora certa e na medida certa proporcionando-me saúde e força para superar as dificuldades.

A esta instituição, seu corpo docente, direção e administração.

Ao meu orientador André Bittencourt Leal, pelas suas correções e incentivos.

A minha esposa Luiza, pelo amor, incentivo, paciência e apoio incondicional.

A meus pais, Nádia e Onecídio, que são responsáveis pela minha formação e educação.

Aos meus irmãos, Atylla, Flávya e Mayra, que sempre estiveram ao meu lado em momentos de felicidade e dificuldades.

Aos colegas do grupo de pesquisa, que estiveram batalhando lado a lado comigo durante todo o percurso do Doutorado.

E a todos que direta ou indiretamente fizeram parte da minha formação, o meu muito obrigado.

“O reator da economia moderna não é a fazenda,
não é a fábrica, não é o banco. É a escola.”
(PETER DRUCKER)

RESUMO

Este trabalho considera o problema da controlabilidade segura de Sistemas a Eventos Discretos (SEDs). Neste contexto, as falhas são consideradas permanentes e são modeladas por eventos não controláveis e não observáveis e são incluídas de forma explícita na modelagem do SED sob análise. Tendo em vista que o uso da diagnose e prognose lógicas de falhas pode levar a soluções muito restritivas, especialmente pela dificuldade de prognosticar a ocorrência de falhas com absoluta certeza, nesta tese adota-se uma abordagem estocástica. As avaliações de diagnose e prognose são realizadas por meio da construção de autômato diagnosticador. São apresentados novos métodos e abordagens para os problemas de diagnose de falhas, prognose de falhas e controlabilidade segura em sistemas a eventos discretos modelados por autômatos probabilísticos. É apresentada a propriedade denominada certeza de anormalidade para autômatos clássicos, bem como a extensão do conceito para autômatos probabilísticos por meio da formalização de um coeficiente de anormalidade. É apresentado um modelo dinâmico para a avaliação de prognose de falhas, o qual possui função de transição probabilística, que é atualizada mediante a observação de eventos em tempo de execução. É apresentada uma proposta de um modelo de diagnosticador denominado Diagnosticador Estocástico Com Saídas (DECS), que contém probabilidades de diagnose de falhas, probabilidades de ocorrência futura de falhas e probabilidades de ocorrência futura de evento proibido após a falha. São apresentadas duas abordagens distintas para o cálculo do DECS, as quais são denominadas de Diagnosticador Estocástico com Probabilidades Estáticas e Diagnosticador Estocástico com Probabilidades Dinâmicas. São introduzidas as propriedades de u-diagnosticabilidade, u-diagnosticabilidade segura, u-prognosticabilidade, controlabilidade segura pela u-diagnose, controlabilidade segura pela u-prognose e controlabilidade segura pelo coeficiente de anormalidade. São apresentadas as condições necessárias e suficientes para que um SED seja u-diagnosticável seguro, controlável seguro pela u-diagnose, controlável seguro pela u-prognose e controlável seguro pelo coeficiente de anormalidade. Tais condições são verificadas sobre o Diagnosticador Estocástico com Probabilidades Estáticas. Por outro lado, o Diagnosticador Estocástico com Probabilidades Dinâmicas é utilizado em tempo de execução, com atualização das probabilidades de maneira dinâmica, com o intuito de fornecer informações para atuação numa estrutura de controle tolerante a falhas, a fim de garantir a controlabilidade segura do sistema. A controlabilidade segura pelo coeficiente de anormalidade é uma generalização do conceito de controlabilidade segura em SEDs, pois a utilização conjunta de diagnose e prognose estocásticas pode garantir controlabilidade segura a SEDs que não possuem DP-Controlabilidade Segura lógica.

Palavras-chave: Diagnose de Falhas, Prognose de Falhas, Controlabilidade Segura, Sistemas a Eventos Discretos, Autômatos Estocásticos.

ABSTRACT

This work considers the problem of safe controllability of Discrete Event Systems (DESs). In this context, faults are considered permanent and are modeled by uncontrollable and unobservable events and are explicitly included in the modeling of the DES under analysis. Bearing in mind that the use of logical fault diagnosis and prognosis can lead to very restrictive solutions, especially due to the difficulty of predicting the occurrence of faults with absolute certainty, this thesis adopts a stochastic approach. Diagnosis and prognosis assessments are carried out by building a diagnoser automata. New methods and approaches to problems of fault diagnosis, fault prognosis and safe controllability in discrete event systems modeled by stochastic automata are presented. The property called certainty of abnormality for classical automata is presented, as well as the extension of the concept to stochastic automata through the formalization of an abnormality coefficient. A dynamic model for evaluating the prognosis of faults is presented, which has a probabilistic transition function, which is updated by observing events at runtime. A proposal for a diagnoser model called Stochastic Diagnoser With Outputs (SDWO) is presented, which contains fault diagnosis probabilities, future occurrence probabilities of faults and probabilities of future occurrence of prohibited event after the fault. Two different approaches for the calculation of SDWO are presented, which are called Stochastic Diagnoser with Static Probabilities and Stochastic Diagnoser with Dynamic Probabilities. The properties of u-diagnosability, safe u-diagnosability, u-prognosability, safe controllability by u-diagnosis, safe controllability by u-prognosis and safe controllability by abnormality coefficient are introduced. The necessary and sufficient conditions are presented for an DES to be safe u-diagnosable, safe controllable by u-diagnosis, safe controllable by u-prognosis, and safe controllable by the coefficient of abnormality. Such conditions are verified on the Stochastic Diagnoser with Static Probabilities. On the other hand, the Stochastic Diagnoser with Dynamic Probabilities is used at runtime, with dynamically updating the probabilities, in order to provide information to operate in a fault-tolerant control structure, in order to guarantee the safe controllability of the system. Safe controllability by the coefficient of abnormality is a generalization of the concept of safe controllability in DES, since the joint use of stochastic diagnosis and prognosis can guarantee safe controllability to DES that do not have logical DP-Safe Controllability.

Keywords: Fault Diagnosis, Fault Prognosis, Safe Controlability, Discrete Event Systems, Stochastic Automata.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ADEF	Autômato Determinístico de Estados Finitos
ANDEF	Autômato Não Determinístico de Estados Finitos
CTF	Controle Tolerante a Falhas
CSUD	Controlabilidade Segura pela u-Diagnose
CSUP	Controlabilidade Segura pela u-Prognose
CSCA	Controlabilidade Segura pelo Coeficiente de Anormalidade
DECS	Diagnosticador Estocástico com Saídas
DEPE	Diagnosticador Estocástico com Probabilidades Estáticas
DEPD	Diagnosticador Estocástico com Probabilidades Dinâmicas
EDD	Estado dinâmico do diagnosticador
EV	Base de pesquisa acadêmica Engineering Village
IEEE	Base de pesquisa acadêmica IEEExplore
SCP	Base de pesquisa acadêmica SCOPUS
SD	Base de pesquisa acadêmica Science Direct
SEDs	Sistema a Eventos Discretos
SEDEs	Sistema a Eventos Discretos Estocásticos
TCS	Teoria de Controle Supervisório
WOS	Base de pesquisa acadêmica Web of Science

LISTA DE SÍMBOLOS

σ	Evento simbólico
Σ	Alfabeto de eventos
s	Cadeia de eventos simbólica
ε	Cadeia vazia
$\emptyset$	Conjunto vazio
Σ^*	Fecho de Kleene do alfabeto de eventos
X	Espaço de estados do autômato gerador G
δ	Função de transição do autômato gerador G
x_0	Estado inicial do autômato gerador G
X_m	Conjunto de estados marcados
$L(G)$	Linguagem gerada a partir de G
$L_m(G)$	Linguagem marcada a partir de G
$L_1 L_2$	Concatenação das linguagens L_1 e L_2
$\overline{L}$	Prefixo fechamento da linguagem L
$t < s$	t é um prefixo estrito de s, em que $s \neq t$.
$\|\|s\|\|$	Norma ou comprimento de uma cadeia s
$\hat{\delta}$	Função de transição estendida
$\Gamma(x)$	Conjunto de eventos ativos num estado $x \in X$
Ac(G)	Componente acessível de G
X_{ac}	Espaço de estados acessíveis do autômato gerador G
δ_{ac}	Função de transição dos estados acessíveis no autômato gerador G
$X_{ac,m}$	Conjunto de estados marcados acessíveis
CoAc(G)	Componente co-acessível de G
X_{coac}	Espaço de estados co-acessíveis do autômato gerador G
δ_{coac}	Função de transição dos estados co-acessíveis no autômato gerador G
x_{0coac}	Estado inicial co-acessível
$Trim(G)$	Operação Trim(G) := CoAc[Ac(G)] = Ac[CoAc(G)]
P_o	Projeção
P_o^{-1}	Projeção inversa
$\Sigma_1 \backslash \Sigma_2$	Conjunto de eventos do alfabeto 1, **exceto** os eventos do alfabeto 2

Σ_o	Conjunto de eventos observáveis
Σ_{uo}	Conjunto de eventos não observáveis
Σ_c	Conjunto de eventos controláveis
Σ_{uc}	Conjunto de eventos não controláveis
p	Função de transição probabilística do autômato probabilístico
δ	Função de transição parcial do autômato probabilístico (Equivalente a função de transição do autômato clássico)
$\Psi_L(f)$	Conjunto de cadeias terminadas por um evento de falha f
L/s	Operação de pós-linguagem (conjunto de cadeias posteriores a cadeia s)
$\mathscr{D}$	Condição de diagnosticabilidade
$\mathscr{P}$	Condição de prognosticabilidade
X_D^N	Conjunto dos estados normais do diagnosticador
X_D^U	Conjunto dos estados incertos do diagnosticador
X_D^C	Conjunto dos estados certos de falha do diagnosticador
X_D^{NB}	Conjunto dos estados do diagnosticador que não são maus estados
X_D^B	Conjunto dos estados do diagnosticador que são maus estados
F_D	Conjunto dos estados normais do diagnosticador que possuem um sucessor imediato que não é normal
$\mathbb{C}$	Condição de acessibilidade dos ciclos de estados certos do diagnosticador
Φ	Conjunto de cadeias proibidas
$\mathscr{K}_f$	Linguagem ilegal ou proibida
ξ	Cadeia ilegal ou proibida
A_{rs}	Autômato rotulador seguro
$\{\varepsilon^{\downarrow C}\}$	Ínfima superlinguagem controlável
G_i^{deg}	i-ésimo modelo para o comportamento não controlado da planta pós-diagnose de falha
FP	Conjunto dos primeiros estados do diagnosticador que asseguram a prognose
$G_j^{deg,p}$	j-ésimo modelo para o comportamento não controlado da planta pós-prognose de falha
FC	Conjunto dos primeiros estados certos de falha do diagnosticador
FB	Conjunto dos primeiros maus estados do diagnosticador
FU	Conjunto dos primeiros estados incertos do diagnosticador

$FC(s)$	Conjunto dos primeiros estados certos de falha alcançados após a cadeia s
$FB(s)$	Conjunto dos primeiros maus estados alcançados após a cadeia s
$FU(s)$	Conjunto dos primeiros estados incertos alcançados pela cadeia s
$FP(s)$	Primeiro estado no qual se assegura a prognose de falhas para a cadeia s
$\phi_{un}(s_o)$	vetor de probabilidades não normalizado após a observação da cadeia s_o
$\phi(s_o)$	vetor de probabilidades normalizado após a observação da cadeia s_o
$Pr(Fs_0)$	Probabilidade de estar em um rótulo de falha após a observação da cadeia s_o
$\|x_D\|$	Quantidade de rótulos do estado x_D
$x_D(i)$	I-ésimo rótulo do estado x_D
$R(x_D(i))$	Indica se o rótulo $x_D(i)$ é normal (N) ou de falha (F)
$E(x_D(i))$	Indica o estado $x \in X$ equivalente ao rótulo $x_D(i)$
$CCD(x_D)$	Conjunto de cadeias que chegam ao estado x_D
$CCG(x_D(i))$	Conjunto de cadeias que chegam ao estado da planta equivalente ao rótulo $x_D(i)$
$SC(L)$	Conjunto que contém todas as subcadeias da linguagem L
$L(G,x)$	Conjunto das cadeias em G que são iniciadas a partir do estado x
$Prob(s,x)$	Probabilidade de ocorrência da cadeia s a partir do estado x
$p(x_{G0},\sigma_1)$	Probabilidade da transição com evento σ_1 a partir do estado x_{G0}
s_o	Cadeia observada (Composta apenas por eventos observáveis)
$PD_{nn}(x_D(i))$	Probabilidade não normalizada de estar no rótulo i do estado x_D
$PD(x_D(i))$	Probabilidade normalizada de estar no rótulo i do estado x_D
$\Omega(x_D)$	Vetor de probabilidades de estar em cada um dos rótulos do estado x_D
$\Omega_F(x_D)$	Soma das probabilidades normalizadas de estar em rótulos de falha para um estado x_D
$\Psi_f(x_D(i))$	Conjunto de cadeias que a partir de um estado $x \in X_G$ e são terminadas por um evento de falha $f_n \in \Sigma_f$
$PF(x_D(i))$	Probabilidade de ocorrência futura da falha f_n a partir do estado relacionado ao rótulo $x_D(i)$
$\Delta_F(x_D)$	Vetor com as probabilidades de ocorrência futura da falha para o estado x_D
$\eta(x_D(i))$	Conjunto das cadeias originadas do estado x, que contém a falha f e são terminadas por um evento proibido
$PEP(x_D(i))$	Probabilidade de ocorrência futura de evento proibido após a falha f a partir do estado relacionado ao rótulo $x_D(i)$

$\Delta_{EP}(x_D)$	Vetor de probabilidades de ocorrência futura de evento proibido após a falha a partir do estado x_D
$\vartheta(x_D)$	Coeficiente de anormalidade do estado x_D
FPF	Conjunto dos estados do diagnosticador atingidos após a ocorrência do primeiro evento observável após a falha
Ξ	Conjunto de estados do diagnosticador atingidos após a ocorrência da falha e que possuem eventos controláveis ativos
Υ	Conjunto dos estados do diagnosticador que são normais e que possuem eventos controláveis ativos que quando desabilitados interrompem a execução de uma cadeia proibida
τ	Conjunto dos estados do diagnosticador que não são maus estados e que possuem eventos controláveis ativos que quando desabilitados interrompem a execução de uma cadeia proibida
FT	Função probabilística dinâmica de uma transição
δ_P	variação de probabilidade a ser redistribuída na função probabilística dinâmica de uma transição
FPO	Fator de ponderação da função probabilística dinâmica de uma transição
$FT(0)$	Valor de probabilidade inicial da função probabilística dinâmica de uma transição
$p(3,f,4)$	Função probabilística de transição dinâmica com o evento f a partir do estado 3 com destino ao estado 4
y^T	Vetor y transposto, em que ^{T} é o operador de transposição.

SUMÁRIO

1 INTRODUÇÃO

Em um cenário mundial de grande concorrência entre empresas, o nível de exigência sobre os processos produtivos tem sido cada vez maior. Além disso, com a evolução de tecnologias relacionadas à Indústria 4.0, os processos têm se tornado mais complexos e a quantidade de informação disponível para a tomada de decisão tem aumentado de forma substancial.

Nesse contexto, temas relacionados com diagnose e prognose de falhas e com o controle tolerante a falhas (CTF) têm despertado grande interesse, tanto por parte da academia quanto pelas grandes corporações (MELNYKOV; KALINOV; ARTEMENKO, 2022; LUO et al., 2022; NIU et al., 2022; ZHENG; HOU, 2022; QIAN; YANG; XUE, 2022).

Um sistema tolerante a falhas é aquele que permanece funcional após a ocorrência de falhas. A tolerância a falhas pode ser interpretada de várias maneiras a partir do fornecimento de características ao sistema, como: continuidade integral/parcial de funcionamento; a prevenção de acidentes ao impedir um comportamento que outrora era permitido, mas que após a falha poderia causar danos (PAOLI; SARTINI; LAFORTUNE, 2011).

Existem duas abordagens para o projeto de Controle Tolerante a Falhas em SEDs. A abordagem passiva e a abordagem ativa. A abordagem passiva lida com o problema de determinação de um controlador geral que satisfaz as especificações de controle tanto em comportamento nominal quanto em comportamento faltoso, utilizando técnicas de controle robusto. Por outro lado, a abordagem ativa utiliza técnicas de controle adaptativo, promovendo alterações nas lógicas de controle para lidar com um comportamento faltoso (PAOLI; SARTINI; LAFORTUNE, 2011).

A diagnose e a prognose de falhas são áreas que se relacionam diretamente com o CTF. No entanto, existe uma dificuldade considerável no processo de representação de sistemas práticos por meio de modelos que incluem o comportamento do sistema pós-falha para utilização em abordagens de diagnose de falhas. Os trabalhos de Cabasino, Giua e Seatzu (2007), Dotoli, Fanti e Mangini (2008), Estrada-Vargas, Lopez-Mellado e Lesage (2010), Moreira e Lesage (2019a), Moreira e Lesage (2019b), Machado, Viana e Moreira (2023) abordam o tema de identificação de modelos para a diagnose de falhas.

Geralmente, a diagnose de falhas é dividida em três etapas: (a) Detecção: determinar se o sistema está operando normalmente ou se uma falha ocorreu; (b) Isolação: localizar o componente que causou a falha (c) Identificação: identificar a natureza da falha, bem como seu impacto e criticidade (ZAYTOON; LAFORTUNE, 2013). Neste trabalho, as três etapas são agrupadas, com a utilização do termo Diagnose de falhas. Alguns trabalhos recentes na área de diagnose de falhas são os de: Hamada e Takai (2022), Dong et al. (2022), Dong, Yin e Li (2023), Hu e Cao (2023), Li et al. (2023).

Além da diagnose de falhas, outra área que tem despertado interesse é a de prognose de falhas. Na prognose de falhas, busca-se inferir sobre a ocorrência futura de falhas (QI et al., 2023; ZHOU et al., 2023; YINGRUI et al., 2022; CHEN; KUMAR, 2022; CAO; LIU; ZHAO,

2022).

Neste trabalho, a temática de diagnose, prognose e controle tolerante a falhas será abordada e estudada especificamente no âmbito de Sistemas a Eventos Discretos (SEDs). Um Sistema a eventos discretos (SED) é um sistema dinâmico que evolui de acordo com a ocorrência abrupta de eventos físicos, em intervalos de tempo em geral irregulares e desconhecidos (CURY, 2001).

Em geral, as técnicas de diagnose/prognose para sistemas a eventos discretos são baseadas em modelos qualitativos, ou seja, a análise é feita pelo comparativo da observação de cadeias de eventos com os modelos (autômatos, redes de Petri, entre outros) ou conjuntos de regras e fórmulas lógicas pré-estabelecidas (WU, 2004).

Sampath et al. (1995) e Genc e Lafortune (2009) foram os trabalhos precursores a utilizarem autômatos como modelos formais em problemas de diagnose e prognose de falhas, respectivamente. No trabalho de Sampath et al. (1995) a determinação se um SED possui diagnosticabilidade é feita com a utilização de autômatos diagnosticadores. Contudo, a diagnosticabilidade também pode ser testada com a utilização de verificadores. A complexidade computacional do cálculo de um verificador é menor do que a de um diagnosticador. Os trabalhos de Jiang et al. (2001), Yoo e Lafortune (2002), Moreira, Jesus e Basilio (2011), Moreira, Basilio e Cabral (2015), Moreira, Basilio e Cabral (2016) tratam sobre a análise de diagnosticabilidade utilizando verificadores.

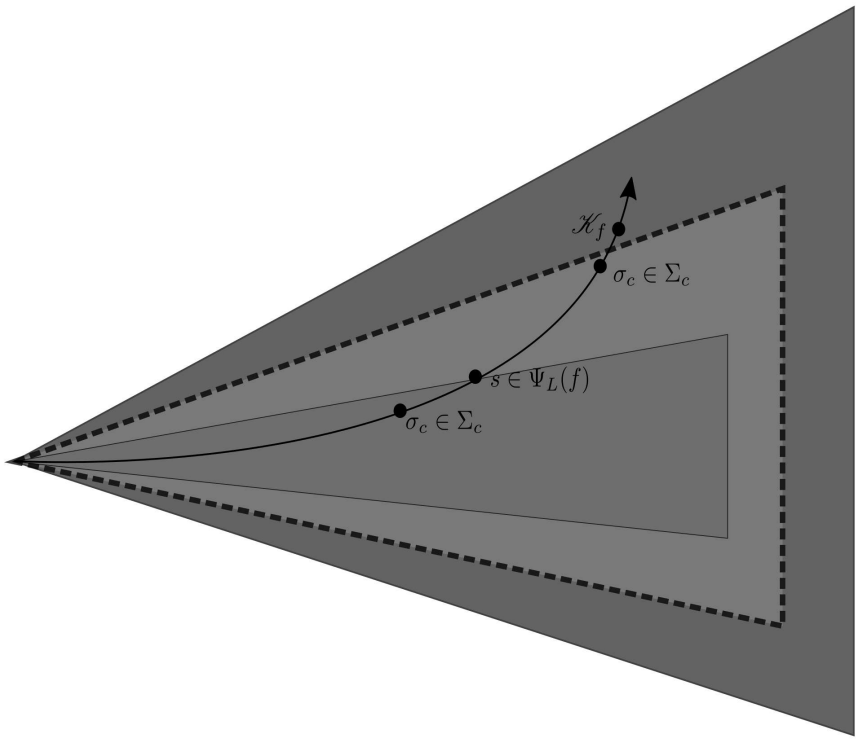
No entanto, o uso do verificador é restrito a utilização para avaliação *offline* da propriedade de diagnosticabilidade. Para uma abordagem de diagnose de falhas em tempo de execução de um SED sob observação parcial, é necessária a utilização do diagnosticador. Nesta tese, utiliza-se autômato Diagnosticador para análises de Diagnose e Prognose de falhas tanto na abordagem *offline* quanto na abordagem *online*. Dessa forma, o comparativo entre as duas abordagens torna-se mais simples.

A controlabilidade segura é uma propriedade fundamental para a adoção da estratégia ativa de CTF. Este conceito foi introduzido por Paoli, Sartini e Lafortune (2011) utilizando a propriedade de diagnosticabilidade segura. Posteriormente, Watanabe et al. (2017) apresentaram uma variante utilizando prognose como requisito para a controlabilidade segura. Recentemente, Watanabe et al. (2022) apresentaram uma proposta de combinar diagnose e prognose de falhas e, com isso, chegar num conceito mais amplo de controlabilidade segura, chamado de DP-controlabilidade Segura.

A Figura 1 ilustra o contexto de controlabilidade segura em SEDs. Nesta, é possível observar a representação de um sistema em malha fechada. A parte verde representa o comportamento do sistema sem a ocorrência de falhas. A parte laranja representa o comportamento do sistema com falha. A parte vermelha representa o comportamento do sistema após a execução de uma cadeia proibida (ou ilegal) após a falha. Uma cadeia proibida é uma sequência de eventos que quando executada após a falha causa uma propagação de danos ao sistema. Um sistema controlável seguro é aquele que possui eventos controláveis que, quando desabilitados, impedem

a ocorrência de uma cadeia ilegal após a falha. Dessa forma, o controlador restringe o sistema ao ponto de operação delimitado pelo contorno pontilhado.

Figura 1 – Esquema para ilustração do contexto de controlabilidade segura.



Fonte: Adaptado de (MOOR, 2016)

Tendo em vista que o uso da diagnose e prognose lógicas de falhas podem levar a soluções muito restritivas, especialmente pela dificuldade de prognosticar a ocorrência de falhas com absoluta certeza, deseja-se estender o conceito de DP-controlabilidade por meio da adição do aspecto estatístico, de modo a atender sistemas cuja linguagem não é logicamente DP-controlável segura.

Thorsley e Teneketzis (2005) e Chen e Kumar (2014) passaram a inserir probabilidades de ocorrência de eventos nos modelos com o intuito de incrementar o nível de detalhamento na representação do comportamento de sistemas reais. No decorrer do texto, os trabalhos referenciados que fazem análise de diagnose, prognose, controlabilidade em autômatos clássicos serão acompanhados dos termos "lógica" e "logicamente", para estabelecer uma distinção destes com os trabalhos que utilizam análises com modelos de autômatos estocásticos.

A utilização da probabilidade permite a obtenção de índices de diagnosticabilidade e prognosticabilidade, para casos que não são logicamente diagnosticáveis ou prognosticáveis. O aspecto estatístico é especialmente importante para fins de prognose de falhas, pois na maioria dos sistemas reais é muito difícil que se possa ter certeza sobre quando uma falha ocorrerá.

A dificuldade no processo de identificação de modelos para representação de sistemas práticos utilizando modelos estocásticos é ainda maior do que o processo de identificação de modelos sem inclusão de aspecto probabilístico. Principalmente para se modelar o comporta-

mento pós-falha. Existem diversos trabalhos que abordam o tema de representação de SEDs por modelos estocásticos, tais como: Al-ani e Hamam (2006), Verwer, Eyraud e Higuera (2014), Mao et al. (2016), Tîrnăucă et al. (2016), Dong et al. (2022), Baioumy et al. (2022).

Os autômatos estocásticos exibidos no Capítulo 4 representam SEDs teóricos. A probabilidade de ocorrência de cada transição é estabelecida arbitrariamente. O foco desta tese é no procedimento de cálculo das probabilidades de diagnose, prognose e cadeia proibida pós falha e no estabelecimento de critérios que utilizem essas informações com o intuito de determinar condições para que o supervisor promova desabilitações de eventos com o objetivo de tentar garantir controlabilidade segura a sistemas que não são DP-Controláveis Seguros.

1.1 ESCOPO

Nesta tese, é abordada a temática de controlabilidade segura em sistemas a eventos discretos (SEDs) representados por autômatos estocásticos de estados finitos. Neste contexto, as falhas são consideradas permanentes, são modeladas por eventos não controláveis e não-observáveis, e são incluídas de forma explícita na modelagem do SED sob análise. As avaliações de diagnose e prognose são realizadas por meio da construção de autômato diagnosticador.

1.2 OBJETIVO GERAL

Apresentar novos métodos ou abordagens para os problemas de diagnose de falhas, prognose de falhas e controlabilidade segura em sistemas a eventos discretos modelados por autômatos estocásticos.

1.3 OBJETIVOS ESPECÍFICOS

Com o propósito de alcançar o objetivo geral da tese, foram definidos os seguintes objetivos específicos:

a) Realizar revisão bibliográfica sobre o tema de diagnose de falhas, prognose de falhas e controlabilidade segura em SEDs modelados por autômatos clássicos;

b) Analisar o estado da arte sobre as abordagens de diagnose e prognose de falhas utilizando autômatos estocásticos;

c) Identificar as lacunas existentes na literatura;

d) Apresentar novas abordagens de análise e cálculos para os problemas da área por meio de exemplos e formalização dos conceitos propostos.

1.4 RESUMO DAS CONTRIBUIÇÕES

Em linhas gerais, o trabalho estende noções e conceitos de diagnose, prognose e controlabilidade formalizados para autômatos clássicos por meio da proposição de abordagens e métodos de cálculos para SEDs representados por autômatos estocásticos. Em resumo, as contribuições são apresentadas nos seguintes itens:

- Proposição de um modelo de diagnosticador denominado Diagnosticador Estocástico com Saídas (DECS), que contém probabilidades de diagnose de falhas, probabilidades de ocorrência futura de falhas e probabilidade de ocorrência futura de evento proibido após a falha.
- Apresentação de duas abordagens distintas para o cálculo do DECS, as quais são denominadas de Diagnosticador Estocástico com Probabilidades Estáticas e Diagnosticador Estocástico com Probabilidade Dinâmicas.
- Introdução do conceito de certeza de anormalidade para autômatos clássicos, bem como a extensão do conceito para autômatos estocásticos por meio da formalização de um coeficiente de anormalidade.
- Introdução das noções de u-diagnosticabilidade, u-diagnosticabilidade segura, u-prognosticabilidade, controlabilidade segura pela u-diagnose, controlabilidade segura pela u-prognose, controlabilidade segura pelo coeficiente de anormalidade.
- Apresentação do modelo com probabilidades de transições dinâmicas para a avaliação da temática de prognose de falhas: estabelecimento de discussão e apresentação de exemplos para esclarecimento das vantagens e desvantagens ao utilizar o modelo estático ou o modelo dinâmico.
- Introdução da noção do Estado Dinâmico do Diagnosticador: apresentação da estrutura, procedimento de obtenção, ilustração com exemplos e identificação da funcionalidade para uma topologia de CTF com probabilidades de diagnose e prognose calculadas em tempo de execução.

1.5 ORGANIZAÇÃO DO DOCUMENTO

O Capítulo 2 apresenta os principais conceitos utilizados no trabalho. É feita uma breve apresentação sobre as definições da teoria de linguagens e autômatos; são definidas operações com linguagens e autômatos. São apresentadas as características das três abordagens para síntese de supervisores na Teoria de Controle Supervisório. Por fim, são apresentados alguns conceitos preliminares da área de Diagnose, Prognose e Controle Tolerante a falhas, tais como: critérios necessários para que as linguagens sejam diagnosticáveis, prognosticáveis, diagnosticáveis seguras e controláveis seguras.

O Capítulo 3 apresenta um levantamento do estado da arte. Inicialmente, é apresentada a metodologia de busca sistemática, utilizada para definir uma base de trabalhos da área, com intuito de determinar os principais trabalhos relacionados ao tema da pesquisa e identificar potenciais lacunas no campo de estudo. Além disso, é apresentada uma revisão desses trabalhos com o propósito de contextualizar o leitor.

No Capítulo 4, é apresentado um modelo de diagnosticador de falhas denominada Diagnosticador Estocástico com Saídas, o qual é calculado por duas abordagens distintas, as quais são denominadas de Diagnosticador Estocástico com Probabilidades Estáticas e Diagnosticador Estocástico com Probabilidade Dinâmicas. São apresentadas as notações, os algoritmos para os cálculos das probabilidades. São abordados exemplos para ilustração dos procedimentos. É apresentado o conceito de certeza de anormalidade para autômatos clássicos. O conceito de certeza de anormalidade é estendido para autômatos estocásticos com a formalização do coeficiente de anormalidade. São apresentadas noções de u-diagnosticabilidade, u-diagnosticabilidade segura, u-prognosticabilidade, controlabilidade segura pela u-diagnose, controlabilidade segura pela u-prognose, controlabilidade segura pelo coeficiente de anormalidade. São apresentadas as condições necessárias e suficientes para u-diagnosticabilidade segura, controlabilidade segura pela u-diagnose e controlabilidade segura pela u-prognose. Além disso, é apresentada uma discussão sobre os modelos a serem utilizados para a avaliação das probabilidades de prognose de SEDs: modelo estático x modelo dinâmico. Os dois modelos são confrontados por meio de exemplos e de uma discussão sobre a melhor forma de representar as características de um sistema fielmente.

No Capítulo 5, são apresentadas as considerações finais da tese e uma discussão sobre temáticas que podem ser abordadas em trabalhos futuros.

2 FUNDAMENTAÇÃO TEÓRICA

Sistema a eventos discretos é um sistema dinâmico que evolui de acordo com a ocorrência abrupta de eventos físicos, em intervalos de tempo em geral irregulares e desconhecidos (CASSANDRAS; LAFORTUNE, 2009; CURY, 2001). Alguns exemplos de SED são: Controle de tráfego aéreo, Sistemas de manufatura, Controle e monitoramento avançado de automóveis e grandes construções, sistemas de transporte inteligentes, etc (PINTO; LEAL; ROSSO, 2017).

Os principais modelos utilizados para representação de sistemas a eventos discretos são os seguintes: Redes de Petri com e sem temporização; Redes de Petri Controladas com e sem temporização; Cadeias de Markov; Teoria das Filas; Processos Semi-Markovianos Generalizados (GSMP) e Simulação; Álgebra de Processos; Álgebra Max-Plus; Lógica Temporal e Lógica Temporal de Tempo Real; Teoria de Linguagens e Autômatos.

Neste capítulo, são apresentados alguns conceitos básicos relacionados à teoria de linguagens e autômatos, autômatos estocásticos, teoria de controle supervisório, diagnose de falhas, prognose de falhas e controle tolerante a falhas.

2.1 LINGUAGENS E AUTÔMATOS COMO MODELOS PARA SEDS

Uma das maneiras formais de representar o comportamento lógico de SEDs é baseada nas teorias de linguagens e autômatos. Nesse contexto, o conjunto de eventos associados ao SED é denominado de alfabeto e denotado por Σ. Um evento simbólico é comumente representado por σ. Uma sequência de eventos pode ser denominada como uma palavra ou uma cadeia, comumente representada por s. Uma cadeia que não possui eventos é denominada vazia e denotada por ε. O conjunto de palavras formadas com eventos de um alfabeto formam uma linguagem. Assim, o comportamento de um SED pode ser entendido como o conjunto de todas as palavras que este SED é capaz de gerar ou processar, conjunto esse que forma a linguagem que representa o comportamento do referido SED. A definição formal de linguagem é apresentada conforme segue:

Definição 2.1.1 (Linguagem)**.** *Uma linguagem L definida a partir de um conjunto de eventos* Σ *é um conjunto de cadeias formadas com os eventos de* Σ*.*

Um autômato é uma estrutura capaz de representar uma linguagem de acordo com regras definidas. Nesta tese, utilizamos o conceito de Autômato Determinístico de Estados Finitos (ADEF), definido conforme segue:

Definição 2.1.2 (Autômato Determinístico de Estados Finitos)**.** *Um ADEF, denotado por G, é representado por uma quíntupla:* $G = (X, \Sigma, \delta, x_0, X_m)$*, em que* X *é o espaço de estados;* Σ *é o alfabeto de eventos;* δ *é a função de transição (possivelmente parcial) definida como* $\delta : X \times \Sigma \rightarrow X$*;* x_0 *é o estado inicial;* X_m *é o conjunto de estados marcados.*

O conceito de estado marcado ou também conhecido como estado final acrescenta um significado especial ao estado, o qual será apresentado na Seção 2.3.

Na representação gráfica do autômato, os estados são representados por nós circulares. Internamente ao círculo é colocado o rótulo que identifica o estado. O estado inicial é indicado por uma seta. Os estados marcados são indicados por círculos duplos concêntricos. As transições são indicadas por arcos que conectam o estado de origem ao estado de destino, acompanhadas pelo rótulo do evento que proporciona esta mudança de estado. A ponta da seta de transição indica o estado de destino.

Um SED é representado por duas linguagens regulares $L(G)$ e $L_m(G)$ que representam, respectivamente, a linguagem gerada e a linguagem marcada para um autômato G. A linguagem gerada representa o conjunto de todas cadeias possíveis em um sistema. A linguagem marcada representa o conjunto de cadeias que atingem um estado marcado. Linguagens regulares podem ser representadas por expressões regulares.

Em expressões regulares, o operador "$+$" indica uma operação lógica "OU". Seja a expressão regular $L = a + b$, a representação desta linguagem L por conjuntos é: $L = \{a, b\}$. O operador "$*$" denominado fecho de Kleene é utilizado para indicar todas as cadeias possíveis construídas a partir dos elementos de um conjunto a que este operador está associado, inclusive a não ocorrência de elemento algum (ε). Por exemplo, a expressão $L = (a+b)^*$ é relacionada ao conjunto: $L = \{\varepsilon, a, b, ab, ba, aa, bb, ...\}$.

O fecho de Kleene de um alfabeto de eventos, denotado por Σ^*, é o conjunto de todas as cadeias de comprimento finito formadas a partir do eventos em Σ, incluindo a cadeia vazia ε. Todas linguagens definidas sobre Σ são, portanto, subconjuntos de Σ^*. Em particular, $\emptyset, \Sigma$ e Σ^* são linguagens definidas sobre Σ.

Antes de apresentar operações sobre linguagens e autômatos, é importante definir alguns termos. Seja uma cadeia arbitrária $s = utv$, em que $t, u, v \in \Sigma^*$ são subcadeias de s. Em particular, a subcadeia t é um prefixo de s, enquanto a subcadeia v é um sufixo de s. Vale destacar que ε e s são subcadeias, prefixos e sufixos de s.

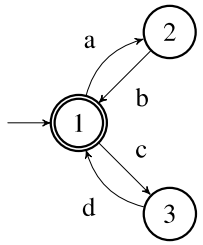
Na Figura 2 ilustra-se a representação de um SED por autômato e por expressões regulares.

2.1.1 Operações sobre linguagens e autômatos

Nesta seção, são apresentadas algumas operações matemáticas definidas para linguagens e autômatos que são relacionadas à temática de diagnose/prognose e CTF e necessárias para a compreensão desta tese.

A operação * é denominada fecho de Kleene. É comum estabelecer essa operação para um alfabeto Σ, de forma a obter um conjunto com todas as cadeias possíveis para este alfabeto. Nota-se que este conjunto é contavelmente infinito ao passo que este contém cadeias com comprimento arbitrariamente muito longos. Por exemplo, o fecho de Kleene de $\Sigma = \{a, c, d\}$ é: $\Sigma^* = \{\varepsilon, a, c, d, aa, ac, ad, ca, cc, cd, da, dc, dd, aaa, ...\}$. Este operador é bastante utilizado em

Figura 2 – Representação de SED por autômatos e linguagens.



$$X = \{1,2,3\}$$
$$\Sigma = \{a,b,c,d\}$$
$$x_0 = 1$$
$$X_m = \{1\}$$
$$\delta(1,a) = 2$$
$$\delta(1,c) = 3$$
$$\delta(2,b) = 1$$
$$\delta(3,d) = 1$$

$$L(G) = (ab+cd)^*(\varepsilon + a + c)$$
$$L_m(G) = (ab+cd)^*$$

Fonte: Elaborado pelo autor (2023)

expressões regulares, para representar de forma compacta um conjunto com um grande número de termos.

A operação concatenação entre linguagens $L_1, L_2 \subseteq \Sigma^*$ resulta em $L_1L_2 = \{s \in \Sigma^* : (s = s_1s_2)(s_1 \in L_1)(s_2 \in L_2)\}$. Por exemplo, para $L_1 = \{ab, abb\}$ e $L_2 = \{c, cda\}$ tem-se $L_1L_2 = \{abc, abcda, abbc, abbcda\}$.

Para $L \subset \Sigma^*$, a operação prefixo fechamento é definida por $\overline{L} := \{s \in \Sigma^* : (\exists t \in \Sigma^*)[st \in L]\}$. Ou seja, $\overline{L}$ é a linguagem que contém todos os prefixos das cadeias contidas em L. Por exemplo, L_3 é prefixo-fechada, pois $L_3 = \overline{L_3} = \{\varepsilon, a, b, ba, bb\}$.

A operação L/s representa a pós-linguagem de L depois da cadeia s. Formalmente, $L/s := \{t \in \Sigma^* : st \in L\}$.

Dadas duas cadeias $t, s \in \Sigma^*$, t é um prefixo de s $(t \leq s)$ se existe $u \in \Sigma^*$ tal que a concatenação de $tu = s$. Denota-se $t < s$, um caso especial de $(t \leq s)$ em que $s \neq t$. Nesse caso, diz-se que t é um prefixo estrito de s.

A norma ou comprimento de uma cadeia $s \in \Sigma^*$ denotado por $||s||$ é a quantidade de eventos presentes nesta, levando em conta a multiplicidade. Por exemplo, para $s1 = aba$ e $s2 = \varepsilon$, tem-se $||s1|| = 3$ e $||s2|| = 0$.

A função de transição estendida $\hat{\delta}$, definida como $\hat{\delta} : X \times \Sigma^* \to X$, tem o mesmo princípio da função de transição δ, porém definida para cadeias de eventos ao invés de um único evento. $\hat{\delta}(x,s) = x'$, tal que $x, x' \in X$ e $s \in \Sigma^*$. $\Gamma(x)$ denota o conjunto de eventos ativos num estado $x \in X$, formalmente $\Gamma(x) = \{\sigma \in \Sigma : f(x,\sigma)$ é definida$\}$.

Um estado $x \in X$ é dito acessível quando existe um caminho do estado inicial x_0 que leve até x, i.e $\hat{\delta}(x_0, s) = x$ é definida. De outra forma, x é dito ser não acessível. A operação Ac(G) é responsável por remover os estados inacessíveis de G. E é formalmente apresentada a seguir:

$$Ac(G) := (X_{ac}, \Sigma, \delta_{ac}, x_0, X_{ac,m}) \text{ , sendo}$$
$$X_{ac} = \{x \in X : (\exists s \in \Sigma^*)[\hat{\delta}(x_0, s) = x]\}$$
$$X_{ac,m} = X_m \cap X_{ac}$$
$$\delta_{ac} = \delta|_{Xac \times \Sigma \to Xac}$$

em que a notação $\delta|_{Xac \times \Sigma \to Xac}$ indica uma restrição da função δ ao domínio de estados acessíveis.

Se for possível a partir de x alcançar um estado marcado, então x é dito co-acessível. Denotada por CoAc(G), a operação de co-acessibilidade realiza a exclusão dos estados que não são co-acessíveis é formalizada a seguir:

$$CoAc(G) := (X_{coac}, \Sigma, \delta_{coac}, x_{0coac}, X_m) \text{ sendo}$$
$$X_{coac} = \{x \in X : (\exists s \in \Sigma^*)[\delta(x, s) \in X_m]\}$$
$$x_{0coac} = \begin{cases} x_0 & \text{se } x_0 \in X_{coac} \\ \text{não definida} & \text{caso contrário} \end{cases}$$
$$\delta_{coac} = \delta|_{Xcoac \times \Sigma \to Xcoac}$$

em que a notação $\delta|_{Xcoac \times \Sigma \to Xcoac}$ indica uma restrição da função δ ao domínio de estados co-acessíveis.

A operação Trim é a realização conjunta das operações de Acessibilidade e Co-Acessibilidade, independentemente da ordem de aplicação.

$$Trim(G) := CoAc[Ac(G)] = Ac[CoAc(G)]$$

A composição paralela (ou síncrona) é utilizada para representar a operação conjunta de subsistemas com intuito de obter um sistema completo. A composição síncrona dos autômatos G_1 e G_2 é formalmente definida por:

$$G_1 \parallel G_2 := A_c(X_1 \times X_2, \Sigma_1 \cup \Sigma_2, \delta, (x_{01}, x_{02}), X_{m1} \times X_{m2})$$

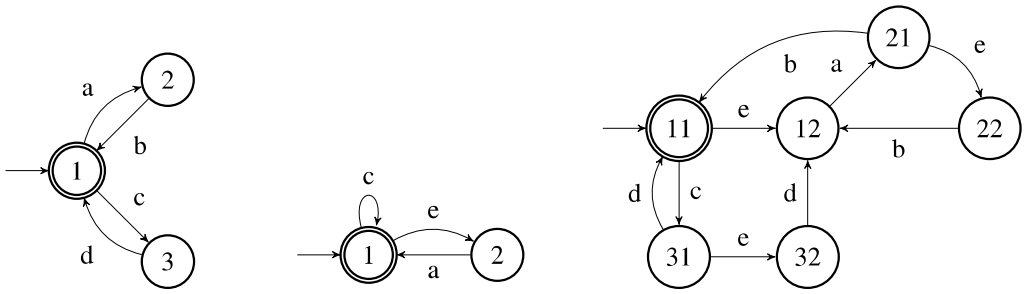
em que

$$\delta((x_1, x_2), e) := \begin{cases} (\delta_1(x_1, e), \delta_2(x_2, e)) & \text{se } e \in \Gamma_1(x_1) \cap \Gamma_2(x_2) \\ (\delta_1(x_1, e), x_2) & \text{se } e \notin \Sigma_2 \ \wedge \ e \in \Gamma_1(x_1) \\ (x_1, \delta_2(x_2, e)) & \text{se } e \notin \Sigma_1 \ \wedge \ e \in \Gamma_2(x_2) \\ \text{não definida} & \text{caso contrário} \end{cases}$$

A função de transição apresentada acima representa a composição de G_1 e G_2. A Figura 3 ilustra o processo de composição. No exemplo desta imagem, temos dois autômatos (G1 e

G2) nos quais $\Sigma_1 = \{a,b,c,d\}$ e $\Sigma_2 = \{a,c,e\}$. É possível observar que: os eventos a e c que são comuns aos dois alfabetos ocorrem de forma sincronizada; os eventos b, d e e que pertencem apenas ao alfabeto de um dos autômatos ocorrem normalmente.

Figura 3 – Exemplo de composição síncrona entre dois autômatos.



(a) G1 (b) G2 (c) G1 ‖ G2

Fonte: Elaborado pelo autor (2023)

2.2 SEDS PARCIALMENTE OBSERVÁVEIS

Evento observável é aquele que pode ser "visto"ou "observado" por um agente observador externo; evento não observável é aquele que o agente observador externo não consegue observar. Para refletir as limitações quanto à observação, o conjunto de eventos Σ é particionado em $\Sigma = \Sigma_o \dot{\cup} \Sigma_{uo}$, em que Σ_o e Σ_{uo} denotam, respectivamente, o conjunto de eventos observáveis e o conjunto de eventos não observáveis.

Apresentado o conceito de observabilidade de eventos, outra importante operação que pode ser aplicada a cadeias ou linguagens, é a operação de projeção. Formalmente, a projeção $P_o : \Sigma \to \Sigma_o$ para símbolos é definida como:

$$P_o(\varepsilon) = \varepsilon$$

$$P_o(\sigma) = \begin{cases} \sigma, & \text{se } \sigma \in \Sigma_o \\ \varepsilon, & \text{se } \sigma \notin \Sigma_o \end{cases}$$

Formalmente, a projeção $P_o : \Sigma^* \to \Sigma_o^*$ para cadeias é definida recursivamente como:

$$P_o(s\sigma) := P_o(s)P_o(\sigma), \;\; s \in \Sigma^* \text{ e } \sigma \in \Sigma$$

A projeção inversa de uma cadeia s que contém apenas eventos pertencentes ao conjunto Σ_o feita em relação ao alfabeto completo Σ é definida como $P_o^{-1}(s) := \{t \in \Sigma^* : P_o(t) = s\}$, com $P_o^{-1} : \Sigma_o \to 2^{\Sigma}$.

As operações de projeção e projeção inversa definidas em relação ao alfabeto de eventos observáveis são utilizadas de forma recorrente nas análises tanto de diagnose quanto de prognose de falhas. Nesse contexto, as falhas em geral são consideradas eventos não observáveis.

2.3 TEORIA DE CONTROLE SUPERVISÓRIO

A Teoria de controle supervisório (TCS) consiste na utilização dos modelos formais, fornecidos pela teoria de linguagens e autômatos, para sintetizar sistematicamente supervisores para sistemas a eventos discretos.

