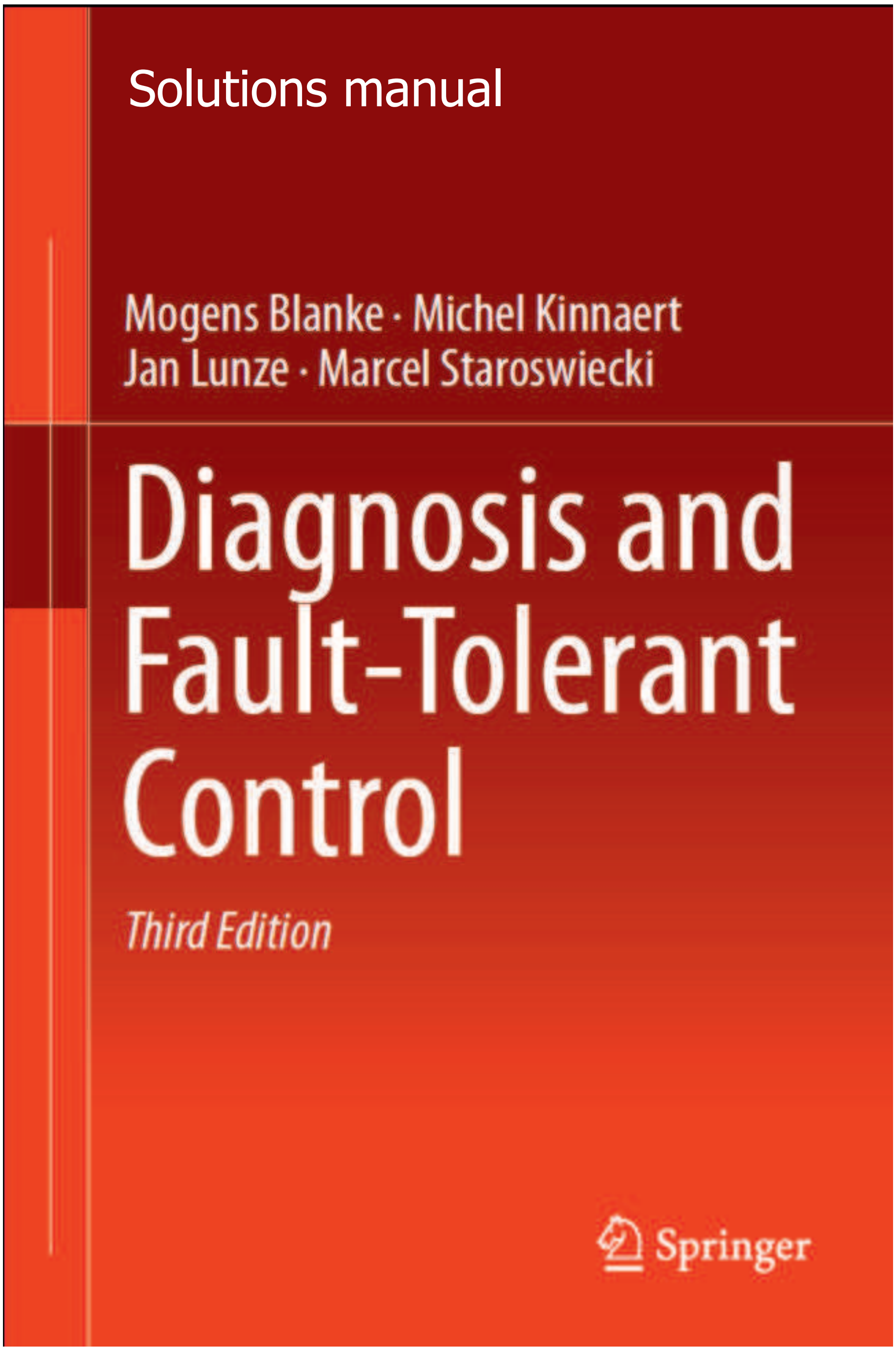

Solutions manual

Mogens Blanke · Michel Kinnaert
Jan Lunze · Marcel Staroswiecki

Diagnosis and Fault-Tolerant Control

Third Edition

Springer

Exercises of Chapter 7

Exercise 7.6 *Hardware redundancy*

Consider a set of three sensors measuring a single quantity denoted x. The measurement system can be modelled as:

