Computer Controlled Systems II – Diagnosis

Diagnosis based on event sequences
Diagnosers and HAZID methods

Katalin Hangos

University of Pannonia
Faculty of Information Technology
Department of Electrical Engineering and Information Systems

hangos.katalin@virt.uni-pannon.hu

Jan 2020

Lecture overview

1. Traces, operations on traces
   - Traces
   - Trace norms
2. Diagnosers
3. Diagnosis based on HAZID information
   - HAZID analysis and its outcomes
   - Traces generated from the HAZOP and FNEA tables

Supporting methods for the diagnosis

1. Traces, operations on traces
   - Traces
   - Trace norms
2. Diagnosers
3. Diagnosis based on HAZID information

Prediction-based diagnosis

General problem statement

Given:

- *The number of faulty modes* N_F (0=normal)
- *Predictive dynamic model* for each faulty mode

$$y^{(Fi)}(k+1) = \mathcal{M}^{(Fi)}(\mathcal{D}[1,k];\ p^{(Fi)}) \ \ , \quad k = 1, 2, \ldots$$

- *Measured data record*: $D[0,k] = \{\ (u(\tau), y(\tau) \mid \tau = 0, \cdots, k\}$
- *Loss function* $J^{(Fi)},\ i = 0, \cdots, N_F$

$$J^{(Fi)}(y - y^{(Fi)}, u) \ = \ \sum_{\tau=1}^{k} [\, r^{(i)T}(\tau) Q r^{(i)}(\tau)\,] \ , \ \ r^{(i)}(\tau) = y(\tau) - y^{(Fi)}(\tau) \ \ , \ \ \tau = 1$$

Compute: The actual faulty mode of the system, i.e. the fault index i that minimizes the loss function.

Fault isolation

Qualitative signals

Qualitative values for variables with "normal" N value

$$\mathcal{Q} = \{H, N, L, 0\}, \quad \mathcal{B} = \{0, 1\}, \quad \mathcal{Q}_{\mathcal{E}} = \{H, N, L, 0, e+, e-\}$$

where *H*igh, *L*ow, *N*ormal, *e*rror.

Qualitative signal: a signal (input, output, state or ***disturbance (fault indicator!)***) with a qualitative range space

Event: occurs when a qualitative signal changes its value.
Formal description of the event e_X:

$$e_X(t, q_X) = (t, [x](t) = q_X)$$

where t is the discrete time instant when the qualitative signal $[x]$ takes the value q_X.

Signal traces – event sequences

The **(signal trace)** of a qualitative signal $[x]$ is the event sequence

$$\mathcal{T}_{(x)}(t_0, t_F) = \{(t_0; [x](t_0) = q_{x0}), (t_1; [x](t_1)] = q_{x1}), ..., (t_F; [x](t_F) = q_{xF})\}$$

defined on the time interval (t_0, t_F) with $q_* \in \mathcal{Q}_x$

A **vector-valued trace of multiple signals** is defined as $\mathcal{T}_{(u,d,y)}(t_0, t_F)$
Simplified notation: by omitting the time, e.g.

$$\mathcal{T}_{(h,T)}(1, 3) = \{(N, N), (L, H), (L, e+)\}$$

For diagnostic purposes we define

- **nominal traces** (for describing normal behaviour)
- **characteristic traces** (for describing faulty behaviour)

Norms of scalar valued signals

- vector norms: $v \in \mathbb{R}^n$

$$||v||_2 = \sqrt{\sum_{i=1}^{n} v_i^2} \;\; , \;\; ||v||_1 = \sum_{i=1}^{n} |v_i| \;\; , \;\; ||v||_\infty = \max |v_i|$$

- ***discrete time signal:*** $f(k) \in \mathbb{R}, \; \forall k \geq 0$

$$\text{norm: } ||f||_q = \left(\sum_{0}^{\infty} |f(k)|_\nu^q \right)^{\frac{1}{q}}$$