No âmbito da TCS, ao executarmos uma cadeia no autômato que atinge um estado marcado, diz-se que o sistema completou uma tarefa. Além disso, é necessária a classificação de eventos quanto à Controlabilidade. Evento controlável é aquele que se pode evitar que aconteça com uma ação de desabilitação emitida pelo supervisor. Por exemplo, ações de controle como: abrir uma válvula, ligar um motor são comumente classificados como eventos controláveis. Evento não controlável é aquele que não pode ser proibido pela ação de supervisor. Por exemplo, falhas, sinais de sensores, términos de processos, eventos que modelam condições climáticas são eventos comumente classificados como não controláveis. O conjunto de eventos controláveis de um sistema é representado por Σ_c e o conjunto de eventos não controláveis por Σ_{uc}, tal que $\Sigma = \Sigma_c \dot{\cup} \Sigma_{uc}$.

Apresentadas as classificações de eventos quanto a observabilidade e controlabilidade, a partir de agora essas classificações serão indicadas na representação gráfica dos autômatos. As transições com eventos controláveis serão representadas por uma seta com um traço no meio; e as transições com eventos não observáveis serão representadas por uma seta tracejada.

Existem diversas metodologias distintas na TCS para a síntese de supervisores, tais como: abordagem monolítica (RAMADGE; WONHAM, 1987b), abordagem modular clássica (RAMADGE; WONHAM, 1987a; WONHAM; RAMADGE, 1988), abordagem modular local(DE QUEIROZ; CURY, 2000b; DE QUEIROZ; CURY, 2000a), técnicas para estabelecimento de controle descentralizado (LIN; WONHAM, 1988), controle hierárquico (WONG; WONHAM, 1996), controle de sistemas temporizados (BRANDIN; WONHAM, 1994), etc.

2.4 AUTÔMATOS ESTOCÁSTICOS

Autômatos estocásticos/probabilísticos são uma generalização de autômatos determinísticos de estados finitos. Visto que existem dois sinônimos utilizados nos trabalhos na área, nesta tese é adotado como padrão o termo autômato estocástico. A diferença é que associa-se uma probabilidade para cada transição. A Figura 4 apresenta um exemplo de autômato estocástico. Rabin (1963) foi um dos precursores na formalização de autômatos estocásticos, mas nesse trabalho será adotada a notação proposta por Thorsley e Teneketzis (2003), onde um autômato estocástico é representado pela quádrupla:

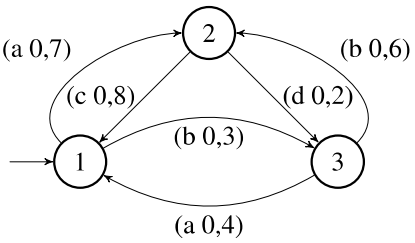
$$G = (X, \Sigma, p, x_0)$$

em que p é a função de transição probabilística definida como $p : X \times \Sigma \to \mathbb{R}_+$ e cuja notação é $p(x, \sigma)$, sendo estabelecida $\forall x \in X$ e $\forall \sigma \in \Sigma$.

Para todo estado $x \in X$, a soma das probabilidades das transições é igual a 100%, $\sum_{\forall \sigma \in \Sigma} p(x,\sigma) = 1$. A partir da função de transição probabilística, definimos a função de transição parcial como $\delta : X \times \Sigma \rightarrow X$. A função de transição probabilística e a função de transição parcial tem a seguinte relação:

$$\delta(x,\sigma) = x' \Rightarrow p(x,\sigma) > 0$$

Figura 4 – Exemplo de autômato estocástico.



Fonte: Elaborado pelo autor (2023)

Autômatos estocásticos podem ser utilizados como modelos em sínteses de supervisores para controle de Sistemas a Eventos Discretos Estocásticos (SEDE), bem como na área de diagnose, prognose e controle tolerante a falhas (escopo desta tese).

2.5 DIAGNOSE E PROGNOSE DE FALHAS EM SEDS

De acordo com Zaytoon e Lafortune (2013), as falhas podem ser classificadas em: permanentes, graduais ou intermitentes. No escopo deste trabalho, serão tratadas falhas permanentes, modeladas por eventos não controláveis e não observáveis.

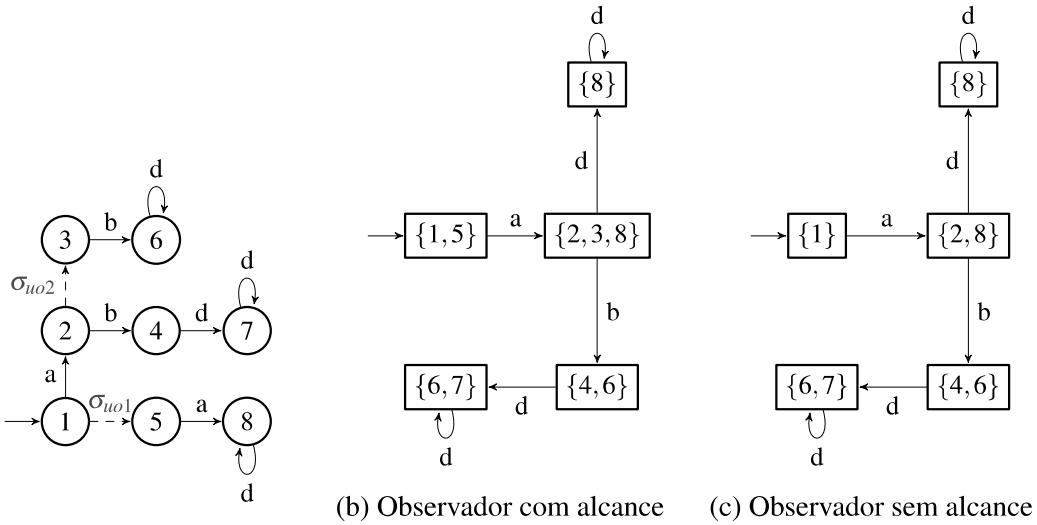
As principais estruturas/arquiteturas para o cálculo de diagnose de falhas são: centralizada, descentralizada e distribuída. Zaytoon e Lafortune (2013) apresentam uma visão geral sobre os trabalhos na área de diagnose de falhas.

Determinada a classificação do evento de falha e tendo como base o conceito de observabilidade, apresenta-se o conceito de observador. O observador é um autômato determinístico que pode ser construído a partir de uma autômato não determinístico (que possui múltiplas transições com o mesmo rótulo a partir de um único estado) ou a partir de um autômato determinístico que possui eventos não observáveis.

Existem duas abordagens para o cálculo do observador: uma contempla o alcance dos eventos não observáveis, enquanto a outra não. O procedimento de cálculo dos observadores sem alcance não observável e com alcance não observável pode ser encontrado, respectivamente em: Sampath et al. (1995) e Carvalho (2011).

A Figura 5 mostra um exemplo de como é obtido o observador para um autômato, utilizando as duas abordagens. Nesta tese será adotada a abordagem que não contempla o alcance dos eventos não observáveis.

Figura 5 – Exemplo de cálculo de observador com e sem alcance não observável.



(a) Planta

(b) Observador com alcance não observável

(c) Observador sem alcance não observável

Fonte: Elaborado pelo autor (2023)

No exemplo da Figura 5, podemos verificar que no estado inicial do autômato da planta (Figura 5(a)) existe uma transição com o evento não observável σ_{uo1} levando ao estado 5. Ao calcularmos o observador com alcance não observável (Figura 5(b)), a possibilidade de ocorrência dessa transição é incluída no estado inicial do observador, ou seja, o estado inicial é o $\{1,5\}$. Por outro lado, no observador sem alcance (Figura 5(c)) a possibilidade de ocorrência do evento não observável σ_{uo1} só é considerada após a observação do evento a, sendo assim o estado inicial do observador sem alcance é o $\{1\}$. Em relação a transição com o evento não observável σ_{uo2}, o procedimento é o mesmo. No observador com alcance, a possibilidade de ocorrência do evento σ_{uo2} já é levada em conta após a observação do evento a atingindo o estado $\{2,3,8\}$ na Figura 5(b), enquanto no outro observador a possibilidade de ocorrência do evento σ_{uo2} só é considerada após a observação da cadeia $s_o = ab$, atingindo o estado $\{4,6\}$ na Figura 5(c).

No autômato observador, todos os eventos não observáveis são removidos. A remoção destes eventos é representada com a criação de estados com múltiplos rótulos, os quais modelam a incerteza de um determinado evento não observável ter acontecido ou não.

2.5.1 Diagnosticabilidade

Um dos primeiros trabalhos a tratar o tema de diagnose de falhas em sistemas a eventos discretos modelados pela teoria de linguagens e autômatos foi o de Sampath et al. (1995). Nesse trabalho, são apresentadas as definições e condições para diagnosticabilidade e as condições suficientes e necessárias para determinar se uma linguagem é diagnosticável ou não diagnosticável. Uma linguagem é diagnosticável, se é possível detectar todas as ocorrências de falha com um

atraso limitado a partir do registro de observação de eventos.

Seja $\Psi_L(f)$ o conjunto de todas as cadeias terminadas por um evento de falha f pertencentes à linguagem L. Formalmente, definido como: $\Psi_L(f) := \{rf \in L : r \in \Sigma^*, f \in \Sigma\}$.

O conceito de diagnosticabilidade e alguns outros conceitos que são apresentados nesta tese, são formalizados para linguagens vivas. Uma linguagem L é viva se ela não contém cadeias terminais, ou seja, para todas as cadeias $s \in L$ existe uma continuação com um evento e, de forma que $se \in L$. O conceito de diagnosticabilidade proposto por Sampath et al. (1995) é apresentado na Definição 2.5.1.

Definição 2.5.1 (Diagnosticabilidade)**.** *Uma linguagem viva e prefixo-fechada é dita diagnosticável em relação à projeção P_o e evento de falha f, se a seguinte condição for verificada:* $(\exists n \in \mathbb{N})(\forall s \in \Psi_L(f))(\forall t \in L/s)((||t|| \geq n \Rightarrow \mathscr{D})$*, onde a condição de diagnosticabilidade $\mathscr{D}$ é expressa por:* $\omega \in P_o^{-1}[P_o(st)] \cap L \Rightarrow f \in \omega$.

Em palavras, para toda cadeia s terminada pelo evento de falha, para toda cadeia t na pós-linguagem da cadeia, tal que t tem comprimento finito, a condição de diagnosticabilidade é satisfeita.

A verificação das propriedades da diagnosticabilidade e da prognosticabilidade é feita a partir do autômato diagnosticador G_D, o qual é obtido pelo cálculo do observador do autômato da planta G composto com o autômato rotulador de falhas A_r.

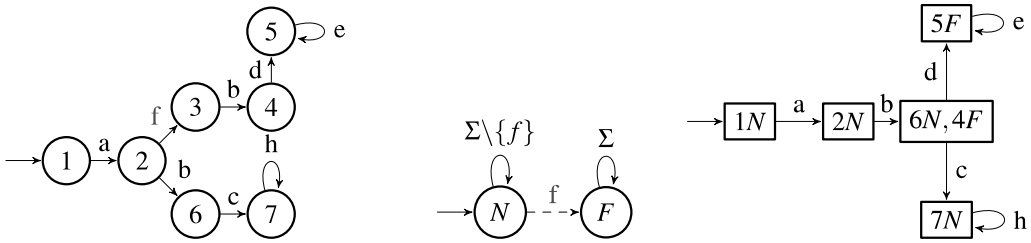
$$G_D = Obs(G \parallel A_r)$$

em que Obs() indica a operação de cálculo do Observador sem alcance dos eventos não observáveis.

A Figura 6 mostra um exemplo de cálculo de um diagnosticador; nela é apresentado um autômato rotulador (Figura 6b) que quando composto com o autômato G, insere rótulos "N" nos estados anteriores a falha e rótulos "F" nos estados posteriores a falha. A Figura 6c mostra o Diagnosticador obtido. Os estados do diagnosticador que possuem apenas rótulos "N" são chamados de estados normais; os estados que possuem rótulos "N" e "F" são chamados de estados incertos; os estados que possuem apenas rótulos "F" são chamados de estados certos de falha. O conjunto de estados X_D do diagnosticador pode ser dividido em alguns subconjuntos: Conjunto dos estados normais $X_D^N = \{x_D \in X_D : x_D \text{ é normal}\}$; Conjunto dos estados incertos $X_D^U = \{x_D \in X_D : x_D \text{ é incerto}\}$; Conjunto dos estados certos de falha $X_D^C = \{x_D \in X_D : x_D \text{ é certo de falha}\}$.

O Teorema 2.5.1 (SAMPATH et al., 1995) estabelece as condições necessárias e suficientes para determinar se uma linguagem é diagnosticável por meio de uma análise *offline* do diagnosticador. Nessa análise, utiliza-se o conceito de ciclos indeterminados, formalmente apresentado na Definição 2.5.2 (SAMPATH et al., 1995).

Figura 6 – Procedimento de obtenção de um Diagnosticador de falhas para um SED.



(a) Planta (b) Rotulador A_r (c) Diagnosticador

Fonte: Elaborado pelo autor (2023)

Definição 2.5.2 (Ciclo indeterminado)**.** *Um conjunto de estados incertos* $x_D^1, x_D^2, ..., x_D^n \in X_D^U$ *forma um ciclo indeterminado se*

1) $x_D^1, x_D^2, ..., x_D^n$ *formam um ciclo no diagnosticador, com* $\delta_D(x_D^l, \sigma_l) = x_D^{l+1}$ *tal que* $l = 1, 2, ..., n-1$ *e* $\delta_D(x_D^n, \sigma_n) = x_D^1$*, em que* $\sigma_l \in \Sigma_o$*, com* $l = 1, 2, ...n$*;*

2) $\exists (x_l^k N)(y_l^r F) \in x_D^l$*, tal que* $x_l^k, y_l^r \in X$*, com* $l = 1, ..., n, k = 1, ..., m$*,* $r = 1, ..., m'$*.*

a) $x_l^1, x_l^2, ...x_l^k$*, formam um ciclo na planta, com* $\delta(x_l^k, \sigma_l) = x_{l+1}^{k+1}$ *tal que* $l = 1, 2, ..., n-1$*,* $k = 1, 2, ..., m-1$ *e* $\delta(x_n^m, \sigma_l) = x_1^1$*, em que* $\sigma_l \in \Sigma_o$*, com* $l = 1, 2, ...n$*;*

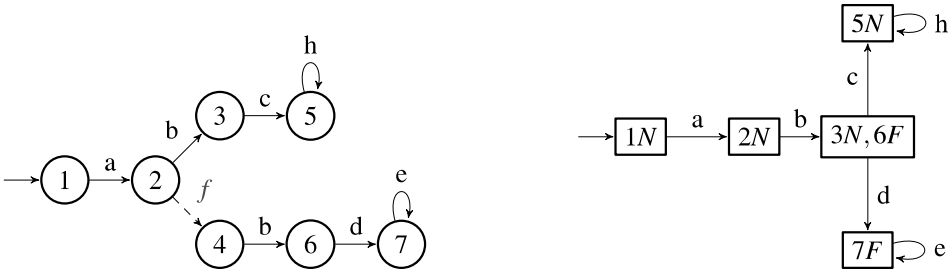
b) $y_l^1, y_l^2, ...y_l^r$*, formam um ciclo na planta, com* $\delta(y_l^r, \sigma_l) = y_{l+1}^{r+1}$ *tal que* $l = 1, 2, ..., n-1$*,* $r = 1, 2, ..., m'-1$ *e* $\delta(y_n^{m'}, \sigma_l) = y_1^1$*, em que* $\sigma_l \in \Sigma_o$*, com* $l = 1, 2, ...n$*;*

Em palavras, um ciclo de estados em um diagnosticador G_D obtido a partir do autômato G, é dito indeterminado se ele corresponde a dois ciclos no autômato G: um anterior a ocorrência da falha e outro posterior a ocorrência da falha.

Teorema 2.5.1 (Condições para Diagnosticabilidade)**.** *Uma linguagem L gerada por um autômato G é diagnosticável em relação à projeção* P_o *e evento* f *se, e somente se, o seu diagnosticador* G_D *não possuir ciclos indeterminados.*

As Figuras 7 e 8 apresentam o exemplo de duas linguagens e seus respectivos diagnosticadores. A linguagem do exemplo da Figura 7 é diagnosticável. Enquanto a linguagem do exemplo da Figura 8 não é diagnosticável. As duas linguagens tem estruturas similares, mas a simples alteração do evento do auto-laço no estado 7 faz com que a falha não seja diagnosticável no exemplo da Figura 8 pois a observação da cadeia $s_o = abc$ leva ao estado (5N7F) que constitui um ciclo indeterminado. Ao passo que no exemplo da Figura 7, após a observação da cadeia $s_o = abc$, com a observação do evento h atinge-se um ciclo de estados normais, enquanto a observação do evento e propicia a diagnose da falha, pois o diagnosticador correspondente atinge um ciclo de estados certos de falha.

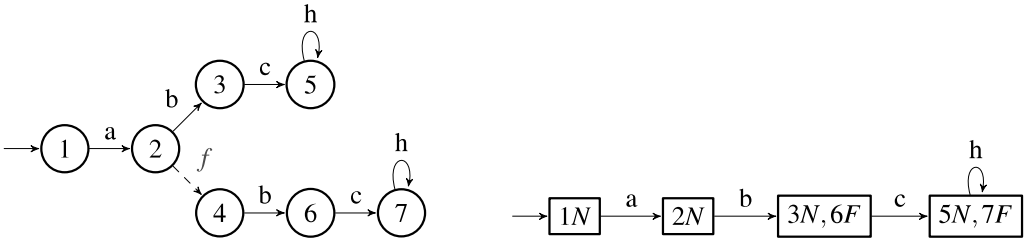
Figura 7 – Exemplo de linguagem diagnosticável.



(a) Planta (b) Diagnosticador

Fonte: (WATANABE, 2019)

Figura 8 – Exemplo de linguagem não diagnosticável.



(a) Planta (b) Diagnosticador

Fonte: (WATANABE, 2019)

2.5.2 Diagnosticabilidade segura

Um sistema diagnosticável seguro é aquele em que a ocorrência de falha é detectada antes da execução de um determinado evento ou cadeia proibidos. O conjunto de cadeias proibidas é representador pelo símbolo Φ definido formalmente como: $\Phi := \{\xi \in \Sigma^* : \xi$ é uma cadeia proibida após a falha$\}$. As cadeias ilegais que compõe o conjunto Φ são subcadeias de uma linguagem ilegal $\mathscr{K}_f$ definida formalmente como: $\mathscr{K}_f := \{y \in L/s : [s \in \Psi_L(f) \wedge \exists \xi \in \Phi : \xi$ é uma subcadeia de $y]\}$. O conceito de diagnosticabilidade segura proposto por Paoli e Lafortune (2005) é apresentado na Definição 2.5.3.

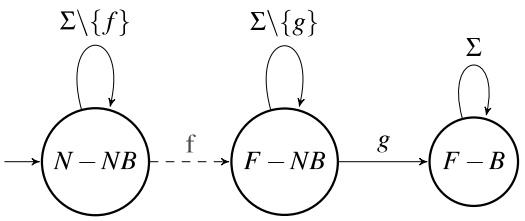
Definição 2.5.3 (Diagnosticabilidade segura)**.** *Uma linguagem L prefixo-fechada, viva, sem ciclos de eventos não observáveis, é dita diagnosticável segura com respeito a projeção P_o, evento f e a linguagem proibida $\mathscr{K}_f$, se as seguintes condições são atendidas.*
1) Condição de Diagnosticabilidade: L é diagnosticável em relação à P_o e f;
2) Condição de segurança: $(\forall s \in \Psi_L(f))(\forall t \in L/s) : ||t|| = n$ considerando que t_c, $||t_c|| = n_{tc}$, seja o mais curto prefixo de t tal que $\mathscr{D}$ seja atendida; então $\overline{t_c} \cap \mathscr{K}_f = \emptyset$.

Em palavras, para que uma linguagem L seja diagnosticável segura se a linguagem for diagnosticável e os menores prefixos de cadeias que propiciam a diagnose não podem fazer parte da linguagem proibida.

Para o cálculo do diagnosticador seguro de uma linguagem, o rotulador sofre algumas alterações em relação ao rotulador utilizado para construir um diagnosticador comum. A Figura 9 apresenta um rotulador seguro (A_{rs}) para a construção de um diagnosticador seguro de uma linguagem com um único evento proibido g.

No diagnosticador seguro, além dos rótulos "N"e "F", os estados recebem os rótulos "NB" e "B". Os rótulos "B"são para estados posteriores a ocorrência de uma cadeia proibida após a falha e são chamados de maus estados. Por outro lado, os estados anteriores a ocorrência de uma cadeia proibida recebem os rótulos "NB"e dessa forma não são considerados maus estados. O conjunto de estados X_D do diagnosticador seguro pode ser dividido nos seguintes subconjuntos: $X_D^{NB} = \{x_D \in X_D : x_D \text{ não é um mau estado}\}$; $X_D^{B} = \{x_D \in X_D : x_D \text{ é um mau estado}\}$.

Figura 9 – Rotulador A_{rs} para obtenção de diagnosticador seguro, considerando o evento proibido g.



Fonte: Elaborado pelo autor (2023)

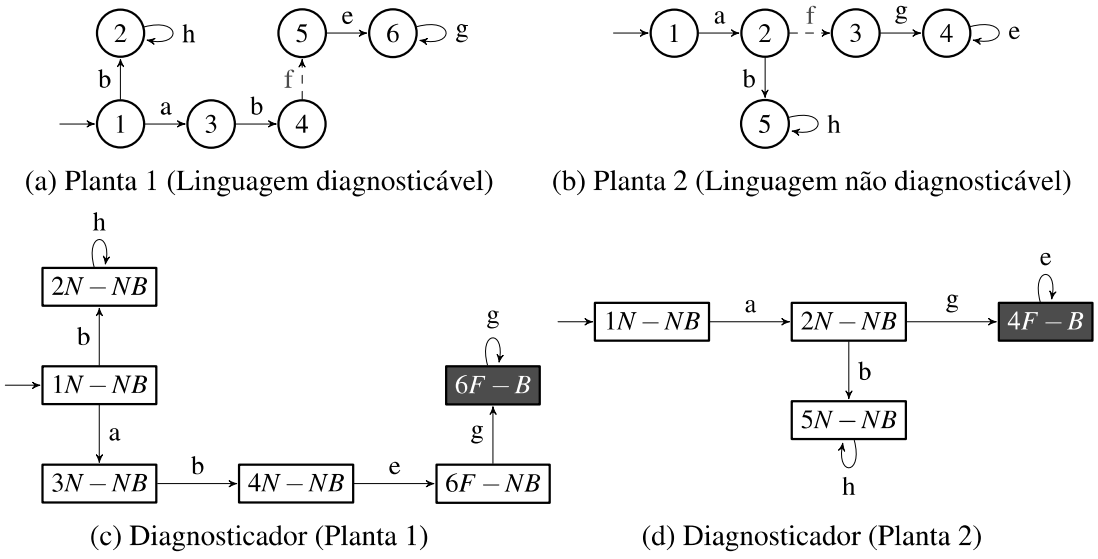
A Figura 10 mostra os autômatos G_1 e G_2, tal que $\Phi_1 = \Phi_2 = \{g\}$; e os respectivos diagnosticadores seguros para as duas linguagens. Nota-se que a primeira linguagem é diagnosticável segura, pois o mau estado é precedido por um estado certo de falha. No entanto, a segunda linguagem não é diagnosticável segura, pois o evento que proporciona a diagnose é o próprio evento proibido, ou seja, o primeiro estado certo de falha é um mau estado.

Watanabe (2019) adaptou as condições para diagnosticabilidade segura apresentada por Paoli, Sartini e Lafortune (2011), apresentando o Teorema 2.5.2 (WATANABE, 2019).

Teorema 2.5.2 (Condições para Diagnosticabilidade Segura)**.** *Considerando um autômato $G = (X, \Sigma, \delta, x_0)$ que gera uma linguagem diagnosticável L. L é diagnosticável segura em relação à projeção P_o, evento f e $\mathscr{K}_f$ se, e somente se, no diagnosticador seguro G_D obtido a partir de G:*
1) Não existe um estado $x_D \in X_D$ que seja incerto de falha e que tenha um componente da forma (q,l) tal que q seja um mau estado e $l = F$.
2) Não existe um par de estados $x_D, x_D^{'} \in X_D$ tal que: (i) x_D seja um estado certo de falha com um componente na forma (q,l) tal que q seja um mau estado e $l = F$; (ii) $x_D^{'}$ seja um estado incerto de falha ou estado normal; (iii) $x_D = \delta(x_D^{'}, \sigma_o)$ com $\sigma_o \in \Sigma_o$.

Em palavras, para que uma linguagem seja diagnosticável segura, o seu diagnosticador não pode conter estados incertos de falha em que o rótulo de falha é associado a um mau estado e todos os primeiros estados certos de falha não podem sem maus estados.

Figura 10 – Exemplo de linguagem diagnosticável segura e não diagnosticável segura.



(a) Planta 1 (Linguagem diagnosticável) (b) Planta 2 (Linguagem não diagnosticável)

(c) Diagnosticador (Planta 1) (d) Diagnosticador (Planta 2)

Fonte: Elaborado pelo autor (2023)

As Subseções 2.5.3, 2.5.5 e 2.5.6 apresentam uma avaliação das propriedades de controlabilidade segura por diagnose, prognose e por diagnose/prognose. Serão apresentados exemplos de quatro ADEF que são formados pelo o mesmo conjunto de eventos $\Sigma = \{a,b,c,d,e,f,g,h,\sigma_{uo1}\}$, tal que: $\Sigma_c = \{c\}$, $\Sigma_{uo} = \{f,\sigma_{uo1}\}$ e $\Phi = \{g\}$.

2.5.3 Controlabilidade segura pela Diagnose

A definição de controlabilidade segura pela diagnose foi inicialmente proposta por Paoli, Sartini e Lafortune (2011). No entanto, ela foi aperfeiçoada por Watanabe et al. (2017) ao considerar que o evento controlável a ser impedido possa fazer parte da cadeia proibida. Portanto, a definição mais recente será utilizada como base.

Definição 2.5.4 (Controlabilidade Segura pela Diagnose)**.** *Dada uma linguagem L viva, prefixo-fechada e que não contém ciclos de eventos não observáveis. L é dita controlável segura pela diagnose com respeito a projeção P_o, ao evento de falha f e a linguagem proibida $\mathscr{K}_f$ se atender às seguintes condições:*
1) Condição de diagnosticabilidade segura: L é diagnosticável segura em relação à P_o, f e $\mathscr{K}_f$.
2) Condição de controlabilidade segura: Considere uma cadeia qualquer $s \in L$ tal que $f \in s$ e $s = v\sigma$ com $\sigma \in \Sigma_o$. Supõe-se que a condição de diagnosticabilidade $\mathscr{D}$ não é atendida para v mas é atendida para s. Então, $(\forall t \in L/s)$tal que $t = u\xi$, com $\xi \in \Phi$, $\exists z \in \Sigma_c$ tal que $z \in t$.

Esta definição, em outras palavras, afirma que para que o sistema seja controlável seguro pela diagnose é necessário que as ocorrências de falha sejam diagnosticáveis seguras e, após a diagnose, deve haver um evento controlável que possa ser usado para impedir a execução de uma cadeia proibida ξ.

Paoli, Sartini e Lafortune (2011) apresentam o Teorema 2.5.3 que estabelece as condições necessárias e suficientes para que uma linguagem seja controlável segura pela diagnose. Seja FC o conjunto dos primeiros estados certos de falha no diagnosticador alcançados a partir do estado inicial, considerando todos os caminhos existentes. Formalmente, $FC := \{x_D \in X_D^C : (\exists s_o \in \Sigma_o^*)$ tal que $(\hat{\delta}_D(x_{D0}, s_o) = x_D)$ e $(\nexists t_o < s_o)(\hat{\delta}_D(x_{D0}, t_o)) \in X_D^C\}$. Para cada estado $x_D^i \in FC$ $(i = 1, ..., m)$, constrói-se um novo modelo não controlável pós-diagnose de falha G_i^{deg}, tomando a parte acessível da planta (comportamento nominal + falha) de todos os estados $x \in X$ associados aos rótulos presentes no i-ésimo estado x_D^i do diagnosticador seguro. A ínfima superlinguagem controlável $\{\varepsilon^{\downarrow C}\}$ é obtida para cada G_i^{deg} por meio da desabilitação de todos eventos controláveis das evoluções possíveis para G_i^{deg}.

Teorema 2.5.3 (Condições para Controlabilidade Segura pela Diagnose)**.** *Considere uma linguagem L gerada por um autômato G e suponha que L é diagnosticável segura em relação à P_o, f e $\mathscr{K}_f$. Seja FC o conjunto dos primeiros estados certos de falha alcançados no diagnosticador seguro G_D obtido a partir de G. A linguagem L é controlável segura pela diagnose se e somente se $\forall x_D \in FC$, a ínfima superlinguagem controlável $\{\varepsilon^{\downarrow C}\}$, calculada a partir do modelo não controlado pós-diagnose de falha G_i^{deg}, não contém nenhum elemento de Φ como subcadeia.*

Simplificando, uma linguagem é controlável segura se ela for diagnosticável segura e existir um evento controlável que pode ser desabilitado e consequentemente impedir a conclusão de uma cadeia proibida.

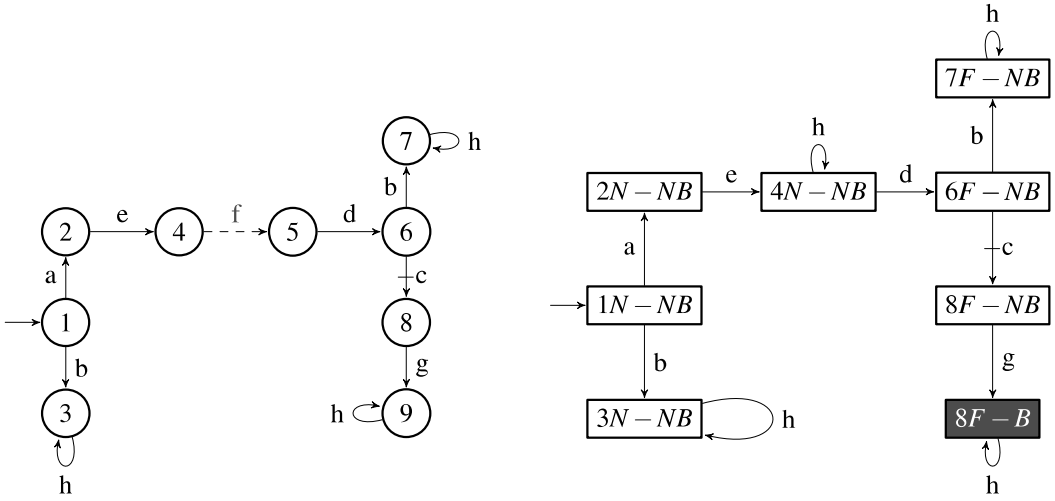
A linguagem gerada pelo autômato apresentado na Figura 11 é controlável segura pela diagnose, pois a falha é detectada de forma segura após a observação da cadeia *aed* atingindo o estado 6 da planta, estado que possui o evento controlável c que pode ser desabilitado para impedir a ocorrência do evento proibido g.

2.5.4 Prognosticabilidade

Além da diagnose de falhas, existe a vertente de estudo de prognose/predição de falhas. Visto que existem dois sinônimos utilizados nos trabalhos na área, nesta tese é adotado como padrão os termos prognose e suas variações: prognosticável e prognosticabilidade. Genc e Lafortune (2009) foram precursores neste campo no contexto de SEDs e formalizaram o conceito apresentado na Definição 2.5.5.

Definição 2.5.5 (Prognosticabilidade)**.** *Dada uma linguagem L prefixo-fechada e viva, as ocorrências do evento de falha $f \in \Sigma$ são prognosticáveis em relação a P_0 se $(\exists n \in \mathbb{N})(\forall s \in \Psi_L(f))(\exists t \in \overline{s})[(f \notin t) \wedge \mathscr{P}]$, onde a condição de prognosticabilidade $\mathscr{P}$ é formalizada como: $(\forall u \in L)(\forall v \in L/u)[(P_o(u) = P_o(t)) \wedge (f \notin u) \wedge (||v|| \geq n) \Rightarrow (f \in v)]$. Além disso, outra premissa para que uma linguagem seja prognosticável é que esta linguagem seja diagnosticável.*

Figura 11 – Exemplo de linguagem controlável segura pela Diagnose.



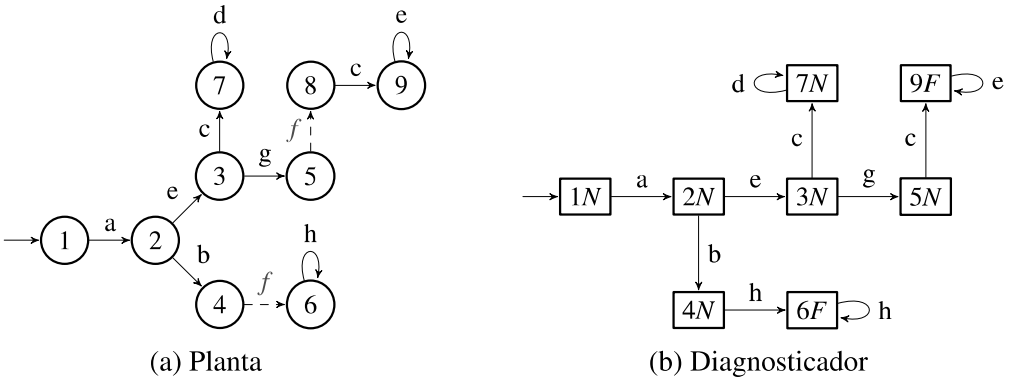
(a) Planta (b) Diagnosticador

Fonte: Elaborado pelo autor (2023)

Em palavras, uma linguagem é prognosticável se é possível inferir sobre todas as ocorrências futuras de falhas com base no registro observável de cadeias que não contêm o evento de falha.

As Figuras 12 e 13 apresentam os exemplos de duas linguagens e seus respectivos diagnosticadores. No exemplo da Figura 12, tem-se a prognose da falha f, pois todas ocorrências de falha são prognosticáveis. Já no segundo exemplo não é possível prognosticar a falha, visto que no estado imediatamente anterior a falha existe ao menos um caminho que não possui ocorrência futura do evento de falha f.

Figura 12 – Exemplo de linguagem prognosticável.

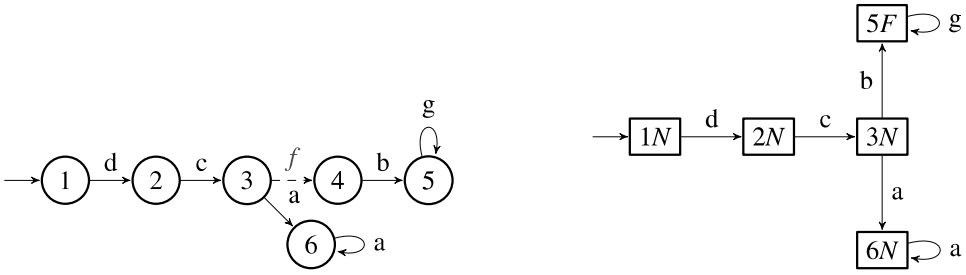


(a) Planta (b) Diagnosticador

Fonte: Modificado de Watanabe (2019)

O Teorema 2.5.4 apresentado por Genc e Lafortune (2009) define as condições necessárias para que uma linguagem seja prognosticável a partir da análise *offline* do autômato diagnosticador. Para o estabelecimento das condições desse teorema, utiliza-se o conjunto F_D que é composto

Figura 13 – Exemplo de linguagem não prognosticável.



(a) Planta (b) Diagnosticador

Fonte: Modificado de Watanabe (2019)

pelos estados normais do diagnosticador que possuem um sucessor imediato que não é normal. $F_D = \{x_D \in X_D^N : (\exists x_D^{'} = \delta_D(x_D, \sigma_o))[(\sigma_o \in \Sigma_o) \wedge (x_D^{'} \notin X_D^N)]\}$.

Teorema 2.5.4 (Condições para Prognosticabilidade)**.** *Seja $G = (X, \Sigma, \delta, x_0)$ o autômato que gera uma linguagem L prefixo-fechada e viva. Seja $G_D = (X_D, \Sigma_o, \delta_D, x_{D0})$ o diagnosticador para G. As ocorrências do evento f são prognosticáveis em L em relação a P_o se e somente se para todo $x_D \in F_D$, a condição $\mathbb{C}$ é satisfeita, sendo $\mathbb{C}$: todos os ciclos $A_c(G_D, x_D)$ são ciclos de estados certos do diagnosticador.*

No diagnosticador do exemplo da Figura 12, tem-se $FD = \{4N, 5N\}$ e para todos estados $x_D \in FD$, os ciclos acessíveis $A_c(G_D, x_D)$ no diagnosticador a partir destes estados são ciclos de estados certos de falha, o que satisfaz as condições do Teorema 2.5.4. Por outro lado, no diagnosticador apresentado na Figura 13 as condições do Teorema 2.5.4 não são atendidas, visto que para o estado ($x_D = 3N \in FD$) existem ciclos acessíveis no diagnosticador que são ciclos de estados normais.

2.5.5 Controlabilidade segura pela Prognose

Watanabe et al. (2017) apresenta o conceito de controlabilidade segura pela prognose. Além disso, estabeleceu as condições necessárias e suficientes para que uma linguagem seja controlável segura pela prognose, conforme apresentado no Teorema 2.5.5.

Definição 2.5.6 (Controlabilidade segura pela Prognose)**.** *Uma linguagem L viva, prefixo-fechada e que não contém ciclos de eventos não observáveis é dita controlável segura pela prognose com respeito à projeção P_o, ao evento de falha f e ao conjunto de cadeias proibidas Φ se ela atender às seguintes condições:*
1) Condição de Prognosticabilidade: As ocorrências do evento f são prognosticáveis em L com relação à P_o.
2) Condição de Controlabilidade Segura: Considerando para qualquer cadeia $s \in L$ tal que $s = tu$, com $f \in u$ e $t = r\sigma$ tal que $\sigma \in \Sigma_o$. Supondo que a condição de prognosticabilidade $\mathscr{P}$

não seja atendida para r, mas seja atendida para t. Então, $(\forall w \in L/t)$ *tal que* $w = uv\xi$*, com* $\xi \in \Phi$ *e* $v \in \Sigma^*$*,* $\exists \sigma_c \in \Sigma_c$ *tal que* $\sigma_c \in w$*.*

Em palavras, para que uma linguagem L seja controlável segura pela Prognose, todas as ocorrências do evento de falha f devem ser prognosticáveis e deve haver em todos os casos ao menos um evento controlável que, quando desabilitado, impeça a conclusão de uma cadeia proibida após a falha.

Seja FP o conjunto dos primeiros estados em G_D que asseguram a prognose. Para cada estado $x_D^j \in FP$ $(j = 1, ..., m')$, constrói-se um modelo que representa o comportamento não controlável pós-prognose de falha $G_j^{deg,p}$, ou seja, o modelo para o comportamento degradado da planta que segue após a cadeia que fornece prognose. A ínfima superlinguagem controlável $\{\varepsilon^{\downarrow C}\}$ é obtida para cada $G_j^{deg,p}$ por meio da desabilitação de todos eventos controláveis das evoluções possíveis para $G_j^{deg,p}$ (PAOLI; SARTINI; LAFORTUNE, 2011).

Teorema 2.5.5 (Condições para Controlabilidade Segura pela Prognose)**.** *Considere uma linguagem L gerada por um autômato G e assuma que as ocorrências do evento* f *são prognosticáveis em relação à* P_o*. Seja* $G_D = (X_D, \Sigma_o, \delta_D, q_{D0})$ *o diagnosticador seguro construído a partir de G. A linguagem L é controlável segura pela prognose se e somente se* $\forall q_J \in FP$*, a ínfima superlinguagem controlável* $\{\varepsilon^{\downarrow C}\}$*, calculada em relação a* $G_J^{deg,p}$ *é tal que* $P_o^{-1}(\varepsilon^{\downarrow C}) \cap L(G_J^{deg,p})$*, não contém nenhum elemento de* Φ *como subcadeia após o evento* f*.*

As condições apresentadas no Teorema 2.5.5 requerem que, para que uma linguagem seja controlável segura pela prognose, a linguagem deve ser prognosticável e conter eventos controláveis após a prognose que, ao serem desabilitados, impeçam a conclusão da cadeia proibida após qualquer ocorrência de falha.

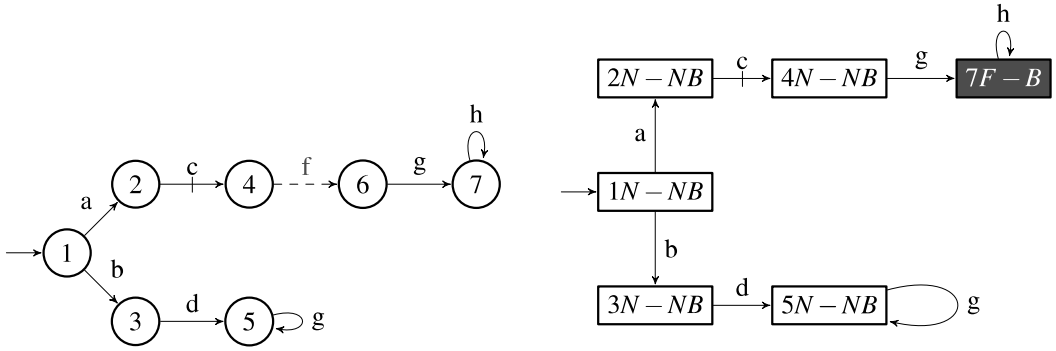
A linguagem gerada pelo autômato, apresentado na Figura 14, é controlável segura pela prognose, pois a falha é prognosticável após a observação do evento *a* existe o evento controlável *c* entre o estado que se tem prognose e a ocorrência do evento proibido *g* após a falha. No entanto, a linguagem não é diagnosticável segura e consequentemente não é controlável segura pela diagnose.

2.5.6 Controlabilidade segura pela Diagnose ou Prognose

No âmbito de controlabilidade segura, Watanabe (2019) propôs uma abordagem que avalia em uma mesma linguagem as propriedades de controlabilidade segura por diagnose e por prognose de forma conjunta realizando uma análise por cadeias. Nesta metodologia, a autora considera, para simplificação, que todos os eventos controláveis são observáveis $\Sigma_c \subset \Sigma_o$.

As Definições 2.5.4 e 2.5.6 são concebidas para uma análise de controlabilidade segura da linguagem como um todo. Watanabe et al. (2022) apresentou uma metodologia para analisar controlabilidade segura de cadeias, tanto pela diagnose quanto para prognose. A Definição 2.5.7 utiliza a abordagem por cadeias. Dessa forma, mesmo se a linguagem não for controlável segura

Figura 14 – Exemplo de linguagem controlável segura pela Prognose.



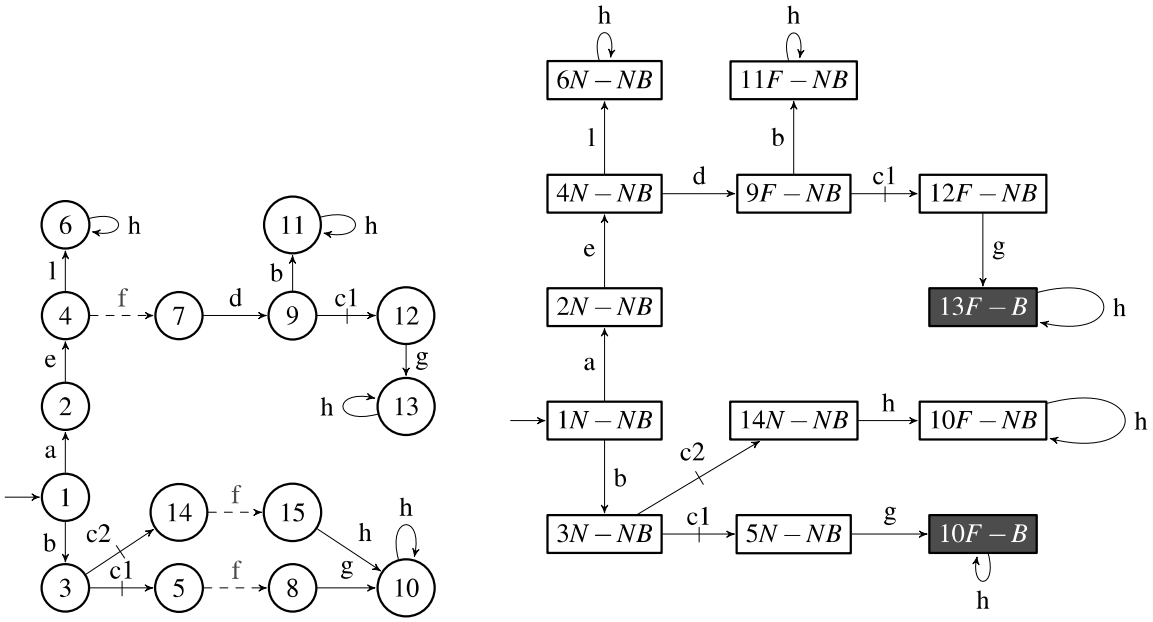
(a) Planta (b) Diagnosticador

Fonte: Elaborado pelo autor (2023)

pela diagnose ou controlável segura pela prognose, o SED pode ser DP-Controlável Seguro se todas as ocorrências de falha atenderem as condições de controlabilidade de cadeias pela diagnose ou pela prognose.

Definição 2.5.7 (DP - Controlabilidade Segura)**.** *Uma linguagem diagnosticável L é dita ser controlável segura pela diagnose ou prognose (DP - Controlável segura) em relação à projeção P_o, ao evento de falha f e ao conjunto de cadeias proibidas Φ se a ocorrência de f em toda cadeia $s \in \Psi_L(f)$ é controlável segura pela diagnose ou controlável segura pela prognose.*

Figura 15 – Exemplo de linguagem controlável segura pela Diagnose ou Prognose.



(a) Planta (b) Diagnosticador

Fonte: Elaborado pelo autor (2023)

O Teorema 2.5.6 apresenta as condições para que um SED seja DP-Controlável Seguro conforme a abordagem por cadeias proposta por Watanabe (2019). Para formalização desse teorema são definidos alguns novos elementos, tais como $FC(s)$ é o conjunto dos primeiros estados certos de falha alcançados após a cadeia s; $FB(s)$ é o conjunto dos primeiros maus estados alcançados após a cadeia s; $FU(s)$ é o conjunto dos primeiros estados incertos alcançados pela cadeia s; $FP(s)$ é o primeiro estado no qual se assegura a prognose de falhas para a cadeia s; a condição $\mathbb{C}$ significa que todos os ciclos na componente acessível do autômato G referente ao estado x_D do diagnosticador são estados certos de falha.