$$\begin{bmatrix} y_1(k) \\ y_2(k) \\ y_3(k) \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} \boldsymbol{x}(k) + \begin{bmatrix} f_1(k) \\ f_2(k) \\ f_3(k) \end{bmatrix} + \begin{bmatrix} v_1(k) \\ v_2(k) \\ v_3(k) \end{bmatrix} \tag{S.1}$$

where $y_i(k), v_i(k)$ and $f_i(k), i = 1, 2, 3$ respectively denote the sensor measurement, the measurement noise, and a possible additive fault. $v_i(k), i = 1, 2, 3$ is assumed to be a Gaussian white noise sequence with zero mean and variance $\sigma_1^2 = \sigma_2^2 = 1$ and $\sigma_3^2 = 2$. Besides, the noise sequences are mutually uncorrelated. The faults are modelled as unknown deterministic signals, and it is assumed that simultaneous faults do not occur. A fault on sensor i thus corresponds to a non-zero value for $f_i(k)$ from an unknown fault occurrence time, say k_0.

1. Let us rewrite equation (S.1) more compactly as

   $$\boldsymbol{y}(k) = \begin{bmatrix} 1 & 1 & 1 \end{bmatrix}^{\mathrm{T}} \boldsymbol{x}(k) + \boldsymbol{f}(k) + \boldsymbol{v}(k) \tag{S.2}$$

   where $\boldsymbol{y}(k) = \begin{bmatrix} y_1(k) & y_2(k) & y_3(k) \end{bmatrix}^{\mathrm{T}}$ and similarly for $\boldsymbol{f}(k)$ and $\boldsymbol{v}(k)$. Let Ω denote a basis for the left null space of $\begin{bmatrix} 1 & 1 & 1 \end{bmatrix}^{\mathrm{T}}$. Show that $\boldsymbol{r}(k) \equiv \Omega \boldsymbol{y}(k)$ is independent of $x(k)$.
2. Prove that $\boldsymbol{r}(k)$ has zero mean in the absence of fault and that its mean is equal to $\Omega_{\cdot,i} f_i(k)$ in the presence of a fault on sensor i. Here $\Omega_{\cdot,i}$ denotes the i-th column of matrix Ω. Besides, show that the variance of $\boldsymbol{r}(k)$ is equal to $\boldsymbol{Q}_r = \Omega \boldsymbol{Q} \Omega^{\mathrm{T}}$ where $\boldsymbol{Q} = \text{ diag } (\sigma_1^2, \sigma_2^2, \sigma_3^2)$
3. Let $\boldsymbol{r}_n = (\Omega \boldsymbol{Q}_r \Omega^{\mathrm{T}})^{-\frac{1}{2}} \boldsymbol{r}(k)$. Show that $\boldsymbol{r}_n(k)$ is distributed as $\mathcal{N}(O, \boldsymbol{I})$ in the absence of fault, and as $\mathcal{N}((\Omega \boldsymbol{Q}_r \Omega^{\mathrm{T}})^{-\frac{1}{2}} \Omega_{\cdot,i} f_i(k), \boldsymbol{I})$ upon occurrence of a fault on the i-th sensor.
4. Assume that positive step-like faults with minimum magnitude equal to 0.5 can occur. Design a multi-CUSUM algorithm of the form presented in section 7.2.6 to detect and isolate such faults.
5. Generate a data sequence according to model (S.1) in which $x(k) = \sin(0.1k)$, the noise properties are as described above, and $f_1(k) = 0.5 \;\; 1_{\{k \geq 20\}}$, $f_2(k) = f_3(k) = 0$ for all k.
6. Process the data generated in point e) by the multi-CUSUM algorithm designed in point d), and check its effectiveness.
7. Check how the magnitude of the fault affects the obtained results by repeating points e) and f) for different fault magnitudes. □

Solution

1. By definition of the left null space of a matrix,

$$\Omega \begin{bmatrix} 1 & 1 & 1 \end{bmatrix}^T = 0$$

and hence,

$$\boldsymbol{r}(k) = \Omega \boldsymbol{y}(k) = \Omega(\boldsymbol{f}(k) + \boldsymbol{v}(k)) \tag{S.3}$$

which does not depend of $\boldsymbol{x}(k)$.