- continuous time signal $f(t) \in \mathbb{R}, \; \forall t \geq 0$

$$\text{norm: } ||f||_q = \left(\int_{0}^{\infty} |f(t)|_\nu^q \right)^{\frac{1}{q}}$$

Norms of traces

Scalar valued trace: discrete time signal with qualitative values

$$\mathcal{T}_{(x)}(t_0, t_F) = \{(t_0; [x](t_0) = q_{x0}), (t_1; [x](t_1)] = q_{x1}), ..., (t_F; [x](t_F) = q_{xF})\}$$

defined on the time interval (t_0, t_F) with $q_* \in \mathcal{Q}_x$ Example:

$$\mathcal{T}_{(h)}(1, 3) = \{(N), (L), (L)\}$$

Norm: based on the norm of discrete time scalar valued real signals using a mapping function $\mathcal{R} : \mathcal{Q}_x \mapsto \mathbb{R}$:

$$\mathcal{R}(q) = \begin{cases} -1 & q = e- \\ 0 & q = 0 \\ 1 & q = L \\ 2 & q = N \\ 3 & q = H \\ 4 & q = e+ \end{cases}$$

Simple dynamic example

Norms of **qualitative input-output traces** can be easily computed

	$[m]$ initial mass in tank	$[v_{in}]$ input flow sequence	$[\chi_{leak}]$ * tank leakage	$[\chi_{meas}]$ * sensor failure	$[v_T^m]$ measured flow sequence
	LOW	(NORMAL,NORMAL,NORMAL)	0	NEG	(LOW, LOW, LOW)
	LOW	(NORMAL,NORMAL,NORMAL)	1	POS	(LOW, LOW, LOW)
	HIGH	(LOW, LOW, LOW)	1	0	(LOW, NO, NO)
	HIGH	(LOW, LOW, LOW)	0	NEG	(LOW, NO, NO)
	...	...	...	...	...
D	NORMAL	(NO, NO, NO)	0	0	(LOW, NO, NO)
D	NORMAL	(NO, NO, NO)	1	POS	(LOW, LOW, LOW)
	NORMAL	(NO, NO, NO)	1	NEG	(e-, e-, e-)
	NORMAL	(NO, NO, NO)	0	POS	(NORMAL, LOW, LOW)
D	NORMAL	(NO, NO, NO)	0	NEG	(NO, e-, e-)
D	NORMAL	(NO, NO, NO)	1	0	(NO, NO, NO)
	...	...	...	...	...

Diagnosers

1. Traces, operations on traces
2. Diagnosers
3. Diagnosis based on HAZID information

Characteristic traces

Characteristic trace for a given fault : the fault can be uniquely determined from that trace

	$[m]$ initial mass in tank	$[v_{in}]$ input flow sequence	$[\chi_{leak}]$ * tank leakage	$[\chi_{meas}]$ * sensor failure	$[v_T{}^m]$ measured flow sequence
	LOW	(NORMAL,NORMAL,NORMAL)	0	NEG	(LOW, LOW, LOW)
	LOW	(NORMAL,NORMAL,NORMAL)	1	POS	(LOW, LOW, LOW)
	HIGH	(LOW, LOW, LOW)	1	0	(LOW, NO, NO)
	HIGH	(LOW, LOW, LOW)	0	NEG	(LOW, NO, NO)
	...	...	...	...	...
D	NORMAL	(NO, NO, NO)	0	0	(LOW, NO, NO)
D	NORMAL	(NO, NO, NO)	1	POS	(LOW, LOW, LOW)
	NORMAL	(NO, NO, NO)	1	NEG	(e-, e-, e-)
	NORMAL	(NO, NO, NO)	0	POS	(NORMAL, LOW, LOW)
D	NORMAL	(NO, NO, NO)	0	NEG	(NO, e-, e-)
D	NORMAL	(NO, NO, NO)	1	0	(NO, NO, NO)
	...	...	...	...	...