Teorema 2.5.6 (Condições para DP-Controlabilidade Segura)**.** *Considere uma linguagem diagnosticável L e um autômato $G = (X, \Sigma, \delta, x_0)$ que gera L. Seja $G_D = (X_D, \Sigma_o, \delta_D, x_{D0})$ o diagnosticador seguro construído a partir de G. A linguagem L é DP-Controlável Segura em relação à P_o, f e Φ se e somente se para toda a cadeia $s \in \Psi_L(f)$ pelo menos uma das seguintes condições é atendida:*
1) Condição para Controlabilidade Segura de uma Cadeia pela Diagnose: $\forall x_D \in FC(s)$ (i) $x_D \notin X_D^B$ e (ii) $\nexists w_o \in \Sigma_{uc}^* : \hat{\delta}_D(x_D, w_o) = x_{D,B}$, sendo $x_{D,B} \in FB(s)$;
2) Condição para Controlabilidade Segura de uma Cadeia pela Prognose: (i) condição $\mathbb{C}$ é atendida para os estados $x_D \in FU(s)$ e (ii) para $x_D^{'} = FP(s), \nexists w_o \in \Sigma_{uc}^* : \hat{\delta}_D(x_D^{'}, w_o) = x_{D,B}$, sendo que $x_{D,B} \in FB(s)$;

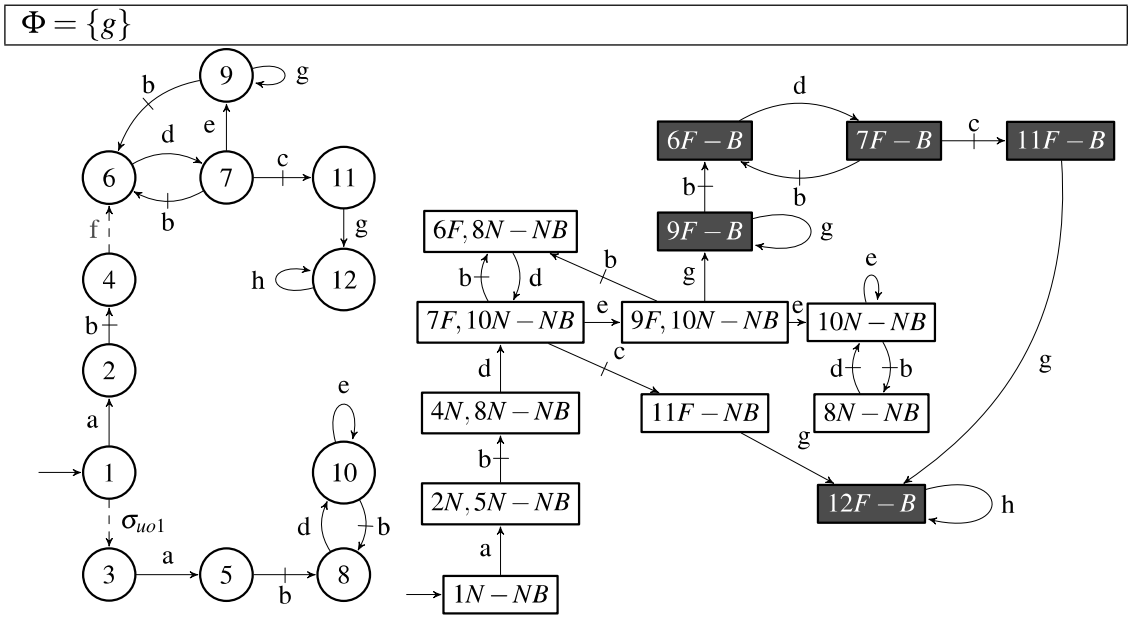
As condições apresentadas no Teorema 2.5.6 definem, portanto, que para uma linguagem seja DP-Controlável Segura na abordagem por cadeias, todas as suas cadeias que contenham a falha devem ser controláveis seguras ou pela diagnose ou pela prognose.

Se analizarmos o SED representado pelo autômato da Figura 15 a partir do conceito de controlabilidade segura de linguagem pela diagnose ou a partir do conceito de controlabilidade segura de linguagem pela prognose, chegaríamos a conclusão que ela não é controlável segura. Mas ao utilizarmos a abordagem por cadeias, mostramos que ela é controlável segura pela diagnose ou prognose. A observação da cadeia *aed* fornece o diagnóstico seguro da falha f, a presença do evento controlável c antes do evento proibido g preenche o segundo critério. A ocorrência do evento de falha no estado 4 não é prognosticável. A ocorrência da falha no estado 5 não é diagnosticável segura, pois o evento que fornece a diagnose é um evento proibido. No entanto, após a observação do evento b, tem-se prognose da falha. Esta característica aliada a presença do evento controlável c, anterior a ocorrência do evento proibido garantem a controlabilidade segura dessa cadeia pela prognose. Logo, a linguagem é controlável segura pela diagnose ou prognose, pois uma ocorrência de falha é controlável segura pela diagnose e a outra ocorrência é controlável segura pela prognose.

A linguagem do exemplo apresentado na Figura 16 não é DP-Controlável Segura, pois a linguagem não satisfaz nenhuma das duas condições apresentadas no Teorema 2.5.6, visto que ao analisarmos a cadeia problemática abf, verificamos que: (a) um dos primeiros estados certos de falha é um mau estado $(9F - B)$, logo ela não é controlável segura pela diagnose; (b) o

primeiro estado incerto do diagnosticador não está associado a apenas ciclos de estados certos de falha, logo a cadeia não é controlável segura pela prognose. Esse exemplo, portanto, pode ser classificado como um dos problemas motivadores dessa tese.

Figura 16 – Exemplo de linguagem não controlável segura.



(a) G (b) G_D

Fonte: Elaborado pelo autor (2023)

2.6 CONTROLE TOLERANTE A FALHAS DE SEDS

A diagnose e a prognose de falhas por si só são relevantes em diversos sistemas. No entanto, um desdobramento importante é a aplicação destas propriedades em controle tolerante a falhas (CTF).

Em um sistema tolerante a falhas, o controlador é responsável por garantir que o sistema opere de acordo com as especificações de controle nominais e continue operando após a ocorrência da falha.

Segundo Fritz e Zhang (2018), existem duas abordagens para o projeto de CTF em SEDs: abordagem ativa e abordagem passiva. Abaixo são apresentadas algumas características comumente presentes nestas topologias.

- A abordagem ativa normalmente utiliza um diagnosticador, que funciona paralelamente ao supervisor, responsável por realizar o chaveamento entre lógicas de controle desenvolvidas especialmente para estabelecer o comportamento adequado ao sistema após a ocorrência de falha; o que caracteriza uma metodologia de controle adaptativo.

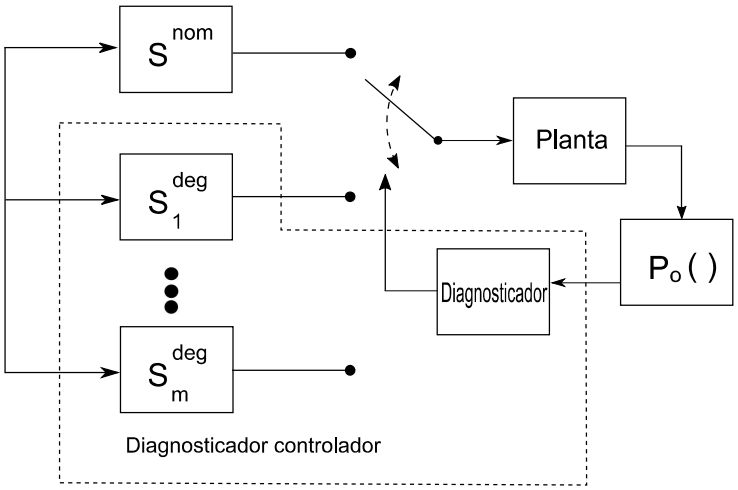
- A abordagem passiva normalmente utiliza técnicas de supervisão sob observação parcial, podendo ser classificada como uma metodologia de controle robusto. Dessa forma, é sintetizado um único supervisor, cujas especificações de controle que o originam foram contempladas de forma a tratar uma eventual ocorrência de falha, sem a necessidade de um agente diagnosticador externo funcionando paralelamente.

Assim como os diferentes modelos de representação de SEDs, as duas abordagens de CTF possuem vantagens e desvantagens. Mas, no escopo dessa tese, será investigada a abordagem ativa.

A Figura 17 apresenta a topologia de Controle Tolerante a Falhas Ativo (CTFA) proposta por Paoli, Sartini e Lafortune (2011). Nessa estrutura, é possível notar que o Diagnosticador é responsável por diagnosticar a ocorrência de falhas por meio da observação dos eventos da Planta. A partir da Diagnose, deve alterar a lógica de controle, de modo a interromper a operação do supervisor nominal (S^{nom}) e passar a usar um dos supervisores degradados (S_1^{deg} a S_m^{deg}) que foram projetados para tratar especificamente de situações pós-falha. O conjunto formado pelo diagnosticador e supervisores degradados é denominado Diagnosticador Controlador.

É importante ressaltar que a estrutura de CTFA só é funcional para um sistema dotado de falhas que atende as condições para alguma das classificações de controlabilidade segura apresentadas na seção anterior, ou seja, a linguagem da planta é controlável segura.

Figura 17 – Exemplo de topologia de controle tolerante a falhas ativo.



Fonte: Modificado de Paoli, Sartini e Lafortune (2011)

2.7 CONSIDERAÇÕES FINAIS

Nesse capítulo, foram apresentados alguns conceitos sobre a representação de SEDs por linguagens e autômatos, operações sobre linguagens, operações sobre autômatos, autômatos estocásticos, SEDs parcialmente observáveis, Teoria de Controle Supervisório, Controle Tolerante a Falhas.

Além disso, foram apresentadas definições e condições necessárias para que uma linguagem L seja diagnosticável; prognosticável; diagnosticável segura; controlável segura pela diagnose na abordagem por linguagem; controlável segura pela prognose na abordagem por linguagem; DP-controlável segura na abordagem por cadeia.

Os conceitos apresentados neste capítulo fornecem uma base contextual para os trabalhos discutidos no estado da arte no Capítulo 3 e para o entendimento da propostas desta tese apresentadas no Capítulo 4.

3 ESTADO DA ARTE

Neste capítulo é apresentado o procedimento utilizado para mapeamento sistemático de literatura, bem como uma análise bibliométrica dos resultados e uma revisão dos trabalhos relacionados à temática desta tese.

3.1 MAPEAMENTO SISTEMÁTICO DE LITERATURA

No mapeamento sistemático de literatura apresentado nesta seção, são buscados trabalhos que abranjam as área de diagnose de falhas, prognose de falhas e controle tolerante a falhas em Sistemas a Eventos Discretos representados por modelos estocásticos. Os conceitos fundamentais e estado da arte relacionados a diagnose de falhas, prognose de falhas e controle tolerante a falhas em Sistemas a Eventos Discretos, representados por modelos não estocásticos foram apresentados nos capítulos anteriores.

Para atingir sucesso na busca por referências, o mapeamento deve ser realizado de forma sistemática para garantir que nenhum trabalho similar fique fora do estudo. Neste trabalho, o mapeamento foi realizado em cinco mecanismos de busca: Engineering Village, IEEExplore, Scopus, Science Direct e Web of Science. O processo foi executado de acordo com os seguintes passos:

1. Determinação de todas as palavras chaves que representam o tema da pesquisa, levando em consideração os sinônimos e a variação em número (plural) de todas as palavras de interesse;

2. Definição da frase de busca a ser utilizada em cada base. Isto é necessário pois os recursos disponíveis em cada base são distintos. Uma boa prática é olhar as dicas de busca (*search tips*) de cada mecanismo;

3. Documentação de todos os descritores, limitadores de busca e a quantidade de resultados obtidos em cada base, com auxílio de uma planilha desenvolvida no *software Microsoft Excel©*;

4. União dos resultados para manutenção de apenas uma versão dos artigos que estão disponíveis em mais de uma base (evitar duplicidade);

5. Leitura dos resumos de todos os documentos para exclusão dos trabalhos não relacionados ao tema da pesquisa.

A Tabela 1 apresenta os dados para realizar as buscas e os resultados obtidos nas cinco bases utilizadas. Nesta, é possível observar que as frases são distintas entre si. Na base Science Direct (SD), o plural é buscado mesmo quando a palavra está dentro do operador de frase exata (" "). Uma característica negativa do mecanismo SD é que no momento não é permitida a utilização de caracteres "curingas", como o asterisco.

Tabela 1 – Parâmetros utilizados e resultados obtidos na busca sistemática. IEEE é a base de busca IEEExplore; SD = Science Direct; WOS = Web of Science; SCP = Scopus; EV = Engineering Village.

Frase	Base	Busca	Resultados	TAK/METADATA	FullText
(likelihood OR stochastic* OR probabilistic*) AND (fail* OR fault*) AND ("discrete event system"OR "discrete event systems")	IEEE	Avançada	126		
	SD	Avançada	81	(likelihood OR stochastic OR stochastical OR probabilistic or probabilistical) AND (fail OR failure OR fault OR faulty)	discrete event system
	WOS	Básica	126	(likelihood OR stochastic* OR probabilistic*) AND (fail* OR fault*)	("discrete event system"OR "discrete event systems")
	SCP	Básica	161	(likelihood OR stochastic* OR probabilistic*) AND (fail* OR fault*) AND ("discrete event system"OR "discrete event systems")	
	EV	Quick	150	(likelihood OR stochastic* OR probabilistic*) AND (fail* OR fault*)	("discrete event system"OR "discrete event systems")

Fonte: Elaborado pelo autor (2023)

Somando o resultado das buscas nas cinco bases, foram localizados 644 documentos. Após a verificação de artigos que aparecem em mais de uma base, restaram 305 documentos. O diagrama de Venn, ilustrado na Figura 18, apresenta a quantidade de documentos que estão presentes individualmente nas bases, bem como as interseções entre os mecanismos. O filtro de conteúdo realizado na etapa de leitura dos resumos restringiu o conjunto de resultados a uma base geral composta por 99 documentos.

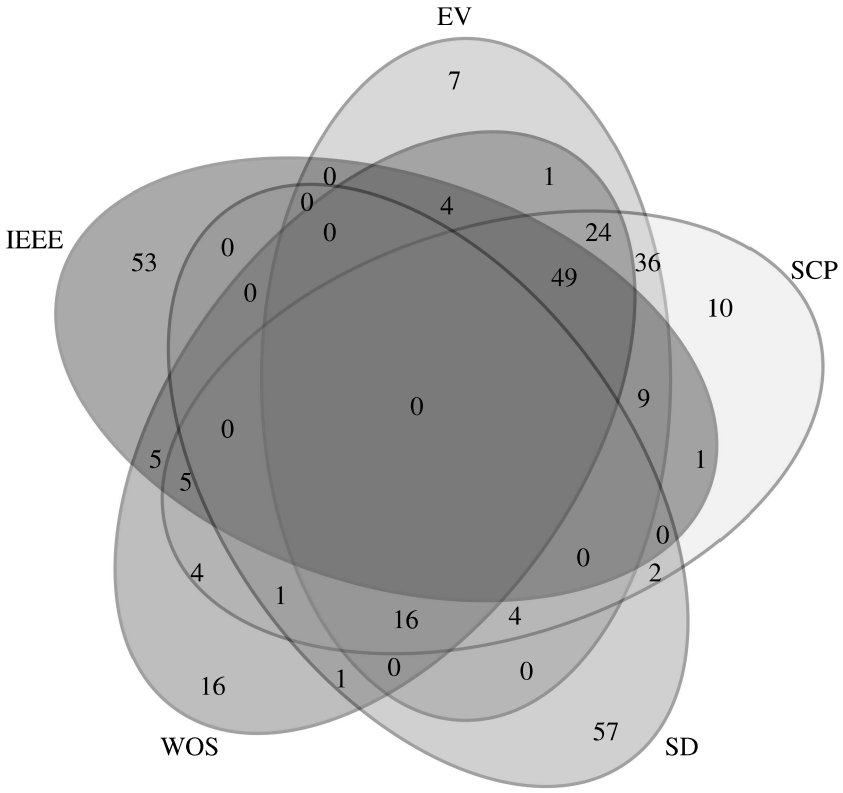
A Figura 19 apresenta a quantidade de publicações por ano no período de 1985 a 2022. É possível observar que nesta década houve um crescimento na quantidade de documentos. O pico de publicações ocorreu entre os anos de 2014 e 2017. A linha na cor laranja na Figura 19 representa uma linha de tendência por regressão linear.

A Figura 20 apresenta uma distribuição dos trabalhos de acordo com o tipo de arquitetura (centralizada, decentralizada e distribuída), de acordo com o objeto de pesquisa (diagnose, prognose ou ambos) e se há ou não proposta de estrutura para controle.

É possível observar na Figura 20 que não há trabalhos que utilizam tanto a diagnose quanto a prognose de falhas para estabelecimento de estrutura de controle em sistemas a eventos discretos modelados por autômatos estocásticos.

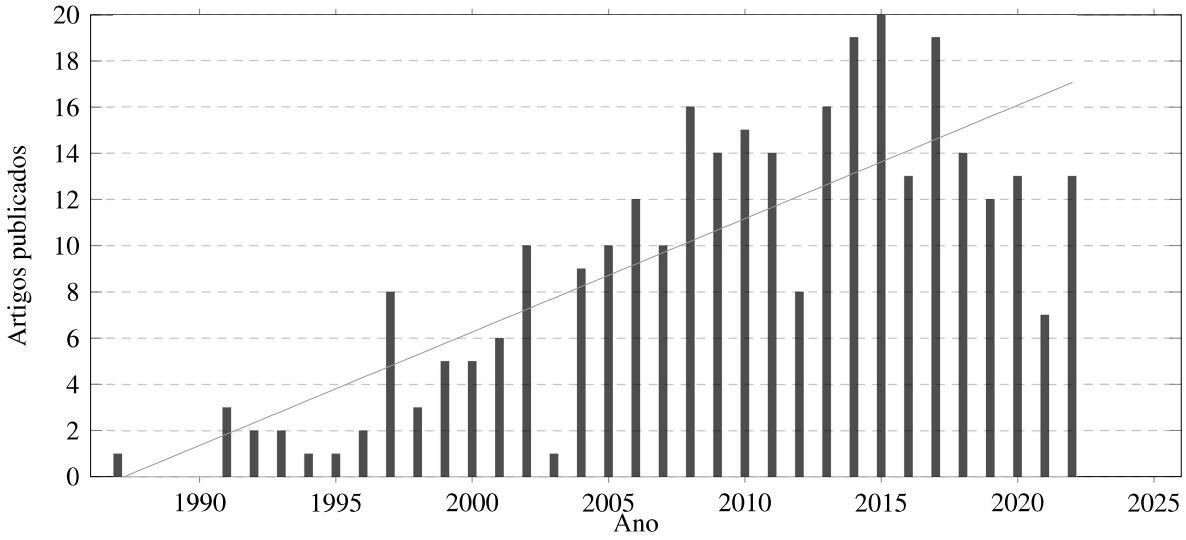
É importante ressaltar que o processo de busca deve ser atualizado periodicamente para rastrear eventuais novos trabalhos. No entanto, a maioria das bases fornece recurso para armazenar a pesquisa e configurar sinalizadores que facilitam esse processo de atualização. Esse

Figura 18 – Diagrama de Venn para avaliação da quantidade de documentos em cada base.



Fonte: Elaborado pelo autor (2023)

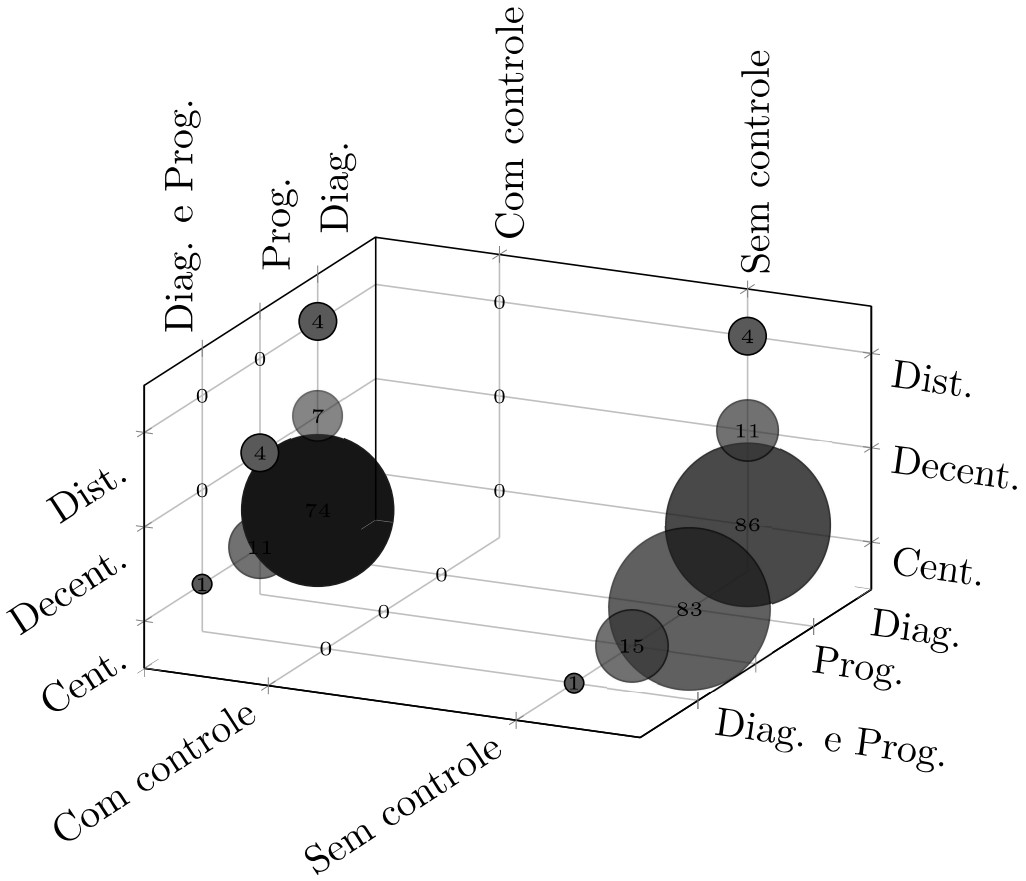
Figura 19 – Classificação dos resultados em relação ao ano de publicação.



Fonte: Elaborado pelo autor (2023)

recurso permite o envio de uma mensagem quando novos documentos forem adicionados à base e satisfaçam os descritores de sua busca. Caso o mecanismo não forneça essa funcionalidade,

Figura 20 – Distribuição quantitativa dos trabalhos pertencentes à base geral.



Fonte: Elaborado pelo autor (2023)

uma opção para simplificar o processo é repetir a busca, comparar a quantidade de resultados e posteriormente aplicar um filtro de data de publicação para encontrar apenas os documentos inseridos após a data de sua última busca.

Na Seção 3.2 são apresentados alguns dos trabalhos que compõem a base geral de documentos. Foi adotada uma ordem de apresentação cronológica dos trabalhos revisados com o propósito de identificar a evolução do estado da arte passo a passo.

3.2 DIAGNOSE, PROGNOSE E CTF EM SEDES

Todos os conceitos relacionados a diagnose, prognose e CTF previamente apresentados com a utilização de ADEF serão referenciados a partir de agora juntamente com a palavras "lógica" ou "logicamente", pois o escopo desta tese e os trabalhos discutidos a seguir serão definidos com base em autômatos estocásticos.

Nas avaliações de diagnose, prognose e controlabilidade lógicas, os resultados obtidos são binários. Ou seja, os sistemas serão diagnosticáveis ou não diagnosticáveis, prognosticáveis ou não prognosticáveis e assim sucessivamente. A utilização de autômatos probabílisticos fornece

uma representação com maior nível de informação relativa à possibilidade de ocorrência de eventos dos sistemas e permite o estabelecimento de limiares percentuais para agir ou não em determinada falha de modo a garantir uma maior segurança ao sistema (WU, 2004).

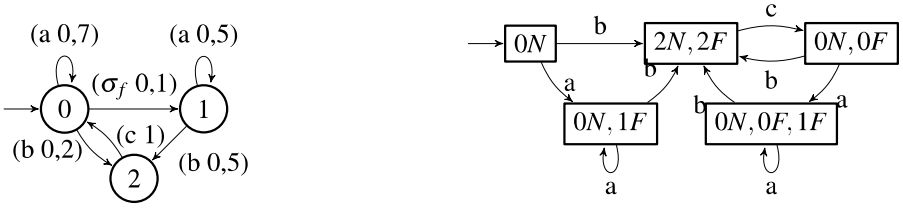
Lunze e Schröder (1999) e Lunze (2000) utilizam autômatos estocásticos em processos para detecção de falhas. Estes trabalhos fornecem uma abordagem de representação de sistemas quantizados, ou seja, sistemas de variáveis contínuas cujos sinais de entrada e saída podem ser medidos apenas com quantizadores. Apesar da natureza contínua, a quantização permite representar estes sistemas na forma de SEDs. Schiller, Schröder e Lunze (2001) apresentam um estudo sobre a avaliação de falhas transientes e propõem um algoritmo para cálculo da probabilidade de diagnose de falha em função de intervalos de tempo para sistemas quantizados.

Barigozzi, Magni e Scattolini (2002) modificam as diretivas usuais de modelagem de subsistemas por meio de autômatos estocásticos utilizando uma tática em que se realiza uma abstração do funcionamento normal do dispositivo, de forma que os eventos e os estados do modelo já são classificados para distinguir o modo de operação normal e os modos de falhas, sem a necessidade de um rotulador ou diagnosticador externo. Além disso, são inseridos no modelo alarmes para auxiliar no processo de diagnose.

Hadjicostis (2002) utilizou autômatos estocásticos para detecção de falhas. Em sua abordagem, a detecção de falhas é obtida analisando como as medições de ocupação de estado obtidas por observação desviam das probabilidades de estado estacionário que são esperadas de um sistema livre de falhas.

Thorsley e Teneketzis (2003,2005), propuseram uma abordagem de diagnosticabilidade estocástica similar a proposta de diagnosticabilidade lógica de (SAMPATH et al., 1995). Nesses trabalhos, são estabelecidos os cálculos para um diagnosticador de falhas estocástico, cujo procedimento de obtenção é o mesmo de Sampath et al. (1995), no entanto a cada transição é associada uma matriz de probabilidade de ordem $m \times n$, onde m é a quantidade de rótulos do estado de saída e n a quantidade de rótulos do estado de chegada. A Figura 21 apresenta um exemplo de autômato estocástico e o diagnosticador estocástico correspondente. A Tabela 2 apresenta as matrizes de probabilidades de cada transição para este exemplo.

Figura 21 – Procedimento de obtenção de um Diagnosticador de falhas para um SEDE.



(a) Autômato G (b) Diagnosticador D_G

Fonte: (THORSLEY; TENEKETZIS, 2005)

onde "O" é o estado de origem, "E" é o evento, "D" é o estado de destino e "M" é a matriz de probabilidade da transição.

Tabela 2 – Matrizes de probabilidades do diagnosticador apresentado na Figura 21.

O	E	D	M
0N	b	2N,2F	$\begin{bmatrix} 0,2 & 0,05 \end{bmatrix}$
0N	a	0N,1F	$\begin{bmatrix} 0,7 & 0,05 \end{bmatrix}$
0N,1F	a	0N,1F	$\begin{bmatrix} 0,7 & 0,05 \\ 0 & 0,5 \end{bmatrix}$
0N,1F	b	2N,2F	$\begin{bmatrix} 0,2 & 0,05 \\ 0 & 0,5 \end{bmatrix}$
2N,2F	c	0N,0F	$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$
0N,0F	b	2N,2F	$\begin{bmatrix} 0,2 & 0,05 \\ 0 & 0,25 \end{bmatrix}$
0N,0F	a	0N,0F,1F	$\begin{bmatrix} 0,7 & 0 & 0,05 \\ 0 & 0,7 & 0,05 \end{bmatrix}$
0N,0F,1F	b	2N,2F	$\begin{bmatrix} 0,2 & 0,05 \\ 0 & 0,25 \\ 0 & 0,5 \end{bmatrix}$
0N,0F,1F	a	0N,0F,1F	$\begin{bmatrix} 0,7 & 0 & 0,05 \\ 0 & 0,7 & 0,05 \\ 0 & 0 & 0,5 \end{bmatrix}$

Fonte: Elaborado pelo autor (2023)

Considerando o diagnosticador da Figura 21 e a observação da cadeia $s_o = aabcaa$, podemos obter a probabilidade de acesso a um estado de falha. Neste contexto, $\phi_{un}(s_o)$ é o vetor de probabilidades não normalizado de alcance a cada rótulo do estado do diagnosticador atingido após a observação da cadeia s_o e $\phi(s_o)$ é o vetor de probabilidades normalizado. Eles são calculados conforme o procedimento a seguir.

$$\phi_{un}(s_o) = \begin{bmatrix} 1 \end{bmatrix} \begin{bmatrix} 0,7 & 0,05 \end{bmatrix} \begin{bmatrix} 0,7 & 0,05 \\ 0 & 0,5 \end{bmatrix} \begin{bmatrix} 0,2 & 0,05 \\ 0 & 0,5 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 0,7 & 0 & 0,05 \\ 0 & 0,7 & 0,05 \end{bmatrix} \begin{bmatrix} 0,7 & 0 & 0,05 \\ 0 & 0,7 & 0,05 \\ 0 & 0 & 0,5 \end{bmatrix}$$

$$\phi_{un}(s_o) = \begin{bmatrix} 0,04802 & 0,026705 & 0,00915 \end{bmatrix}$$

$$\phi(s_o) = \begin{bmatrix} 0,5725 & 0,3184 & 0,1091 \end{bmatrix}$$

O estado alcançado no diagnosticador é o (0N, 0F, 1F)

$$Pr(Fs_0) = Pr(0Fs_o) + Pr(1Fs_o) = 0,4275$$

Além da concepção do diagnosticador estocástico, Thorsley e Teneketzis (2005) apresentam as definições de duas propriedades de diagnosticabilidade estocástica que são avaliadas no autômato que representa o sistema: A-diagnosticabilidade (ver Definição 3.2.1) e AA-diagnosticabilidade (ver Definição 3.2.2). Ambas propriedades são mais fracas que a diagnosticabilidade lógica, ou seja, as condições necessárias e suficientes para atender estas propriedades são menos restritivas do que as condições de diagnosticabilidade lógica.

O conceito de componentes recorrentes é utilizado nas condições para A-Diagnosticabilidade, AA-Diagnosticabilidade e Diagnosticabilidade Segura para SEDEs. Um estado é denomi-

nado componente recorrente quando a probabilidade deste estado ser revisitado é igual a 100%. Para classificar se um componente é recorrente ou transiente, utiliza-se a Matriz de Markov associada ao diagnosticador. Nesta matriz, são apresentadas todas as probabilidades de acesso aos demais componentes do diagnosticador a partir de cada um destes componentes. A notação ρ_{xy} indica a probabilidade de, a partir de um estado x, acessar um estado y. Considerando um estado x, tal que $\rho_{xx} = 1$, este estado é chamado de recorrente. Por outro lado, se para um estado x, tem-se $\rho_{xx} < 1$, este estado é chamado transiente (THORSLEY; TENEKETZIS, 2005).

Definição 3.2.1 (A - Diagnosticabilidade)**.** *Uma linguagem prefixo-fechada L que é viva é F_i-A-diagnosticável em relação à projeção P_o e função de transição probabilística p se:*

$$(\forall \beta > 0)(\exists N \in \mathbb{N})(\forall s \in \Psi_L(f) \wedge n \geq N)$$
$$\{Prob(t : D(st) = 0 | t \in L/s \wedge ||t|| = n) < \beta\}$$

em que a função da condição de diagnosticabilidade é:

$$D(st) = \begin{cases} 1, & se \ \ \omega \in P_o^{-1}[P_o(st)] \cap L \Rightarrow f \in \omega \\ 0, & \text{caso contrário} \end{cases}$$

Teorema 3.2.1 (Condição necessária e suficiente para A-Diagnosticabilidade)**.** *Uma linguagem L gerada por um autômato estocástico G é F_i-A-diagnosticável, se e somente se, cada elemento lógico de seu diagnosticador D contendo um componente recorrente que tenha o rótulo de falha F seja certo de falha.*

Definição 3.2.2 (AA - Diagnosticabilidade)**.** *Uma linguagem prefixo-fechada L que é viva é F_i-AA-diagnosticável em relação à projeção P_o e função de transição probabilística p se:*

$$(\forall \beta > 0 \wedge \forall \alpha < 1)(\exists N \in \mathbb{N})(\forall s \in \Psi_L(f) \wedge n \geq N)$$
$$\{Prob(t : D_\alpha(st) = 0 | t \in L/s \wedge ||t|| = n) < \beta\}$$

em que a função da condição de diagnosticabilidade é:

$$D_\alpha(st) = \begin{cases} 1, & se \ \ Prob(\omega : f \in \omega | \omega \in P_o^{-1}[P_o(st)] \cap L > \alpha) \\ 0, & \text{caso contrário} \end{cases}$$

Teorema 3.2.2 (Condição suficiente para AA-Diagnosticabilidade)**.** *Uma linguagem L gerada por um autômato estocástico G é F_i-AA-diagnosticável se para cada elemento lógico de seu diagnosticador D obtido a partir de G, o conjunto de componentes recorrentes seja certo de falha.*

Tabela 3 – Cadeias que geram a observação - Exemplo da Figura 21.

Observação $\Rightarrow$	$s_o = aabcaa$	prob $P^{-1}(s_o)$	Σprob$P^{-1}(s_o)$
Estado $\Rightarrow$	0N,0F,1F		
Rótulos $\Downarrow$	Cadeias que geram a observação $\Downarrow$		
0N	$aabcaa$	$0,04802$	$0,04802$
0F	$aa\sigma_F bcaa$	$0,012005$	$0,026705$
	$a\sigma_F abcaa$	$0,008575$	
	$\sigma_F aabcaa$	$0,006125$	
1F	$aabca\sigma_F a$	$0,00343$	$0,00915$
	$aa\sigma_F bca\sigma_F a$	$0,0008575$	
	$a\sigma_F abca\sigma_F a$	$0,0006125$	
	$\sigma_F aabca\sigma_F a$	$0,0004375$	
	$aabc\sigma_F aa$	$0,00245$	
	$aa\sigma_F bc\sigma_F aa$	$0,0006125$	
	$a\sigma_F abc\sigma_F aa$	$0,0004375$	
	$\sigma_F aabc\sigma_F aa$	$0,0003125$	

Fonte: Elaborado pelo autor (2023)

Wang, Chattopadhyay e Ray (2004) apresentam a p-diagnosticabilidade. Nesse trabalho, os autores calculam as probabilidades de atingir cada rótulo do diagnosticador após a observação de determinada cadeia s_o. Este procedimento é feito avaliando no autômato estocástico do sistema quais cadeias geram aquela observação e fazendo um cálculo de normalização. Após isso, se estabelece uma matriz de probabilidade de cada falha ter ocorrido $\Pi^f(q_d)$, onde q_d é o estado correspondente do diagnosticador após a observação de so. A matriz tem ordem $m \times n$, onde m é o número de estados do autômato estocástico e n a quantidade de eventos de falhas.

Aplicando o procedimento proposto por Wang, Chattopadhyay e Ray (2004) no exemplo da Figura 21, podemos verificar as cadeias que geram a observação $s_o = aabcaaa$ na Tabela 3 e chegamos ao seguinte resultado:

$$Pr(Fs_0) = \frac{0,026705 + 0,00915}{0,04802 + 0,026705 + 0,00915} = 42,75\%$$

É possível observar que apesar de adotarem abordagens bem distintas, tanto para o cálculo quanto para a apresentação dos valores obtidos Thorsley e Teneketzis (2005) e Wang, Chattopadhyay e Ray (2004) chegam aos mesmos resultados.

Athanasopoulou e Hadjicostis (2004) focam no cálculo da probabilidade de *aliasing* (distorção ou recobrimento) do resultado de diagnóstico utilizando um diagnosticador externo e avaliando três diferentes cenários de sincronização entre o autômato da planta e o diagnosticador.

Thorsley e Teneketzis (2006) avaliam a diagnosticabilidade de sistemas cíclicos utilizando aquisição ativa de informações e determinando o custo de observação. A abordagem é formalizada

para os casos lógicos e estocásticos.

Athanasopoulou, Lingxi Li e Hadjicostis (2006) consideram como falhas erros na observação das cadeias, tais como a remoção de um evento que ocorreu ou a inserção de um evento que não ocorreu proporcionando uma transmissão de cadeia distinta da cadeia realizada. A análise ocorre com a elaboração de dois autômatos estocásticos para representação de um sistema, um modelo livre de falha e um com falha. A ocorrência de falha é determinada por meio da comparação das probabilidades da cadeia observada nos dois modelos.

Zemouri e Faure (2006) avaliam apenas falhas que promovem uma alteração no intervalo de tempo entre eventos, utilizando autômatos estocásticos temporizados. Neste caso, o modelo convencional de intervalo com limites inferior e superior para o tempo de ocorrência do evento é substituída por uma curva de distribuição normal da probabilidade de ocorrência do evento em função do tempo. Esta prática, segundo o autor, serve para reduzir a quantidade de alarmes falsos fornecidos pelo diagnosticador.

Whiteford e Kwong (2007) utilizam uma abordagem que envolve a observação das saídas do sistema e uma técnica utilizada em problemas de otimização. Neste trabalho, o algoritmo de diagnose calcula de forma iterativa (até garantir que o limiar de confiança estabelecido pelo usuário) as probabilidades de falhas para sistemas representados por modelos incompletos.

Deepa, Ranjan e Manohar (2007) adotam uma estrutura probabilística para determinar através de uma análise matemática o melhor momento de sincronização do diagnosticador externo com o propósito de reduzir a probabilidade de *aliasing*, ou seja, a probabilidade de que o diagnosticador incorretamente declare que o sistema está livre de falhas.

Nouioua e Dague (2008) determinam um grau de não diagnosticabilidade para sistemas que não são logicamente diagnosticáveis; esse grau é determinado a partir do cálculo das probabilidades das cadeias cuja a ocorrência de falha não é lógicamente diagnosticável.

Thorsley, Yoo e Garcia (2008) propõem uma avaliação de sistemas que contam com eventos cuja observação é não confiável. Desta forma, ele propõe uma variação das definições de diagnosticabilidade estocásticas propostas em (THORSLEY; TENEKETZIS, 2003). São estabelecidas as *uA-diagnosability* e *uAA-diagnosability* que contemplam eventos que possuem probabilidades de perda de detecção ou de erro de classificação.

Biswas et al. (2008) apresentam uma metodologia de cálculo de diagnosticador e verificação de diagnosticabilidade para sistemas discretos híbridos temporizados, utilizando no processo o conceito de transições justas e não justas. No âmbito de autômatos temporizados, transições justas são aquelas que ficam habilitadas por um intervalo de tempo finito; transições não justas são aquelas que ficam habilitadas por tempo infinito. Além da proposição de uma nova condição de diagnosticabilidade e seus requisitos necessários e suficientes, é feito um comparativo entre *fair DTHS diagnosability* e *A-diagnosability*.

De forma análoga ao proposto por Athanasopoulou, Lingxi Li, Hadjicostis (2006) , Athanasopoulou e Hadjicostis (2008) utilizam dois modelos para representação do sistema (um modelo com falhas e o outro livre de falhas. O diagnosticador, por meio da observação e da

comparação das probabilidades das cadeias em cada modelo, determina qual modelo é mais provável que forneça aquela observação. Além disso, é estabelecido um procedimento de cálculo para a probabilidade do diagnosticador fornecer um resultado incorreto.

Liu e Qiu (2008) apresentam uma noção de diagnosticabilidade segura para SEDEs a partir da suposição que L(G) é F_i - *A-diagnosable* (THORSLEY; TENEKETZIS, 2005). Além disso, apresentam as condições necessárias e suficientes para que a definição seja atendida. A Definição 3.2.3 apresenta a noção de diagnosticabilidade segura para SEDEs e o Teorema 3.2.3 apresenta as condições necessárias e suficientes.

Definição 3.2.3 (Diagnosticabilidade Segura para SEDEs)**.** *Uma linguagem L gerada por um autômato estocástico* $G = (X, \Sigma, p, x_{G0})$ *é diagnosticável seguro se:*

$$(\forall \beta > 0)(\exists N \in \mathbb{N})(\forall s \in \Psi_L(f))(\forall t \in L/s \wedge ||t|| \geq N)(\exists v \in \bar{t})(\bar{v} \cap \mathscr{K}_f = \emptyset)$$

e ao menos uma das seguintes condições é atendida:
1) $D(sv) = 1$.
2) para qualquer $t \in L/s$ *que* $||t|| = N$*, temos:*

$$Prob(t : D(sv) = 0) < \beta$$

em que a função de diagnosticabilidade é:

$$D(sv) = \begin{cases} 1, & se \ \ \omega \in P_o^{-1}[P_o(st)] \cap L \Rightarrow f \in \omega \\ 0, & \text{caso contrário} \end{cases}$$

Teorema 3.2.3 (Condições para Diagnosticabilidade Segura para SEDEs)**.** *Uma linguagem L gerada por um autômato estocástico* $G = (X, \Sigma, p, x_0)$ *é diagnosticável segura em relação ao evento de falha f se e somente se o diagnosticador seguro* $D = (X_D, \Sigma_o, \delta_D, x_{D0})$ *satisfaz as seguintes condições:*
1) Não existe estado em D que é incerto de falha e possui uma componente recorrente com o rótulo de falha.
2) Não existem três estados em D com as seguintes características: estado incerto de falha x_{D1}*, estado* x_{D2} *com uma componente que é rótulo de mau estado e um estado* x_{D3} *com uma componente recorrente de mau estado, tal que* $\delta_D(x_{D1}, \sigma) = x_{D2}$ *e* $\delta_D(x_{D2}, \alpha) = x_{D3}$*, em que* $\sigma \in \Sigma_o$ *e* $\alpha \in \Sigma_o^*$.

Chang et al. (2013) propõem um modelo de prognosticabilidade estocástica denominado *AAS-predictability* que consiste na utilização das probabilidades de ocorrência dos eventos fornecidas pelo autômato estocástico que modela o sistema para determinar se a linguagem é *asymptotically almost sure*, ou seja, a prognose é quase certa ao analisarmos cadeias com comprimento n tendendo a infinito.

Chen e Kumar (2014; 2015) apresentam a S_m*-prognosability*, que consiste numa classificação de prognosticabilidade estocástica que determirna se o sistema é prognosticável ao analisar

m passos anteriores a ocorrência da falha. A S_m-*prognosability* é avaliada em um autômato de teste T construído a partir da planta refinada G_R, tal que G_R é obtida a partir da planta G e da especificação livre de falha R. Além disso, a S_m-*prognosability* é formalizada para atender taxas de alarme falso P^{fa} e de perda de detecção P^{md}.

Bertrand, Haddad e Lefaucheux (2014) propõem classificações de diagnosticabilidade em níveis; analisam a complexidade computacional do problema de avaliação da diagnosticabilidade e prognosticabilidade. Por fim, propõem o conceito de *prediagnosability* que avalia a complexidade de forma conjunta dos problemas que envolvem diagnose e prognose.

Lian e Shu (2016) apresentam uma abordagem para cálculo das probabilidades de prognose de falha a partir da observação de eventos prévios a falhas. A utilização da observação de eventos é componente da estimativa de probabilidade do estado atual e serve de suporte para o cálculo da probabilidade de ocorrência futura de falha. São fornecidos algoritmos para os cálculos das probabilidades de prognose.

Nouioua, Dague e Ye (2017) estabelecem um procedimento de síntese de um autômato demoninado *lightestimator*, que é obtido a partir de um diagnosticador simplificado resultante do diagnosticador convencional conforme apresentado em (SAMPATH et al., 1995; THORSLEY; TENEKETZIS, 2003). Nesse trabalho, os autores propõem o cálculo de um grau de prognosticabilidade, estabelecendo os valores de probabilidade para cada estado: a) falha ocorrer e ser prognosticável; b) falha ocorrer e não ser prognosticável; c) falha não ocorrer.

Calder e Sevegnani (2019) desenvolveram uma aplicação para avaliação de disponibilidade de serviços, prognose de falhas de componentes, previsão de custos de manutenção. A estrutura é baseada nos modelos de cadeias markovianas de tempo contínuo e de lógica temporal estocástica.

Liu e Yang (2018) e Liu et al. (2020) apresentam uma abordagem para determinar se um sistema tem diagnosticabilidade estocástica segura, utilizando autômatos verificadores.

A revisão de literatura foi focada em trabalhos com abordagens centralizadas. Para abordagens descentralizadas de diagnose consulte (NEIDIG; LUNZE, 2005; LIU et al., 2008; TAKAI; USHIO, 2010); diagnose distribuída (GENG; OUYANG; ZHAO, 2017); prognose descentralizada (LIU, 2017).

3.3 CONSIDERAÇÕES FINAIS

A avaliação do estado da arte indica um cenário onde não existem trabalhos que tratam sobre controlabilidade segura em sistemas a eventos discretos modelados por autômatos estocásticos utilizando diagnose e prognose de falhas, seja em uma abordagem *offline* para verificação se a linguagem atende as condições da propriedade ou seja em uma estrutura de controle tolerante a falhas a fim de fornecer informações para atuação numa estrutura de controle tolerante a falhas a fim de garantir controlabilidade segura do sistema.

4 CONTRIBUIÇÕES AO TEMA DE CONTROLABILIDADE SEGURA EM SEDE

Neste capítulo são apresentadas as contribuições desta tese, as quais estão relacionadas à propriedade de controlabilidade segura em SEDs modelados por autômatos estocásticos. É proposto o Diagnosticador Estocástico com Saídas (DECS). O DECS é um autômato com saídas (máquina de Moore), no qual as probabilidades de diagnose, prognose e de ocorrência futura de cadeia proibida são as saídas apresentadas em cada estado do diagnosticador.