2. In the absence of fault, $\boldsymbol{f}(k) = 0$, and thus

$$E(\boldsymbol{r}(k)) = \Omega E(\boldsymbol{v}(k)) = 0.$$

In the presence of a fault on sensor i, only the i^{th} component of $\boldsymbol{f}(k)$ is non zero. Taking the expected value of (S.3) yields:

$$E(\boldsymbol{r}(k)) = \Omega \boldsymbol{f}(k) = \Omega_{.,i} f_i(k)$$

As far as the variance of the residual is concerned, by definition,

$$\begin{aligned} \boldsymbol{Q}_r &= E\left[(\boldsymbol{r}(k) - E(\boldsymbol{r}(k)))(\boldsymbol{r}(k) - E(\boldsymbol{r}(k)))^T\right] \\ &= \Omega E\left[\boldsymbol{v}(k)\boldsymbol{v}(k)^T\right] \Omega^T \\ &= \Omega \boldsymbol{Q} \Omega^T \end{aligned} \tag{S.4}$$

3. By hypothesis $v_i(k)$ are normally distributed, hence $\boldsymbol{r}(k)$ is normally distributed as well since it is made of a linear combination of Gaussian signals. In the absence of fault, direct computation of the mean yields:

$$E(\boldsymbol{r}_n(k)) = (\Omega \boldsymbol{Q} \Omega^T)^{-\frac{1}{2}} E(\boldsymbol{r}(k)) = 0$$

where the last inequality results from the previous point. Similarly, in the presence of fault, one deduces from the previous point:

$$E(\boldsymbol{r}_n(k)) = (\Omega \boldsymbol{Q} \Omega^T)^{-\frac{1}{2}} E(\boldsymbol{r}(k)) = (\Omega \boldsymbol{Q} \Omega^T)^{-\frac{1}{2}} \Omega_{.,i} f_i(k).$$

Finally the computation of the variance yields:

$$\begin{aligned} &E\left[(\boldsymbol{r}_n(k) - E(\boldsymbol{r}_n(k)))(\boldsymbol{r}_n(k) - E(\boldsymbol{r}_n(k)))^T\right] \\ &= (\Omega \boldsymbol{Q} \Omega^T)^{-\frac{1}{2}} \Omega \boldsymbol{Q} \Omega^T (\Omega \boldsymbol{Q} \Omega^T)^{-\frac{T}{2}} = I \end{aligned}$$

4. The log-likelihood ratios to be used in the recursive algorithm for fault detection and isolation have the form

$$s_k(q, 0) = \boldsymbol{\mu}_q \boldsymbol{Q}_{r_n}^{-1} (\boldsymbol{r}_n(k) - \frac{1}{2}\boldsymbol{\mu}_q) \qquad q = 1, 2, 3$$

Since the normalized residual has a covariance matrix equal to the identity, the three loglikelihood ratios to be used are obtained from the above expression by setting $\boldsymbol{Q}_{r_n} = \boldsymbol{I}_3$ and computing $\boldsymbol{\mu}_q = (\mathit{\Omega} \boldsymbol{Q} \mathit{\Omega}^T)^{-\frac{1}{2}} \mathit{\Omega}_{.,q} f_q(k)$ with $f_q(k) = 0.5$. It yields:

$$\boldsymbol{\mu}_1 = \begin{bmatrix} -0.3006 \\ -0.2442 \end{bmatrix} \qquad \boldsymbol{\mu}_2 = \begin{bmatrix} 0.3824 \\ -0.0612 \end{bmatrix} \qquad \boldsymbol{\mu}_3 = \begin{bmatrix} -0.0818 \\ 0.3055 \end{bmatrix}$$

5. Example of MATLAB Code

   ```
   nitmax= 1000; % nitmax is the number of data samples
   k=1:nitmax;
   y=[1;1;1]*sin(0.1*k);
   y(1,:)=y(1,:)+[zeros(1,20) 0.5*ones(1,nitmax-20)];
   % Generation of the measurement noise
   v0=randn(3,nitmax);
   v=diag([1 1 sqrt(2)])*v0;
   % Obtaining the noisy measurements
   y=y+v;
   plot(k,y)
   ```