The *characteristic trace for the positive additive sensor fault* is:

$$\mathcal{T}_{(v_{in}, v_{out}^m)}(1, 4) = \{(0, H), (0, N), (0, L), (0, L)\}$$

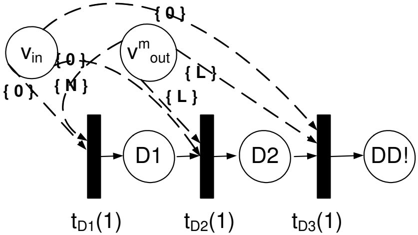
Diagnosers

Diagnoser of a fault : a discrete event system (*a discrete observer*) that selectively detects (i.e. *isolates*) the characteristic trace of a fault

Diagnoser CPN structure:

- a separate transition to each event $e_{t_{t_i}}$ in the characteristic trace
- *internal places*: after each time step
  p_{Dt_i}: the ith event in the characteristic trace have occurred
- *connection to the measured signal places with test edges*

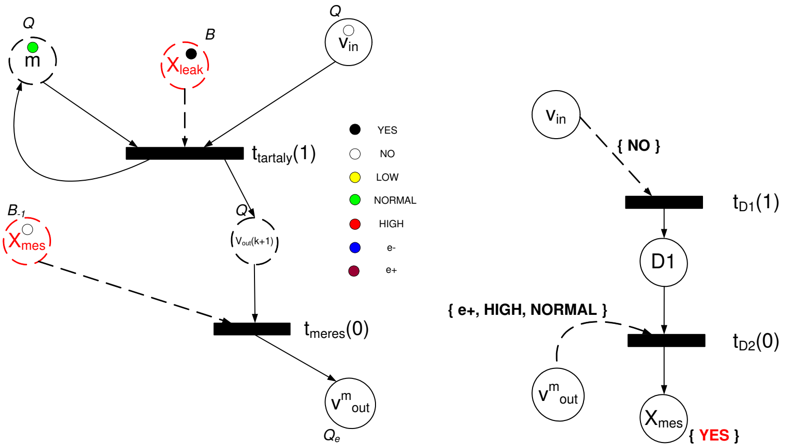
Example: $\mathcal{T}_{(v_{in}, v_{out}^m)}(1, 3) = \{(0, N), (0, L), (0, L)\}$