São apresentadas duas abordagens distintas para o cálculo do DECS, as quais são denominadas de Diagnosticador Estocástico com Probabilidades Estáticas (DEPE) e Diagnosticador Estocástico com Probabilidades Dinâmicas (DEPD). São introduzidas as propriedades de u-diagnosticabilidade, u-diagnosticabilidade segura, u-prognosticabilidade, controlabilidade segura pela u-diagnose, controlabilidade segura pela u-prognose e controlabilidade segura pelo coeficiente de anormalidade. São apresentadas as condições necessárias e suficientes para que um SED seja u-diagnosticável seguro, controlável seguro pela u-diagnose e controlável seguro pela u-prognose. Tais condições são verificadas com a utilização do Diagnosticador Estocástico com Probabilidades Estáticas. Por outro lado, o Diagnosticador Estocástico com Probabilidades Dinâmicas é utilizado em tempo de execução, com atualização das probabilidades de maneira dinâmica, de modo a fornecer informações para atuação numa estrutura de controle tolerante a falhas a fim de garantir controlabilidade segura do sistema.

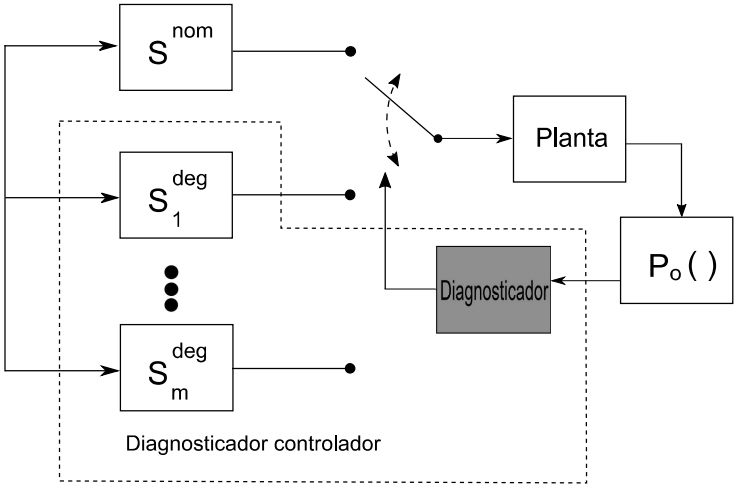
A Figura 22 retoma a topologia de controle tolerante a falhas proposta por Paoli, Sartini e Lafortune (2011), apresentada na Figura 17 no Capítulo 2. Nessa figura, o elemento Diagnosticador recebe destaque. Em Paoli, Sartini e Lafortune (2011), o autômato diagnosticador está relacionado apenas à diagnose como parâmetro de análise para controlabilidade segura. Watanabe et al. (2022) estendem o conceito de controlabilidade segura ao utilizar de forma conjunta diagnose e prognose de falhas como parâmetros na análise de controlabilidade segura. Nesta tese, a concepção do DECS e das demais propriedades e conceitos são direcionadas a aumentar a gama de informações disponíveis no elemento diagnosticador, utilizando diagnose e prognose estocásticas.

A utilização de uma abordagem estocástica para análises de diagnose e prognose de falhas permite que as condições para a controlabilidade segura lógica sejam relaxadas, de forma que um SED que não apresenta controlabilidade segura nos termos apresentados por Watanabe et al. (2022) possa ser controlável seguro por algum dos mecanismos de controlabilidade segura introduzidos nesta tese.

4.1 DIAGNOSTICADOR ESTOCÁSTICO COM SAÍDAS: ABORDAGEM COM PROBABILIDADES ESTÁTICAS

O modelo para representação de estados do DEPE é apresentado na Figura 23a, na qual o campo 1 é o local para os rótulos do estado do diagnosticador, o campo 2 contém a probabilidade de uma falha já ter ocorrido (diagnose estocástica) ao se alcançar este estado do diagnosticador,

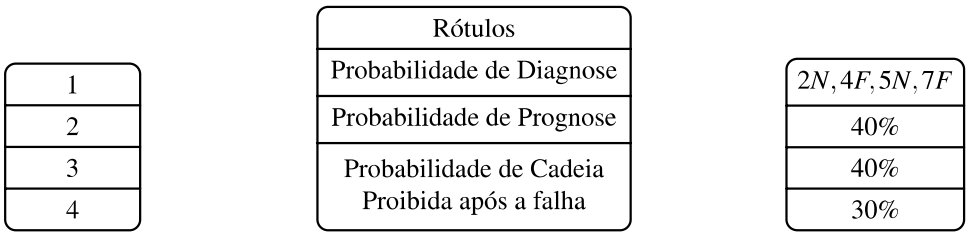
Figura 22 – Topologia de controle tolerante a falhas ativo.



Fonte: Modificado de Paoli, Sartini e Lafortune (2011)

o campo 3 contém a probabilidade de a falha ocorrer no futuro (prognose estocástica) a partir deste estado do diagnosticador e o campo 4 contempla a probabilidade de uma cadeia proibida ocorrer após a falha a partir do estado atual.

Figura 23 – Representação proposta para os estados do Diagnosticador Estocástico com Saídas.



(a) Modelo (b) Composição (c) Exemplo

Fonte: Elaborado pelo autor (2023)

A Figura 23c ilustra um exemplo de estado do DEPE, no qual é possível observar que no campo 2 apresenta-se uma probabilidade de 40% da falha ter acontecido, o que corresponde à soma das probabilidades de estar nos rótulos $4F$ e $7F$, e uma probabilidade ponderada de 40% da falha ocorrer no futuro a partir dos estados relacionados aos rótulos $2N$ e $5N$. Por fim, há uma probabilidade ponderada de 30% de ocorrer uma cadeia proibida após a falha. Essas probabilidades exibidas são calculadas pela soma e/ou cálculos de ponderação a partir de outros valores de probabilidades. A Tabela 4 apresenta os valores utilizados para obter as probabilidades exibidas nesse exemplo de estado (Figura 23c).

A seguir, é apresentado um memorial de cálculo para mostrar como são obtidas as probabilidades exibidas no estado $(2N, 4F, 5N, 7F)$ utilizando as probabilidades da Tabela 4.
Probabilidade (Campo 2) = $15\% + 25\% = 40\%$

Tabela 4 – Probabilidades utilizadas no cálculo do exemplo de estado apresentado na Figura 23c.

	2N	4F	5N	7F
Probabilidade de ter atingido o rótulo	40%	15%	20%	25%
Probabilidade futura de falha a partir do rótulo	60%	0%	80%	0%
Probabilidade futura de cadeia proibida após a falha a partir do rótulo	0%	60%	30%	60%

Fonte: Elaborado pelo autor (2023)

Probabilidade (Campo 3) = $(40\%) \cdot (60\%) + (20\%) \cdot (80\%) = 40\%$

Probabilidade (Campo 4) = $(15\%) \cdot (60\%) + (20\%) \cdot (30\%) + (25\%) \cdot (60\%) = 30\%$

A Subseção 4.1.1 é destinada à apresentação das notações e definições necessárias para a formalização dos métodos e elaboração dos algoritmos para cálculo das probabilidades de: a) atingir cada rótulo do estado do diagnosticador; b) ocorrência futura de falha a partir de cada rótulo de todos os estados do diagnosticador; c) ocorrência futura de evento ou cadeia proibida pós falha a partir de cada rótulo de todos os estados do diagnosticador.

4.1.1 Formalização de métodos

Sejam os autômatos de um SEDE $G = (X, \Sigma, p, x_0)$ e do diagnosticador $D = (X_D, \Sigma_o, \delta_D, x_{D0})$. As seguintes notações são importantes para a formalização dos métodos adotados nesta tese: $|x_D|$ representa a quantidade de rótulos do estado $x_D \in X_D$; $x_D(i)\,[i = 1, 2, ..., |x_D|]$ é utilizado para indicar o i-ésimo rótulo do estado $x_D \in X_D$ do diagnosticador; $R(x_D(i))$ indica se o rótulo $x_D(i)$ é um rótulo normal "N" ou um rótulo de falha "F"; $E(x_D(i))$ é utilizado para indicar o estado $x \in X$ equivalente ao rótulo $x_D(i)$; $CCD(x_D)$ representa o conjunto de cadeias do diagnosticador que levam do estado inicial x_{D0} ao estado x_D, ou seja, $CCD(x_D) := \{s_o \in L(D) : \hat{\delta_D}(x_{D0}, s_o) = x_D\}$; $CCG(x_D(i))$ representa o conjunto de cadeias que chegam ao estado da planta equivalente ao rótulo $x_D(i)$ do estado x_D do diagnosticador, definido por $CCG(x_D(i)) := \{s \in (P_o^{-1}(CCD(x_D)) \cap L(G)) : \hat{\delta}(x_0, s) = E(x_D(i))\}$.

A operação $SC(L)$ retorna um conjunto que contém todas as subcadeias da linguagem L, ou seja, $SC(L) := \{t \in \Sigma^* : \exists s = utv \in L\}$. É importante ressaltar que u e v podem corresponder à cadeia vazia ε, e que nesse caso s é uma subcadeia de s; por exemplo, supondo $L = \{a, abc, abbb\}$ temos $SC(L) = \{\varepsilon, a, b, c, ab, bb, bc, abc, abb, bbb, abbb\}$.

Seja $L(G, x)$ o conjunto de todas as cadeias em G que são iniciadas a partir do estado $x \in X$, formalmente definido como: $L(G, x) := \{\omega \in \Sigma^* : \hat{\delta}(x, \omega) \in X\}$. O cálculo da probabilidade de ocorrência de uma cadeia $s \in L(G, x)$, representado por $Prob(s, x)$, é realizado pelo produto da probabilidade de cada transição que compõe a cadeia s. Seja $s = \sigma_1\sigma_2...\sigma_n \in \Sigma^*$, com $\delta(x_i, \sigma_i) = x_{i+1}$ para $i = 1, 2, ..., n$, temos:

$$Prob(s,x_1) = p(x_1,\sigma_1)\cdot p(x_2,\sigma_2)\cdot \ldots \cdot p(x_n,\sigma_n) = \prod_{i=1}^{n} p(x_i,\sigma_i) \quad (1)$$

O procedimento de cálculo exibido a seguir para o campo 2 é denominado Abordagem *Offline* para Cálculo de Diagnose. Nesse campo, é exibida a probabilidade de estar em um rótulo de falha. Se o estado é normal (o estado possui apenas rótulos N), a probabilidade de diagnose é 0%. Se o estado é certo de falha (o estado possui apenas rótulos F), a probabilidade de diagnose é de 100%, sendo assim, não é necessário fazer cálculo. O cálculo deve ser feito para determinar a probabilidade de diagnose em estados incertos.

Nesse campo, pode-se ter um valor ou uma faixa de valores, caso o estado possa ser atingido por cadeias que contêm ciclos. Dessa forma, o primeiro valor é obtido ao considerar as ocorrências das cadeias que levam ao estado sem execuções dos ciclos ($n = 0$), enquanto o segundo valor considera um grande número de ocorrências dos ciclos ($n \to \infty$) nas cadeias que levam ao estado.

Ao considerarmos a observação de uma cadeia s_o, o cálculo da soma das probabilidades das cadeias que geram a observação s_o no diagnosticador, e que atingem o estado corresponde no autômato da planta, resulta em um valor não normalizado. A probabilidade não normalizada de estar no rótulo $x_D(i)$ do estado x_D é representada por $PD_{nn}(x_D(i))$ e obtida conforme segue:

$$PD_{nn}(x_D(i)) = \sum_{s \in CCG(x_D(i))} Prob(s,x_0) \quad (2)$$

A probabilidade normalizada de estar no rótulo $x_D(i)$ do estado x_D é representada por $PD(x_D(i))$, sendo obtida pela razão da probabilidade não normalizada do rótulo pela soma das probabilidades não normalizadas de todos os rótulos contidos no estado x_D:

$$PD(x_D(i)) = \frac{PD_{nn}(x_D(i))}{\sum_{j=1}^{|x_D|} PD_{nn}(x_D(j))} \quad (3)$$

Após a obtenção das probabilidades normalizadas de estar em cada um dos rótulos do estado x_D, agrupamos esses valores em um vetor $\Omega(x_D)$ conforme a Equação (4):

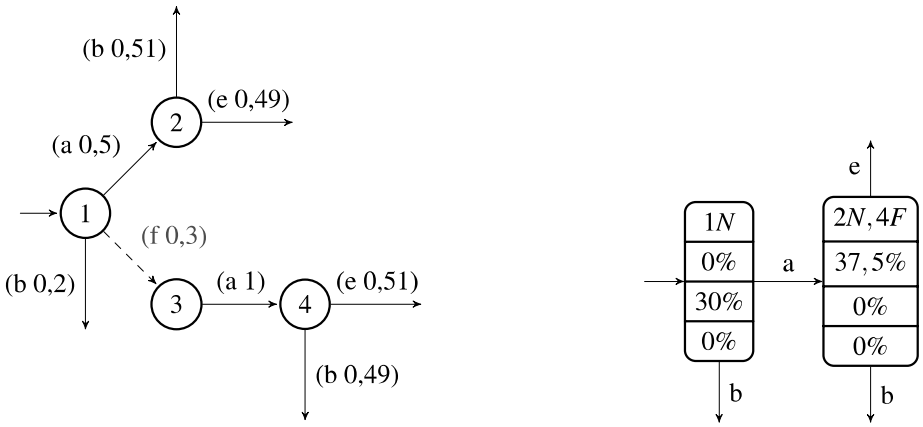
$$\Omega(x_D) = [PD(x_D(1))...PD(x_D(|x_D|))] \quad (4)$$

A soma das probabilidades normalizadas de estar em rótulos de falha para um estado x_D é representada por $\Omega_F(x_D)$ e calculada conforme segue:

$$\Omega_F(x_D) = \sum_{i=1}^{|x_D|} PD(x_D(i)) \qquad \text{tal que } R(x_D(i)) = "F" \quad (5)$$

O valor obtido (ou faixa de valores, se houver ciclos) para $\Omega_F(x_D)$ é apresentado no campo 2 do modelo de estado do DEPE. O autômato apresentado na Figura 24 é utilizado para

Figura 24 – Exemplo para ilustração do procedimento de cálculo do campo 2.



(a) Planta (b) Diagnosticador

Fonte: Elaborado pelo autor (2023)

exemplificar o cálculo da probabilidade de diagnose. O memorial de cálculo para a probabilidade de diagnose no estado $(2N,4F)$ do diagnosticador da Figura 24 é exibido a seguir.

$x_D = (2N,4F)$
$CCD(2N,4F) = \{a\}$
$CCG(2N) = \{a\}$
$CCG(4F) = \{fa\}$

$$PD(2N) = \frac{Prob(a,1)}{Prob(a,1)+prob(fa,1)} = \frac{0,5}{0,5+0,3} = 62,5\%$$

$$PD(4F) = \frac{Prob(fa,1)}{Prob(a,1)+prob(fa,1)} = \frac{0,3}{0,5+0,3} = 37,5\%$$

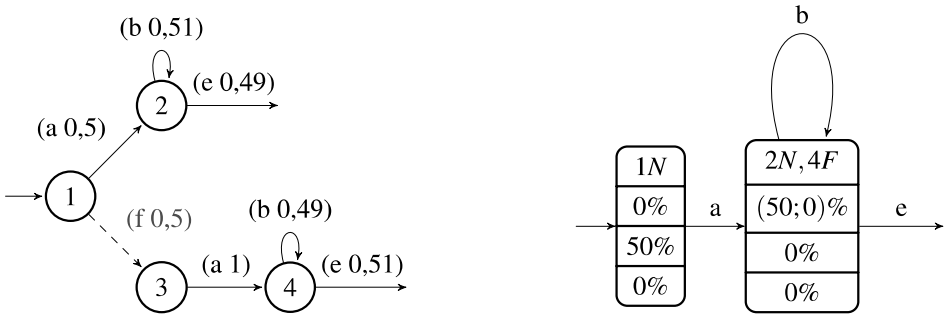
$\Omega(x_D) = [0,625 \;\; 0,375]$

$\Omega_F(x_D) = 37,5\%$

O autômato e o diagnosticador apresentados na Figura 25 são utilizados para ilustrar como é feito o cálculo da faixa de probabilidades de estar em cada rótulo do estado de um diagnosticador em um estado que pode ser atingido por ciclos de eventos. O memorial de cálculo para a probabilidade de diagnose no estado $(2N,4F)$ do diagnosticador da Figura 25 é exibido a seguir.

$x_D = (2N,4F)$
$CCD(2N,4F) = ab^*$
$CCG(2N) = ab^*$
$CCG(4F) = fab^*$

Figura 25 – Exemplo para ilustrar o procedimento de cálculo da probabilidade de diagnose quando existem ciclos.



(a) Planta (b) Diagnosticador

Fonte: Elaborado pelo autor (2023)

$$PD((2N)(0)) = \frac{Prob(a,1)}{Prob(a,1)+prob(fa,1)} = \frac{0{,}5}{0{,}5+0{,}5\cdot 1} = 50\%$$
$$PD((2N)(\infty)) = \frac{Prob(ab^n,1)}{Prob(ab^n,1)+prob(fab^n,1)} = \frac{0{,}5\cdot(0{,}51^n)}{0{,}5\cdot(0{,}51^n)+0{,}5\cdot 1\cdot(0{,}49^n)} = 100\%$$

$$PD((4F)(0)) = \frac{Prob(fa,1)}{Prob(a,1)+prob(fa,1)} = \frac{0{,}5\cdot 1}{0{,}5+0{,}5\cdot 1} = 50\%$$
$$PD((4F)(\infty)) = \frac{Prob(fab^n,1)}{Prob(ab^n,1)+prob(fab^n,1)} = \frac{0{,}5\cdot 1\cdot(0{,}49^n)}{0{,}5\cdot(0{,}51^n)+0{,}5\cdot 1\cdot(0{,}49^n)} = 0\%$$

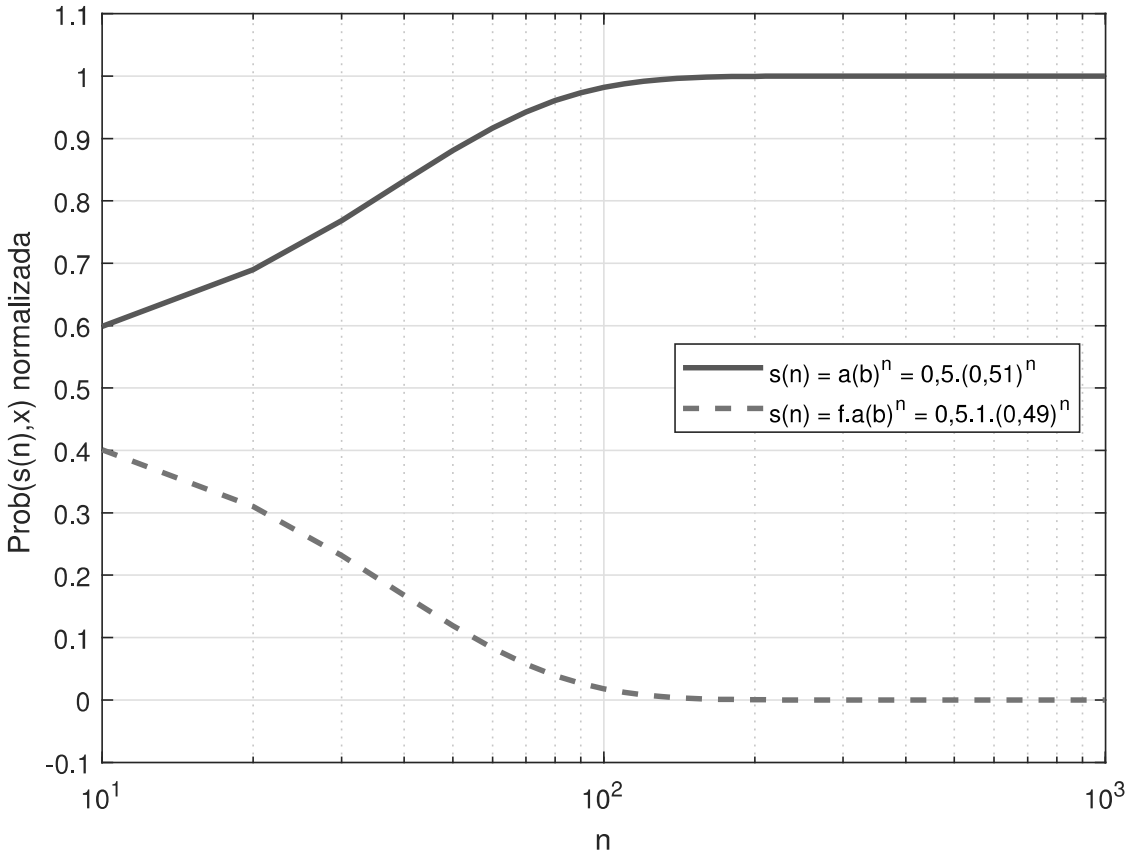
$$\Omega(2N,4F) = [(0,5;1)\ \ (0,5;0)]$$

$$\Omega_F(x_D) = (50;0)\%$$

Após a observação do evento a, o estado lógico alcançado no diagnosticador da Figura 25 é o (2N,4F). Devido às probabilidades de ocorrência das cadeias a e fa, a probabilidade inicial de estar em cada um dos dois rótulos é igual a 50%. Nesse mesmo estado, podemos observar a presença de um auto-laço com o evento b. No entanto, a ocorrência do evento b tem probabilidades distintas nos estados equivalentes 2 e 4 no autômato gerador. Dessa forma, a probabilidade de estar nos rótulos (2N) e (4F) varia a cada observação do evento b. O gráfico apresentado na Figura 26 mostra a probabilidade normalizada de estar em cada um dos rótulos à medida que o evento b se repete.

Analisando a Figura 26, podemos observar que mesmo com uma diferença considerada pequena entre as probabilidades de ocorrência do evento b nos estados correspondentes aos rótulos 2N e 4F, vemos que conforme n aumenta a probabilidade de estar no rótulo 2N aumenta e a probabilidade de estar no rótulo 4F diminui. Além disso, podemos identificar que a partir de $n = 200$, as probabilidades tendem a um determinado limite, sendo que as probabilidades normalizadas das cadeias ab^n (curva em azul com traço sólido) que levam ao rótulo 2N tendem a 100%, enquanto as probabilidades normalizadas das cadeias fab^n (curva em vermelho com traço pontilhado) que levam ao rótulo 4F tendem a 0%. Tendo em vista que nos exemplos tratados a

Figura 26 – Probabilidades normalizadas de cadeias que contém ciclos à medida que $n \to \infty$, em que os valores são calculados para o exemplo apresentado na Figura 25.



Fonte: Elaborado pelo autor (2023)

seguir em que se utiliza a Abordagem *Offline* para Cálculo da Diagnose, a diferença dos valores de probabilidades associadas aos ciclos de eventos na planta é sempre maior do que a tratada neste exemplo, então em todos eles se utilizará $n = 200$ para o cálculo quando $n \to \infty$.

O Algoritmo 1 apresenta a sequência de passos necessários para o cálculo das probabilidades de atingir cada rótulo de cada estado do DEPE. O Algoritmo 1 possui duas estruturas de repetição. O laço de repetição da Linha 1 permite o acesso a todos os estados do diagnosticador. O laço de repetição da Linha 6 permite o acesso aos rótulos do estado do diagnosticador que está sendo analisado. As estruturas condicionais da Linha 3 e 7 determinam qual procedimento de cálculo deve ser adotado. Se o estado tem um único rótulo, a probabilidade de se estar naquele rótulo é de 100%. Se o estado tiver mais de um rótulo, deve-se verificar se o estado possui algum ciclo de eventos. Nesse caso, é calculada uma faixa de probabilidades. Caso contrário, é um valor único de probabilidade. As funções Calcule $CCD(x_D)$ e Calcule $PD(x_D(i))$ não são apresentadas como algoritmo, mas o procedimento matemático para estabelecer o conjunto e calcular as probabilidades é descrito acima, utilizando as Equações (1), (2) e (3).

É importante destacar que nos casos em que houver somas ou multiplicações de faixas

Algoritmo 1: Cálculo das probabilidades de estar em cada rótulo do estado do DEPE.

```
   Dados: G,D
   Resultado: PD
1  para cada estado x_D ∈ X_D não analisado faça
2      Calcule CCD(x_D);
3      se |x_D| == 1 então
4          PD(x_D) = 1;
5      senão
6          para cada rótulo x_D(i) não analisado faça
7              se para algum x'_D : δ̂_D(x_D0, v_o) = x'_D, com v_o ∈ Σ*_o
                ∃t_o ∈ SC(CCD(x_D)) : δ̂_D(x'_D, t_o) = x'_D então
8                  Calcule PD(x_D(i)(0)); // Cálculo do valor de probabilidade
                       para n=0
9                  Calcule PD(x_D(i)(∞)); // Cálculo do valor de probabilidade
                       para n → ∞
10             senão
11                 Calcule PD(x_D(i));
12             fim
13         fim
14     fim
15 fim
```

de probabilidades, a operação é feita limitante inferior com limitante inferior e limitante superior com limitante superior, em que o limitante inferior é calculado com $n = 0$ e o superior com $n \to \infty$. Além disso, o vetor $\Omega(x_D)$ é utilizado para ponderar as probabilidades de ocorrência futura de falha e de evento proibido após a falha para obter os valores que são apresentados, respectivamente, nos campos 3 e 4 do modelo de estado do DEPE.

A seguir, apresenta-se procedimento realizado para o cálculo da probabilidade de prognose apresentada no campo 3 em cada estado x_D do diagnosticador. Neste procedimento é utilizado o Modelo Estático para análise de Prognose. O conjunto de cadeias que a partir de um estado qualquer $x \in X$ são terminadas pelo evento de falha $f \in \Sigma_f$ é definido como $\Psi_f(x_D(i)) := \{\omega f \in L(G,E(x_D(i))),$ com $\omega \in \Sigma^*$ e $f \in \Sigma\}$. Vale destacar que o conjunto $\Psi_f(x_D(i))$ associado a um $x_D(i)$ que possui $R(x_D(i))$ = "F" é sempre um conjunto vazio, visto que as falhas tratadas no escopo desta tese são consideradas permanentes.

A soma das probabilidades das cadeias contidas no conjunto $\Psi_f(x_D(i))$ é a probabilidade de ocorrência futura da falha f a partir do estado x associado ao rótulo $x_D(i)$, sendo representada por $PF(x_D(i))$, tal que $x_D \in X_D$ e $i \in \mathbb{N} : i|_1^{|x_D|}$. O cálculo da probabilidade de cada cadeia é obtido pela Equação (1). Neste caso, a soma já é um resultado normalizado e pode ser obtida por:

$$PF(x_D(i)) = \sum_{s \in \Psi_f(x_D(i))} Prob(s, x_D(i)) \tag{6}$$

Após a obtenção das probabilidades de ocorrência futura de falha a partir de cada rótulo

do estado x_D, agrupamos esses valores em um vetor $\Delta_F(x_D)$ tal que:

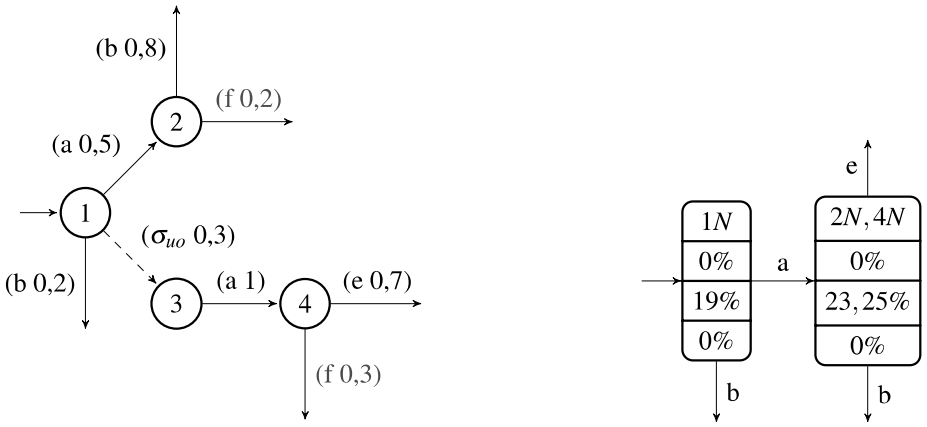
$$\Delta_F(x_D) = [PF(x_D(1))...PF(x_D(|x_D|))] \tag{7}$$

O produto do vetor $\Omega(x_D)$ pelo vetor $\Delta_F(x_D)$ transposto ($\Delta_F^T(x_D)$) resulta na probabilidade (ou faixa de probabilidades) apresentada no campo 3 (Figura 23a) dos estados do DEPE. De forma análoga ao caso das probabilidades do campo 2, se existirem cadeias em $\Psi_f(x)$ que possuem ciclos, é necessário calcular uma faixa de probabilidades, cujos limites são obtidos fazendo $n = 0$ e $n \to \infty$. Nesse caso, diferentemente do procedimento apresentado para a diagnose em que se é calculada a probabilidade das cadeias considerando um grande número de ocorrências dos ciclos ($n \to \infty$), para a prognose o limitante do intervalo é calculado somando a probabilidade de todas as cadeias possíveis que são terminadas pelo eventos de falha, utilizando a Equação (8) que representa a soma de uma série geométrica, cujo resultado é convergente pois a razão é menor que 1.

$$\sum_{n=0}^{\infty} a \cdot q^n = \frac{a}{1-q} \tag{8}$$

O exemplo apresentado na Figura 27 é utilizado para ilustrar o procedimento de cálculo da probabilidade de prognose para um estado do diagnosticador.

Figura 27 – Exemplo para ilustração do procedimento de cálculo do campo 3.



(a) Planta (b) Diagnosticador

Fonte: Elaborado pelo autor (2023)

O memorial de cálculo para a probabilidade de prognose a partir do estado $(2N, 4N)$ do diagnosticador da Figura 27 é exibido a seguir.

$x_D = (2N, 4N)$

$\Omega(2N, 4N) = [0,675 \;\; 0,325]$

$\Psi_f(2N) = \{f\}$
$PF(2N) = Prob(f,2) = 20\%$

$\Psi_f(4N) = \{f\}$
$PF(4N) = Prob(f,4) = 30\%$

$\Delta_F(2N,4N) = [0,2 \;\; 0,3]$

$$\Omega(2N,4F) \cdot \Delta_F^T(2N,4N) = \begin{bmatrix} 0,675 & 0,325 \end{bmatrix} \begin{bmatrix} 0,2 \\ 0,3 \end{bmatrix} = 23,25\%$$

O autômato e o diagnosticador apresentados na Figura 28 são utilizados para exemplificar o cálculo da probabilidade de prognose quando existem ciclos anteriores a ocorrência do evento de falha. O memorial de cálculo para a probabilidade de prognose no estado $(1N)$ do diagnosticador da Figura 28 é exibido a seguir.
$x_D = (1N)$
$\Omega(1N) = [1]$

$\Psi_f(1N) = a^*f$
$PF((2N)(0)) = Prob(f,2) = 10\%$
$PF((2N)(\infty)) = Prob(a^nf,2) = 16,67\%$

$\Delta_F(1N) = [(0,1;0,1667)]$

$$\Omega(1N) \cdot \Delta_F^T(1N) = \begin{bmatrix} 1 \end{bmatrix} \begin{bmatrix} (0,1;0,1667) \end{bmatrix} = (10;16,67)\%$$

Figura 28 – Exemplo para ilustração do procedimento de cálculo da probabilidade de prognose quando existem ciclos de eventos anteriores ao evento de falha.

(a) Planta (b) Diagnosticador

Fonte: Elaborado pelo autor (2023)

O Algoritmo 2 apresenta a sequência de passos necessários para o cálculo das probabilidades de ocorrência de falhas futuras para cada rótulo de cada estado do DEPE.

Algoritmo 2: Cálculo das probabilidades de ocorrência futura de falha a partir de cada rótulo do estado do DEPE.

Dados: G,D
Resultado: PF
1 **para cada** *estado* $x_D \in X_D$ *não analisado* **faça**
2 **para cada** *rótulo* $x_D(i)$ *não analisado* **faça**
3 Calcule $\Psi_f(x_D(i))$;
4 **se** *para algum* $x'_D : \hat{\delta}_D(x_{D0}, v_o) = x'_D$, *com* $v_o \in \Sigma^*$
 $\exists t_o \in SC(\Psi_f(x_D(i))) : \hat{\delta}_D(x'_D, t_o) = x'_D$ **então**
5 Calcule $PF(x_D(i)(0))$; `// Cálculo do valor de probabilidade para n=0`
6 Calcule $PF(x_D(i)(\infty))$; `// Cálculo do valor de probabilidade para n= ∞`
7 **senão**
8 Calcule $PF(x_D(i))$;
9 **fim**
10 **fim**
11 **fim**

O Algoritmo 2 também utiliza duas estruturas de repetição (Linhas 1 e 2) para navegar entre estados e rótulos do diagnosticador. A estrutura condicional da Linha 4 verifica se existe um ciclo de eventos entre o estado do rótulo analisado e o estado em que o evento de falha está ativo. Caso exista, é estabelecida uma faixa de probabilidades, caso contrário é um valor único de probabilidade.

Assim como no Algoritmo 1, existem funções apresentadas no Algoritmo 2 que não são apresentadas na forma de algoritmo, mas cujo procedimento de cálculo foi apresentado anteriormente nesta seção.

A probabilidade de ocorrência futura de evento proibido após a falha é calculada a partir de cada rótulo $x_D(i)$ de cada estado $x_D \in X_D$ do diagnosticador. Seja $\eta(x_D(i))$, o conjunto das cadeias a partir do estado x, equivalente ao rótulo $x_D(i)$, que são terminadas por uma cadeia proibida $\xi \in \Phi$, formalmente definido na Equação (9).

$$\eta(x_D(i)) := \begin{array}{ll} \{v\xi \in L(G, E(x_D(i)))\} & \text{se } R(x_D(i)) = \text{"}F\text{"} \\ \{sv\xi \in L(G, E(x_D(i)))\} & \text{se } R(x_D(i)) = \text{"}N\text{"} \end{array} \tag{9}$$

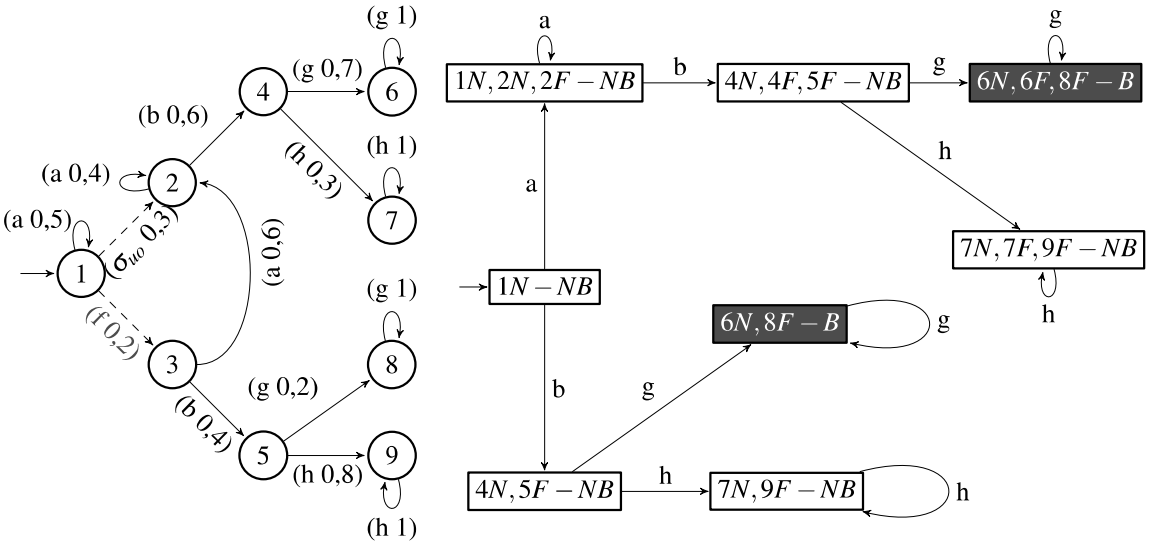
em que $s \in \Psi_f(x)$, $v \in \Sigma^*$ e $\xi \in \Phi$.

É possível observar na Equação (9) que o conjunto $\eta(x_D(i))$ é definido de duas maneiras, de forma a atender duas situações distintas: (a) $x_D(i)$ é um rótulo de falha; (b) $x_D(i)$ é um rótulo normal. Para diminuir a complexidade computacional em um algoritmo que calcula $\eta(x_D(i))$, o conjunto $\eta(x_D(i))$ associado a um $x_D(i)$ que possui R($x_D(i)$) = "N", mas cujo estado E($x_D(i)$) pode ser acessado por uma cadeia que contém a falha é sempre um conjunto vazio, visto que as falhas tratadas no escopo desta tese são consideradas permanentes. O exemplo apresentado na

Figura 29 é utilizado para demonstrar como são estabelecidos os conjuntos $\eta(x_D(i))$ para um estado x_D do diagnosticador.

Neste capítulo, são utilizadas cores para destaque de algumas características nas figuras que contém autômatos relacionados a plantas e autômatos diagnosticadores. A cor vermelha ( ) é utilizada para ilustrar os maus estados do diagnosticador. A cor amarela ( ) é utilizada para dar ênfase em alguma característica do exemplo. Ex: estado do autômato da planta, estado do diagnosticador, campo do estado do DECS, etc.

Figura 29 – Exemplo para ilustração do estabelecimento dos conjuntos $\eta(x_D(i))$ para um estado x_D do diagnosticador.



(a) Planta (b) Diagnosticador

Fonte: Elaborado pelo autor (2023)

Procedimento para obtenção do conjunto $\eta(x_D)$
Estado x_D = (1N,2N,2F - NB)
$x_D(1) = 1N$
$R(x_D(1)) = "N"$
$\eta(1N) = a^*f(b+aa^*b)g$ em que $s = a^*f$, $v = b+aa^*b$ e $\xi = g$

$x_D(2) = 2N$
$R(x_D(2)) = "N"$
$\eta(2N) = \emptyset$

$x_D(3) = 2F$
$R(x_D(3)) = "F"$
$\eta(2F) = a^*bg$ em que $v = a^*b$ e $\xi = g$

A soma das probabilidades das cadeias contidas no conjunto $\eta(x_D(i))$ é a probabilidade de ocorrência futura de evento proibido após a falha f a partir do rótulo $x_D(i)$, sendo representada por $PEP(x_D(i))$, tal que $x_D \in X_D$ e $i \in \mathbb{N} : i|_1^{|x_D|}$. O cálculo da probabilidade de cada cadeia é obtido pela Equação (1).

$$PEP(x_D(i)) = \sum_{s \in \eta(x_D(i))} Prob(s, x_D(i)) \tag{10}$$

Após a obtenção das probabilidades de ocorrência futura de evento proibido após a falha a partir de cada rótulo do estado x_D, agrupamos esses valores em um vetor $\Delta_{EP}(x_D)$ tal que:

$$\Delta_{EP}(x_D) = [PEP(x_D(1))...PEP(x_D(|x_D|))] \tag{11}$$

O produto do vetor $\Omega(x_D)$ pelo vetor $\Delta_{EP}(x_D)$ transposto ($\Delta_{EP}^T(x_D)$) resulta na probabilidade (ou faixa de probabilidades) apresentada no campo 4 (Figura 23a) dos estados do DEPE. De forma análoga aos caso das probabilidades do campo 2 e 3, se existirem cadeias em $\eta(x_D(i))$ que possuem ciclos, é necessário calcular uma faixa de probabilidades, cujos limites são obtidos fazendo $n = 0$ e $n \to \infty$.

O exemplo apresentado na Figura 29 é utilizado para ilustrar o procedimento de cálculo da probabilidade de ocorrência futura da cadeia proibida após a falha a partir de um estado do diagnosticador. O memorial de cálculo para o estado $(1N, 2N, 2F - NB)$ do diagnosticador da Figura 29 é exibido a seguir.

$x_D = (1N, 2N, 2F - NB)$
$\Omega(x_D) = [(67,56;29,42)\%\ \ (16,22;35,29)\%\ \ (16,22;35,29)\%]$

$\eta(1N) = a^* f(b + aa^* b)g$
$PEP((1N(0)) = Prob(fbg, 1) + Prob(fabg, 1)$
$PEP((1N(0)) = 0,2 \cdot 0,4 \cdot 0,2 + 0,2 \cdot 0,6 \cdot 0,6 \cdot 0,7 = 6,64\%$

$PEP((1N(\infty)) = \sum_{n=0}^{\infty} Prob(a^n fbg, 1) + \sum_{n=0}^{\infty} Prob(a^n faa^n bg, 1)$
$PEP((1N(\infty)) = \sum_{n=0}^{\infty} 0,5^n \cdot 0,2 \cdot 0,4 \cdot 0,2 + \sum_{n=0}^{\infty} 0,5^n \cdot 0,2 \cdot 0,6 \cdot 0,4^n \cdot 0,6 \cdot 0,7 = 9,5\%$

$\eta(2N) = \emptyset$
$PEP((2N) = 0\%$

$\eta(2F) = a^* bg$
$PEP((2F(0)) = Prob(bg, 2)$
$PEP((2F(0)) = 0,6 \cdot 0,7 = 42\%$

$PEP((2F(\infty)) = \sum_{n=0}^{\infty} Prob(a^n bg, 2)$
$PEP((2F(\infty)) = \sum_{n=0}^{\infty} 0,4^n \cdot 0,6 \cdot 0,7 = 70\%$

$\Delta_{EP}(1N, 2N, 2F - NB) = [(0,0664; 0,095)\%\ \ 0\%\ \ (0,42; 0,7)\%]$

$$\Omega(x_D) \cdot \Delta_{EP}^T(x_D) = \begin{bmatrix} (0,6756; 0,2942) & (0,1622; 0,329) & (0,1622; 0,3529) \end{bmatrix} \begin{bmatrix} (0,0664; 0,095) \\ 0\% \\ (0,42; 0,7) \end{bmatrix}$$

$\Omega(x_D) \cdot \Delta_{EP}^T(x_D) = (11,30; 27,5)\%$

O Algoritmo 3 apresenta a sequência de passos necessários para o cálculo das probabilidades de ocorrências futuras de evento proibido após a falha para cada rótulo de cada estado do DEPE.

Algoritmo 3: Cálculo das probabilidades de ocorrência futura de evento proibido após falha a partir de cada rótulo do estado do DEPE.

```
   Dados: G,D
   Resultado: PEP
1  para cada estado x_D ∈ X_D não analisado faça
2      para cada rótulo x_D(i) não analisado faça
3          Calcule η(x_D(i));
4          se para algum x'_D : δ̂_D(x_D0, v_o) = x'_D, com v_o ∈ Σ*_o
             ∃t_o ∈ SC(η(x_D(i)))|δ̂_D(x'_D, t_o) = x'_D então
5              Calcule PEP(x_D(i)(0)); // Cálculo do valor de probabilidade
                   para n=0
6              Calcule PEP(x_D(i)(∞)); // Cálculo do valor de probabilidade
                   para n → ∞
7          senão
8              Calcule PEP(x_D(i));
9          fim
10     fim
11 fim
```

O Algoritmo 3 também utiliza duas estruturas de repetição (Linhas 1 e 2) para navegar entre estados e rótulos do diagnosticador. A estrutura condicional da Linha 4 verifica se existe um ciclo de eventos entre o estado do rótulo analisado e o estado atingido após a execução da cadeia proibida após a falha. Caso exista, é estabelecida uma faixa de probabilidades, caso contrário é um valor único de probabilidade. Neste caso, diferentemente do procedimento apresentado para a diagnose em que se é calculada a probabilidade das cadeias com (n$\rightarrow \infty$), para a probabilidade de ocorrência futura de cadeia proibida, o limitante do intervalo é calculado somando a probabilidade de todas as cadeias possíveis que são terminadas por uma cadeia proibida após a falha.

Assim como nos Algoritmos 1 e 2 , existem funções apresentadas no Algoritmo 3 que não são apresentadas na forma de algoritmo, mas cujo procedimento de cálculo foi apresentado anteriormente nesta seção.

Os Algoritmos 1, 2 e 3 apresentam as sequências de passos completas desde os estabelecimentos dos conjuntos até as etapas de cálculos de probabilidades que são exibidas nos DECSs. No entanto, a implementação até o momento é parcial. O procedimento de cálculo das probabilidades foi codificado de forma particular para cada exemplo no software matemático Matlab©. Enquanto o procedimento de estabelecimento dos conjuntos $CCD(x_D)$, $CCG(x_D(i))$, $\Psi_f(x_D(i))$ e $\eta(x_D(i))$ é feito manualmente. A implementação completa, bem como a elaboração de provas de corretude são questões a serem abordadas em trabalhos futuros.

Apesar da não implementação do procedimento de estabelecimento dos conjuntos $CCD(x_D)$, $CCG(x_D(i))$, $\Psi_f(x_D(i))$ e $\eta(x_D(i))$. É possível afirmar que há convergência, pois todos os conjuntos podem ser representados por expressões regulares.

4.1.2 Exemplos

Nesta seção são apresentados exemplos de autômatos e diagnosticadores cujas linguagens não são logicamente diagnosticáveis. Os exemplos foram escolhidos para mostrar que uma análise tanto da diagnose quanto da prognose estocástica de falhas fornece informações que podem auxiliar no Controle Tolerante a Falhas (CTF). Informações estas, que não são fornecidas em análises de diagnose ou prognose lógicas.