6. Example of MATLAB code
   See Figure S.1.

```
% Computation of the mean of the residual in the different faulty modes

Omega=null([1 1 1])';
Normal_fact=inv((sqrtm(Omega*diag([1 1 2])*Omega')))*Omega;
mu_1=Normal_fact*[0.5;0;0];
mu_2=Normal_fact*[0;0.5;0];
mu_3=Normal_fact*[0;0;0.5];

% Initialization of the 3 CUSUM algorithms
gbar_1=0;
gbar_2=0;
gbar_3=0;


% Initialization of the other program parameters
stop=0;
[n_r,m_r]=size(Omega);
nit=1; % number of iterations (equal to the number of measurement samples)
r_n=zeros(n_r,nitmax); % r_n stands for the normalized residual vector
g1=zeros(1,nitmax);% g1 to g3 stand for the test functions used in the FDI
algorithm
g2=zeros(1,nitmax); % All values are stored to be able to plot their evolution
g3=zeros(1,nitmax);

h=10;  %  h stands for the threshold in the test functions

while (stop==0) & (nit <= nitmax),
    r_n(:,nit)=inv((sqrtm(Omega*diag([1 1 2])*Omega')))*Omega*y(:,nit);
    gbar_1=max(0,gbar_1+mu_1'*(r_n(:,nit)-0.5*mu_1));
    gbar_2=max(0,gbar_2+mu_2'*(r_n(:,nit)-0.5*mu_2));
    gbar_3=max(0,gbar_3+mu_3'*(r_n(:,nit)-0.5*mu_3));
    g1(nit)=min(gbar_1-gbar_2, gbar_1-gbar_3);
    g2(nit)=min(gbar_2-gbar_1, gbar_2-gbar_3);
    g3(nit)=min(gbar_3-gbar_1, gbar_3-gbar_2);
    if g1(nit)>h, disp('alarm fault sensor 1'), stop=1, end;
    if g2(nit)>h, disp('alarm fault sensor 2'), stop=1, end;
    if g3(nit)>h, disp('alarm fault sensor 3'), stop=1, end;
    nit=nit+1;
end;
```

Fig. S.1. MATLAB code for point 6

Exercises of Chapter 8

Exercise 8.1 *Lattice-based analysis*

Consider an over-actuated system with three actuators and two sensors:

$$\begin{pmatrix} \dot{x}_1(t) \\ \dot{x}_2(t) \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 2 \end{pmatrix} \begin{pmatrix} x_1(t) \\ x_2(t) \end{pmatrix} + \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} u_1(t) \\ u_2(t) \\ u_3(t) \end{pmatrix}$$

$$\begin{pmatrix} y_1(t) \\ y_2(t) \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} x_1(t) \\ x_2(t) \end{pmatrix}$$

In order to understand the generality of the lattice-based analysis, this exercise considers, instead of the quadratic control problem, a simple specification that allows hand calculations. The specification is as follows: the two closed-loop eigenvalues are wished to be real and equal to -2 when output feedback is used, namely for $i = 1, 2, 3$ one has $u_i(t) = k_{i1} y_1(t) + k_{i2} y_2(t)$ where k_{i1}, k_{i2} are the control gains to be designed.

1. Characterise the set of admissible nominal control laws.
2. Assuming the two sensors are not faulty, analyse the effect of actuator faults under the reconfiguration strategy.
3. Is it possible to analyse the effect of sensor faults under the reconfiguration strategy in the same way? □

Solution

1. Replacing u_i by their values, one gets the closed-loop behaviour

   $$\begin{pmatrix} \dot{x}_1 \\ \dot{x}_2 \end{pmatrix} = \begin{pmatrix} k_{22} + k_{32} & 1 + k_{21} + k_{31} + k_{22} + k_{32} \\ -1 + k_{12} + k_{32} & 2 + k_{11} + k_{31} + k_{12} + k_{32} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$$

   whose eigenvalues satisfy the specification if and only if

   $$\begin{aligned} k_{11} + k_{12} + k_{22} + k_{31} + 2k_{32} \;&=\; -6 \\ k_{21} + k_{31} + 3k_{22} - k_{12} + 2k_{32} - k_{12}k_{21} - & \\ -k_{12}k_{31} - k_{32}k_{21} + k_{11}k_{22} + k_{31}k_{22} + k_{11}k_{32} \;&=\; 3 \end{aligned}$$