Diagnoser for the leaking tank with sensor example

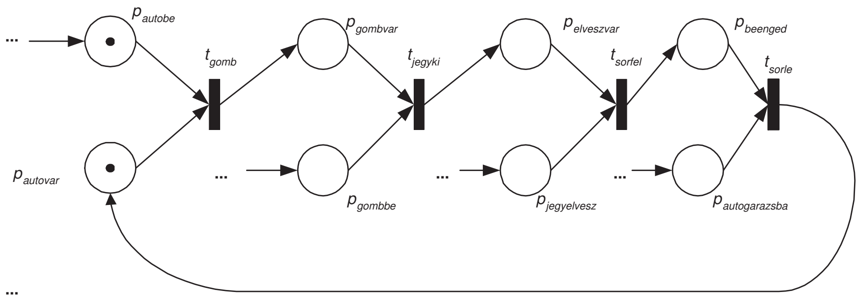
Fault: positive additive sesor fault

Characteristic trace: $(0; v_{in} = 0), (1; v^m_{out} = H)$

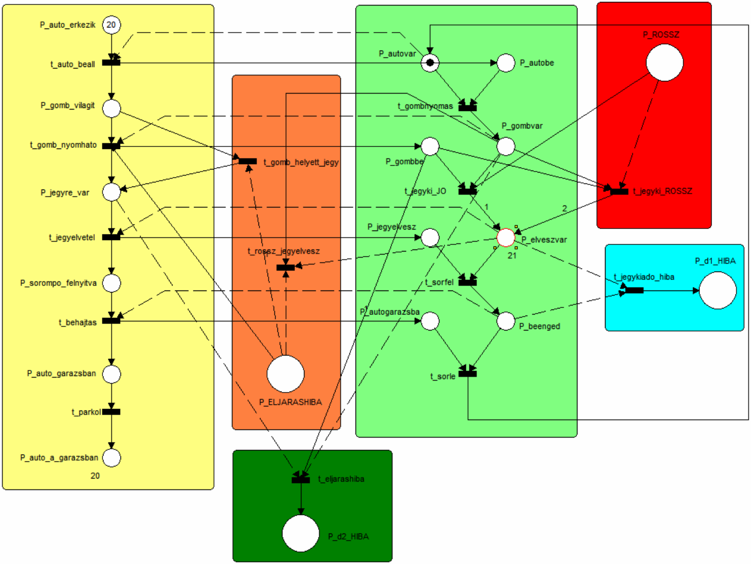


Example: garage gate - recall

Petri net model - graphical description



Diagnosers for the garage gate operated by a driver



Diagnosis based on HAZID information

Risk management

It is obligatory for each (safety critical) plant or equipment (a car, for example)

Goal: For the possible failures/faults (causes) and their implied hazards (consequences)

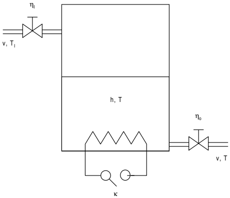
- to systematically collect them
- to evaluate their probability and seriousness (hazardousness)
- to find cause-consequence relationships
- to find possible preventive actions and rehabilitation possibilities

HAZID: *hazard identification*

HAZID analysis

- using a given "patented" procedure: *HAZOP ĂŠs FMEA*
- multidisciplinary expert team
- the results of the analysis is verbal, *arranged in tables*
- the basis of official licensing, it should be regularly updated

Example: Continuous Coffee Machine



Operation:

- continuous, the inlet valve η_I and the outlet valve η_O take values between 0 and 1, κ is the heating valve
- continuous inflow $v_I = \eta_I v$, outflow $v_O = \eta_O v$ and heating $f = \kappa H$

Dynamic model equations (from first engineering principles)

$$
\begin{aligned}
\frac{dh}{dt} &= \frac{v}{A}\eta_I - \frac{v}{A}\eta_O && \text{(mass)} \\
\frac{dT}{dt} &= \frac{v}{Ah}(T_I - T)\eta_I + \frac{H}{c_p \rho h}\kappa && \text{(energy)}
\end{aligned}
\qquad (1)
$$

Hazard and Operability analysis – HAZOP

Characterization

- *it is processed following measured characteristic (important) variables (signals)*
- their ***Deviation*** s are analysed (primary key column)
- standard deviations for each characteristic variable type
- the possible (**Causes**), the hazardous (**Consequences**) of a **Deviation** are collected (together with the possible preventive actions)

The format of the HAZOP table

Guideword		**Deviation**	**Causes**	**Consequences**

A part of HAZOP analysis for the continuous coffee machine

System: coffee machine with continuous operation
Variable: level h

Guideword		**Deviation**	**Causes**	**Consequences**
Low		h Low	inflow None	outflow Low temperature High
		h Low	outflow High	temperature High h None

Fault Mode and Effect Analysis – FMEA

Characterization

- *it is processed following the components of the system*
- their possible ***Failure modes*** are analysed (primary key column)
- standard failure modes for each component type
- the possible **Failure mode causes**, the local consequences (**Local effects**) and the system level consequences (**System effects**) of a **Failure mode** are collected

The format of the FMEA table

Component		Failure mode	Failure mode causes		Local effects	System effects

A part of FMEA analysis for the continuous coffee machine

System: coffee machine with continuous operation
Component: inflow controlling valve η_I

Component		**Failure mode**	Failure mode causes		**Local effects**	**System effects**
inflow valve η_I		stocked	breaking		inflow None	level Low
η_I		outstated	breaking		inflow High	level High