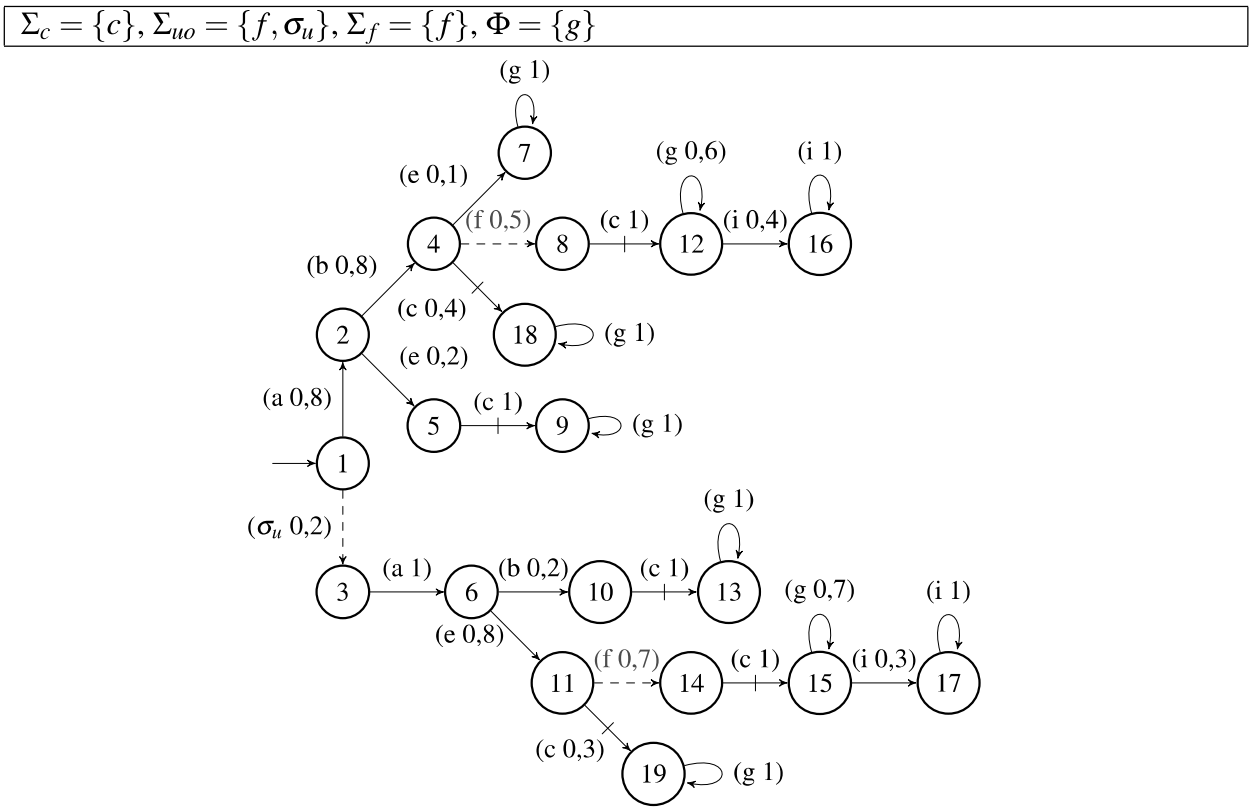
Conforme apresentado no Capítulo 2 (vide Figura 5), existem duas abordagens de cálculo de observador. Nesta tese, será utilizado o observador sem inclusão do alcance de eventos não observáveis para os cálculos dos diagnosticadores. Opta-se por esse observador, pois em geral os estados do diagnosticador sem alcance não observável tendem a ter menos rótulos que os estados do diagnosticador com alcance dos eventos não observáveis. A opção por menos rótulos, reduz a quantidade de operações matemáticas a serem realizadas. Além disso, trabalhos relacionados ao tema também utilizam diagnosticador sem alcance de eventos não observáveis, tais como: Thorsley e Teneketzis (2005), Liu e Qiu (2008).

O DEPE ilustrado na Figura 31 está associado ao autômato $G1$ apresentado na Figura 30. É possível observar que $L(G1)$ não é logicamente diagnosticável e, portanto, não prognosticável também. Ao realizarmos a verificação conforme a abordagem por cadeias proposta por Watanabe et al. (2021), concluímos que o autômato não é DP-controlável seguro.

No entanto, ao analisar os valores do DEPE, temos informações para impor lógicas de controle cautelares devido a altas probabilidades de a falha ter ocorrido ou de vir a ocorrer. Por exemplo, no estado (5N,11N) a probabilidade de ocorrência futura de falha é de 35% e de um evento proibido ocorrer após a falha é de 24,5%. Neste ponto, é possível desabilitar o evento controlável c. Outro ponto de interesse é o estado (4N,10N), no qual existe uma probabilidade de ocorrência futura de falha de 47,06% e de evento proibido após a falha de 28,24%.

O Apêndice A apresenta o memorial de cálculo para demonstrar como são obtidas as

Figura 30 – Autômato G1 - Exemplo com linguagem logicamente não diagnosticável.



Fonte: Elaborado pelo autor (2023)

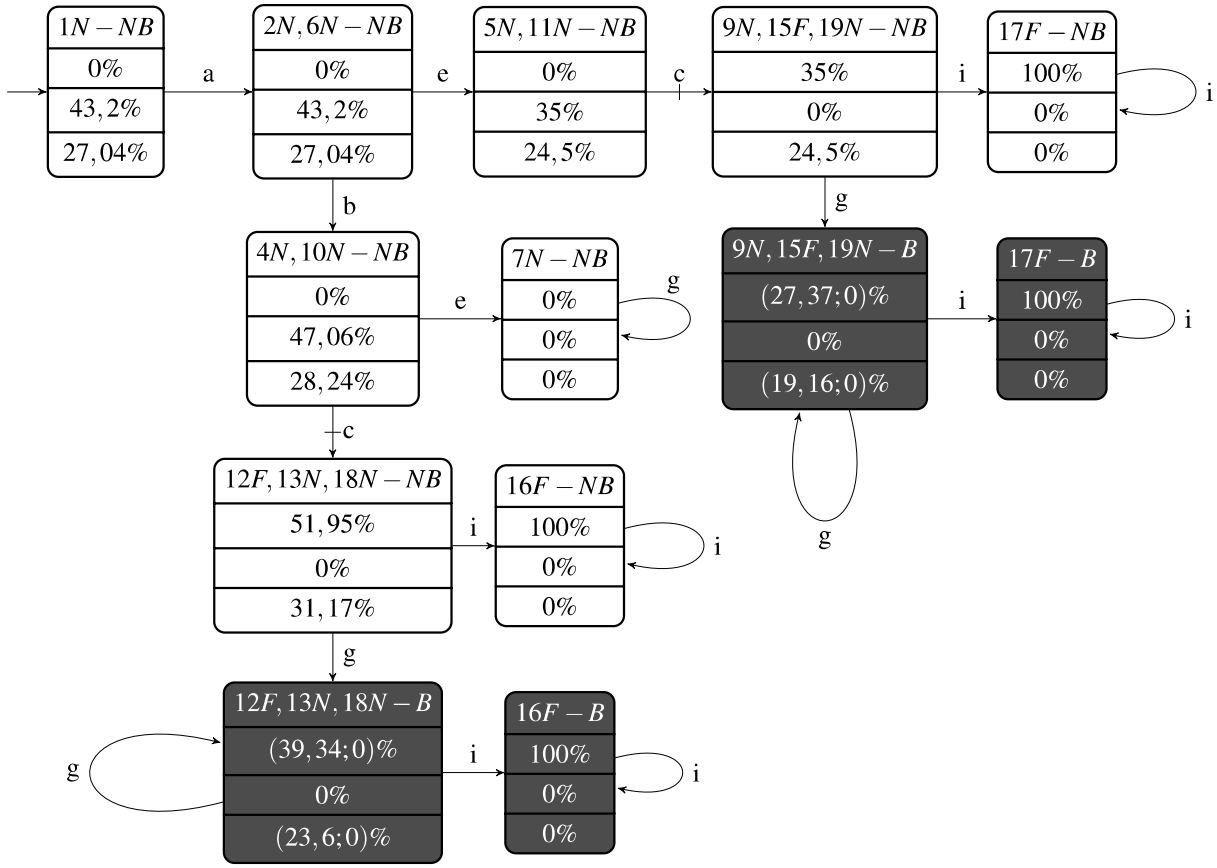
probabilidades do DEPE com a utilização dos Algoritmos 1, 2 e 3 adotando como exemplo o autômato (Figura 32) e seu diagnosticador correspondente (Figura 33).

É possível observar no diagnosticador da Figura 33 que nos estados que contêm ciclos de eventos e nos anteriores a estes são estabelecidas faixas de probabilidades relacionadas à prognose. O primeiro valor dessa faixa representa a probabilidade de ocorrência futura de falha ao considerarmos apenas as cadeias que levam à falha de maneira imediata, ou seja, sem ocorrência de ciclos. Enquanto o segundo limitante da faixa representa a soma de todas as cadeias possíveis terminadas pelo evento de falha. Neste exemplo em particular, verificamos um único valor de probabilidade nos campos destinados à diagnose, pois a probabilidade de ocorrência do evento do ciclo é a mesma para todos os rótulos do ciclo.

Em todos os casos, o primeiro valor da faixa é a probabilidade para $n = 0$ e o segundo para $n \to \infty$; dessa forma, fica evidente o comportamento das probabilidades à medida que ocorrem repetições dos eventos ou cadeias que compõem o ciclo.

No estado (1N) (Figura 33) tem-se uma probabilidade de ocorrência de falha futura de 9% ao considerar que não haverá nenhuma transição do auto-laço do evento e. Esta probabilidade se aproxima de 10% quando n tende a infinito, pois a probabilidade de ficar eternamente em um ciclo cuja probabilidade do evento é menor do que 100% é nula, ou seja, eventualmente ocorrerá o evento f ou o evento b, sendo que ambos compõem caminhos cuja falha ocorreu ou sua

Figura 31 – DEPE obtido para o autômato G1 (Figura 30).



Fonte: Elaborado pelo autor (2023)

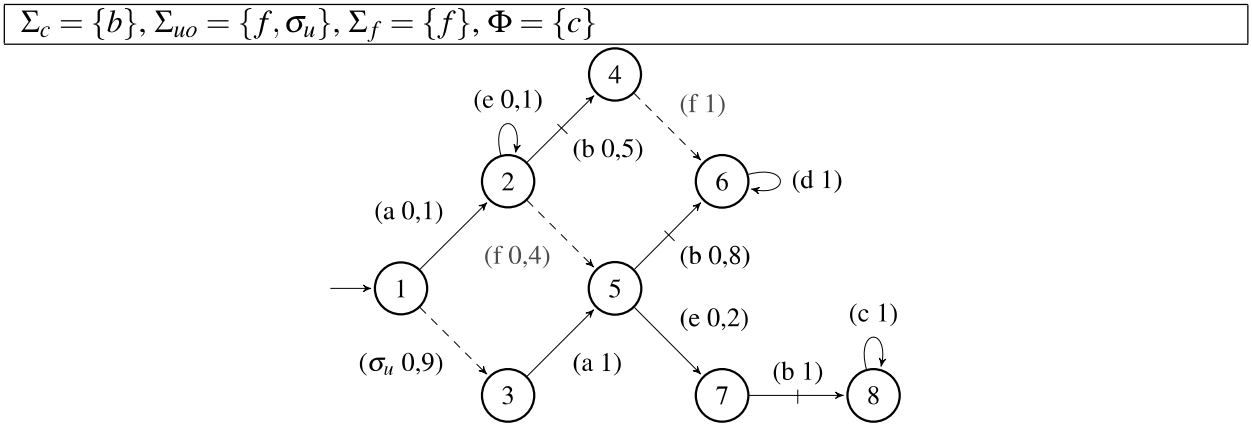
ocorrência futura é certa. Este comportamento é revisitado na Seção 4.2 como uma propriedade que pode ser avaliada em autômatos clássicos, mas que pode ser abordada com maior nível de detalhe em autômatos estocásticos.

4.2 CERTEZA DE ANORMALIDADE E COEFICIENTE DE ANORMALIDADE

No exemplo apresentado na Figura 32, na Seção 4.1.2, podemos observar uma característica interessante ao realizarmos uma avaliação conjunta de diagnose e prognose de falhas, cuja aplicação é útil para problemas reais em que somente diagnose ou somente prognose não são suficientes para impedir a execução de um comportamento indesejado no SED sob análise. Essa propriedade é uma contribuição denominada Certeza de Anormalidade quando avaliada em autômatos clássicos em que se encontra uma estrutura de estados conforme ilustrada na Figura 34. A Certeza de Anormalidade é definida conforme segue:

Definição 4.2.1 (Certeza de Anormalidade)**.** *Uma cadeia $r \in L(G)$ tal que $f \in r$ leva à certeza de anormalidade se $\exists t \in L(G) : P_o(r) = P_o(t)$, com $f \notin t$ e $(\forall u \in L(G) : P_o(u) = P_o(t)$, com $f \notin u)(\exists n \in \mathbb{N})(\forall \omega \in L(G/t) \cup L(G/u)), ||\omega|| \geq n \Rightarrow f \in \omega$.*

Figura 32 – Autômato G2 - Linguagem logicamente não diagnosticável.



Fonte: Elaborado pelo autor (2023)

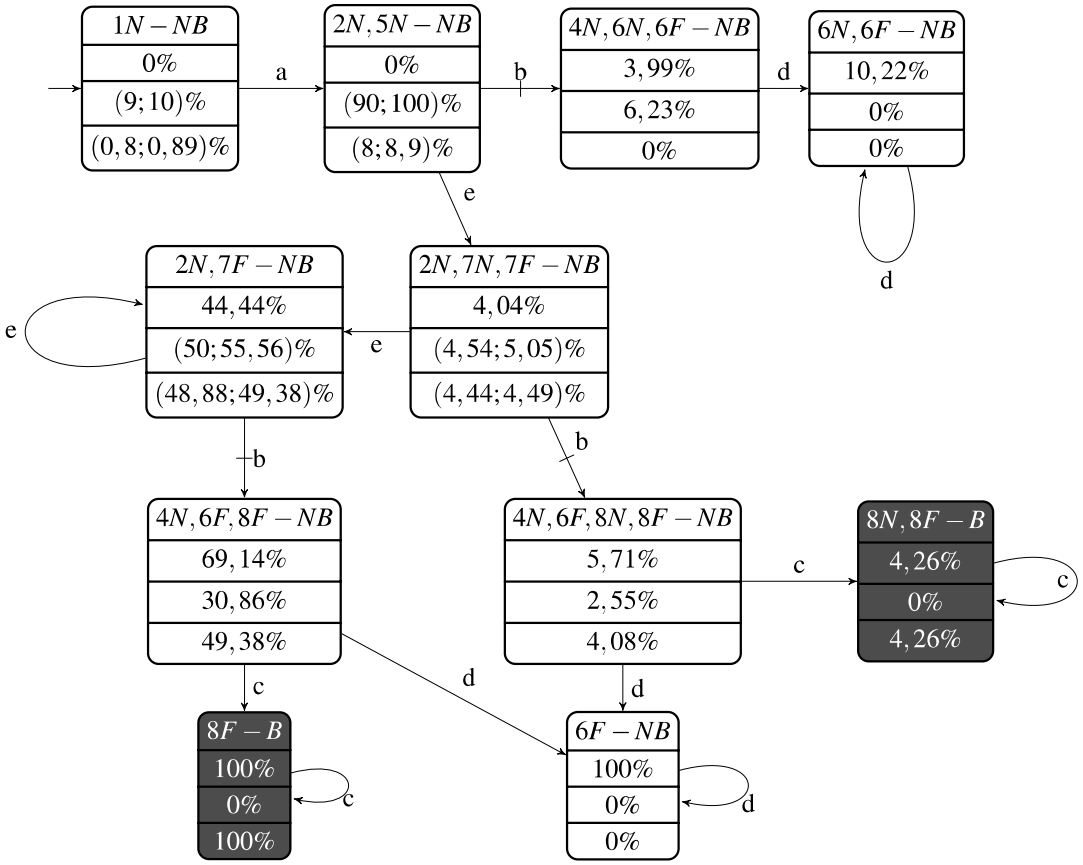
Em palavras, uma cadeia r, que possui o evento de falha, leva à certeza de anormalidade se existe uma cadeia t, sem falhas e com a mesma observação de r, tal que todas as suas continuações levam à ocorrência de falha em um número finito de eventos. Além disso, qualquer outra cadeia u que seja livre de falhas e tenha a mesma observação de r e t, é tal que todas as suas continuações também levam à ocorrência de falha em um número finito de eventos.

Podemos verificar no exemplo da Figura 34 que após a observação da cadeia $s_o = ba$, atinge-se o estado (6F,7N). Neste estado, temos a garantia que a falha aconteceu (pois a planta atingiu o rótulo 6F) ou virá a acontecer (pois todos os caminhos que seguem a partir do rótulo 7N levam à falha). Neste estado, podemos dizer que há certeza de anormalidade. Esta propriedade fornece mais um parâmetro a ser utilizado em sínteses de controladores seguros para autômatos clássicos.

O exemplo apresentado na Figura 35 ilustra a utilização da certeza de anormalidade como parâmetro para controlabilidade segura. Neste exemplo, a linguagem não é DP-Controlável segura, pois a ocorrência da falha na cadeia ef não é controlável segura pela diagnose ou prognose. No entanto, após a observação da cadeia $s_o = ej$, atinge-se o estado (17N,19F), no qual é possível afirmar que a falha ocorreu ou que ela ocorrerá no futuro, ou seja, que se tem certeza de anormalidade. A partir dessa informação, pode-se desabilitar o evento controlável $c3$ impedindo que a planta atinja um mau estado.

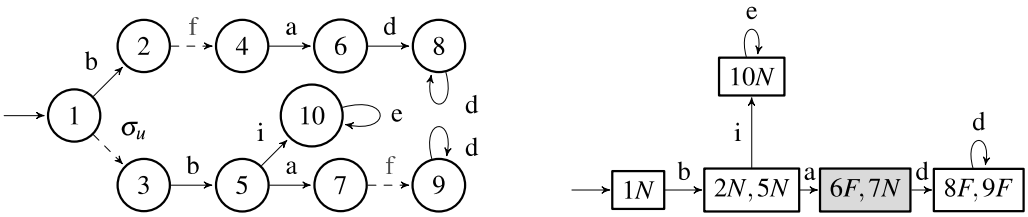
O exemplo apresentado na Figura 36 é utilizado para a ilustração do coeficiente de anormalidade. O coeficiente de anormalidade $\vartheta(x_D)$ é obtido para cada estado do diagnosticador ao realizamos a soma da probabilidade de estar em um rótulo de falha com a probabilidade de ocorrência futura da falha a partir deste mesmo estado. Este coeficiente representa uma probabilidade da falha ter acontecido ou da falha ocorrer no futuro. O coeficiente não é exibido no modelo de estado do DEPE, mas seu valor é obtido para todos os estados x_D, ao realizar a soma das probabilidades apresentadas nos campos 2 e 3, conforme apresentado na Equação (12).

Figura 33 – DEPE obtido para o autômato G2 (Figura 32).



Fonte: Elaborado pelo autor (2023)

Figura 34 – Exemplo para ilustrar a certeza de anormalidade em um SED.



(a) Planta (b) Diagnosticador

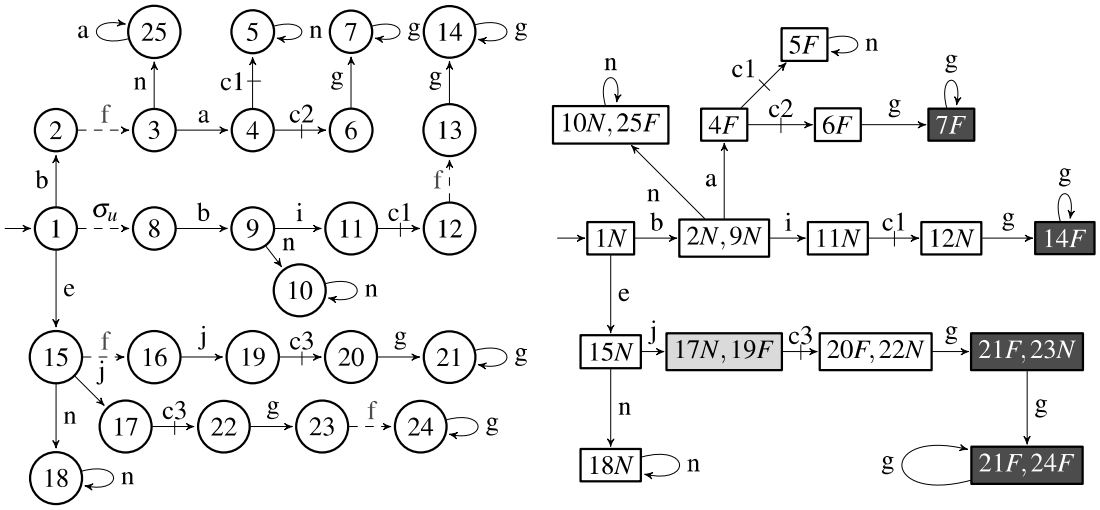
Fonte: Elaborado pelo autor (2023)

$$\vartheta(x_D) = \Omega_F(x_D) + \Omega(x_D) \cdot \Delta_F(x_D)^T \tag{12}$$

tal que $\forall x_D \in X_D, 0 \leq \vartheta(x_D) \leq 1$.

Para o DEPE ilustrado na Figura 36, tem-se os seguintes coeficientes de anormalidade: $\vartheta(1N-NB) = 18\%$, $\vartheta(2N,5N-NB) = 18\%$, $\vartheta(6F,7N-NB) = 64,29\%$, $\vartheta(8F,11F-NB) = 100\%$, $\vartheta(10N-NB) = 0\%$, $\vartheta(13N-NB) = 0\%$, $\vartheta(12F,14F-NB) = 100\%$, $\vartheta(11F-B) = 100\%$ e $\vartheta(8F-NB) = 100\%$.

Figura 35 – Exemplo para ilustrar a utilização da certeza de anormalidade no contexto de controlabilidade segura para um SED. Os rótulos NB e B são omitidos neste diagnosticador seguro. Dessa forma, os maus estados são indicados apenas pela ilustração em vermelho.



(a) Planta (b) Diagnosticador

Fonte: Elaborado pelo autor (2023)

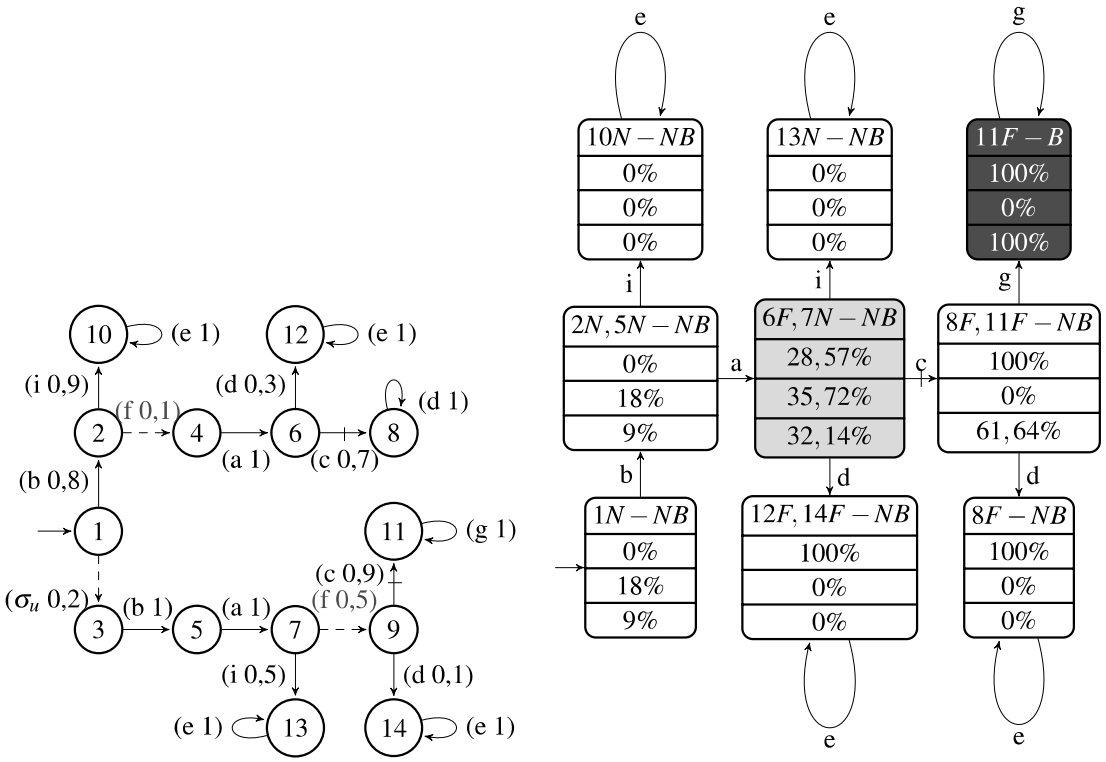
No exemplo da Figura 36 verificamos que essa linguagem não é DP-Controlável segura e que após a cadeia $s_o = ba$, atinge-se o estado (6F,7N) com coeficiente de anormalidade $\vartheta(6F, 7N) = 28,57\% + 35,71\% = 64,28\%$. Assim, de acordo com o projetista, se esse valor for aceitável para que uma ação de controle seja tomada a fim de evitar propagação de danos ao SED, então o evento controlável c pode ser desabilitado para impedir a execução do evento proibido g após a falha.

4.3 CONTROLABILIDADE SEGURA EM SEDS UTILIZANDO DEPE

Nesta seção são apresentadas novas noções de diagnosticabilidade, diagnosticabilidade segura e prognosticabilidade. Estes conceitos são necessários para as posteriores definições de controlabilidade segura que utilizam diagnose ou prognose baseadas em probabilidades.

A Definição 4.3.1 apresenta uma nova noção de diagnosticabilidade. A u-Diagnosticabilidade é concebida para autômatos estocásticos e seus DEPEs equivalentes. Esta definição é elaborada com um relaxamento dos demais conceitos de diagnosticabilidade existentes para que a propriedade seja mais facilmente atendida, com o objetivo de fornecer diagnosticabilidade a SEDs que não são logicamente diagnosticáveis, A-Diagnosticáveis ou AA-Diagnosticáveis. Essa definição difere em relação às definições de diagnosticabilidade lógica (SAMPATH et al., 1995) e as definições de A-Diagnosticabilidade e AA-Diagnosticabilidade (THORSLEY; TENEKETZIS, 2005), pois na u-diagnosticabilidade não há necessidade de atender a condição de diagnosticabilidade da Definição 2.5.1. Além disso, para a u-diagnosticabilidade não há

Figura 36 – Exemplo para ilustração do coeficiente de anormalidade em SEDEs.



(a) Planta (b) DEPE

Fonte: Elaborado pelo autor (2023)

exigência que os componentes recorrentes do diagnosticador que contenham rótulos de falhas sejam apenas estados certos de falha tal qual as condições dos Teoremas 3.2.1 e 3.2.2.

Definição 4.3.1 (u-Diagnosticabilidade)**.** *Uma linguagem prefixo-fechada L que é viva e que não contém ciclos de eventos não observáveis é dita ser u-diagnosticável em relação à projeção Po e evento de falha f se a seguinte condição for verificada:* $(\exists n \in \mathbb{N})(\forall s \in \Psi_L(f))(\forall t \in L/s : ||t|| \geq n)(\exists \sigma_o \in \Sigma_o : \sigma_o \in t)$.

Em palavras, de acordo com essa definição, toda linguagem viva é u-diagnosticável. Essa definição parece sem propósito, no entanto, a partir desse conceito introduz-se a u-Diagnosticabilidade e consequentemente a controlabilidade segura pela u-diagnose. Sendo assim, essa definição tem uma aplicabilidade importante no contexto de SEDEs.

A característica que objetivou a definição dessa noção de diagnosticabilidade distinta em relação às noções existentes, é que ao observarmos um evento $\sigma_o \in \Sigma_o$ que faz parte da pós-linguagem de $s \in \Psi_L(f)$, existirá, na hipótese mais conservadora, uma incerteza da ocorrência de falha e, consequentemente, uma probabilidade mínima, diferente de zero, de a falha ter ocorrido. A partir deste momento, teremos uma probabilidade do sistema estar em estados normais ou em estados pós-falha. Deseja-se fornecer essas informações para que o projetista possa definir ações de controle para impedir a execução de um comportamento indesejado ao SED sob análise.

Estabelecendo desta forma, uma propriedade de controlabilidade segura pela u-diagnose, que é anunciada a seguir.

De forma análoga ao estudo de diagnose em autômatos clássicos, apresentamos na Definição 4.3.2 a noção de u-Diagnosticabilidade Segura.

Definição 4.3.2 (u-Diagnosticabilidade Segura)**.** *Uma linguagem prefixo-fechada L que é viva e que não contém ciclos de eventos não observáveis é dita ser u-diagnosticável segura em relação à projeção Po, evento f, conjunto de cadeias proibidas* Φ *e a linguagem proibida* $\mathscr{K}_f$ *se atender à seguinte condição:* $(\forall s \in \Psi_L(f))(\forall t = v\xi \in L/s$, *com* $v \in \Sigma^*$ *e* $\xi \in \Phi), (\exists u < t : \sigma_o \in u \wedge u \cap \mathscr{K}_f = \emptyset$, *com* $\sigma_o \in \Sigma_o)$

Em palavras, para que uma linguagem L seja u-diagnosticável segura, para todas cadeias t pós evento de falha que são terminadas por uma subcadeia ilegal, deve existir um prefixo estrito de t que contenha ao menos um evento observável e cuja interseção com a linguagem ilegal resulte em um conjunto vazio.

Seja FU o conjunto dos primeiros estados incertos no diagnosticador alcançados a partir do estado inicial, considerando todos os caminhos existentes. Formalmente, $FU := \{x_D \in X_D^U : (\exists s_o \in \Sigma_o^*)$ tal que $(\hat{\delta}_D(x_{D0}, s_o) = x_D)$ e $(\nexists t_o < s_o)(\hat{\delta}_D(x_{D0}, t_o)) \in X_D^U\}$.

Seja FPF o conjunto dos estados do diagnosticador atingidos após a ocorrência do primeiro evento observável após a falha. Formalmente, $FPF := \{x_D \in FU \cup FC : x_D = \hat{\delta}_D(x_{D0}, s_o\sigma_o)$, com $s_o = P_o(s)$ tal que $s \in \Psi_L(f)$ e $\sigma_o \in \Sigma_o\}$.

Proposição 4.3.1 (Condição para u-Diagnose Segura)**.** *Considere uma linguagem L e um autômato* $G = (X, \Sigma, p, x_0)$ *que gera L. Seja* $D = (X_D, \Sigma_o, \delta_D, x_{D0})$ *o diagnosticador seguro construído a partir de G. A linguagem L é u-diagnosticável segura em relação a projeção Po, evento f e conjunto* Φ *se e somente se* $\nexists x_D \in FPF : x_D \in X_D^B$.

Prova.

(SOMENTE SE) A Prova é feita por contradição. Suponha que L é u-diagnosticável segura, mas que $\exists x_D \in FPF$ tal que $x_D \in X_D^B$. Pela definição do FPF sabe-se que $x_D \in FU \cup FC$ e que x_D é alcançado a partir do estado inicial do diagnosticador com uma cadeia $s_o\sigma_o$, com $s_o = P_o(s)$ tal que $s \in \Psi_L(f)$ e $\sigma_o \in \Sigma_o$. Ainda , como $x_D \in X_D^B$, pode-se afirmar que $\exists t = v\xi \in L/s$, com $v \in \Sigma^*$ e $\xi \in \Phi$ tal que $P_o(t) = \sigma_o$. Além disso, como o diagnosticador adotado não inclui o alcance não observável, para que $x_D \in x_D^B$ é necessário que σ_o seja o último evento de t, de modo que σ_o é o evento proibido ou é o último evento de uma cadeia proibida na qual os demais eventos são não observáveis. Sendo assim, $\nexists u < t : \sigma_o \in u$ e $t \cap \mathscr{K}_f \neq \emptyset$, o que viola a condição estabelecida na Definição 4.3.2. Portanto, a linguagem L não é u-diagnosticável segura, contrariando a hipótese inicial.

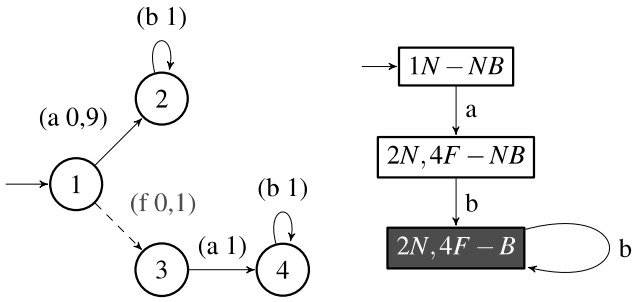
(SE) Suponha que $\nexists x_D \in FPF$ tal que $x_D \in X_D^B$. Pela definição do FPF, pode-se afirmar que $\forall x_D \in FU \cup FC : x_D = \hat{\delta}_D(x_{D0}, s_o\sigma_o)$, com $s_o = P_o(s)$ tal que $s \in \Psi_L(f)$ e σ_o, tem-se que $x_D \notin X_D^B$. Dessa forma, sabe-se que σ_o é tal que $\forall u \in L/s : u \in \overline{P_o^{-1}(\sigma_o)} \Rightarrow u \cap \mathscr{K}_f = \emptyset$. Sendo assim, pode-

se afirmar que $(\forall s \in \Psi_L(f))(\forall t = v\xi \in L/s$, com $v \in \Sigma^*$ e $\xi \in \Phi)$, $(\exists u < t : \sigma_o \in u \wedge u \cap \mathscr{K}_f = \emptyset$, com $\sigma_o \in \Sigma_o)$ e, portanto, que L é u-diagnosticável segura. □

A Proposição 4.3.1 requer que para que uma linguagem seja u-diagnosticável segura, todos estados do diagnosticador pertencentes ao conjunto FPF não sejam maus estados.

Na Figura 37 é apresentado um exemplo para ilustrar as diferenças entre Diagnosticabilidade Segura para SEDEs proposto por Liu e Qiu (2008) e o conceito de u-Diagnosticabilidade Segura proposto nesta tese.

Figura 37 – Exemplo para comparativo entre Diagnosticabilidade Segura para SEDEs e u-Diagnosticabilidade Segura



(a) G (b) D

	1N,NB	2N,NB	4F,NB	4F,B
1N,NB	0	0,9	0,1	0
2N,NB	0	1	0	0
4F,NB	0	0	1	0
4F,B	0	0	0	1

(c) Matriz de Markov associada a D

Fonte: Elaborado pelo autor (2023)

De acordo com a Figura 37c, vemos que os componentes (2N,NB), (4F,NB) e (4F,B) são componentes recorrentes, uma vez que a probabilidade desses componentes serem revisitdos é de 100%. Desta forma, existe no diagnosticador um estado x_D que é incerto de falha e que possui uma componente recorrente que carrega o rótulo de falha, característica que viola as condições do Teorema 3.2.3. Sendo assim, a linguagem deste exemplo não é diagnosticável segura segundo a noção proposta por Liu e Qiu (2008). No entanto, a linguagem deste mesmo exemplo é considerada u-diagnosticável segura, pois todos estados $x_D \in FPF$ não são maus estados (ver Proposição 4.3.1).

Apresentados os conceitos de u-diagnose e u-diagnose segura, introduzimos a Definição 4.3.3 com o estabelecimento de uma noção de Controlabilidade Segura pela u-Diagnose (CSUD).

Definição 4.3.3 (Controlabilidade Segura pela u-Diagnose)**.** *Uma linguagem prefixo-fechada L que é viva e que não contém ciclos de eventos não observáveis é dita ser controlável segura pela u-diagnose em relação à projeção Po, evento f, conjunto de cadeias proibidas Φ e a linguagem proibida $\mathscr{K}_f$ se atender às seguintes condições:*

1) Condição de u-diagnosticabilidade segura: L é u-diagnosticável segura em relação à Po, f, Φ e $\mathscr{K}_f$.

2) Condição de controlabilidade segura: Considere $s \in \Psi_L(f)$ e $u = u'\sigma_o \in L/s$ tal que $u \cap \mathscr{K}_f = \emptyset$, com $u' \in \Sigma^*$ e $\sigma_o \in \Sigma_o$. Suponha que a condição de u-diagnosticabilidade segura não é atendida

para u', mas que é atendida para u. Então, $\forall \omega = v\xi \in L/su$, *com* $v \in \Sigma^*$ *e* $\xi \in \Phi$, $\exists \sigma_c \in \Sigma_c$ *tal que* $\sigma_c \in \omega$.

Em palavras, para que o sistema seja controlável seguro pela u-diagnose é necessário que as ocorrências de falha sejam u-diagnosticáveis seguras e, após a u-diagnose, deve haver um evento controlável que possa ser usado para impedir a execução de uma cadeia proibida ξ. Na Proposição 4.3.2 são apresentadas as condições para que uma linguagem seja controlável segura pela u-diagnose. Com intuito de possibilitar que a análise da controlabilidade segura seja feita apenas com base no modelo do diagnosticador, consideramos que todos os eventos controláveis são observáveis. Essa mesma hipótese foi adotada por Watanabe (2019), e se justifica pelo fato de que normalmente nos sistemas de controle centralizado as ações de controle estão relacionadas a saídas do dispositivo de controle, as quais são naturalmente observáveis por parte do referido dispositivo.

Proposição 4.3.2 (Condições suficientes e necessárias para Controlabilidade Segura pela u-Diagnose)**.** *Considere uma linguagem L e um autômato* $G = (X, \Sigma, p, x_0)$ *que gera L, sendo* $\Sigma_c \subseteq \Sigma_o$. *Seja* $D = (X_D, \Sigma_o, \delta_D, x_{D0})$ *o diagnosticador seguro construído a partir de G. A linguagem L é controlável segura pela u-diagnose em relação a projeção Po, evento f e conjunto* Φ *se e somente se as seguintes condições são atendidas para todo* $x_D \in FPF$*:*
1) $x_D \notin X_D^B$.
2) $\nexists \omega_o \in \Sigma_{uc}^* : \hat{\delta}_D(x_D, \omega_o) = x'_D | x'_D \in FB$.

Prova.
(SOMENTE SE) A Prova é feita por contradição. Assuma que L é controlável segura pela u-diagnose, mas que a condição (1) desta proposição não é atendida. Assim, $\exists x_D \in FPF$ tal que $x_D \in X_D^B$ e, pela Proposição 4.3.1, pode-se afirmar que L não é u-diagnosticável segura, o que viola a condição (1) da Definição 4.3.3. Sendo assim, pode-se concluir que L não é controlável segura pela u-diagnose, o que contraria a hipótese inicial. Assumindo novamente que L é controlável segura pela u-diagnose, considere agora que a condição (1) desta proposição é atendida, mas que o mesmo não ocorre para a condição (2). Dessa forma, tem-se que $\exists x_D \in FPF$ para o qual $\exists \omega_o \in \Sigma_{uc}^* : \hat{\delta}_D(x_D, \omega_o) = x'_D$ sendo que $x'_D \in FB$. Como a condição (1) é atendida, pela Proposição 4.3.1 sabe-se que L é u-diagnosticável segura e assim, de acordo com a Definição 4.3.2 tem-se que $(\forall s \in \Psi_L(f))(\forall t = v\xi \in L/s$, com $v \in \Sigma^*$ e $\xi \in \Phi)$, $(\exists u < t : \sigma_o \in u \wedge u \cap \mathscr{K}_f = \emptyset$, com $\sigma o \in \Sigma_o)$. Sem perda de generalidade, assuma que $u = \sigma_o$. De acordo com a definição de FPF, tem-se que $\hat{\delta}_D(x_{D0}, s_o\sigma_o) = x_D \in FPF$, com $s_o = P_o(s)$ e $\sigma_o \in \Sigma_o$. Assim, $\hat{\delta}_D(x_{D0}, s_o\sigma_o\omega_o) = x'_D \in FB$, com $\omega_o \in \Sigma_o^*$. Uma vez que $u \cap \mathscr{K}_f = \emptyset$, pode-se afirmar que $\omega_o = P_o(\omega)$ é tal que $\omega = v\xi$, com $v \in \Sigma^*$ e $\xi \in \Phi$. Ainda, como $\omega_o \in \Sigma_{uc}^*$ e $\Sigma_c \subseteq \Sigma_o$, tem-se que $\omega \in P_o^{-1}(\omega_o)$ é tal que $\omega \in \Sigma_{uc}^*$. Portanto, para $s \in \Psi_L(f)$ e $u = \sigma_o \in L/s$ tal que $u \cap \mathscr{K}_f = \emptyset$, sendo que a condição de u-diagnosticabilidade segura é atendida para u, $\exists \omega = v\xi \in L/su$ para o qual $\nexists \sigma_c \in \Sigma_c : \sigma_c \in \omega$. Sendo assim, a condição (2) da Definição 4.3.3 não é satisfeita e, portanto, L não é controlável segura pela u-diagnose, o que contraria a hipótese inicial.

(SE) Assuma que a condição (1) desta proposição é atendida. Então, $\forall x_D \in FPF$ tem-se que $x_D \notin FB$. Assim, pela Proposição 4.3.1 pode-se afirmar que L é u-diagnosticável segura, de modo que a condição (1) da Definição 4.3.3 é satisfeita. Resta provar então que a condição (2) dessa definição também é atendida. Assuma agora que a condição (2) desta proposição é satisfeita, i.e., $\forall x_D \in FPF, \nexists \omega_o \in \Sigma_{uc}^*$ tal que $\hat{\delta_D}(x_D, \omega_o) = x'_D$, com $x'_D \in FB$. Em outras palavras, $\forall \omega_o \in \Sigma_o^*$ tal que $\hat{\delta_D}(x_D, \omega_o) = x'_D \in FB$ tem-se que $\exists \sigma_c \in \Sigma_c$ tal que $\sigma_c \in \omega_o$. Pela definição de FPF, tem-se que $x_D = \hat{\delta_D}(x_{D0}, s_o\sigma_o)$, com $s_o = P_o(s)$ tal que $s \in \Psi_L(f)$ e $\sigma_o \in \Sigma_o$. Assim, para $x'_D = \hat{\delta_D}(x_D, \omega_o)$ tem-se que $x'_D = \hat{\delta_D}(x_{D0}, s_o\sigma_o\omega_o)$ é tal que $\exists \sigma_c \in \omega_o$. Como L é u-diagnosticável segura, de acordo com a Definição 4.3.2 tem-se que $(\forall s \in \Psi_L(f))(\forall t = v\xi \in L/s$, com $v \in \Sigma^*$ e $\xi \in \Phi)$, $(\exists u < t : \sigma_o \in u \wedge u \cap \mathscr{K}_f = \emptyset$, com $\sigma_o \in \Sigma_o)$. Sem perda de generalidade, assuma que $u = \sigma_o$ e que $t = uv'\xi \in L/s$ é a cadeia que leva ao estado na planta que corresponde ao estado $x'_D \in FB$ no diagnosticador. Assim $\omega = v'\xi \in L/su$ é tal que $P_o(\omega) = \omega_o$. Como $\sigma_c \in \Sigma_c$ tal que $\sigma_c \in \omega_o$, então $\sigma_c \in \omega$. Dessa forma, a condição (2) da Definição 4.3.3 é satisfeita e, portanto, L é controlável segura pela u-diagnose.

□

Em palavras, as condições da Proposição 4.3.2 requerem que os estados do diagnosticador que fazem parte do conjunto FPF não sejam maus estados e que não exista uma cadeia ω_o a partir dos estados $x_D \in FPF$ que seja composta apenas por eventos não controláveis e que leve até algum estado pertencente ao conjunto dos primeiros maus estados.

Com base na Definição 4.3.3 e nas condições apresentadas na Proposição 4.3.2 podemos afirmar que a linguagem do exemplo da Figura 33 é controlável segura pela u-diagnose, pois os estados pertencentes ao conjunto FPF para este exemplo $(4N, 6N, 6F-NB)$ e $(2N, 7N, 7F-NB)$ não são maus estados e não existem cadeias compostas apenas por eventos não controláveis que levem a maus estados.

A linguagem do exemplo da Figura 31 não é controlável segura pela u-diagnose, pois a partir dos estados $(9N, 15F, 19N-NB)$ e $(12F, 13N, 18N-NB)$, pertencentes a FPF, existem cadeias compostas apenas por eventos não controláveis que levam aos estados $(9N, 15F, 19N-B)$ e $(12F, 13N, 18N-B)$, respectivamente, os quais são maus estados. Sendo assim, após a u-diagnose não existe um evento controlável que, se desabilitado, impede a ocorrência de uma cadeia proibida pós-falha.

A controlabilidade segura pela u-diagnose é classificada em três níveis: Forte, Regular e Fraca, mediante o menor valor das probabilidades de diagnose de falha nos estados incertos e certos de falha que não são maus estados e que possuem eventos controláveis ativos, que quando desabilitados impedem a ocorrência de um evento proibido ou conclusão de uma cadeia proibida pós-falha. Os parâmetros para classificação são definidos a seguir.

Seja Ξ o conjunto de estados do diagnosticador que são incertos ou certos de falha, não são maus estados, e que possuem eventos controláveis ativos, como $\Xi := \{x_D \in (X_D^U \cup X_D^C) \cap X_D^{NB} : \exists \sigma_c \in \Gamma(x_D)$, com $\sigma_c \in \Sigma_c \wedge \exists s_o \in \Sigma_o^* : \hat{\delta_D}(x_D, \sigma_c s_o) = x'_D$, tal que $x'_D \in X_D^B\}$. O conjunto Ξ

tem validade apenas para SEDEs que atendem as condições de controlabilidade segura pela u-diagnose. Nas próximas figuras, os estados do diagnosticador pertencentes ao conjuntos Ξ são ilustrador na cor azul ( ).

Para classificação do nível de controlabilidade segura pela u-diagnose deseja-se selecionar em cada caminho que a partir do estado inicial leva a um estado pertencente ao conjunto dos primeiros maus estados, o estado que possui a maior probabilidade de diagnose. Posteriormente, seleciona-se a menor probabilidade de diagnose entre esses caminhos, de modo a atender o pior cenário no procedimento de classificação do nível de controlabilidade segura pela u-diagnose da linguagem. Cada cadeia $s_o \in CCD(x'_D)$ que a partir do estado inicial x_{D0} leva a um estado $x'_D \in FB$ do diagnosticador é considerada um caminho.

O Algoritmo 4 apresenta como é selecionado o valor de referência para classificação da CSUD OPT(Ξ).