   The two equations can be solved in terms of the output feedback gains and moreover the solution is not unique, therefore the designer can select one that fits best some extra criterion.
2. Assuming the two sensors are not faulty, analyse the effect of actuator faults under the reconfiguration strategy.
   To study the recoverability of an actuator configuration, one has to check whether the design equations can be solved when the output feedback gains associated with the missing actuators are zeroed. For example, configuration 1 is recoverable if and only if

$$\begin{aligned} k_{11} + k_{12} &= -6 \\ k_{12} &= -3 \end{aligned}$$

has a solution, which is the case. Note that configuration 1 being recoverable, its predecessors 12,13 and 123 are recoverable. Note also that there is only one solution for configuration 1 but some degrees of freedom exist for its predecessors.
Similarly it can be checked that configuration 2 and its predecessors 12, 23 and 123 are recoverable, since

$$\begin{aligned} k_{22} &= -6 \\ k_{21} + 3k_{22} &= 3 \end{aligned}$$

has a solution, while configuration 3 is not recoverable because it is impossible to satisfy

$$\begin{aligned} k_{31} + 2k_{32} &= -6 \\ k_{31} + 2k_{32} &= 3 \end{aligned}$$

However, its predecessors 13, 23 and 123 are recoverable. Fig. S.2 shows the lattice of configurations of the three actuators system. White configurations are recoverable, grey configurations are not recoverable, and minimal recoverable configurations have a bold contour. The /12 means that both sensors 1 and 2 are healthy.

3. The procedure is the same, since switching-off a faulty sensor implies that the associated output feedback gain is zeroed. For example, assuming sensor 1 is faulty but actuators 123 are healthy, configuration $123/2$ is recoverable because

$$\begin{aligned} k_{12} + k_{22} + 2k_{32} &= -6 \\ 3k_{22} - k_{12} + 2k_{32} &= 3 \end{aligned}$$

has a solution.
So is configuration $123/1$ associated with the design equations

$$\begin{aligned} k_{11} + k_{31} &= -6 \\ k_{21} + k_{31} &= 3 \end{aligned}$$

and configuration $12/2$ associated with

$$\begin{aligned} k_{12} + k_{22} &= -6 \\ 3k_{22} - k_{12} &= 3 \end{aligned}$$

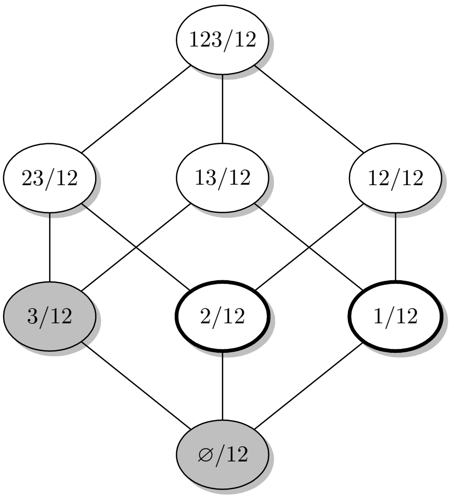

Fig. S.2. Recoverable configurations when the two sensors are healthy

but configurations $1/2$ and 2/1 are not recoverable, being respectively associated with the design equations

$$\begin{aligned} k_{12} &= -6 \\ k_{12} &= -3 \end{aligned}$$

and

$$\begin{aligned} 0 &= -6 \\ k_{21} &= 3 \end{aligned}$$

Fig. S.3 shows the recoverability span when sensor 1 is faulty.
Remark that one single lattice can be drawn considering the healthy/faulty state of each of the five components, as shown on Fig. S.4.