Correspondence between the elements of the HAZOP and FMEA tables

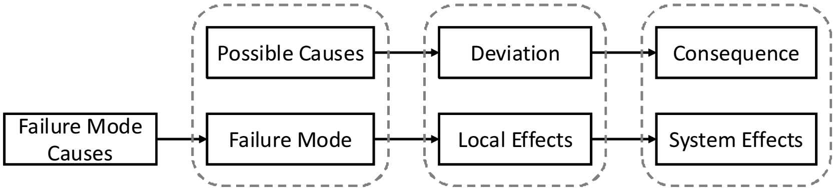
Joint syntax for the elements: pairs – *events*

<Deviation> = (<Measured variable> <Guide word>)

<Failure mode> = (<Component id> <Failure type>)

<Cause> = (<Variable> <Guide word>), etc.

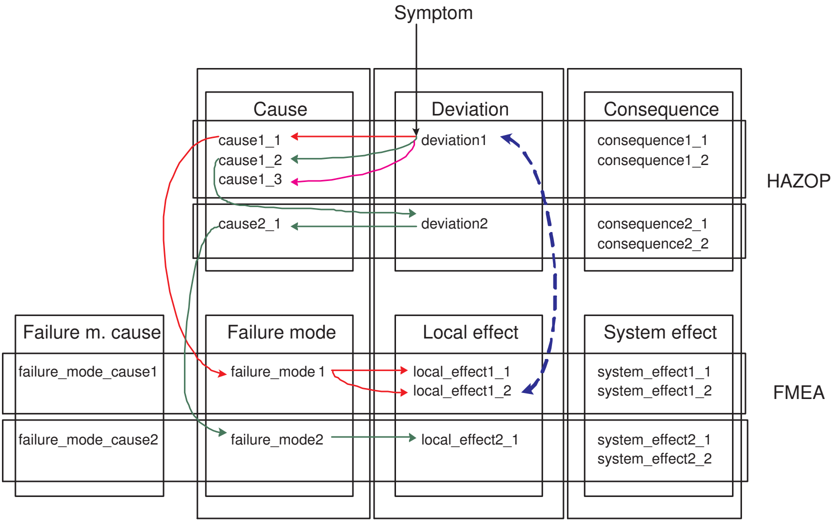
PĂŠldĂĄk: <SCT.Level> <Low>, <SCT> <Leakage>



Traces from the rows of the tables

- <Deviation>: events related to measured variables/signals
- <Failure mode>: special qualitative event – *the goal of diagnosis*

Retrieving characteristic traces from HAZID tables



Example for retrieving a trace

Deviation	Possible causes	Consequences
<NO><Feed to TB (F2)>	(1) <VB><is><closed> (2) <VA><is><closed> (3) <L><is><ruptured> (4) <L><is><blocked> (5) <NO><Feed to PA>	* <NO><Feed to press> * <NO><Feed to VC>
<NO><Feed to PA (F1)>	(1) <TA><is><broken> (2) <TA><is><leaked> (3) <L1><is><leaked> (4) <TA><is not><filled> (5) <PA><does not possess> <capability to pump>	* <NO><Feed to press> * <NO><Feed to VA>

Com-ponent	Description	Failure mode	Possible causes	Effects: Local	Effects: System
VB	TB inflow control valve	Closed	mechanical fail closed operator closed	<NO><Feed to TB>	<NO><Feed to press>
		Opened	mechanical fail opened operator opened	<MORE><Feed to TB>	<MORE><Feed to press>
		Stuck	maintenance failure corrosion	<LESS><Feed to TB>	<LESS><Feed to press>
TA	Bulk tank TA	Broken	corrosion vehicle damage operator damage	<NO><Feed to PA>	<NO><Feed to press>
		Leaked	corrosion	<LESS><Feed to PA>	<LESS><Feed to press>