Algoritmo 4: Procedimento de seleção de estados para classificação do nível de CSUD.

```
   Dados: D,FB,Ξ
   Resultado: OPT(Ξ)
1  para cada estado x'_D ∈ FB não analisado faça
2      Calcule CCD(x'_D) para n=0;
3      para cada cadeia s_o ∈ CCD(x'_D) não analisada faça
4          para cada estado x_D ∈ Ξ não analisado faça
5              se ∃t_o ∈ s_o : δ̂_D(x_D0, t_o) = x_D então
6                  Ant(x'_D) = Ant(x'_D) ∪Ω_F(x_D);
7              senão
8              fim
9          fim
10         BPP = BPP ∪ max(Ant(x'_D));
11         Ant(x'_D) = Ant(x'_D) ∩ ∅ ;
12     fim
13 fim
14 OPT(Ξ)= min(BPP);
```

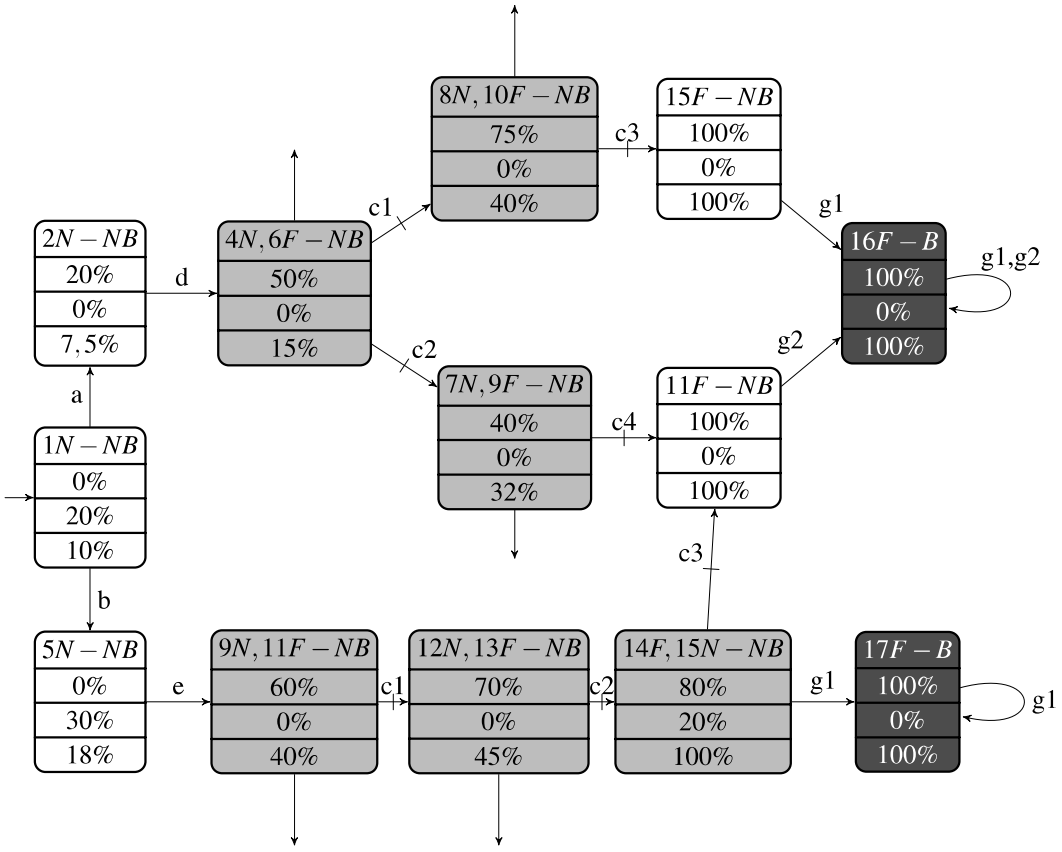
O Algoritmo 4 possui três estruturas de repetição. O laço de repetição da Linha 1 é utilizado para acessar os estados pertencentes ao conjunto dos primeiros maus estados do diagnosticador. Na Linha 2 é estabelecido o conjunto de cadeias que a partir do estado inicial leva ao primeiro mau estado analisado no ciclo, sem considerar ocorrências de ciclos ($n = 0$). O laço de repetição na Linha 3 é utilizado para verificar cada cadeia pertencente ao conjunto $CCD(x'_D)$ (cada cadeia representa um caminho a partir do estado inicial x_{D0} ao estado $x'_D \in FB$). O laço de repetição na Linha 4 é para acessar os estados $x_D \in \Xi$. Na Linha 5, a estrutura condicional verifica se o estado $x_D \in \Xi$ atual pode ser acessado por um prefixo da cadeia atual, ou seja, se o estado faz parte do caminho analisado. Caso a condição seja atendida, na Linha 6 armazenamos o valor da probabilidade de diagnose deste estado x_D no vetor Ant(x'_D) que é utilizado para armazenar todas as probabilidades de diagnose dos estados $x_D \in \Xi$ presentes no caminho representado

por s_o. Após o armazenamento de todas as probabilidades referentes ao caminho, na Linha 10 é armazenada a maior probabilidade do caminho atual no vetor BPP que é utilizado para armazenamento das maiores probabilidades de cada caminho. Na Linha 11, o vetor Ant(x'_D) é esvaziado para que seja analisado o próximo caminho. Por fim, na Linha 14 é atribuído a $OPT(\Xi)$ o menor valor de probabilidade de diagnose do vetor BPP.

Apresenta-se então a seguinte classificação para a controlabilidade segura pela u-diagnose em função do valor de $OPT(\Xi)$:

- Forte: $OPT(\Xi) \geq 0,75$
- Regular: $0,25 \leq OPT(\Xi) < 0,75$
- Fraca: $0 < OPT(\Xi) \leq 0,25$

Figura 38 – Diagnosticador para ilustração do método de classificação da controlabilidade segura pela u-diagnose, em que os estados pertencentes a Ξ são coloridos em azul.



Fonte: Elaborado pelo autor (2023)

A Figura 38 apresenta um trecho de um diagnosticador para ilustrar casos em que existe mais de um evento controlável que pode ser desabilitado em cada caminho que a partir do estado inicial x_{D0} leva a um estado $x'_D \in FB$. Nesse diagnosticador, tem-se $\Xi = \{(4N, 6F -$

$NB), (8N, 10F-NB), (7N, 9F-NB), (9N, 11F-NB), (12N, 13F-NB), (14F, 15N-NB)\}$. O conjunto dos primeiros maus estados neste exemplo é: $FB = \{(16F-B), (17F-B)\}$. Abaixo são exibidos os passos para classificação da controlabilidade segura pela u-diagnose para o exemplo apresentado na Figura 38, utilizando o Algoritmo 4:

$x'_D = 16F-B$
$CCD(16F-B) = adc1c3g1 + adc2c4g2 + bec1c2c3g2$
$s_o = adc1c3g1$
Os estados (4N,6F) e (8N,10F) satisfazem a condição da Linha 4.
Ant(x'_D) = [0,50 0,75]
BPP = [0,75]
Ant(x'_D) = []

$s_o = adc2c4g2$
Os estados (4N,6F) e (7N,9F) satisfazem a condição da Linha 4.
Ant(x'_D) = [0,50 0,40]
BPP = [0,75 0,50]
Ant(x'_D) = []

$s_o = bec1c2c3g2$
Os estados (9N,11F),(12N,13F) e (14F,15N) satisfazem a condição da Linha 4.
Ant(x'_D) = [0,60 0,70 0,80]
BPP = [0,75 0,50 0,80]
Ant(x'_D) = []

$x'_D = 17F-B$
$CCD(17F-B) = bec1c2g1$
$s_o = bec1c2g1$
Os estados (9N,11F) e (12N,13F) satisfazem a condição da Linha 4.
Ant(x'_D) = [0,60 0,70]
BPP = [0,75 0,50 0,80 0,70]
Ant(x'_D) = []

OPT(Ξ) = 0,50

De acordo com o memorial apresentado acima, a linguagem referente ao exemplo da Figura 38 tem controlabilidade segura regular pela u-diagnose.

Determinado o método de classificação do nível de CSUD, revisitamos a Figura 33 para mais um exemplo de classificação. Nesta, temos dois caminhos distintos que contêm cadeias

que levam a maus estados. Neste exemplo, temos o evento b nos estados $(2N, 7N, 7F - NB)$ e $(2N, 7F - NB)$ que quando desabilitado impede a ocorrência do evento proibido c após a falha. Em cada um destes estados existe uma probabilidade da falha ter acontecido: 4,04% no estado $(2N, 7N, 7F - NB)$ e 44,44% no estado $(2N, 7F - NB)$. De acordo com a classificação dos níveis de CSUD, esta linguagem tem controlabilidade segura fraca pela u-diagnose.

Além da diagnose de falhas, a prognose de falhas pode ser utilizada como parâmetro para o estabelecimento de controlabilidade segura em um SED. Apresentamos na Definição 4.3.4 uma noção de u-prognosticabilidade. Nesta noção, o objetivo é fornecer informações de probabilidades de ocorrências futuras de falha que são utilizadas posteriormente no estabelecimento de uma noção de controlabilidade segura pela u-prognose (CSUP).

Definição 4.3.4 (u-Prognosticabilidade)**.** *Uma linguagem prefixo-fechada L que é viva e que não contém ciclos de eventos não observáveis é dita ser u-prognosticável em relação à projeção Po e evento f se atender à seguinte condição:* $(\forall s \in \Psi_L(f))\{\ Prob(s, x_0) > 0\}$.

Em palavras, para que uma linguagem seja u-prognosticável basta que as probabilidades de ocorrência das cadeias s pertencentes ao conjuntos $\Psi_L(f)$ sejam não nulas. Sendo assim, toda linguagem viva que contém evento de falha é u-prognosticável. Essa definição parece sem propósito, no entanto, a partir desse conceito introduz-se a controlabilidade segura pela u-prognose, a qual possui aplicabilidade importante no contexto de SEDEs. A Definição 4.3.5 apresenta uma noção de controlabilidade segura pela u-prognose.

Definição 4.3.5 (Controlabilidade Segura pela u-Prognose)**.** *Uma linguagem prefixo-fechada L que é viva, não contém ciclos de eventos não observáveis e é u-prognosticável é dita ser controlável segura pela u-prognose em relação à projeção Po, evento f, conjunto de cadeias proibidas Φ e a linguagem proibida $\mathscr{K}_f$ se e somente se:* $\forall \omega = sv\xi \in L$, *com* $s \in \Psi_L(f)$, $v \in \Sigma^*$ *e* $\xi \in \Phi$, $\exists \sigma_c \in \Sigma_c$ *tal que* $\sigma_c \in s$ *ou* $v = t\sigma_c u$, *com* $t \in \Sigma_{uo}^*$ *e* $u \in \Sigma^*$.

Em palavras, a definição afirma que para que uma linguagem L seja controlável segura pela u-prognose, L deve ser u-prognosticável e, após a u-prognose, deve haver um evento controlável que possa ser desabilitado a fim de impedir a execução de cadeias proibidas após a falha. Esse evento controlável pode fazer parte da própria cadeia s (estar antes da falha) ou pode ser o primeiro evento observável após a falha na cadeia cuja continuidade leva à cadeia proibida. A Proposição 4.3.3 apresenta formalmente a condição para que uma linguagem L seja controlável segura pela u-prognose em uma análise do diagnosticador gerado a partir de L. Pelo mesmo motivo que foi apresentado na introdução das condições para controlabilidade segura pela u-diagnose, considera-se aqui que os eventos controláveis são observáveis, i.e., $\Sigma_c \subseteq \Sigma_o$.

Proposição 4.3.3 (Condições suficientes e necessárias para Controlabilidade Segura pela u-Prognose)**.** *Considere uma linguagem L e um autômato* $G = (X, \Sigma, p, x_0)$ *que gera L, sendo* $\Sigma_c \subseteq \Sigma_o$. *Seja* $D = (X_D, \Sigma_o, \delta_D, x_{D0})$ *o diagnosticador seguro construído a partir de G. A linguagem L é*

controlável segura pela u-prognose em relação a projeção Po, evento f e conjunto Φ *se e somente se,* $\forall \omega_o \in \Sigma_o^* : \hat{\delta}_D(x_{D0}, \omega_o) \in FB$, $(\exists r_o\sigma_c \in \overline{\omega_o} : \hat{\delta}_D(x_{D0}, r_o) \in X_D^N$, *com* $\sigma_c \in \Sigma_c)$.

Prova.

(SOMENTE SE) A Prova é feita por contradição. Assuma que L é controlável segura pela u-prognose, mas que $\exists \omega_o \in \Sigma_o^* : \hat{\delta}_D(x_{D0}, \omega_o) = x_D \in FB$ para a qual $\nexists r_o\sigma_c \in \overline{\omega_o}$ tal que $\hat{\delta}_D(x_{D0}, r_o) \in X_D^N$, com $\sigma_c \in \Sigma_c$ e $r_o \in \Sigma_{uc}^*$. Assuma então que para $\omega_o \in \Sigma_o^* : \hat{\delta}_D(x_{D0}, \omega_o) = x_D \in FB$, $r_o\sigma_c \in \overline{\omega_o}$ é tal que $\hat{\delta}_D(x_{D0}, r_o) = x_D^U \cup X_D^C$, com $\sigma_c \in \Sigma_c$ e $r_o \in \Sigma_{uc}^*$. Ainda, como $\hat{\delta}_D(x_{D0}, r_o) \notin x_D^N$, sabe-se qie para r tal que $P_o(r) = r_o$, tem-se que $f \in r$ e que $r = st$, com $\sigma_o \in t$ para algum $\sigma_o \in \Sigma_o$. Sem perda de generalidade, assuma que $r = s\sigma_o$. Assim, $r_o = s_o\sigma_o$, com $s_o = P_o(s)$. Uma vez que $r_o \in \Sigma_{uc}^*$ e $\Sigma_c \subseteq \Sigma_o$, então para $r_o = P_o(r)$ pode-se afirmar que $r \in \Sigma_{uc}^*$. Sendo assim, $s \in \Sigma_{uc}^*$ e $\sigma_o \in \Sigma_{uc} \cap \Sigma_o$. Agora, como $x_D \in FB$, sabe-se que a cadeia $\omega \in L : P_o(\omega) = \omega_o$ é tal que $\omega = sv\xi$, com $s \in \Psi_L(f)$, $v \in \Sigma^*$ e $\xi \in \Phi$. Dessa forma, $\exists \omega = sv\xi \in L$, com $s \in \Psi_L(f)$, $v \in \Sigma^*$ e $\xi \in \Phi$, para a qual $\nexists \sigma_c \in \Sigma_c$ tal que $\sigma_c \in s$ ou $v = t\sigma_c u$, com $t \in \sigma_{uo}^*$ e $u \in \Sigma^*$. Sendo assim, pela Definição 4.3.5, conclui-se que L não é controlável segura pela u-prognose, o que contraria a hipótese inicial.

(SE) A Prova é feita por contradição. A partir da suposição que L não é controlável segura pela u-prognose, pela Definição 4.3.5 tem-se que $\exists \omega = sv\xi \in L$, com $s \in \Psi_L(f)$, $v \in \Sigma^*$ e $\xi \in \Phi$, para a qual $\nexists \sigma_c \in \Sigma_c$ tal que $\sigma_c \in s$ ou $v = t\sigma_c u$, com $t \in \Sigma_{uo}^*$ e $u \in \Sigma^*$. Sabe-se ainda que $\omega_o = P_o(\omega)$ é tal que $\hat{\delta}_D(x_{D0}, \omega_o) = x_D \in FB$. Assuma que o primeiro evento controlável $\sigma_c \in \Sigma_c$ existente na cadeia ω esteja após algum evento observável existente após a falha, i.e., $\omega = sv\xi$ é tal que $\nexists \sigma_c \in s$ e $v = t\sigma_c u$, com $t \notin \Sigma_{uo}^*$. Sem perda de generalidade, assuma que $t = \sigma_o \in \Sigma_o$ e que $u = \varepsilon$, i.e., $v = \sigma_o\sigma_c$. Assuma agora que $r = s\sigma_o$. Então, $r_o = P_o(r) = s_o\sigma_o$. Sabe-se que no diagnosticador $r_o = P_o(r)$ é tal que $\hat{\delta}_D(x_{D0}, r_o) = x'_D \notin X_D^N$. Sendo assim, $\nexists r_o\sigma_c \in \overline{\omega_o} : \hat{\delta}_D(x_{D0}, r_o) = x'_D \in X_D^N$, com $\sigma_c \in \Sigma_c$, o que viola a condição desta proposição, contrariando a hipótese inicial.

□

A condição da Proposição 4.3.3 requer que para uma linguagem seja controlável segura pela u-prognose, todo mau estado pertencente ao conjunto dos primeiros maus estados, e toda cadeia que leve do estado inicial até esse mau estado, deve existir um evento controlável que parte de um estado normal e que, quando desabilitado, impede de se alcançar esse mau estado.

Analogamente a CSUD, a CSUP é classificada em níveis conforme os critérios a seguir. Seja Υ o conjunto dos estados do diagnosticador que são normais e que possuem eventos controláveis ativos que quando desabilitados impedem a execução de uma cadeia proibida após a falha. Formalmente, $\Upsilon = \{x_D \in X_D^N : \exists \sigma_c \in \Gamma(x_D)$, com $\sigma_c \in \Sigma_c \wedge \exists s_o \in \Sigma_o^* : \hat{\delta}_D(x_D, \sigma_c s_o) = x'_D$, tal que $x'_D \in FB\}$. O Algoritmo 5 apresenta como é selecionado o valor de referência OPT(Υ) para classificação da CSUP. Nas próximas figuras, os estados do diagnosticador pertencentes ao conjunto Υ são ilustrados na cor verde ( ).

O Algoritmo 5 possui estrutura similar ao Algoritmo 4. As diferenças consistem na utilização do conjunto Υ ao invés do conjunto Ξ e no armazenamento das probabilidades de

Algoritmo 5: Procedimento de seleção de estados para classificação do nível de CSUP.

Dados: D,FB,Υ
Resultado: OPT(Υ)
para cada *estado* $x'_D \in FB$ *não analisado* **faça**
  Calcule $CCD(x'_D)$ para n=0;
  para cada *cadeia* $s_o \in CCD(x'_D)$ *não analisada* **faça**
    para cada *estado* $x_D \in \Upsilon$ *não analisado* **faça**
      se $\exists t_o \in \overline{s_o} : \hat{\delta}_D(x_{D0}, t_o) = x_D$ **então**
        $\text{Ant}(x'_D) = \text{Ant}(x'_D) \cup \Omega(x_D) \cdot \Delta_F(x_D)^T$;
      senão
      fim
    fim
    $\text{BPP} = \text{BPP} \cup \max(\text{Ant}(x'_D))$;
    $\text{Ant}(x'_D) = \text{Ant}(x'_D) \cap \emptyset$;
  fim
fim
OPT(Υ)= min(BPP);

prognose ao invés das probabilidades de diagnose.

Apresenta-se então a seguinte classificação para a controlabilidade segura pela u-diagnose em função do valor de $OPT(\Upsilon)$:

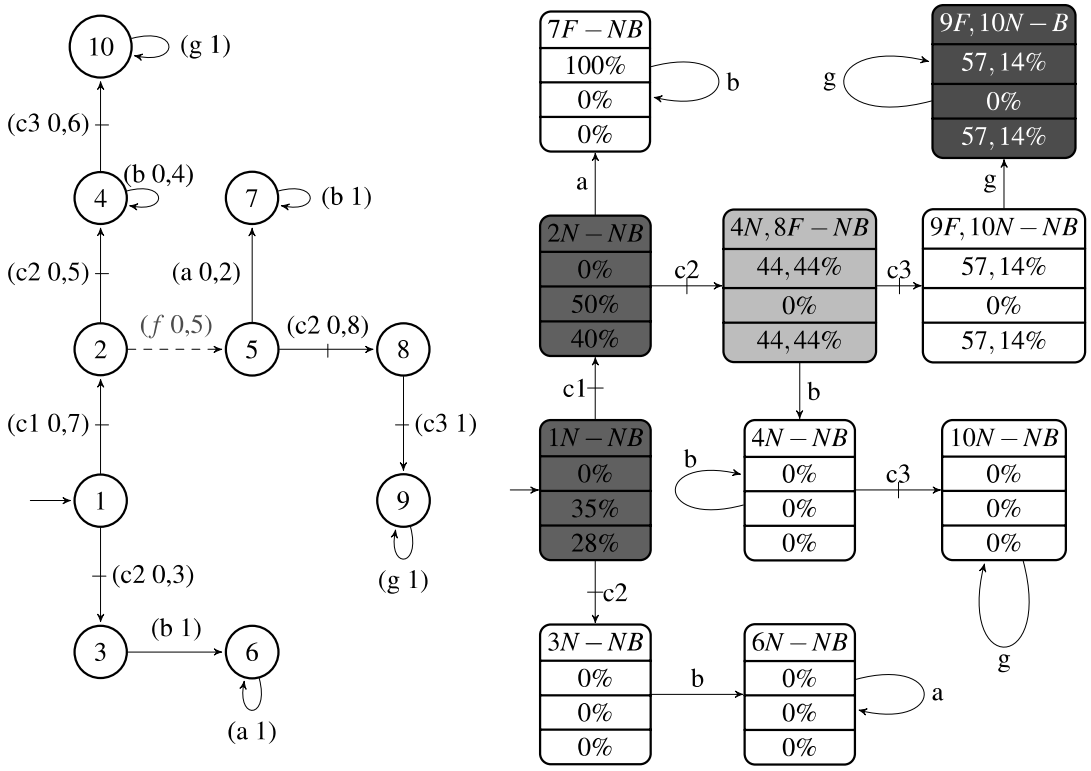
- Forte: $OPT(\Upsilon) \geq 0,75$
- Regular: $0,25 \leq OPT(\Upsilon) < 0,75$
- Fraca: $0 < OPT(\Upsilon) \leq 0,25$

O exemplo da Figura 39 apresenta uma linguagem que é controlável segura tanto pela u-diagnose quanto pela u-prognose. Neste exemplo, temos $\Xi = \{(4N, 8F)\}$ e $\Upsilon = \{(1N), (2N)\}$. Utilizando os Algoritmos 4 e 5, obtemos OPT(Ξ) = 44,44% e OPT(Υ) = 50%. Portanto, a linguagem é controlável segura regular pela u-diagnose e controlável segura regular pela u-prognose.

A Definição 4.3.6 apresenta noção de controlabilidade segura pelo coeficiente de anormalidade (CSCA) na qual se utilizam de forma conjunta as propriedades de u-diagnose e u-prognose. A utilização deste conceito tem o objetivo de relaxar as condições para controlabilidade segura com intuito de atender sistemas que não são controláveis seguros pela u-diagnose ou que não são controláveis seguros pela u-prognose.

Definição 4.3.6 (Controlabilidade Segura pelo Coeficiente de Anormalidade)**.** *Uma linguagem prefixo-fechada L que é viva e que não contém ciclos de eventos não observáveis é dita ser controlável segura pelo coeficiente de anormalidade em relação à projeção Po, evento f, conjunto de cadeias proibidas* Φ *e a linguagem proibida* $\mathscr{K}_f$ *se e somente se:* $\forall \omega \in L$ *tal que* $\omega = sv\xi$*, com* $s \in \Psi_L(f)$ *e* $\xi \in \Phi$*,* $\exists z \in \Sigma_c$ *tal que* $z \in \omega$*.*

Figura 39 – Exemplo para ilustração da classificação de CSUP.



Fonte: Elaborado pelo autor (2023)

Pela definição, para que uma linguagem seja controlável segura pelo coeficiente de anormalidade, todas as cadeias que a partir do estado inicial, que contém a falha e que são terminadas por uma cadeia proibida após a falha devem conter ao menos um evento controlável que, quando desabilitado, impeça a conclusão da cadeia proibida após a falha. Desse modo, têm-se uma união das noções de controlabilidade segura pela u-diagnose e controlabilidade segura pela u-prognose, pois na CSCA o evento controlável, cuja desabilitação impede a cadeia proibida após a falha pode estar tanto antes da falha quanto após a falha e até mesmo ser o último evento da cadeia proibida. A Proposição 4.3.4 apresenta formalmente a condição para que uma linguagem L seja controlável segura pelo coeficiente de anormalidade em uma análise do diagnosticador gerado a partir de L.

Proposição 4.3.4 (Condições suficientes e necessárias para Controlabilidade Segura pelo Coeficiente de Anormalidade)**.** *Considere uma linguagem L e um autômato* $G = (X, \Sigma, p, x_0)$ *que gera L. Seja* $D = (X_D, \Sigma_o, \delta_D, x_{D0})$ *o diagnosticador seguro construído a partir de G. A linguagem L é controlável segura pelo coeficiente de anormalidade em relação a projeção Po, evento f e conjunto* Φ *se e somente se,* $\forall \omega_o \in \Sigma_o^* : \hat{\delta}_D(x_{D0}, \omega_o) = x'_D \in FB, \exists \sigma_c \in \Sigma_c : \sigma_c \in \omega_o$.

Prova.

(SOMENTE SE) A Prova é feita por contradição. Assuma que L é controlável segura pelo coeficiente de anormalidade, mas que $\exists \omega_o \in \Sigma_o^* : \hat{\delta}_D(x_{D0}, \omega_o) = x'_D \in FB$, para a qual $\nexists \sigma_c \in \Sigma_c :$

$\sigma_c \in \omega_o$. Como $x'_D \in FB$, sabe-se que a cadeia $\omega \in \Sigma^*$ que na planta leva do estado inicial x_0 ao estado x' correspondente ao estado x'_D do diagnosticador é tal que $\omega = sv\xi$, com $s \in \Psi_L(f)$, $\xi \in \Phi$ e $P_o(\omega) = \omega_o$. Além disso, como $\omega_o \in \Sigma^*_{uc}$ e $\Sigma_c \subseteq \Sigma_o$, pode-se afirmar que $\omega \in \Sigma^*_{uc}$, i.e., $\nexists \sigma_c \in \Sigma_c : \sigma_c \in \omega$. Dessa forma, pela Definição 4.3.6, pode-se concluir que L não é controlável segura pelo coeficiente de anormalidade, o que contraria a hipótese inicial.
(SE) A Prova é feita por contradição. Suponha que a condição desta proposição seja atendida, mas que L não é controlável segura pelo coeficiente de anormalidade. A partir da suposição que L não é controlável segura pelo coeficiente de anormalidade tem-se, pela Definição 4.3.6, que $\exists \omega \in L$ tal que $\omega = sv\xi$, com $s \in \Psi_L(f)$ e $\xi \in \Phi$ para a qual $\nexists z \in \Sigma_c : z \in \omega$. Como $\omega = sv\xi$, sabe-se que a cadeia $\omega_o = P_o(\omega)$ leva do estado inicial x_{D0} do diagnosticador a um estado $x'_D \in FB$, i.e., $\hat{\delta}_D(x_{D0}, \omega_o) = x'_D \in FB$. Como $\nexists z \in \Sigma_c : z \in \omega$ e $\Sigma_c \subseteq \Sigma_o$, então $\nexists z \in \Sigma_c : z \in \omega_o$. Sendo assim, $\exists \omega_o \in \Sigma^*_o : \hat{\delta}_D(x_{D0}, \omega_o) = x'_D \in FB$ tal que $\nexists \sigma_c \in \Sigma_c : \sigma_c \in \omega_o$, o que viola a condição desta proposição, contrariando a hipótese inicial. □

Analogamente a CSUD e CSUP, a CSCA pode ser classificada em níveis conforme os critérios a seguir. Seja τ o conjunto dos estados do diagnosticador que não são maus estados e que possuem eventos controláveis ativos que quando desabilitados impedem a execução de uma cadeia proibida após a falha. Formalmente, $\tau = \{x_D \in X_D^{NB} : \exists \sigma_c \in \Gamma(x_D)$, com $\sigma_c \in \Sigma_c \wedge \exists s_o \in \Sigma^*_o : \hat{\delta}_D(x_D, \sigma_c s_o) = x'_D$, tal que $x'_D \in FB\}$. Vale destacar que o conjunto τ é a união dos conjuntos Ξ e Υ, i.e., $\tau = \Xi \cup \Upsilon$. O Algoritmo 6 apresenta como é selecionado o valor de referência OPT(τ) para classificação da CSCA.

Algoritmo 6: Procedimento de seleção de estados para classificação do nível de CSCA.

Dados: D,FB,τ
Resultado: OPT(τ)
para cada *estado* $x'_D \in FB$ *não analisado* **faça**
  Calcule $CCD(x'_D)$ para n=0;
  para cada *cadeia* $s_o \in CCD(x'_D)$ *não analisada* **faça**
    para cada *estado* $x_D \in \tau$ *não analisado* **faça**
      se $\exists t_o \in \overline{s_o} : \hat{\delta}_D(x_{D0}, t_o) = x_D$ **então**
        Ant(x'_D) = Ant(x'_D) $\cup (\Omega_F(x_D) + \Omega(x_D) \cdot \Delta_F(x_D)^T)$;
      senão
      fim
    fim
    BPP = BPP $\cup$ max(Ant(x'_D));
    Ant(x'_D) = Ant(x'_D) $\cap \emptyset$;
  fim
fim
OPT(τ)= min(BPP);

O Algoritmo 6 também possui estrutura similar ao Algoritmo 4. As diferenças consistem na utilização do conjunto τ ao invés do conjunto Ξ e no armazenamento dos coeficientes

de anormalidade ao invés das probabilidades de diagnose. Desta forma, é estabelecido para cada caminho o maior coeficiente de anormalidade, mas para classificação é utilizado o menor coeficiente entre os caminhos, de modo a atender o pior cenário.

Apresenta-se então a seguinte classificação para a controlabilidade segura pela u-diagnose em função do valor de $OPT(\tau)$:

- Forte: $OPT(\tau) \geq 0,75$
- Regular: $0,25 \leq OPT(\tau) < 0,75$
- Fraca: $0 < OPT(\tau) \leq 0,25$

4.4 ABORDAGEM *ONLINE* PARA CÁLCULO DE DIAGNOSE

Nas seções anteriores nesse capítulo, vimos que o procedimento de cálculo das probabilidades de diagnose do DEPE é feito *offline*. Esta abordagem possui uma desvantagem em relação a abordagem online de cálculo proposta por Thorsley e Teneketzis (2005), pois o cálculo *offline* não utiliza a informação fornecida pela observação de eventos. O procedimento *offline* de cálculo das probabilidades de diagnose para cada estado $x_D \in X_D$ é realizado a partir da suposição de todas as cadeias que a partir do estado inicial x_{D0} levam ao estado x_D. Utilizando este procedimento em linguagens que possuem ciclos, estabelecemos intervalos de probabilidades ao invés de valores atualizados e pontuais.

O exemplo da Figura 40 é utilizado para ilustrar a diferença entre cálculo *offline* e *online* para as probabilidades de diagnose.

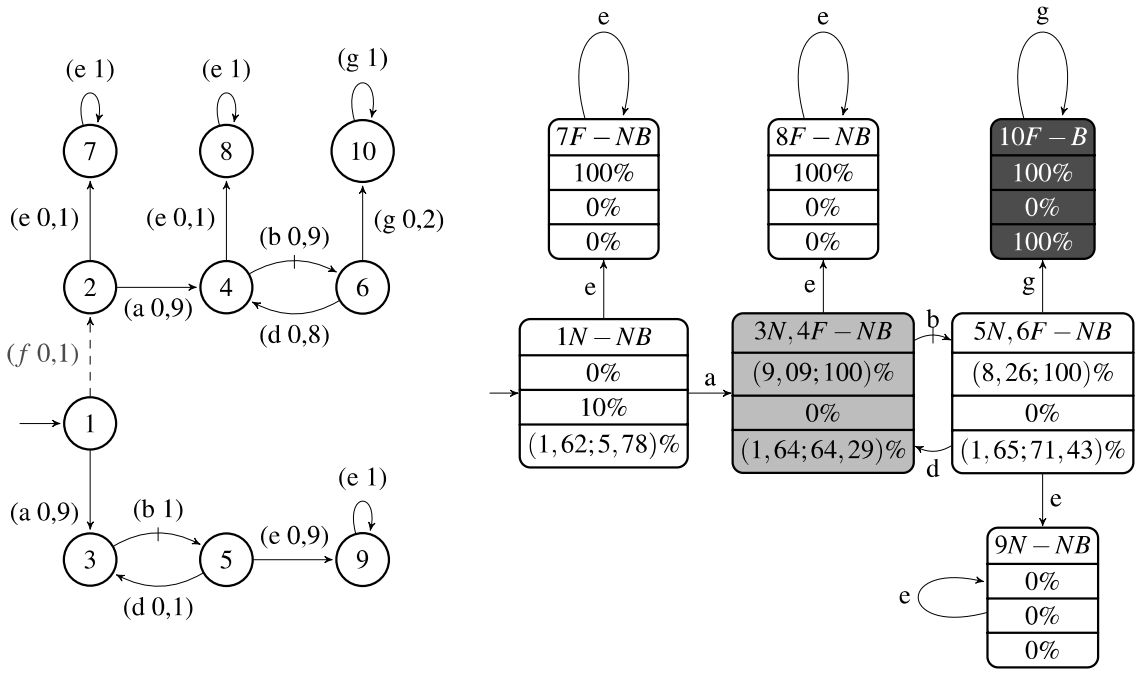
O memorial de cálculo abaixo apresenta os dois procedimentos: a) procedimento de cálculo para abordagem *offline*, considerando o conjunto de cadeias que alcança o estado (3N,4F - NB) no diagnosticador; b) procedimento de cálculo para a cadeia $s_o = abdbdbd$ que alcança o estado (3N,4F - NB).

$$CCD(3N,4F-NB) = a(bd)^*$$
$$CCG(3) = a(bd)^*$$
$$CCG(4) = fa(bd)^*$$

$$PD(3N)(0) = \frac{Prob(a,1)}{Prob(a,1)+Prob(fa,1)} = 90,91\%$$
$$PD(3N)(\infty) = \frac{Prob(a(bd)^n,1)}{Prob(a(bd)^n,1)+Prob(fa(bd)^n,1)} = 0\%$$

$$PD(4F)(0) = \frac{Prob(fa,1)}{Prob(a,1)+Prob(fa,1)} = 9,09\%$$
$$PD(4F)(\infty) = \frac{Prob(fa(bd)^n,1)}{Prob(a(bd)^n,1)+Prob(fa(bd)^n,1)} = 100\%$$

Figura 40 – Exemplo cuja faixa de probabilidade para a diagnose, calculada *offline*, é inviável para utilização em CTF *online*.



Fonte: Elaborado pelo autor (2023)

$$s_o = abdbdbd$$

$$\phi_{un}(s_o) = \begin{bmatrix}1\end{bmatrix}\begin{bmatrix}0,9 & 0,09\end{bmatrix}\begin{bmatrix}1 & 0\\ 0 & 0,9\end{bmatrix}\begin{bmatrix}0,1 & 0\\ 0 & 0,8\end{bmatrix}\begin{bmatrix}1 & 0\\ 0 & 0,9\end{bmatrix}\begin{bmatrix}0,1 & 0\\ 0 & 0,8\end{bmatrix}\begin{bmatrix}1 & 0\\ 0 & 0,9\end{bmatrix}\begin{bmatrix}0,1 & 0\\ 0 & 0,8\end{bmatrix}$$

$$\phi_{un}(s_o) = \begin{bmatrix}0,0009 & 0,0336\end{bmatrix}$$

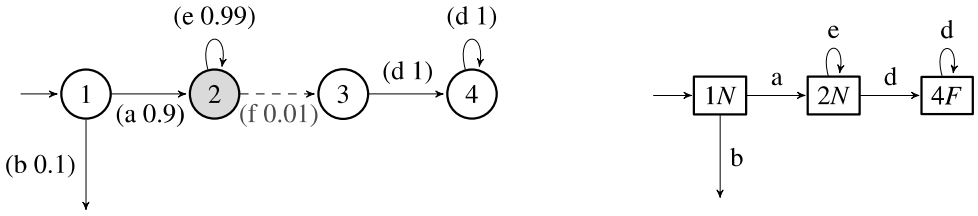
$$\phi(s_o) = \begin{bmatrix}0,0261 & 0,9739\end{bmatrix}$$

A abordagem *offline* resulta em um intervalo (9,09 ; 100)% para a probabilidade da falha ter acontecido. Os valores desta faixa equivalem aos valores do cálculo segundo a abordagem *online* para as cadeias $s_o = a$ e $s_o = a(bd)^n$ (com n suficientemente grande). A probabilidade de estar no rótulo 4F, calculada pela abordagem *online*, para qualquer cadeia $s_o = a(bd)^n$ está dentro da faixa de probabilidades calculada pela abordagem *offline*. No entanto, a faixa estabelecida pela abordagem *offline*, em geral, é ampla e não adequada para tomada de decisões de desabilitações. Para este mesmo exemplo, a abordagem *online* para o cálculo da probabilidade diagnose para a cadeia $s_o = abdbdbd$ resulta em uma probabilidade de 97,39% da falha ter acontecido. Esta informação é suficiente para a desabilitação do evento controlável b, para impedir que o evento proibido g aconteça após a falha.

O comparativo entre abordagens *offline* e *online* ilustra o impacto de cada método no cálculo das probabilidades de diagnose. No entanto, existe um aspecto que impacta na definição do intervalo de probabilidades de prognose. A Figura 41 apresenta um exemplo, no qual podemos notar que após a observação da cadeia $s_o = a$, atingimos o estado do diagnosticador de rótulo

único 2N. Neste estado, o conjunto de cadeias terminadas pelo evento de falha é representado por $\Psi_f(2) = \{e^*f\}$. De acordo com o procedimento de análise para a prognose apresentado nas seções anteriores, estabelecemos, para este exemplo, uma faixa de probabilidades para a ocorrência futura de falha. O primeiro valor é associado a probabilidade de ocorrência futura da falha sem ocorrência do auto-laço com evento e, enquanto o segundo valor representa a soma das probabilidade de todas as cadeias e^*f terminadas pela falha. Ou seja, teríamos o intervalo de probabilidades para ocorrência futura da falha de (1; 100)%. A subseção a seguir apresenta uma discussão sobre os modelos e métodos utilizados para análise das probabilidades de ocorrências futuras do evento de falha e as probabilidades de ocorrências futuras de eventos proibidos após a falha.

Figura 41 – Exemplo cujo modelo estático, para análise de prognose, é inviável para utilização em CTF *online*.



Fonte: Elaborado pelo autor (2023)

4.4.1 Discussão sobre metodologia de análise das probabilidade de cadeias futuras

A opção pela utilização da abordagem *offline* ou *online* para o cálculo das probabilidades de diagnose impacta nas probabilidades ponderadas de ocorrências futuras de falha e nas probabilidades de ocorrências futuras de eventos proibidos após a falha.

O procedimento de análise apresentado na seções anteriores utiliza o modelo que denominamos como estático. Pois a probabilidade de casa transição é fixa e independe do histórico de observação.

Nesta subseção, explicamos o motivo para a proposta de um modelo dinâmico. A abordagem *online* fornece um valor único de probabilidade de diagnose, o qual é atualizado mediante a observação. O modelo dinâmico apresentado na próxima seção tem o objetivo de replicar esta característica para as análises das probabilidade de cadeias futuras.

O procedimento de análise das probabilidades de cadeias futuras utilizando modelo dinâmico considera apenas a probabilidade de cadeias futuras que não contém ciclos. Dessa forma, ao invés de uma faixa de probabilidades, tem-se um único valor que é sempre atualizado conforme o estado é revisitado. Além disso, propõe-se um método de atualização das probabilidades de cada transição no modelo da planta sob análise mediante o histórico de observação. Estas duas alterações no procedimento de análise buscam modelar duas ocasiões:

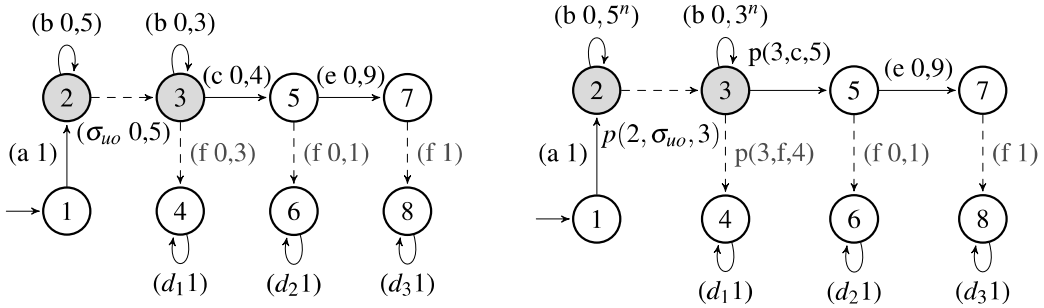
- Justiça entre a frequência de eventos com diferentes probabilidades em um estado que faz parte de um ciclo.
- Aumento da suscetibilidade a falha mediante desgaste por operação.

4.5 MODELO DINÂMICO PARA CÁLCULO DE PROGNOSE

O modelo dinâmico para análise de prognose consiste na substituição das probabilidades de transições com valores estáticos por funções de transição probabilísticas, as quais denominamos como probabilidades dinâmicas.

A Figura 42 apresenta um comparativo entre o modelo que utiliza probabilidades estáticas e o modelo com utilização de probabilidades dinâmicas. Inicialmente apresentamos a atualização das probabilidades de transições com base na repetição de um determinado evento ao observamos o histórico de observação via diagnosticador. Neste exemplo, o evento em questão é o evento *b*. A cada ocorrência do evento *b* o índice *n* é incrementado em uma unidade. Este índice é iniciado com valor 1, pois está associado à probabilidade da ocorrência do evento *b* pela primeira vez.

Figura 42 – Comparativo entre modelo estático (esquerda) e dinâmico (direita) para cálculo de prognose



Fonte: Elaborado pelo autor (2023)

Desta forma, o modelo base ao invés de contar com uma probabilidade estática para cada transição, ele tem uma função probabilística dinâmica para cada transição, conforme Equação (13).

$$FT(n) = \delta_P \cdot FPO + FT(0) \tag{13}$$

em que $FT(n)$ é a função probabilística dinâmica em função do índice n; δ_P é a variação de probabilidade a ser redistribuída; FPO é o fator de ponderação; $FT(0)$ é o valor de probabilidade inicial da transição.

É importante ressaltar que ao alterarmos a probabilidade de uma determinada transição, temos que rebalancear as probabilidades das demais transições que saem deste estado para que a soma ainda seja 100%.

A seguir apresentamos o procedimento de determinação das funções probabilísticas dinâmicas para o exemplo da Figura 42.

$p(3,f,4) = (0,3-0,3^n) \cdot \frac{0,3}{0,3+0,4} + 0,3$
$p(3,c,5) = (0,3-0,3^n) \cdot \frac{0,4}{0,3+0,4} + 0,4$
$p(2,\sigma_{uo},3) = 1-0,5^n$

O estado 3 possui um auto-laço com o evento b e duas transições de saída com os eventos f e c. No modelo estático, que permanece sendo utilizado para as análises de diagnose, a probabilidade da transição do auto-laço com o evento b é de 30%. Esta probabilidade é substituída pela função $p(3,b,3) = 0,3^n$ em alusão a probabilidade de repetições de eventos de um ciclo. Neste caso, após a primeira ocorrência do evento b a probabilidade da ocorrência do segundo evento b passa a ser de 9%. O delta de 21% deve ser redistribuído de forma ponderada entre os eventos f e c, conforme apresentado no memorial de cálculo descrito acima.

Em seguida, apresentamos a análise de prognose de falhas para o exemplo da Figura 42 contemplando três diferentes cenários. Neste procedimento, é adotado o modelo com probabilidades de transições dinâmicas e são calculadas apenas as probabilidades de cadeias imediatas terminadas pelo evento de falha (sem ocorrências de ciclos). Se fosse utilizado o conceito de estabelecimento de faixa de probabilidades utilizando o modelo com transições definidas por probabilidades estáticas, a faixa seria de (35; 100)% para ocorrência futura de falha após observação da cadeia $s_o = a$.

- Análise de cadeias imediatas terminadas por evento de falha.
- $\Psi_f(2N) = \{\sigma_{uo}f, \sigma_{uo}cf, \sigma_{uo}cef\} \quad \Psi_f(3N) = \{f, cf, cef\}$

Primeiro Cenário:

$s_o = a \quad n = 1 \quad x_D = (2N) \quad \Omega(2N) = [1]$
$p(2,\sigma_{uo},3)_{(n=1)} = 0,5 \qquad p(3,f,4)_{(n=1)} = 0,3 \qquad p(3,c,5)_{(n=1)} = 0,4$

$PF(\Psi_f(2N)) = Prob(\sigma_{uo}f,2) + Prob(\sigma_{uo}cf,2) + Prob(\sigma_{uo}cef,2)$
$PF(\Psi_f(2N)) = 0,5 \cdot 0,3 + 0,5 \cdot 0,4 \cdot 0,1 + 0,5 \cdot 0,4 \cdot 0,9 \cdot 1$
$PF(\Psi_f(2N)) = 0,35$
$\Delta_F = [0,35]$

$\Omega(x_D) \cdot \Delta_F(x_D)^T = 0,35 = 35\%$

Segundo Cenário:

$s_o = abbbb \quad n = 5$
$x_D = (2N, 3N) \quad \Omega(2N, 3N) = [0,5911 \;\; 0,4089]$

$p(2, \sigma_{uo}, 3)_{(n=5)} = 0,9688$
$p(3, f, 4)_{(n=5)} = 0,4275$
$p(3, c, 5)_{(n=5)} = 0,5700$

$PF(\Psi_F(2N)) = Prob(\sigma_{uo} f, 2) + Prob(\sigma_{uo} cf, 2) + Prob(\sigma_{uo} cef, 2)$
$PF(\Psi_f(2N)) = 0,9688 \cdot 0,4275 + 0,9688 \cdot 0,5700 \cdot 0,1 + 0,9688 \cdot 0,5700 \cdot 0,9 \cdot 1$
$PF(\Psi_f(2N)) = 0,9664$

$PF(\Psi_f(3N)) = Prob(f, 3) + Prob(cf, 3) + Prob(cef, 3)$
$PF(\Psi_f(3N)) = 0,4275 + 0,5700 \cdot 0,1 + 0,5700 \cdot 0,9 \cdot 1$
$PF(\Psi_f(3N)) = 0,9975$

$\Delta_F = [0,9664 \;\; 0,9975]$

$\Omega(x_D) \cdot \Delta_F(x_D)^T = 0,9787 = 97,87\%$

Terceiro Cenário:

$s_o = abbbbbbbbbbbbbbbbbbb \quad n = 20$
$x_D = (2N, 3N) \quad \Omega(2N, 3N) = [0,5714 \;\; 0,4286]$
$p(2, \sigma_{uo}, 3)_{(n=20)} \approx 1,0000$
$p(3, f, 4)_{(n=20)} = 0,4286$
$p(3, c, 5)_{(n=20)} = 0,5714$

$PF(\Psi_f(2N)) = Prob(\sigma_{uo} f, 2) + Prob(\sigma_{uo} cf, 2) + Prob(\sigma_{uo} cef, 2)$
$PF(\Psi_f(2N)) = 1 \cdot 0,4286 + 1 \cdot 0,5714 \cdot 0,1 + 1 \cdot 0,5714 \cdot 0,9 \cdot 1$
$PF(\Psi_f(2N)) \approx 1$

$PF(\Psi_f(3N)) = Prob(f, 3) + Prob(cf, 3) + Prob(cef, 3)$
$PF(\Psi_f(3N)) = 0,4286 + 0,5714 \cdot 0,1 + 0,5714 \cdot 0,9 \cdot 1$
$PF(\Psi_f(3N)) \approx 1$

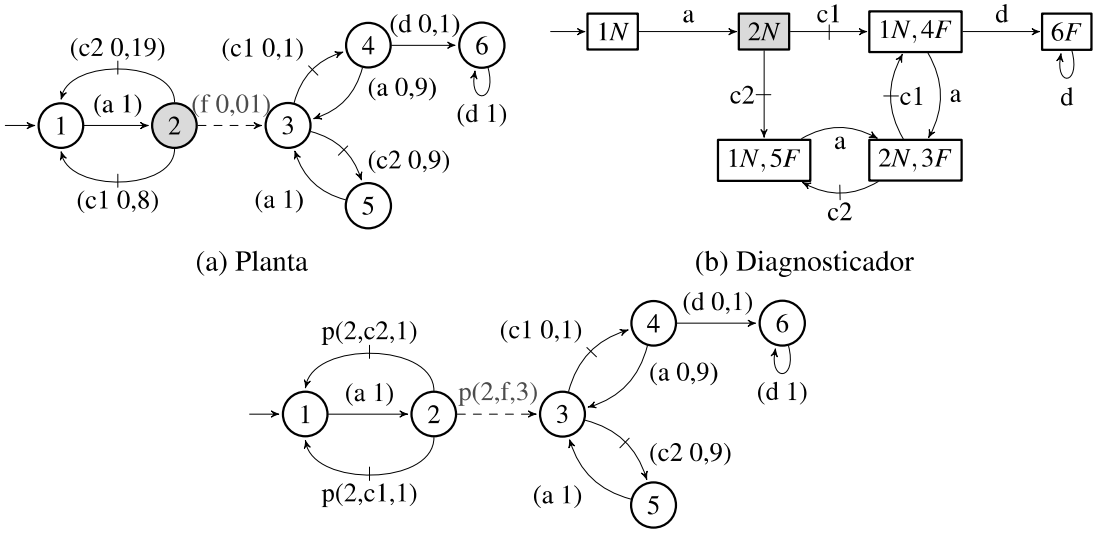
$$\Delta_F = [1 \;\; 1]$$

$$\Omega(x_D) \cdot \Delta_F(x_D)^T = 1 = 100\%$$

Ao avaliarmos os três cenários, verificamos que à medida que observamos as repetições das transições com o evento b, uma nova transição com o evento b tem sua probabilidade reduzida e as demais transições com eventos que saem dos ciclos e levam a caminhos que possuem o evento de falha se tornam maiores. Desse modo, a probabilidade de ocorrência futura de falha que no primeiro cenário era de 35% atinge o valor de aproximadamente 100% no terceiro cenário.

A definição dos termos da função probabilística dinâmica é apresentada para um exemplo (Figura 42) em que há ciclos apenas com um evento. Se houverem ciclos com mais eventos, deve-se manter um índice associado a repetição de cada evento e as funções probabilísticas dinâmicas devem ser atualizadas de modo a garantir que a soma das probabilidades das transições de saída de um estado $x \in X$ deve ser sempre 100% e que a variação de probabilidade associada a um ciclo deve ser sempre redistribuída ponderadamente às demais transições de saída deste estado. A Figura 43 apresenta um exemplo que consta com ciclos associados a dois eventos $c1$ e $c2$.

Figura 43 – Exemplo para ilustração da função probabilística dinâmica quando há ciclos associados a mais de um evento.



(a) Planta

(b) Diagnosticador

(c) Modelo Dinâmico

Fonte: Elaborado pelo autor (2023)

Abaixo são exibidas as funções probabilísticas dinâmicas para o exemplo da Figura 43.

$$p(2,c1,1) = 0,8^n + (0,19 - 0,19^m) \cdot \frac{0,8^n}{1-0,19^m}$$

$$p(2,c2,1) = 0,19^m + (0,8 - 0,8^n) \cdot \frac{0,19^n}{1-0,8^n}$$

$$p(2,f,3) = 0,01 + (0,19 - 0,19^m) \cdot \frac{1-0,8^n-0,19^m}{1-0,19^m} + (0,8 - 0,8^n) \cdot \frac{1-0,8^n-0,19^m}{1-0,8^n}$$

É possível observar que no estado 2 existem dois ciclos $(c1a)^*$ e $(c2a)^*$. Aos ciclos são associados os índices m e n, ambos iniciados com o valor 1, os quais indicam a m-ésima ocorrência do evento $c2$ e a n-ésima ocorrência do $c1$. A variação da probabilidade do ciclo associado a $c1$ é redistribuída ponderadamente entre $c2$ e f. Assim como, a variação da probabilidade do ciclo associado a $c2$ é redistribuída ponderadamente para $c1$ e f. Dessa forma, na função probabilística dinâmica com o evento de falha f, existem dois termos $\delta_P \cdot FPO$.

A Tabela 5 apresenta uma breve descrição das abordagens *offline* e *online* e dos modelos dinâmico e estático.

Tabela 5 – Características das abordagens *offline* e *online* e dos modelos dinâmico e estático.

Modelo ou Abordagem	**Descrição**
Abordagem offline (Diagnose)	Probabilidades de estar em cada rótulo do estado sem considerar a observação. Faz-se uma suposição de todas as cadeias que levam a um estado e calcula-se um valor ou uma faixa de valores de probabilidades (quando há ciclos com diferentes probabilidades no autômato da planta).
Abordagem online (Diagnose)	Probabilidades de estar em cada rótulo do estado considerando a observação.
Modelo estático (Prognose)	Probabilidades de cada transição com valores fixos.
Modelo dinâmico (Prognose)	Probabilidades de cada transição com valores dinâmicos (atualizados mediante observação de eventos em tempo de execução).

Fonte: Elaborado pelo autor (2023)

4.6 DIAGNOSTICADOR ESTOCÁSTICO COM SAÍDAS: ABORDAGEM COM PROBABILIDADES DINÂMICAS

Apresentada a característica negativa do DEPE para utilização em CTF *online* e estabelecida uma discussão sobre as diferentes abordagens em relação às probabilidades de prognose, apresentamos uma alternativa similar ao DEPE, porém com valores únicos ao invés de faixas de probabilidades. Essa alternativa é chamada de Diagnosticador Estocástico com Probabilidades Dinâmicas (DEPD).

Nesta metodologia, os estados do DEPD possuem os mesmos campos do modelo de estado do DEPE, vide Figura 23a. No entanto, o procedimento de cálculo das probabilidades

exibidas em cada campo sofre alterações. Estas alterações são apresentadas nesta seção.

Para o campo 2, ao invés de realizar um cálculo com a suposição de todas as cadeias que atingem o estado x_D, leva-se em consideração apenas a cadeia s_o observada. Os campos 3 e 4 são obtidos da mesma forma do DEPE, porém são ponderados pelo campo 2, que agora é calculado de forma *online*.

A partir do exemplo da Figura 40 é apresentado a seguir o procedimento de cálculo das probabilidades para os campos 2,3 e 4 do EDD alcançado no DEPD mediante a observação da cadeia $s_o = abdbdb$.

O cálculo da probabilidade do campo 2, pode ser feito de acordo com o procedimento apresentado no Algoritmo 1, ao considerarmos CCD(x_D) = s_o. Não há alteração nos métodos para obtenção dos vetores $\Delta_F(x_D)$ e $\Delta_{EP}(x_D)$ e nas Equações para cálculo das probabilidades ponderadas de ocorrência futura de falha e para o cálculo das probabilidades ponderadas de ocorrência futura de evento proibido após a falha permanecem os mesmos.

Cálculo do campo 2:

$s_o = abdbdb$

CCD(5N,6F-NB) = $\{abdbdb\}$

CCG(5) = $\{abdbdb\}$

CCG(6) = $\{fabdbdb\}$

$$PD(5N) = \frac{Prob(abdbdb,1)}{Prob(abdbdb,1)+Prob(fabdbdb,1)} = \frac{0{,}9\cdot1\cdot0{,}1\cdot1\cdot0{,}1\cdot1}{0{,}9\cdot1\cdot0{,}1\cdot1\cdot0{,}1\cdot1+0{,}1\cdot0{,}9\cdot0{,}9\cdot0{,}8\cdot0{,}9\cdot0{,}8\cdot0{,}9} = 17{,}65\%$$

$$PD(6F) = \frac{Prob(fabdbdb,1)}{Prob(abdbdb,1)+Prob(fabdbdb,1)} = \frac{0{,}1\cdot0{,}9\cdot0{,}9\cdot0{,}8\cdot0{,}9\cdot0{,}8\cdot0{,}9}{0{,}9\cdot1\cdot0{,}1\cdot1\cdot0{,}1\cdot1+0{,}1\cdot0{,}9\cdot0{,}9\cdot0{,}8\cdot0{,}9\cdot0{,}8\cdot0{,}9} = 82{,}35\%$$

$$\Omega(5N,6F-NB) = [0{,}1765 \quad 0{,}8235]$$

$$\Omega_F(5N,6F-NB) = 82{,}35\%$$

Cálculo do campo 3:

$\Psi_f(5N) = \emptyset$

PF(5N) = 0%

$\Psi_f(6F) = \emptyset$

PF(6F) = 0%

$\Delta_F(5N,6F-NB) = [0 \quad 0]$

$$\Omega(x_D)\cdot\Delta_F(x_D)^T = \begin{bmatrix}0{,}1765 & 0{,}8235\end{bmatrix}\begin{bmatrix}0\\0\end{bmatrix} = 0\%$$

Cálculo do campo 4:

$\eta(5N) = \emptyset$

PEP(5N) = 0%

$\eta(6F) = gg*$

PEP(6F) = 20%

$\Delta_{EP}(5N, 6F - NB) = [0 \;\; 0,2]$

$$\Omega(x_D) \cdot \Delta_{EP}(x_D)^T = \begin{bmatrix} 0,1765 & 0,8235 \end{bmatrix} \begin{bmatrix} 0 \\ 0,2 \end{bmatrix} = 16,47\%$$

A Figura 44 apresenta um comparativo entre o estados do DEPE e do DEPD alcançados após a observação da cadeia s_o para o exemplo da Figura 40.

Figura 44 – Comparativo entre estado do DEPE e estado do DEPD para o exemplo da Figura 40, com $s_o = abdbdb$.

$5N, 6F - NB$
$(8,26; 100)\%$
0%
$(1,65; 71,43)\%$

$5N, 6F - NB$
$82,35\%$
0%
$16,47\%$

Fonte: Elaborado pelo autor (2023)

Todas as probabilidades apresentadas nos estados do DEPD são constantemente atualizadas mediante a observação de eventos. Dessa forma, optamos por exibir o diagnosticador lógico e apresentar apenas as probabilidades atualizadas para o estado atual, o qual denominamos Estado Dinâmico do Diagnosticador (EDD).

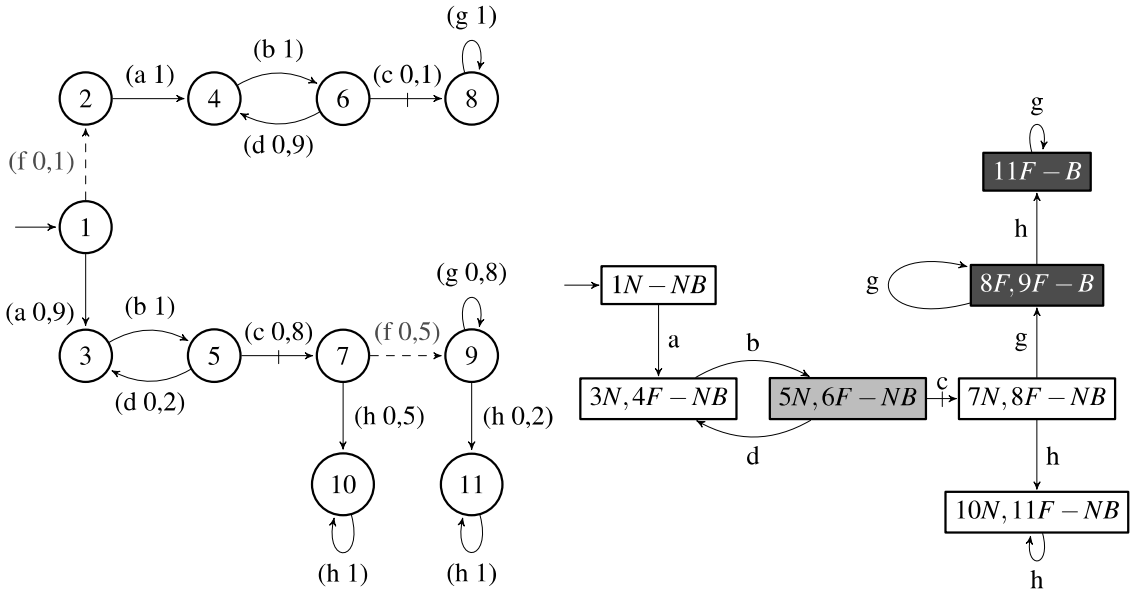
O exemplo apresentado na Figura 45 é utilizado para ilustrar as alterações nos valores de probabilidades dos EDDs para diferentes cadeias. Este exemplo contém um ciclo de estados incertos que corresponde a dois ciclos com probabilidades distintas no autômato da planta. A composição do EDD é feita conforme as duas abordagens para cálculo da prognose. Dessa forma, também podemos comparar a diferença das probabilidades para análise da prognose ao utilizarmos modelos estáticos ou dinâmicos.

Neste exemplo são analisadas as cadeias $s_o = a(bd)^m b$ à medida que m é incrementado. O estado lógico alcançado com s_o é o $(5N, 6F - NB)$. Neste estado, temos o evento controlável c ativo. Ou seja, é possível desabilitá-lo para impedir a ocorrência do evento proibido g que não deve acontecer depois da falha (nos estados 8 e 9 da planta). É válido ressaltar que nesse estado, a falha pode ou não ter acontecido e que a falha pode ou não acontecer no futuro. Dessa forma, as probabilidades se tornam extremamente importantes para a tomada de qualquer decisão numa topologia de CTF.

O Apêndice B apresenta um código fonte escrito para o *software* Matlab ©. Com a utilização deste, pode-se calcular as probabilidades relacionadas ao exemplo da Figura 45.

Temos para este exemplo $\Psi_f(5) = cf$ e $\Psi_f(6) = \emptyset$. A Tabela 6 apresenta as Equações para transições dinâmicas para análise de prognose levando em consideração o histórico de observação e o valor da probabilidade calculado para diferentes valores de n. Vale destacar que o

Figura 45 – Exemplo para análise das probabilidades do EDD.



(a) Planta (b) Diagnosticador

Fonte: Elaborado pelo autor (2023)

índice m é para a quantidade de repetições do ciclo bd e o índice n é utilizado para cálcular a probabilidade de ocorrência de um determinado evento pela n-ésima vez. Simplificando, para $m = 0$, temos $n = 1$.

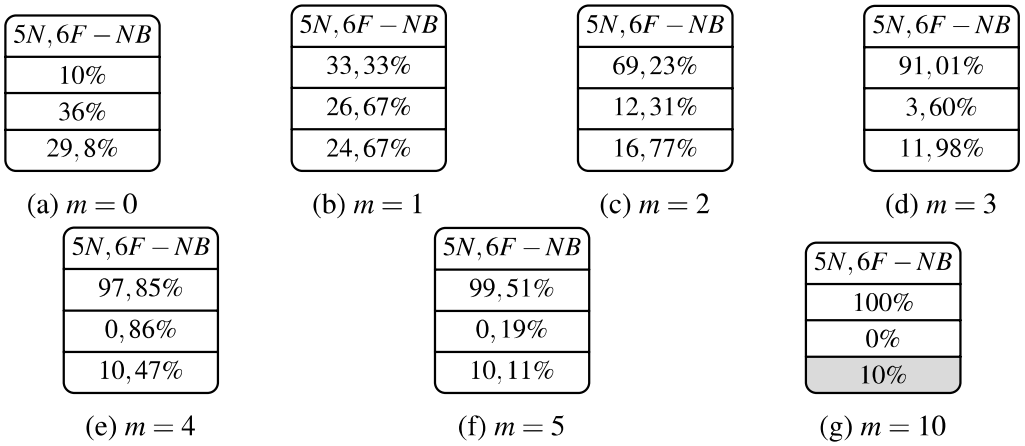
Tabela 6 – Funções de transições dinâmicas para o exemplo da Figura 45.

Função	n=1	n=2	n=3	n=4	n=5	n=10
$p(5,d) = 0,2^n$	0,2	0,04	0,008	0,0016	0,00032	0,0000001024
$p(6,d) = 0,9^n$	0,9	0,81	0,729	0,6561	0,59049	0,3486784401
$p(5,c) = (0,2-0,2^n)+0,8$	0,8	0,96	0,992	0,9984	0,99968	0,9999998976
$p(6,c) = (0,9-0,9^n)+0,1$	0,1	0,19	0,271	0,3439	0,40951	0,6513215599

Fonte: Elaborado pelo autor (2023)

A Figura 46 apresenta os EDDs resultantes após a observação da cadeia $s_o = a(bd)^m b$. Para o cálculo das probabilidades de ocorrência futura de falha foi utilizado o modelo estático de avaliação da prognose. Avaliando a imagem, podemos notar que a medida que m aumenta, a probabilidade da falha ter acontecido torna-se maior e a probabilidade da falha acontecer no futuro torna-se menor. Se considerarmos a cadeia $s_o = ab$, ou seja nenhuma repetição do ciclo, temos uma probabilidade de 10% da falha ter acontecido e de 36% da falha acontecer no futuro. Em contraponto, com apenas dez repetições do ciclo, a probabilidade da falha ter acontecido é aproximadamente 100% e da falha acontecer no futuro 0%. Como utilizamos neste cálculo o modelo estático para análise das probabilidades de eventos futuros, a probabilidade de ocorrência do evento proibido após a falha tende a 10% conforme m é incrementado.

Figura 46 – EDD obtidos para a cadeia $s_o = a(bd)^m b$ para diferentes valores de m - Modelo estático para análise de prognose.



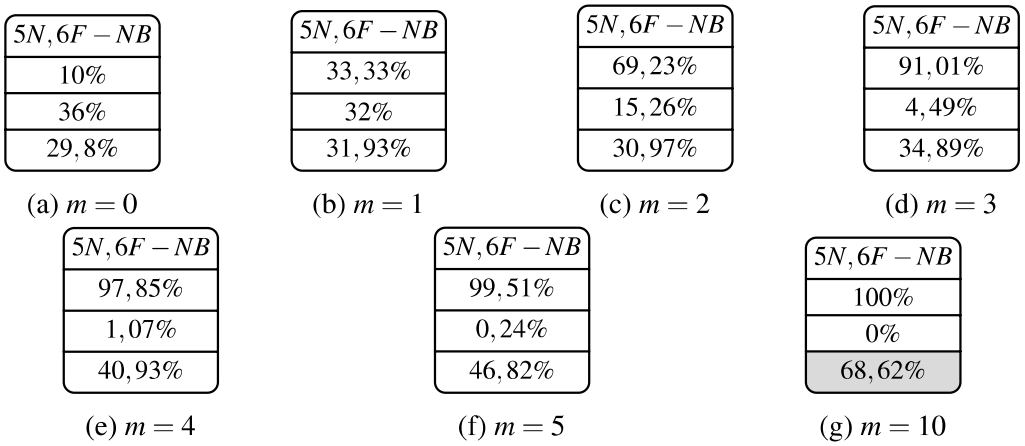
(a) $m = 0$ (b) $m = 1$ (c) $m = 2$ (d) $m = 3$

(e) $m = 4$ (f) $m = 5$ (g) $m = 10$

Fonte: Elaborado pelo autor (2023)

Em qualquer exemplo analisado que haja um ciclo de eventos, mas que possua um evento ativo que interrompe o ciclo, a probabilidade de ficar infinitamente no ciclo é nula. Um ponto que pode ser analisado é que à medida que o ciclo se repete várias vezes, a probabilidade de ocorrência do evento que interrompe o ciclo torne-se mais significativa. Esse comportamento pode ser modelado com a utilização de uma análise de prognose baseada em um modelo com probabilidades de transições dinâmicas que são atualizadas conforme o histórico de observação.

Figura 47 – EDD obtidos para a cadeia $s_o = a(bd)^m b$ para diferentes valores de m - Modelo dinâmico para análise de prognose.



(a) $m = 0$ (b) $m = 1$ (c) $m = 2$ (d) $m = 3$

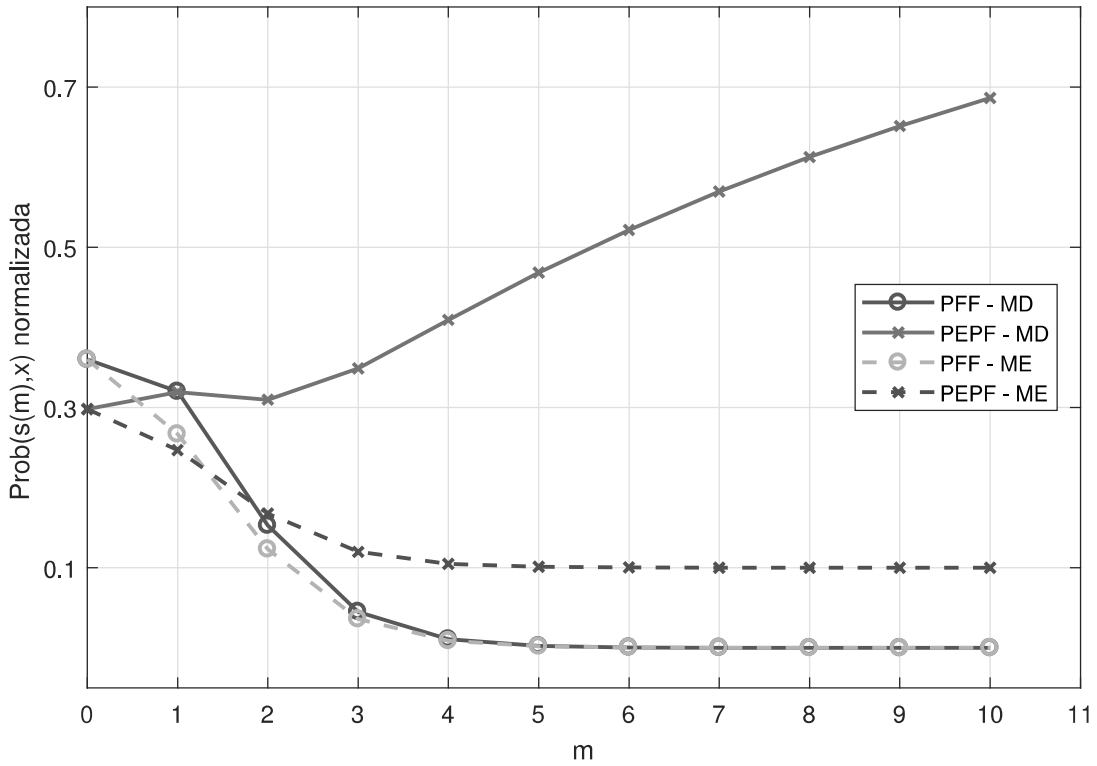
(e) $m = 4$ (f) $m = 5$ (g) $m = 10$

Fonte: Elaborado pelo autor (2023)

Os EDDs apresentados na Figura 47 possuem valores distintos para as probabilidades de ocorrência futura da falha em relação aos EDDs da análise estática. Estas diferenças não são tão significativas pois à medida que o ciclo se repete a probabilidade da falha ter acontecido tende a 100% e a probabilidade da falha acontecer no futuro tende a 0%. No entanto, o comportamento

da probabilidade de ocorrência de evento proibido após a falha é bem interessante. Após a ocorrência de 10 ciclos da cadeia *ab*, temos uma probabilidade de 100% de estar no rótulo $6F$, no qual a probabilidade atualizada de ocorrência da cadeia proibida *cg* é de 68,62% em contraste aos 10% da análise estática. Nesses dois casos, as decisões de desabilitação com certeza seriam diferentes. O gráfico apresentado na Figura 48 mostra a variação das probabilidades de ocorrência futura de falha e de ocorrência futura de cadeia proibida após a falha em análises com modelo estático e modelo dinâmico.

Figura 48 – Avaliação das probabilidades futuras de falha e evento proibido - ME x MD



Fonte: Elaborado pelo autor (2023)

em que PFF é a Probabilidade de Falha Futura (Valor exibido no campo 3 dos EDDs); PEPF é a Probabilidade de Evento Proibido Futuro após a falha (Valor exibido no campo 4 dos EDDs); MD indica que foi utilizado o Modelo Dinâmico para os cálculos, enquanto ME indica a utilização do Modelo Estático.

4.7 CONTROLABILIDADE SEGURA EM SEDS UTILIZANDO DEPD

As definições apresentadas na Seção 4.3 formalizadas para o DEPE são válidas para o DEPD. A única diferença é o procedimento de classificação dos níveis de controlabilidade segura. Na Seção 4.3, com a utilização do DEPE, dispõe-se de probabilidades estáticas. Dessa forma, é possível estabelecer níveis para CSUD, CSUP e CSCA para cada SED analisado. No

entanto, com a utilização do DEPD, ao invés de estabelecer um nível de controlabilidade segura para a linguagem, estabelecemos critérios para desabilitações de acordo com as os valores de probabilidades de diagnose, probabilidades de prognose, probabilidades de ocorrência futura de evento proibido e coeficientes de anormalidade para cada EDD.

A Figura 49 ilustra um exemplo prático de um sistema de climatização abordado inicialmente por Sampath et al. (1995). Este sistema é utilizado para ilustração de uma proposta de utilização do DEPD em uma topologia de controle tolerante a falhas em tempo de execução da planta. Na figura, são apresentados o autômato que representa a lógica de controle do sistema com a falha incluída no modelo e o diagnosticador lógico correspondente. Para este exemplo, tem-se $\Phi = \{l\}$. A Tabela 7 contém a descrição dos eventos. As funções de transições dinâmicas são apresentadas a seguir:

$$p(1,o,2) = p(2,l,3) = p(3,d,4) = p(4,c,1) = 0,9999^n$$
$$p(1,f,5) = p(2,f,6) = p(3,f,7) = p(4,f,8) = 1 - 0,9999^n$$

Tabela 7 – Descrição dos eventos do exemplo da Figura 49.

Evento	Descrição
o	Abre válvula
l	Liga bomba
d	Desliga bomba
c	Fecha válvula
f	Válvula travar fechada

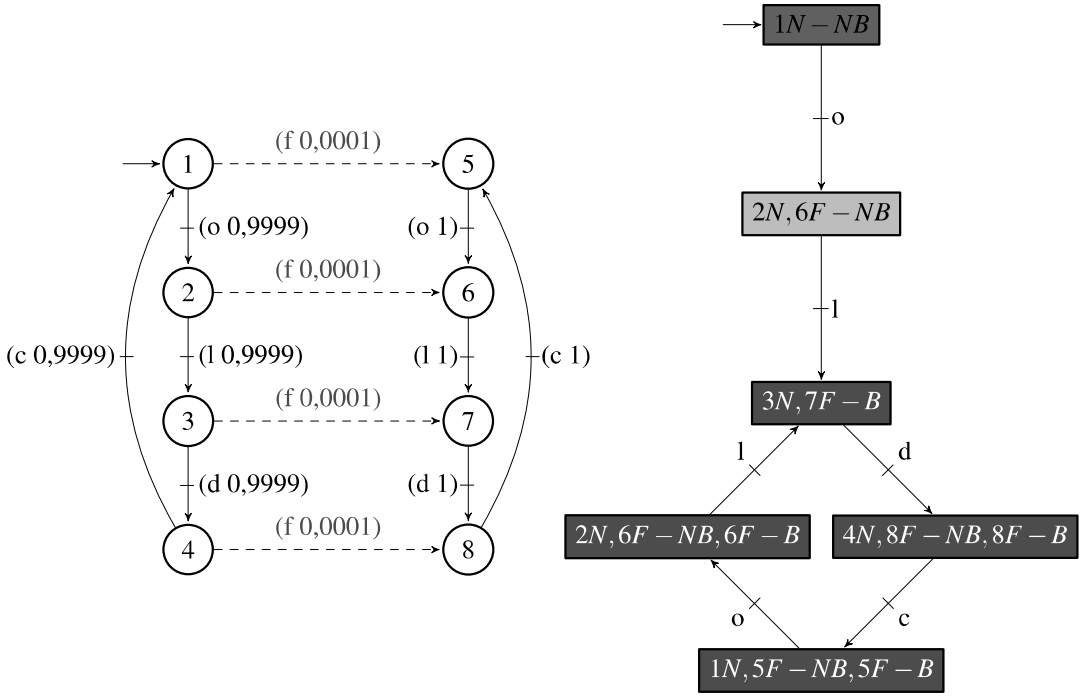
Fonte: Elaborado pelo autor (2023)

Os critérios de desabilitação utilizados devem ser estabelecidos pelo projetista, de acordo com a severidade da falha e do impacto da ocorrência de um comportamento proibido após a falha. Para este exemplo, os critérios sugeridos para desabilitação dos eventos controláveis que impedem a ocorrência de eventos proibidos após a falha são:

- Para $x_D \in \Xi$, desabilitar σ_c se $\Omega_F(x_D) > 70\%$
- Para $x_D \in \Upsilon$, desabilitar σ_c se $\Omega(x_D) \cdot \Delta_F(x_D)^T > 90\%$
- Para $x_D \in \Upsilon$, desabilitar σ_c se $\Omega(x_D) \cdot \Delta_{EP}(x_D)^T > 75\%$
- Para $x_D \in \Upsilon$, desabilitar σ_c se $\vartheta(x_D) > 80\%$

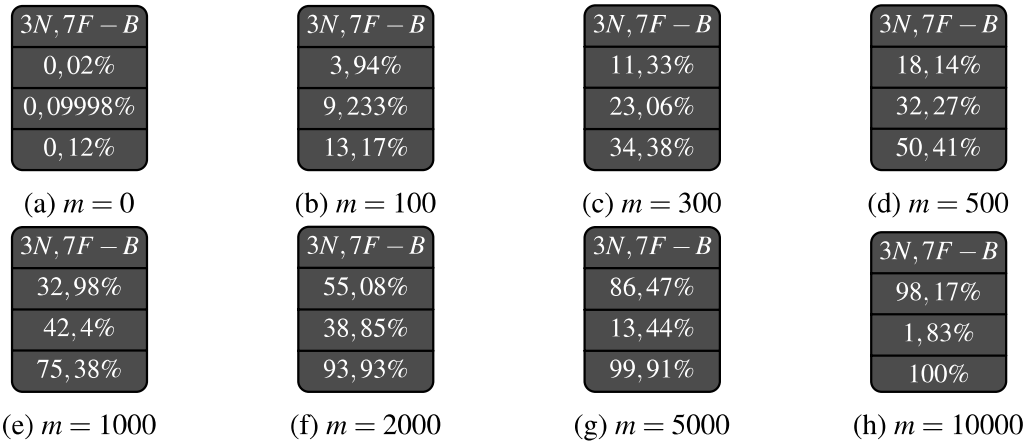
Em palavras, o evento controlável σ_c deve ser desabilitado no estado x_D se algum dos critérios for atendido: a) probabilidade de diagnose for superior a 70% ou b) probabilidade de prognose superior a 90% ou c) probabilidade de ocorrência futura de evento proibido após a falha de 75% ou d) coeficiente de anormalidade superior a 80%.

Figura 49 – Exemplo para ilustração da utilização do DEPD em CTF.



Fonte: Elaborado pelo autor (2023)

Figura 50 – EDD obtidos para a cadeia $s_o = ol(dcol)^m$ para diferentes valores de m, para o exemplo da Figura 49.



(a) $m = 0$ (b) $m = 100$ (c) $m = 300$ (d) $m = 500$

(e) $m = 1000$ (f) $m = 2000$ (g) $m = 5000$ (h) $m = 10000$

Fonte: Elaborado pelo autor (2023)

A Figura 50 apresenta os EDDs para o exemplo da Figura 49, para a cadeia $s_o = ol(dcol)^m$ para diferentes valores de m. O evento controlável l pertencente ao conjunto de cadeias ilegais Φ deve ser desabilitado, de acordo com os critérios de desabilitação, após aproximadamente 1000 ciclos, pois a probabilidade futura de evento proibido neste estado é superior a 75%.

4.8 CONSIDERAÇÕES FINAIS

Um importante aspecto da metodologia proposta para o DEPE é que o cálculo das probabilidades é feito de forma única e *offline*, característica essa que difere da metodologia de Thorsley e Teneketzis (2005). O cálculo matricial *online* apresentado em Thorsley e Teneketzis (2005) fornece um valor único de probabilidade, o qual é atualizado mediante observação de eventos, enquanto o cálculo *offline* apresentado nessa proposta fornece em geral uma faixa de valores. Apesar da utilização da faixa ser menos precisa que um único valor, a disponibilidade das probabilidades *offline* permitiu a introdução dos conceitos de u-diagnose, u-diagnose segura, u-prognose, controlabilidade seguras pela u-diagnose, pela u-prognose e pelo coeficiente de anormalidade.

Os exemplos apresentados consideram apenas um evento de falha f. No entanto, o método é aplicável para sistemas com múltiplas falhas distintas. Recomenda-se o cálculo de um DECS para cada falha pois a construção de um DECS multi-falha implicaria em um autômato muito carregado de informações, cuja interpretação dos valores seria complexa.

No exemplo da Figura 33 é possível observar que as faixas de probabilidades relacionadas à diagnose nos estados (2N,7N,7F), (4N,6N,8N,8F) e (8N,8F) possuem variações entre seus limites inferiores a 1%. Essa característica ocorre pois a probabilidade de ocorrência múltipla (tendendo ao infinito) de um evento ou subcadeia tende a zero.

Em contrapartida, a variação dos limites de probabilidades relacionadas à prognose nos estados (2N,5N) e (2N,7N,7F) do DECS da Figura 33 é de 10%. Pois a ocorrência repetida do evento *e* que configura um ciclo no estado 2 no autômato da Figura 32, avaliada a longo prazo, tem probabilidade nula. No entanto, numa análise pontual, considerando uma única ocorrência conclui-se que existe 10% de chance da falha não ocorrer.

5 CONCLUSÃO E TRABALHOS FUTUROS

Nesta tese, tratou-se do problema de controlabilidade segura de SEDs utilizando probabilidades de diagnose de falhas, probabilidades de ocorrências futuras de falhas e probabilidades de ocorrências futuras de eventos proibidos após as falhas.

Após realizarmos a revisão sistemática apresentada no Capítulo 3, verificamos que existem trabalhos na literatura que abordam diagnose estocástica de falhas, prognose estocástica de falhas e até diagnose estocástica segura de falhas, mas não existem trabalhos que reúnem estas propriedades conjuntamente visando a implantação de uma análise de controlabilidade segura em SEDs, seja por avaliação *offline* ou por utilização destas informações em uma estrutura de CTF *online*.

O trabalho apresentado por Watanabe (2019) utiliza uma análise de diagnose e prognose conjunta de falhas em uma avaliação de controlabilidade segura para autômatos clássicos, mas a utilização de autômatos estocásticos como formalismo de modelagem nesta tese permitiu expandir esta noção de DP-Controlabilidade Segura lógica. Dessa forma, podemos atuar no controle em sistemas que não possuem controlabilidade segura lógica ao utilizarmos as probabilidades fornecidas pelo Diagnosticador Estocástico com Probabilidades Estáticas (DEPE) ou pelo Diagnosticador Estocástico com Probabilidades Dinâmicas (DEPD), quando as probabilidades calculadas ultrapassam limites arbitrados pelos projetistas.

O DEPE fornece informações para uma avaliação *offline* das propriedades de u-diagnosticabilidade, u-diagnosticabilidade segura, u-prognosticabilidade, controlabilidade segura pela u-diagnose, controlabilidade segura pela u-prognose e controlabilidade segura pelo coeficiente de anormalidade.

O DEPE pode ser utilizado em uma estrutura de controle *online*. No entanto, como o procedimento de cálculo das probabilidades de diagnose é baseado na suposição de todas cadeias possíveis que atingem cada estado do diagnosticador para o estabelecimento de uma faixa de probabilidades, não são utilizadas as informações de observação.

Dessa forma, para uma estrutura de controle *online* recomenda-se a utilização do DEPD, cujas probabilidades relacionadas a diagnose são calculadas em tempo de execução e utilizadas para o cálculo de probabilidades ponderadas para ocorrências futuras de falha e de cadeias proibidas após a falha que são apresentadas no Estado Dinâmico do Diagnosticador (EDD).

Apresentamos a propriedade da certeza de anormalidade em autômatos clássicos e estendemos o conceito para autômatos estocásticos por meio da formalização do coeficiente de anormalidade. Esta propriedade e este coeficiente acrescentam informações que podem indicar situações inseguras nos sistemas sob análise e embasar a tomada de determinadas ações de controle para garantir confiabilidade e segurança de operação.

Foi realizada uma discussão sobre as cadeias que realmente devem ser contabilizadas em uma análise de predição de falhas e de eventos proibidos. Neste ponto, foi sugerido um novo modelo para análise da prognose, cujas probabilidades de transição são dinâmicas e baseadas no

histórico de observação.

As principais vantagens da utilização de um modelo dinâmico para análise de prognose estocástica estão na possibilidade de incluir no modelo características de sistemas, tais como: a justiça entre a frequência de eventos com diferentes probabilidades em um estado que faz parte de um ciclo e a modelagem do aumento da suscetibilidade a falha em sistemas mediante desgaste por operação.

Os tópicos apresentados a seguir são temas sugeridos para trabalhos futuros:

- Avaliação de equações que podem ser utilizadas no cálculo das probabilidades de transições dinâmicas, ou até mesmo um procedimento de atualização baseado em tabela de consulta;
- Interconexão da metodologia apresentada com o procedimento de Análise de Modos de Falha e seus Efeitos (FMEA) para a definição dos limites de probabilidades para atuação do controle mediante a severidade da falha;
- Utilização de Verificador nas análises *offline* efetuadas nas seções 4.1 a 4.3;
- Formalização do conceito de Controlabilidade Segura pela Certeza de Anormalidade no âmbito de autômatos clássicos;
- Implementação total dos algoritmos para automatizar o procedimento de cálculo das probabilidades do DECS.

REFERÊNCIAS

Al-Ani, T.; Hamam, Y. A learning based stochastic approach for fault diagnosis in a continuous stirred tank reactor. **MESM**, v. 6, p. 28–30, 2006. Citado na página 22.

Athanasopoulou, E.; Hadjicostis, C. N. Synchronization-based fault detection in discrete event systems. In: **2004 43rd IEEE Conference on Decision and Control (CDC) (IEEE Cat. No.04CH37601)**. [S.l.: s.n.], 2004. v. 1, p. 57–62 Vol.1. Citado na página 54.

Athanasopoulou, E.; Hadjicostis, C. N. Probability of error bounds for failure diagnosis and classification in hidden markov models. In: **2008 47th IEEE Conference on Decision and Control**. [S.l.: s.n.], 2008. p. 1477–1482. Citado na página 55.

Athanasopoulou, E.; Lingxi Li; Hadjicostis, C. N. Probabilistic failure diagnosis in finite state machines under unreliable observations. In: **2006 8th International Workshop on Discrete Event Systems**. [S.l.: s.n.], 2006. p. 301–306. Citado na página 55.

Baioumy, M. et al. Towards stochastic fault-tolerant control using precision learning and active inference. In: SPRINGER. **Machine Learning and Principles and Practice of Knowledge Discovery in Databases: International Workshops of ECML PKDD 2021, Virtual Event, September 13-17, 2021, Proceedings, Part I**. [S.l.], 2022. p. 681–691. Citado na página 22.

Barigozzi, A.; Magni, L.; Scattolini, R. A probabilistic approach for fault detection and isolation in industrial systems. **IFAC Proceedings Volumes**, v. 35, n. 1, p. 7 – 12, 2002. ISSN 1474-6670. 15th IFAC World Congress. Citado na página 51.

Bertrand, N.; Haddad, S.; Lefaucheux, E. Foundation of diagnosis and predictability in probabilistic systems. In: . [S.l.: s.n.], 2014. v. 29, p. 417–429. Cited By 18. Citado na página 57.

Biswas, S. et al. Diagnosability of fair discrete event systems. **Asian Journal of Control**, v. 10, n. 6, p. 651–665, 2008. ISSN 15618625. Citado na página 55.

Brandin, B.A.; Wonham, W.M. Supervisory control of timed discrete-event systems. **IEEE Transactions on Automatic Control**, v. 39, n. 2, p. 329–342, 1994. Citado na página 30.

Cabasino, M. P.; Giua, A.; Seatzu, C. Identification of petri nets from knowledge of their language. **Discrete Event Dynamic Systems**, Springer, v. 17, p. 447–474, 2007. Citado na página 19.

Calder, M.; Sevegnani, M. Stochastic model checking for predicting component failures and service availability. **IEEE Transactions on Dependable and Secure Computing**, v. 16, n. 1, p. 174–187, 2019. Citado na página 57.

Cao, W.; Liu, F.; Zhao, R. Decentralized failure prognosis of stochastic discrete-event systems and a test algorithm. **IEEE Transactions on Automation Science and Engineering**, v. 19, n. 4, p. 2944–2954, 2022. Citado 2 vezes nas páginas 19 e 20.

Carvalho, L. K. **Diagnose robusta de sistemas a eventos discretos**. Tese (Doutorado) — Tese (Doutorado em UFRJ COPPE-PEE Programa de Engenharia Elétrica . . . , 2011. Citado na página 31.

Cassandras, C. G.; Lafortune, S. **Introduction to discrete event systems**. [S.l.]: Springer Science & Business Media, 2009. Citado na página 25.

Chang, M. et al. On fault predictability in stochastic discrete event systems. **Asian Journal of Control**, v. 15, n. 5, p. 1458–1467, 2013. Citado na página 56.

Chen, J.; Kumar, R. Failure prognosability of stochastic discrete event systems. In: . [S.l.]: Institute of Electrical and Electronics Engineers Inc., 2014. p. 2041–2046. ISBN 9781479932726. ISSN 07431619. Cited By 13. Citado na página 21.

Chen, J.; Kumar, R. Stochastic failure prognosability of discrete event systems. **IEEE Transactions on Automatic Control**, v. 60, n. 6, p. 1570–1581, June 2015. ISSN 0018-9286. Nenhuma citação no texto.

Chen, J.; Kumar, R. Stochastic failure prognosis of discrete event systems. **IEEE Transactions on Automatic Control**, v. 67, n. 10, p. 5487–5492, 2022. Citado 2 vezes nas páginas 19 e 20.

Cury, J. E. R. Teoria de controle supervisório de sistemas a eventos discretos. **V Simpósio Brasileiro de Automação Inteligente (Minicurso)**, p. 8, 2001. Citado 2 vezes nas páginas 20 e 25.

de Queiroz, M. H.; Cury, J.E.R. Modular supervisory control of large scale discrete event systems. In: ____. **Discrete Event Systems: Analysis and Control**. Boston, MA: Springer US, 2000. p. 103–110. ISBN 978-1-4615-4493-7. Citado na página 30.

de Queiroz, M. H.; Cury, J. E. R. Modular control of composed systems. In: **Proceedings of the 2000 American Control Conference. ACC (IEEE Cat. No.00CH36334)**. [S.l.: s.n.], 2000. v. 6, p. 4051–4055 vol.6. Citado na página 30.

Deepa, S.; Ranjan, P. V.; Manohar, S. S. Probabilistic approach to fault detection in discrete event systems. In: **2007 International Conference on Signal Processing, Communications and Networking**. [S.l.: s.n.], 2007. p. 614–617. Citado na página 55.

Dong, W. et al. Fault diagnosis of discrete-event systems under non-deterministic observations with output fairness. In: **2022 IEEE 61st Conference on Decision and Control (CDC)**. [S.l.: s.n.], 2022. p. 4256–4262. Citado na página 19.

Dong, W.; Yin, X.; Li, S. A uniform framework for diagnosis of discrete-event systems with unreliable sensors using linear temporal logic. **IEEE Transactions on Automatic Control**, p. 1–16, 2023. Citado na página 19.

Dong, Z. et al. A stochastic learning algorithm for machine fault diagnosis. **Shock and Vibration**, Hindawi, v. 2022, 2022. Citado na página 22.

Dotoli, M.; Fanti, M. P.; Mangini, A. M. Real time identification of discrete event systems using petri nets. **Automatica**, v. 44, n. 5, p. 1209–1219, 2008. ISSN 0005-1098. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0005109807004542>. Citado na página 19.

Estrada-Vargas, A. P.; Lopez-Mellado, E.; Lesage, J. J. A comparative analysis of recent identification approaches for discrete-event systems. **Mathematical Problems in Engineering**, Hindawi, v. 2010, 2010. Citado na página 19.

Fritz, R.; Zhang, P. Overview of fault-tolerant control methods for discrete event systems. **IFAC-PapersOnLine**, v. 51, n. 24, p. 88–95, 2018. ISSN 2405-8963. 10th IFAC Symposium on Fault Detection, Supervision and Safety for Technical Processes SAFEPROCESS 2018. Disponível em: <https://www.sciencedirect.com/science/article/pii/S2405896318322249>. Citado na página 44.

Genc, S.; Lafortune, S. Predictability of event occurrences in partially-observed discrete-event systems. **Automatica**, v. 45, n. 2, p. 301 – 311, 2009. ISSN 0005-1098. Citado 3 vezes nas páginas 20, 38 e 39.

Geng, X.; Ouyang, D.; Zhao, X. Failure diagnosis for distributed stochastic discrete event systems. **Mathematical Problems in Engineering**, v. 2017, 2017. ISSN 1024123X. Decentralized informations;Diagnosability;Failure Diagnosis;Global modeling;Local model;Probabilistic structures;Stochastic discrete event systems;. Citado na página 57.

Hadjicostis, C. N. Probabilistic fault detection in finite-state machines based on state occupancy measurements. In: **Proceedings of the 41st IEEE Conference on Decision and Control, 2002.** [S.l.: s.n.], 2002. v. 4, p. 3994–3999 vol.4. Citado na página 51.

Hamada, T.; Takai, S. Reliable diagnosability for decentralized diagnosis of discrete event systems with single-level inference. In: **2022 American Control Conference (ACC)**. [S.l.: s.n.], 2022. p. 3746–3751. Citado na página 19.

Hu, Y.; Cao, S. Asynchronous diagnosability enforcement in discrete event systems based on supervisory control. **IEEE Sensors Journal**, v. 23, n. 9, p. 10071–10079, 2023. Citado na página 19.

Jiang, S. et al. A polynomial algorithm for testing diagnosability of discrete-event systems. **IEEE Transactions on Automatic Control**, IEEE, v. 46, n. 8, p. 1318–1321, 2001. Citado na página 20.

Li, S. et al. Robust diagnosability analysis using basis reachability graph. **IEEE Access**, v. 11, p. 9751–9762, 2023. Citado na página 19.

Lian, F. J; Shu, S. L. Online Prognosis of Stochastic Discrete Event Systems. In: **Proceedings of the 2016 international conference on computer engineering and information systems**. [S.l.]: ATLANTIS PRESS, 2016. (ACSR-Advances in Comptuer Science Research, 52), p. 435–443. ISBN 978-94-6252-283-1. ISSN 2352-538X. Citado na página 57.

Lin, F.; Wonham, W.M. Decentralized supervisory control of discrete-event systems. **Information Sciences**, v. 44, n. 3, p. 199–224, 1988. ISSN 0020-0255. Disponível em: <https://www.sciencedirect.com/science/article/pii/0020025588900023>. Citado na página 30.

Liu, F. Decentralized predictability of discrete event systems. In: **2017 29th Chinese Control And Decision Conference (CCDC)**. [S.l.: s.n.], 2017. p. 2914–2919. Citado na página 57.

Liu, F.; Qiu, D. Safe diagnosability of stochastic discrete event systems. **IEEE Transactions on Automatic Control**, v. 53, n. 5, p. 1291–1296, June 2008. ISSN 0018-9286. Citado 3 vezes nas páginas 56, 72 e 80.

Liu, F. et al. Decentralized diagnosis of stochastic discrete event systems. **IEEE Transactions on Automatic Control**, v. 53, n. 2, p. 535–546, 2008. Citado na página 57.

Liu, F.; Yang, P. Safe diagnosis of stochastic discrete event systems by constructing safe verifier. **Lecture Notes in Electrical Engineering**, Springer Verlag, v. 458, p. 523–529, 2018. Cited By 0. Citado na página 57.

Liu, F. et al. Verification of safe diagnosability of stochastic discrete-event systems. **International Journal of Control**, p. 1–20, 2020. Cited By 0. Citado na página 57.

Lunze, J. Diagnosis of quantised systems. In: . [S.l.: s.n.], 2000. v. 33, n. 11, p. 29 – 40. ISSN 1474-6670. 4th IFAC Symposium on Fault Detection, Supervision and Safety for Technical Processes 2000 (SAFEPROCESS 2000), Budapest, Hungary, 14-16 June 2000. Citado na página 51.

Lunze, J.; Schröder, J. Process diagnosis based on a discrete-event description. In: . Berlin, Boston: De Gruyter, 1999. v. 47, n. 8, p. 358 – 365. Citado na página 51.

Luo, Y. et al. Improved fault tolerance for dual active bridge converters under three phase shift control. In: **2022 IEEE 17th Conference on Industrial Electronics and Applications (ICIEA)**. [S.l.: s.n.], 2022. p. 272–277. Citado na página 19.

Machado, T. H. de M.C.; Viana, G. S.; Moreira, M. V. Event-based automaton model for identification of discrete-event systems for fault detection. **Control Engineering Practice**, v. 134, p. 105474, 2023. ISSN 0967-0661. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0967066123000436>. Citado na página 19.

Mao, H. et al. Learning deterministic probabilistic automata from a model checking perspective. **Machine Learning**, Springer, v. 105, p. 255–299, 2016. Citado na página 22.

Melnykov, V.; Kalinov, A.; Artemenko, A. Methods for adjustment fault-tolerant control systems for induction motors with damaged stator windings. In: **2022 IEEE 4th International Conference on Modern Electrical and Energy System (MEES)**. [S.l.: s.n.], 2022. p. 1–6. Citado na página 19.

Moor, T. A discussion of fault-tolerant supervisory control in terms of formal languages. **Annual Reviews in Control**, v. 41, p. 159–169, 2016. ISSN 1367-5788. Disponível em: <https://www.sciencedirect.com/science/article/pii/S1367578816300049>. Citado na página 21.

Moreira, M. V; Basilio, J. C; Cabral, F. G. "polynomial time verification of decentralized diagnosability of discrete event systems" versus "decentralized failure diagnosis of discrete event systems": A critical appraisal. **IEEE Transactions on Automatic Control**, IEEE, v. 61, n. 1, p. 178–181, 2015. Citado na página 20.

Moreira, M. V.; Basilio, J. C.; Cabral, F. G. "polynomial time verification of decentralized diagnosability of discrete event systems" versus "decentralized failure diagnosis of discrete event systems": A critical appraisal. **IEEE Transactions on Automatic Control**, v. 61, n. 1, p. 178–181, 2016. Citado na página 20.

Moreira, M. V; Jesus, T. C; Basilio, J. C. Polynomial time verification of decentralized diagnosability of discrete event systems. **IEEE Transactions on Automatic Control**, IEEE, v. 56, n. 7, p. 1679–1684, 2011. Citado na página 20.

Moreira, M. V.; Lesage, J. J. Discrete event system identification with the aim of fault detection. **Discrete Event Dynamic Systems**, Springer, v. 29, p. 191–209, 2019. Citado na página 19.

Moreira, M. V.; Lesage, J. J. Fault diagnosis based on identified discrete-event models. **Control Engineering Practice**, v. 91, p. 104101, 2019. ISSN 0967-0661. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0967066119301170>. Citado na página 19.

Neidig, J.; Lunze, J. Decentralised diagnosis of automata networks. **IFAC Proceedings Volumes**, v. 38, n. 1, p. 400 – 405, 2005. ISSN 1474-6670. 16th IFAC World Congress. Citado na página 57.

Niu, L. et al. An analytical framework for control synthesis of cyber-physical systems with safety guarantee. In: **2022 IEEE 61st Conference on Decision and Control (CDC)**. [S.l.: s.n.], 2022. p. 1533–1540. Citado na página 19.

Nouioua, F.; Dague, P. A probabilistic analysis of diagnosability in discrete event systems. In: . Patras, Greece: [s.n.], 2008. v. 178, p. 224 – 228. ISSN 09226389. Diagnosability;Probabilistic analysis;Reducible Markov chains;. Citado na página 55.

Nouioua, F.; Dague, P.; Ye, L. Predictability in probabilistic discrete event systems. In: . Rome, Italy: [s.n.], 2017. v. 456, p. 381 – 389. ISSN 21945357. Probabilistic discrete event systems;. Citado na página 57.

Paoli, A.; Lafortune, S. Safe diagnosability for fault-tolerant supervision of discrete-event systems. **Automatica**, v. 41, n. 8, p. 1335 – 1347, 2005. ISSN 00051098. Discrete event systems;Fault diagnosis;Fault tolerant control;Finite state machines;Supervision;. Citado na página 35.

Paoli, A.; Sartini, M.; Lafortune, S. Active fault tolerant control of discrete event systems using online diagnostics. **Automatica**, v. 47, n. 4, p. 639 – 649, 2011. ISSN 0005-1098. Citado 9 vezes nas páginas 19, 20, 36, 37, 38, 41, 45, 58 e 59.

Pinto, L. I.; Leal, A. B.; Rosso, R. S. U. Safe dynamic reconfiguration through supervisory control in iec 61499 compliant systems. p. 753–758, 2017. Citado na página 25.

Qi, H. et al. Probabilistic reachability prediction of unbounded petri nets: A machine learning method. **IEEE Transactions on Automation Science and Engineering**, p. 1–13, 2023. Citado 2 vezes nas páginas 19 e 20.

Qian, W.; Yang, L.; Xue, Y. Fault-tolerant control of aircraft rudder surfaces based on pseudo-inverse planning and sliding mode control. In: **CSAA/IET International Conference on Aircraft Utility Systems (AUS 2022)**. [S.l.: s.n.], 2022. v. 2022, p. 894–899. Citado na página 19.

Rabin, M. O. Probabilistic automata. **Information and Control**, v. 6, n. 3, p. 230 – 245, 1963. ISSN 0019-9958. Citado na página 30.

Ramadge, P. J.; Wonham, W.M. Modular feedback logic for discrete event systems. **SIAM Journal on Control and Optimization**, SIAM, v. 25, n. 5, p. 1202–1218, 1987. Citado na página 30.

Ramadge, P. J.; Wonham, W.M. Supervisory control of a class of discrete event processes. **SIAM Journal on Control and Optimization**, v. 25, n. 1, p. 206–230, 1987. Citado na página 30.

Sampath, M. et al. Diagnosability of discrete-event systems. **IEEE Transactions on automatic control**, IEEE, v. 40, n. 9, p. 1555–1575, 1995. Citado 8 vezes nas páginas 20, 31, 32, 33, 51, 57, 77 e 104.

Schiller, F.; Schröder, J.; Lunze, J. Diagnosis of transient faults in quantised systems. **Engineering Applications of Artificial Intelligence**, v. 14, n. 4, p. 519 – 536, 2001. ISSN 0952-1976. Citado na página 51.

Takai, S.; Ushio, T. Decentralized diagnosis of discrete event systems modeled by mealy automata with nondeterministic output functions. In: **Proceedings of the 2010 American Control Conference**. [S.l.: s.n.], 2010. p. 2613–2618. Citado na página 57.

Thorsley, D.; Teneketzis, D. Diagnosability of stochastic automata. In: **42nd IEEE International Conference on Decision and Control (IEEE Cat. No.03CH37475)**. [S.l.: s.n.], 2003. v. 6, p. 6289–6294 Vol.6. Citado 3 vezes nas páginas 30, 55 e 57.

Thorsley, D.; Teneketzis, D. Diagnosability of stochastic discrete-event systems. **IEEE Transactions on Automatic Control**, IEEE, v. 50, n. 4, p. 476–492, 2005. Citado 10 vezes nas páginas 21, 51, 52, 53, 54, 56, 72, 77, 91 e 106.

Thorsley, D.; Teneketzis, D. Diagnosis of cyclic discrete-event systems using active acquisition of information. In: **2006 8th International Workshop on Discrete Event Systems**. [S.l.: s.n.], 2006. p. 248–255. Citado na página 54.

Thorsley, D.; Yoo, T.; Garcia, H. E. Diagnosability of stochastic discrete-event systems under unreliable observations. In: **2008 American Control Conference**. [S.l.: s.n.], 2008. p. 1158–1165. Citado na página 55.

Tîrnăucă, C. et al. Behavioral modeling based on probabilistic finite automata: An empirical study. **Sensors**, MDPI, v. 16, n. 7, p. 958, 2016. Citado na página 22.

Verwer, S.; Eyraud, R.; Higuera, C. De La. Pautomac: a probabilistic automata and hidden markov models learning competition. **Machine learning**, Springer, v. 96, p. 129–154, 2014. Citado na página 22.

Wang, X.; Chattopadhyay, I.; Ray, A. Probabilistic fault diagnosis in discrete event systems. In: . Nassau, Bahamas: [s.n.], 2004. v. 5, p. 4794 – 4799. ISSN 01912216. Discrete event systems;Dynamical systems;Fault diagnosis;State transition probability;. Citado na página 54.

Watanabe, A. T.Y. et al. Fault prognosis of discrete event systems: An overview. **Annual Reviews in Control**, v. 51, p. 100–110, 2021. ISSN 1367-5788. Disponível em: <https://www.sciencedirect.com/science/article/pii/S1367578821000134>. Citado na página 72.

Watanabe, A. T. Y. Controlabilidade segura de sistemas a eventos discretos utilizando diagnose e prognose online. **Universidade do Estado de Santa Catarina, Programa de Pós-Graduação em Engenharia Elétrica**, p. 144, 2019. Citado 8 vezes nas páginas 35, 36, 39, 40, 41, 43, 81 e 107.

Watanabe, A. T. Y. et al. Safe controllability using online prognosis. **IFAC-PapersOnLine**, Elsevier, v. 50, n. 1, p. 12359–12365, 2017. Citado 3 vezes nas páginas 20, 37 e 40.

Watanabe, A. T. Y. et al. Combining online diagnosis and prognosis for safe controllability. **IEEE Transactions on Automatic Control**, v. 67, n. 10, p. 5563–5569, 2022. Citado 3 vezes nas páginas 20, 41 e 58.

Whiteford, T. M.; Kwong, R. Probabilistic fault diagnosis in discrete event systems with incomplete models. **IFAC Proceedings Volumes**, v. 40, n. 6, p. 97 – 102, 2007. ISSN 1474-6670. 1st IFAC Workshop on Dependable Control of Discrete Systems. Citado na página 55.

Wong, K.; Wonham, W.M. Hierarchical control of discrete-event systems. **Discrete Event Dynamic Systems: Theory and Applications**, v. 6, p. 241–273, 07 1996. Citado na página 30.

Wonham, W. M.; Ramadge, P. J. Modular supervisory control of discrete-event systems. **Mathematics of control, signals and systems**, Springer, v. 1, n. 1, p. 13–30, 1988. Citado na página 30.

Wu, N. E. Coverage in fault-tolerant control. **Automatica**, v. 40, n. 4, p. 537 – 548, 2004. ISSN 0005-1098. Citado 2 vezes nas páginas 20 e 51.

Yingrui, Z. et al. z-reliable se-coprognosability of discrete event systems and an algebraic state space approach to verification. **IEEE Transactions on Circuits and Systems II: Express Briefs**, v. 69, n. 12, p. 4894–4898, 2022. Citado 2 vezes nas páginas 19 e 20.

Yoo, T-S; Lafortune, S. Polynomial-time verification of diagnosability of partially observed discrete-event systems. **IEEE Transactions on automatic control**, IEEE, v. 47, n. 9, p. 1491–1495, 2002. Citado na página 20.

Zaytoon, J.; Lafortune, S. Overview of fault diagnosis methods for discrete event systems. **Annual Reviews in Control**, v. 37, n. 2, p. 308 – 320, 2013. ISSN 1367-5788. Citado 2 vezes nas páginas 19 e 31.

Zemouri, R.; Faure, J. M. Diagnosis of discrete event system by stochastic timed automata. In: **2006 IEEE Conference on Computer Aided Control System Design, 2006 IEEE International Conference on Control Applications, 2006 IEEE International Symposium on Intelligent Control**. [S.l.: s.n.], 2006. p. 1861–1866. Citado na página 55.

Zheng, J.; Hou, Z. Model free adaptive iterative learning control based fault-tolerant control for subway train with speed sensor fault and over-speed protection. **IEEE Transactions on Automation Science and Engineering**, p. 1–13, 2022. Citado na página 19.

Zhou, Y. et al. A state space approach to decentralized fault se-coprognosability of partially observed discrete event systems. **IEEE Transactions on Cybernetics**, v. 53, n. 3, p. 2028–2033, 2023. Citado 2 vezes nas páginas 19 e 20.

APÊNDICE A – MEMORIAL DE CÁLCULO PARA OBTENÇÃO DE UM DECS PARA O AUTÔMATO GERADOR E DIAGNOSTICADOR APRESENTADOS NAS FIGURAS 32 E 33

Nesse apêndice serão apresentados os procedimentos realizados para obtenção de um DECS. Os cálculos serão apresentados em quatro etapas:

1. Cálculo das probabilidades de estar em cada rótulo de cada estado do DECS;
2. Cálculo das probabilidades de ocorrência futura de falha a partir de cada rótulo de cada estado do DECS;
3. Cálculo das probabilidades de ocorrência futura de evento proibido falha a partir de cada rótulo de cada estado do DECS;
4. Cálculo do valor que é exibido em cada estado do DECS a partir do resultado dos passos anteriores.

1º Passo

Estado (1N)

PD(1N) = 1

$\Omega(1N) = [1]$

Estado (2N,5N)

CCD(2N,5N) = $\{a\}$

PD(2N)= $\frac{Prob(a,1)}{Prob(a,1)+Prob(\sigma_u a),1} = \frac{0,1}{0,1+0,9 \cdot 1} = 10\%$

PD(5N)= $\frac{Prob(\sigma_u a),1}{Prob(a,1)+Prob(\sigma_u a,1)} = \frac{0,9 \cdot 1}{0,1+0,9 \cdot 1} = 90\%$

$\Omega(2N,5N) = [0,1 \quad 0,9]$

Estado(4N,6N,6F)

CCD(4N,6N,6F) = $\{ab\}$

PD(4N) = $\frac{Prob(ab,1)}{Prob(ab,1)+Prob(\sigma_u ab,1)+Prob(afb,1)} = \frac{0,1 \cdot 0,5}{0,1 \cdot 0,5+0,9 \cdot 1 \cdot 0,8+0,1 \cdot 0,4 \cdot 0,8} = 6,23\%$

PD(6N) = $\frac{Prob(\sigma_u ab,1)}{Prob(ab,1)+Prob(\sigma_u ab,1)+Prob(afb,1)} = \frac{0,9 \cdot 1 \cdot 0,8}{0,1 \cdot 0,5+0,9 \cdot 1 \cdot 0,8+0,1 \cdot 0,4 \cdot 0,8} = 89,78\%$

PD(6F) = $\frac{Prob(afb,1)}{Prob(ab,1)+Prob(\sigma_u ab,1)+Prob(afb,1)} = \frac{0,1 \cdot 0,4 \cdot 0,8}{0,1 \cdot 0,5+0,9 \cdot 1 \cdot 0,8+0,1 \cdot 0,4 \cdot 0,8} = 3,99\%$

$\Omega(4N,6N,6F) = [0,0623 \quad 0,8978 \quad 0,0399]$

Estado(6N,6F)

CCD(6N,6F) = $abdd^*$

PD(6N)(0) = $\frac{Prob(\sigma_u abd,1)}{Prob(\sigma_u abd,1)+Prob(afbd,1)+Prob(abfd,1)} = \frac{0,9 \cdot 1 \cdot 0,8 \cdot 1}{0,9 \cdot 1 \cdot 0,8 \cdot 1+0,1 \cdot 0,4 \cdot 0,8 \cdot 1+0,1 \cdot 0,5 \cdot 1 \cdot 1} = 89,78\%$

PD(6N)(∞) = $\frac{Prob(\sigma_u abdd^n,1)}{Prob(\sigma_u abdd^n,1)+Prob(afbdd^n,1)+Prob(abfdd^n,1)}$

$= \frac{0,9 \cdot 1 \cdot 0,8 \cdot 1 \cdot 1^n}{0,9 \cdot 1 \cdot 0,8 \cdot 1 \cdot 1^n + 0,1 \cdot 0,4 \cdot 0,8 \cdot 1 \cdot 1^n + 0,1 \cdot 0,5 \cdot 1 \cdot 1 \cdot 1^n} = 89,78\%$

$\text{PD(6F)}(0) = \frac{Prob(afbd,1) + Prob(abfd,1)}{Prob(\sigma_u abd,1) + Prob(afbd,1) + Prob(abfd,1)} = \frac{0,1 \cdot 0,4 \cdot 0,8 \cdot 1 + 0,1 \cdot 0,5 \cdot 1 \cdot 1}{0,9 \cdot 1 \cdot 0,8 \cdot 1 + 0,1 \cdot 0,4 \cdot 0,8 \cdot 1 + 0,1 \cdot 0,5 \cdot 1 \cdot 1} = 10,22\%$

$\text{PD(6F)}(\infty) = \frac{Prob(afbdd^n,1) + Prob(abfdd^n,1)}{Prob(\sigma_u abdd^n,1) + Prob(afbdd^n,1) + Prob(abfdd^n,1)}$

$= \frac{0,1 \cdot 0,4 \cdot 0,8 \cdot 1 \cdot 1^n + 0,1 \cdot 0,5 \cdot 1 \cdot 1 \cdot 1^n}{0,9 \cdot 1 \cdot 0,8 \cdot 1 \cdot 1^n + 0,1 \cdot 0,4 \cdot 0,8 \cdot 1 \cdot 1^n + 0,1 \cdot 0,5 \cdot 1 \cdot 1 \cdot 1^n} = 10,22\%$

$\Omega(6N, 6F) = [0,8978 \quad 0,1022]$

Estado(2N,7N,7F)

CCD(2N,7N,7F) = $\{ae\}$

$\text{PD(2N)} = \frac{Prob(ae,1)}{Prob(ae,1) + Prob(\sigma_u ae,1) + Prob(afe,1)} = \frac{0,1 \cdot 0,1}{0,1 \cdot 0,1 + 0,9 \cdot 1 \cdot 0,2 + 0,1 \cdot 0,4 \cdot 0,2} = 5,05\%$

$\text{PD(7N)} = \frac{Prob(\sigma_u ae,1)}{Prob(ae,1) + Prob(\sigma_u ae,1) + Prob(afe,1)} = \frac{0,9 \cdot 1 \cdot 0,2}{0,1 \cdot 0,1 + 0,9 \cdot 1 \cdot 0,2 + 0,1 \cdot 0,4 \cdot 0,2} = 90,91\%$

$\text{PD(7F)} = \frac{Prob(afe,1)}{Prob(ae,1) + Prob(\sigma_u ae,1) + Prob(afe,1)} = \frac{0,1 \cdot 0,1}{0,1 \cdot 0,1 + 0,9 \cdot 1 \cdot 0,2 + 0,1 \cdot 0,4 \cdot 0,2} = 4,04\%$

$\Omega(2N, 7N, 7F) = [0,0505 \quad 0,9091 \quad 0,0404]$

Estado(2N,7F)

CCD(2N,7F) = aee^*e

$\text{PD(2N)}(0) = \frac{Prob(aee,1)}{Prob(aee,1) + Prob(aefe,1)} = \frac{0,1 \cdot 0,1 \cdot 0,1}{0,1 \cdot 0,1 \cdot 0,1 + 0,1 \cdot 0,1 \cdot 0,4 \cdot 0,2} = 55,56\%$

$\text{PD(2N)}(\infty) = \frac{Prob(aee^*e,1)}{Prob(aee^*e,1) + Prob(aee^*fe,1)} = \frac{0,1 \cdot 0,1 \cdot 0,1^n \cdot 0,1}{0,1 \cdot 0,1 \cdot 0,1^n \cdot 0,1 + 0,1 \cdot 0,1 \cdot 0,1 \cdot 0,1^n \cdot 0,4 \cdot 0,2} = 55,56\%$

$\text{PD(7F)}(0) = \frac{Prob(aefe,1)}{Prob(aee,1) + Prob(aefe,1)} = \frac{0,1 \cdot 0,1 \cdot 0,4 \cdot 0,2}{0,1 \cdot 0,1 \cdot 0,1 + 0,1 \cdot 0,1 \cdot 0,4 \cdot 0,2} = 44,44\%$

$\text{PD(7F)}(\infty) = \frac{Prob(aee^*fe,1)}{Prob(aee^*e,1) + Prob(aee^*fe,1)} = \frac{0,1 \cdot 0,1 \cdot 0,1^n \cdot 0,4 \cdot 0,2}{0,1 \cdot 0,1 \cdot 0,1^n \cdot 0,1 + 0,1 \cdot 0,1 \cdot 0,1 \cdot 0,1^n \cdot 0,4 \cdot 0,2} = 44,44\%$

$\Omega(2N, 7F) = [0,5556 \quad 0,4444]$

Estado (4N,6F,8F)

CCD(4N,6F,8F) = $aeee^*b$

$\text{PD(4N)} = \frac{Prob(aeeb,1)}{Prob(aeeb,1) + Prob(aeefb,1) + Prob(aefeb,1)}$

$= \frac{0,1 \cdot 0,1 \cdot 0,1 \cdot 0,1 \cdot 0,5}{0,1 \cdot 0,1 \cdot 0,1 \cdot 0,1 \cdot 0,5 + 0,1 \cdot 0,1 \cdot 0,1 \cdot 0,1 \cdot 0,4 \cdot 0,8 + 0,1 \cdot 0,1 \cdot 0,1 \cdot 0,4 \cdot 0,2 \cdot 1} = 30,86\%$

$\text{PD(6F)} = \frac{Prob(aeefb,1)}{Prob(aeeb,1) + Prob(aeefb,1) + Prob(aefeb,1)}$

$= \frac{0,1 \cdot 0,1 \cdot 0,1 \cdot 0,1 \cdot 0,4 \cdot 0,8}{0,1 \cdot 0,1 \cdot 0,1 \cdot 0,1 \cdot 0,5 + 0,1 \cdot 0,1 \cdot 0,1 \cdot 0,1 \cdot 0,4 \cdot 0,8 + 0,1 \cdot 0,1 \cdot 0,1 \cdot 0,4 \cdot 0,2 \cdot 1} = 19,75\%$

$\text{PD(8F)} = \frac{Prob(aefeb,1)}{Prob(aeeb,1) + Prob(aeefb,1) + Prob(aefeb,1)}$

$= \frac{0,1 \cdot 0,1 \cdot 0,1 \cdot 0,4 \cdot 0,2 \cdot 1}{0,1 \cdot 0,1 \cdot 0,1 \cdot 0,1 \cdot 0,5 + 0,1 \cdot 0,1 \cdot 0,1 \cdot 0,1 \cdot 0,4 \cdot 0,8 + 0,1 \cdot 0,1 \cdot 0,1 \cdot 0,4 \cdot 0,2 \cdot 1} = 49,38\%$

$\Omega(4N, 6F, 8F) = [0,3086 \quad 0,1975 \quad 0,4938]$

Estado (4N,6F,8N,8F)

CCD(4N,6F,8N,8F) = $\{aeb\}$

PD(4N) = $\frac{Prob(aeb,1)}{Prob(aeb,1)+Prob(aefb,1)+Prob(\sigma_u aeb,1)+Prob(afeb,1)}$

= $\frac{0,1\cdot0,1\cdot0,5}{0,1\cdot0,1\cdot0,5+0,1\cdot0,1\cdot0,4\cdot0,8+0,9\cdot1\cdot0,2\cdot1+0,1\cdot0,4\cdot0,2\cdot1} = 2,55\%$

PD(6F) = $\frac{Prob(aefb,1)}{Prob(aeb,1)+Prob(aefb,1)+Prob(\sigma_u aeb,1)+Prob(afeb,1)}$

= $\frac{0,1\cdot0,1\cdot0,4\cdot0,8}{0,1\cdot0,1\cdot0,5+0,1\cdot0,1\cdot0,4\cdot0,8+0,9\cdot1\cdot0,2\cdot1+0,1\cdot0,4\cdot0,2\cdot1} = 1,63\%$

PD(8N) = $\frac{Prob(\sigma_u aeb,1)}{Prob(aeb,1)+Prob(aefb,1)+Prob(\sigma_u aeb,1)+Prob(afeb,1)}$

= $\frac{0,9\cdot1\cdot0,2\cdot1}{0,1\cdot0,1\cdot0,5+0,1\cdot0,1\cdot0,4\cdot0,8+0,9\cdot1\cdot0,2\cdot1+0,1\cdot0,4\cdot0,2\cdot1} = 91,74\%$

PD(8F) = $\frac{Prob(afeb,1)}{Prob(aeb,1)+Prob(aefb,1)+Prob(\sigma_u aeb,1)+Prob(afeb,1)}$

= $\frac{0,1\cdot0,4\cdot0,2\cdot1}{0,1\cdot0,1\cdot0,5+0,1\cdot0,1\cdot0,4\cdot0,8+0,9\cdot1\cdot0,2\cdot1+0,1\cdot0,4\cdot0,2\cdot1} = 4,08\%$

$\Omega(4N,6F,8N,8F) = [0,0255 \;\; 0,0163 \;\; 0,9174 \;\; 0,0408]$

Estado (8N,8F)

CCD(8N,8F) = $aebcc^*$

PD(8N)(0) = $\frac{Prob(\sigma_u aebc,1)}{Prob(\sigma_u aebc,1)+Prob(afebc,1)} = \frac{0,9\cdot1\cdot0,2\cdot1\cdot1}{0,9\cdot1\cdot0,2\cdot1\cdot1+0,1\cdot0,4\cdot0,2\cdot1\cdot1} = 95,74\%$

PD(8N)(∞) = $\frac{Prob(\sigma_u aebcc^*,1)}{Prob(\sigma_u aebcc^*,1)+Prob(afebcc^*,1)} = \frac{0,9\cdot1\cdot0,2\cdot1\cdot1\cdot1^n}{0,9\cdot1\cdot0,2\cdot1\cdot1\cdot1^n+0,1\cdot0,4\cdot0,2\cdot1\cdot1\cdot1^n} = 95,74\%$

PD(8F)(0) = $\frac{Prob(afebc,1)}{Prob(\sigma_u aebc,1)+Prob(afebc,1)} = \frac{0,1\cdot0,4\cdot0,2\cdot1\cdot1}{0,9\cdot1\cdot0,2\cdot1\cdot1+0,1\cdot0,4\cdot0,2\cdot1\cdot1} = 4,26\%$

PD(8F)(∞) = $\frac{Prob(afebcc^*,1)}{Prob(\sigma_u aebcc^*,1)+Prob(afebcc^*,1)} = \frac{0,9\cdot1\cdot0,2\cdot1\cdot1\cdot1^n}{0,9\cdot1\cdot0,2\cdot1\cdot1\cdot1^n+0,1\cdot0,4\cdot0,2\cdot1\cdot1\cdot1^n} = 4,26\%$

$\Omega(8N,8F) = [0,9574 \;\; 0,0426]$

Estado (6F)

CCD(6F) = $aebdd^*$

PD(6F)(0) = PD(6F)(∞) = 1

$\Omega(6F) = [1]$

Estado (8F)

CCD(8F) = $aeee^*bcc^*$

PD(8F)(0) = PD(8F)(∞) = 1

$\Omega(8F) = [1]$

2º Passo

Estado (1N)

$\Psi_f(1N) = ae^*bf + ae^*f$

PF(1N)(0) = $Prob(abf,1) + Prob(af,1) = 0,1\cdot0,5\cdot1 + 0,1\cdot0,4 = 9\%$

PF(1N)(∞) = $\sum_{n=0}^{\infty} Prob(ae^nbf,1) + \sum_{n=0}^{\infty} Prob(ae^nf,1) = \sum_{n=0}^{\infty} 0,1\cdot0,1^n\cdot0,5\cdot1 + 0,1\cdot0,1^n\cdot$

$0,4 = 10\%$
$\Delta_F(1N) = [(0,09;0,1)]$

Estado (2N,5N)
$\Psi_f(2N) = e^* bf + e^* f$
PF(2N)(0) = $Prob(bf,2) + Prob(f,2) = 0,5 \cdot 1 + 0,4 = 90\%$
PF(2N)(∞) = $\sum_{n=0}^{\infty} Prob(e^n bf,2) + \sum_{n=0}^{\infty} Prob(e^n f,2) = \sum_{n=0}^{\infty} 0,1^n \cdot 0,5 \cdot 1 + 0,1^n \cdot 0,4 = 100\%$
$\Psi_f(5N) = \emptyset$
PF(5N) = 0%
$\Delta_F(2N,5N) = [(0,9;1) \quad 0]$

Estado (4N,6N,6F)
$\Psi_f(4N) = \{f\}$
PF(4N) = $Prob(f,4) = 100\%$
$\Psi_f(6N) = \emptyset$
PF(6N) = 0%
$\Psi_f(6F) = \emptyset$
PF(6F) = 0%
$\Delta_F(4N,6N,6F) = [1 \quad 0 \quad 0]$

Estado (6N,6F)
$\Psi_f(6N) = \emptyset$
PF(6N) = 0%
$\Psi_f(6F) = \emptyset$
PF(6F) = 0%
$\Delta_F(6N,6F) = [0 \quad 0]$

Estado (2N,7N,7F)
$\Psi_f(2N) = e^* bf + e^* f$
PF(2N)(0) = $Prob(bf,2) + Prob(f,2) = 0,5 \cdot 1 + 0,4 = 90\%$
PF(2N)(∞) = $\sum_{n=0}^{\infty} Prob(e^n bf,2) + \sum_{n=0}^{\infty} Prob(e^n f,2) = \sum_{n=0}^{\infty} 0,1^n \cdot 0,5 \cdot 1 + 0,1^n \cdot 0,4 = 100\%$
$\Psi_f(7N) = \emptyset$
PF(7N) = 0%
$\Psi_f(7F) = \emptyset$

PF(7F) = 0%

$\Delta_F(2N, 7N, 7F) = [(0,9;1) \;\; 0 \;\; 0]$

Estado (2N,7F)

$\Psi_f(2N) = e^* bf + e^* f$

PF(2N)(0) = $Prob(bf, 2) + Prob(f, 2) = 0,5 \cdot 1 + 0,4 = 90\%$

PF(2N)(∞) = $\sum_{n=0}^{\infty} Prob(e^n bf, 2) + \sum_{n=0}^{\infty} Prob(e^n f, 2) = \sum_{n=0}^{\infty} 0,1^n \cdot 0,5 \cdot 1 + 0,1^n \cdot 0,4 = 100\%$

$\Psi_f(7F) = \emptyset$

PF(7F) = 0%

$\Delta_F(2N, 7F) = [(0,9;1) \;\; 0]$

Estado (4N,6F,8F)

$\Psi_f(4N) = \{f\}$

PF(4N) = $Prob(f, 4) = 100\%$

$\Psi_f(6F) = \emptyset$

PF(6F) = 0%

$\Psi_f(8F) = \emptyset$

PF(8F) = 0%

$\Delta_F(4N, 6F, 8F) = [1 \;\; 0 \;\; 0]$

Estado (4N,6F,8N,8F)

$\Psi_f(4N) = \{f\}$

PF(4N) = $Prob(f, 4) = 100\%$

$\Psi_f(6F) = \emptyset$

PF(6F) = 0%

$\Psi_f(8N) = \emptyset$

PF(8N) = 0%

$\Psi_f(8F) = \emptyset$

PF(8F) = 0%

$\Delta_F(4N, 6F, 8N, 8F) = [1 \;\; 0 \;\; 0 \;\; 0]$

Estado (8N,8F)

$\Psi_f(8N) = \emptyset$

PF(8N) = 0%

$\Psi_f(8F) = \emptyset$

PF(8F) = 0%

$\Delta_F(8N, 8F) = [0 \;\; 0]$

Estado (6F)

$\Psi_f(6F) = \emptyset$

PP(6F) = 0% $\Delta_F(6F) = [0]$

Estado (8F)

$\Psi_f(8F) = \emptyset$

PP(8F) = 0% $\Delta_F(8F) = [0]$

3º Passo

Estado (1N)

$\eta(1N) = ae^* febcc^*$

PEP(1N)(0) = $Prob(afebc, 1) = 0,1 \cdot 0,4 \cdot 0,2 \cdot 1 \cdot 1 = 0,8\%$

PEP(1N)(∞) = $\sum_{n=0}^{\infty} Prob(ae^n febcc^n, 1) = \sum_{n=0}^{\infty} 0,1 \cdot 0,1^n \cdot 0,4 \cdot 0,2 \cdot 1 \cdot 1 \cdot 1^n = 0,89\%$

$\Delta_{EP}(1N) = [(0,008; 0,0089)]$

Estado (2N,5N)

$\eta(2N) = e^n febcc^*$

PEP(2N)(0) = $Prob(febc, 2) = 0,4 \cdot 0,2 \cdot 1 \cdot 1 = 8\%$

PEP(2N)(∞) = $\sum_{n=0}^{\infty} Prob(e^n febcc^*, 2) = \sum_{n=0}^{\infty} 0,1^n \cdot 0,4 \cdot 0,2 \cdot 1 \cdot 1 \cdot 1^n = 8,89\%$

$\eta(5N) = \emptyset$

PP(5N) = 0%

$\Delta_{EP}(2N, 5N) = [(0,08; 0,0889) \;\; 0]$

Estado (4N,6N,6F)

$\eta(4N) = \emptyset$

PEP(4N) = 0%

$\eta(6N) = \emptyset$

PEP(6N) = 0%

$\eta(6F) = \emptyset$

PEP(6F) = 0%

$\Delta_{EP}(4N, 6N, 6F) = [0 \;\; 0 \;\; 0]$

Estado (6N,6F)

$\eta(6N) = \emptyset$

PEP(6N) = 0%

$\eta(6F) = \emptyset$

PEP(6F) = 0%

$\Delta_{EP}(6N, 6F) = [0 \;\; 0]$

Estado (2N,7N,7F)

$\eta(2N) = e^n febcc^*$

PEP(2N)(0) = $Prob(febc, 2) = 0,4 \cdot 0,2 \cdot 1 \cdot 1 = 8\%$

PEP(2N)(∞) = $\sum_{n=0}^{\infty} Prob(e^n febcc^*, 2) = \sum_{n=0}^{\infty} 0,1^n \cdot 0,4 \cdot 0,2 \cdot 1 \cdot 1 \cdot 1^n = 8,89\%$

$\eta(7N) = \emptyset$

PEP(7N) = 0%

$\eta(7F) = bcc^*$

PEP(7F) = $Prob(bc, 7) = 1 \cdot 1 = 100\%$

$\Delta_{EP}(2N, 7N, 7F) = [(0,08; 0,0889) \;\; 0 \;\; 1]$

Estado (2N,7F)

$\eta(2N) = e^n febcc^*$

PEP(2N)(0) = $Prob(febc, 2) = 0,4 \cdot 0,2 \cdot 1 \cdot 1 = 8\%$

PEP(2N)(∞) = $\sum_{n=0}^{\infty} Prob(e^n febcc^*, 2) = \sum_{n=0}^{\infty} 0,1^n \cdot 0,4 \cdot 0,2 \cdot 1 \cdot 1 \cdot 1^n = 8,89\%$

$\eta(7F) = bcc^*$

PEP(7F) = $Prob(bc, 7) = 1 \cdot 1 = 100\%$

$\Delta_{EP}(2N, 7F) = [(0,08; 0,0889) \;\; 1]$

Estado (4N,6F,8F)

$\eta(4N) = \emptyset$

PEP(4N) = 0%

$\eta(6F) = \emptyset$

PEP(6F) = 0%

$\eta(8F) = cc^*$

PEP(8F) = $Prob(c) = 1 = 100\%$

$\Delta_{EP}(4N, 6F, 8F) = [0 \;\; 0 \;\; 1]$

Estado (4N,6F,8N,8F)

$\eta(4N) = \emptyset$

PEP(4N) = 0%

$\eta(6F) = \emptyset$

PEP(6F) = 0%

$\eta(8N) = \emptyset$

PEP(8N) = 0%

$\eta(8F) = cc^*$

PEP(8F) = $Prob(c, 8)$ = 1 = 100%

$\Delta_{EP}(4N, 6F, 8N, 8F) = [0 \;\; 0 \;\; 0 \;\; 1]$

Estado (8N,8F)

$\eta(8N) = \emptyset$

PEP(8N) = 0%

$\eta(8F) = cc^*$

PEP(8F) = $Prob(c, 8)$ = 1 = 100%

$\Delta_{EP}(8N, 8F) = [0 \;\; 1]$

Estado (6F)

$\eta(6F) = \emptyset$

PEP(6F) = 0%

$\Delta_{EP}(6F) = [0]$

Estado (8F)

$\eta(8F) = cc^*$

PEP(8F) = $Prob(c, 8)$ = 1 = 100%

$\Delta_{EP}(8F) = [1]$

4º Passo

Estado (1N)

$\Omega(1N) = [1]$

$\Delta_F(1N) = [(0,09; 0,1)]$

$\Delta_{EP}(1N) = [(0,008; 0,0089)]$
$\Omega_F(x_D) = 0\%$
$\Omega(x_D) \cdot \Delta_F(x_D)^T = (9; 10\%$
$\Omega(x_D) \cdot \Delta_{EP}(x_D)^T = (0,8; 0,89)\%$

Estado (2N,5N)
$\Omega(2N, 5N) = [0,1 \;\; 0,9]$
$\Delta_F(2N, 5N) = [(0,9; 1) \;\; 0]$
$\Delta_{EP}(2N, 5N) = [(0,08; 0,0889) \;\; 0]$
$\Omega_F(x_D) = 0\%$
$\Omega(x_D) \cdot \Delta_F(x_D)^T = (90; 100)\%$
$\Omega(x_D) \cdot \Delta_{EP}(x_D)^T = (8; 8,89)\%$

Estado (4N,6N,6F)
$\Omega(4N, 6N, 6F) = [0,0623 \;\; 0,8978 \;\; 0,0399]$
$\Delta_F(4N, 6N, 6F) = [1 \;\; 0 \;\; 0]$
$\Delta_{EP}(4N, 6N, 6F) = [0 \;\; 0 \;\; 0]$
$\Omega_F(x_D) = 3,99\%$
$\Omega(x_D) \cdot \Delta_F(x_D)^T = 6,23\%$
$\Omega(x_D) \cdot \Delta_{EP}(x_D)^T = 0\%$

Estado(6N,6F)
$\Omega(6N, 6F) = [0,8978 \;\; 0,1022]$
$\Delta_F(6N, 6F) = [0 \;\; 0]$
$\Delta_{EP}(6N, 6F) = [0 \;\; 0]$
$\Omega_F(x_D) = 10,22\%$
$\Omega(x_D) \cdot \Delta_F(x_D)^T = 0\%$
$\Omega(x_D) \cdot \Delta_{EP}(x_D)^T = 0\%$

Estado(2N,7N,7F)
$\Omega(2N, 7N, 7F) = [0,0505 \;\; 0,9091 \;\; 0,0404]$
$\Delta_F(2N, 7N, 7F) = [(0,9; 1) \;\; 0 \;\; 0]$
$\Delta_{EP}(2N, 7N, 7F) = [(0,08; 0,0889) \;\; 0 \;\; 1]$
$\Omega_F(x_D) = 4,04\%$
$\Omega(x_D) \cdot \Delta_F(x_D)^T = (4,54; 5,05)\%$
$\Omega(x_D) \cdot \Delta_{EP}(x_D)^T = (4,44; 4,49)\%$

Estado(2N,7F)
$\Omega(2N, 7F) = [0,5556 \;\; 0,4444]$

$\Delta_F(2N,7F) = [(0,9;1) \;\; 0]$
$\Delta_{EP}(2N,7F) = [(0,08;0,0889) \;\; 1]$
$\Omega_F(x_D) = 44,44\%$
$\Omega(x_D) \cdot \Delta_F(x_D)^T = (50;55,56)\%$
$\Omega(x_D) \cdot \Delta_{EP}(x_D)^T = (48,88;49,38)\%$

Estado (4N,6F,8F)
$\Omega(4N,6F,8F) = [0,3086 \;\; 0,1975 \;\; 0,4938]$
$\Delta_F(4N,6F,8F) = [1 \;\; 0 \;\; 0]$
$\Delta_{EP}(4N,6F,8F) = [0 \;\; 0 \;\; 1]$
$\Omega_F(x_D) = 69,14\%$
$\Omega(x_D) \cdot \Delta_F(x_D)^T = 30,86\%$
$\Omega(x_D) \cdot \Delta_{EP}(x_D)^T = 49,38\%$

Estado (4N,6F,8N,8F)
$\Omega(4N,6F,8N,8F) = [0,0255 \;\; 0,0163 \;\; 0,9174 \;\; 0,0408]$
$\Delta_F(4N,6F,8N,8F) = [1 \;\; 0 \;\; 0 \;\; 0]$
$\Delta_{EP}(4N,6F,8N,8F) = [0 \;\; 0 \;\; 0 \;\; 1]$
$\Omega_F(x_D) = 5,71\%$
$\Omega(x_D) \cdot \Delta_F(x_D)^T = 2,55\%$
$\Omega(x_D) \cdot \Delta_{EP}(x_D)^T = 4,08\%$

Estado (8N,8F)
$\Omega(8N,8F) = [0,9574 \;\; 0,0426]$
$\Delta_F(8N,8F) = [0 \;\; 0]$
$\Delta_{EP}(8N,8F) = [0 \;\; 1]$
$\Omega_F(x_D) = 4,26\%$
$\Omega(x_D) \cdot \Delta_F(x_D)^T = 0\%$
$\Omega(x_D) \cdot \Delta_{EP}(x_D)^T = 4,26\%$

Estado (6F)
$\Omega(6F) = [1]$
$\Delta_F(6F) = [0]$
$\Delta_{EP}(6F) = [0]$

$\Omega_F(x_D) = 100\%$

$\Omega(x_D) \cdot \Delta_F(x_D)^T = 0\%$
$\Omega(x_D) \cdot \Delta_{EP}(x_D)^T = 0\%$

Estado (8F)

$\Omega(8F) = [1]$

$\Delta_F(8F) = [0]$

$\Delta_{EP}(8F) = [1]$

$\Omega_F(x_D) = 100\%$

$\Omega(x_D) \cdot \Delta_F(x_D)^T = 0\%$

$\Omega(x_D) \cdot \Delta_{EP}(x_D)^T = 100\%$

APÊNDICE B – SCRIPT PARA MATLAB © - CÁLCULO PARA EXEMPLO DA FIGURA 45.

Código B.1 – Cálculo Probabilidades Exemplo 45

```
clc
close all
syms n
d1=.2^n; %delta(5,d)=3
d2=.9^n; %delta(6,d)=4
c1=(.2-.2^n)+.8; %delta(5,c)=7
c2=(.9-.9^n)+.1; %delta(6,d)=8
a=[.9 .1];
b=[1 0; 0 1];
d=[.2 0; 0 .9];

X = input('Por favor informe quantas vezes o ciclo se repetiu : ')

clc
%A variavel X indica a quantidade de ciclos, mas o indice n para calculo da
    probabilidade de transicao dinamica eh incrementado em uma unidade para
    cada repeticao do ciclo.
Y=X+1;

% CALCULO DOS VALORES DAS TRANSICOEES DINAMICAS
vald1 = vpa(subs(d1,n,Y));
vald2 = vpa(subs(d2,n,Y));
valc1 = vpa(subs(c1,n,Y));
valc2 = vpa(subs(c2,n,Y));

% CALCULO DAS MATRIZES DeltaF e DeltaEP
deltafstatic= [.8*.5 0];
deltafdinamic=[valc1*.5 0];
deltaepstatic= [.8*.5*.8 .1*1];
deltaepdinamic=[valc1*.5*.8 valc2*1];

%CALCULO DOS CAMPOS DO EDD UTILIZANDO MODELO ESTATICO PARA ANALISE DA
    PROGNOSE
omega= vpa((a*((b*d)^X)*b)/(sum(a*((b*d)^X)*b)),4);
omegaf=vpa(omega(2),4)
odfs= vpa(omega*deltafstatic',4)
odeps= vpa(omega*deltaepstatic',4)

%CALCULO DOS CAMPOS DO EDD UTILIZANDO MODELO DINAMICO PARA ANALISE DA
    PROGNOSE
omega= vpa((a*((b*d)^X)*b)/(sum(a*((b*d)^X)*b)),4);
omegaf=vpa(omega(2),4)
odfd= vpa(omega*deltafdinamic',4)
odepd= vpa(omega*deltaepdinamic',4)
```