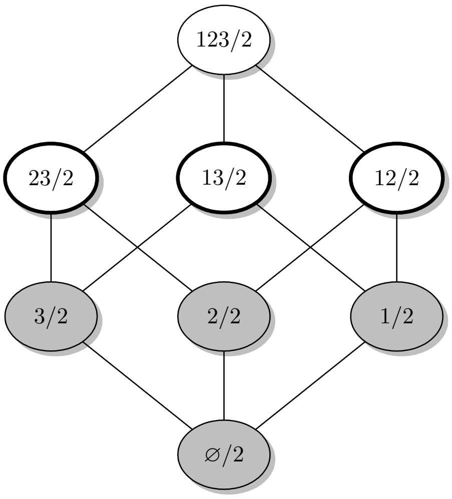

Fig. S.3. Recoverable configurations when sensor 1 is faulty

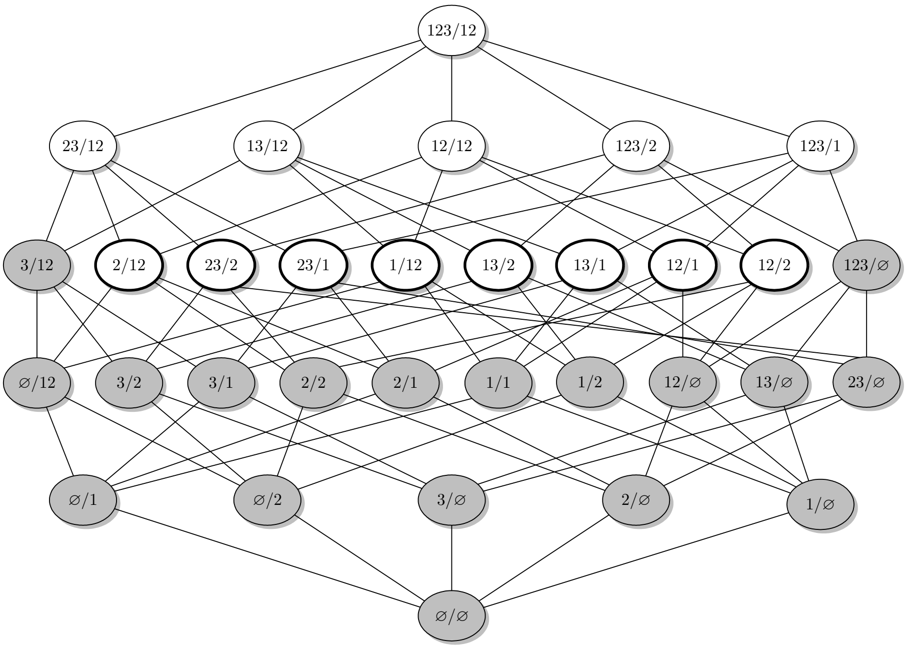

Fig. S.4. Recoverable configurations of the 5 components system

Exercise 8.2 *Reliable control*

Let $abcd$ be the four actuators of a linear time-invariant system:

$$\boldsymbol{A} = \begin{pmatrix} 0 & 0.17 & 0.17 & 0.33 \\ -0.17 & -0.17 & 0.17 & 0 \\ 0.33 & 0.33 & 0 & 0.17 \\ 0 & 0.17 & 0 & 0 \end{pmatrix}$$

$$\boldsymbol{B}_0 = \begin{pmatrix} 0.50 & 0 & 0 & 0 \\ 0 & 0.25 & 0 & 0 \\ 0 & 0 & 0.25 & 0 \\ 0 & 0 & 0 & 0.25 \end{pmatrix},$$

where matrix $\boldsymbol{A}$ is unstable, having the following set of eigenvalues:

$$\Lambda(\boldsymbol{A}) = \{-0.39; -0.031 \pm 0.141j; 0.28\}.$$

We are interested in the optimal quadratic control using the following weighting matrices:

$$\boldsymbol{Q} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \quad \text{and} \quad \boldsymbol{R} = I_4.$$

Faulty actuators are recovered, if possible, using the reconfiguration strategy. Under the recoverability specification that the optimal cost of the reconfigured system should not exceed 4 times the optimal cost of the healthy system, all configurations are recoverable except $\{ac, ad, bc, a, b, c, d\}$ as shown in Fig. S.5, where the white nodes are recoverable while the grey nodes are not.

1. From Fig. S.5 identify the minimal recoverable configurations.

2. Compute the coverage and the redundancy degrees. Is the system fail-operational with respect to the first fault? Configurations ab, bd, cd are respectively recovered by the optimal state feedbacks $\boldsymbol{u}_{ab} = \boldsymbol{K}_{ab}\boldsymbol{x}$, $\boldsymbol{u}_{bd} = \boldsymbol{K}_{bd}\boldsymbol{x}$ and $\boldsymbol{u}_{cd} = \boldsymbol{K}_{cd}\boldsymbol{x}$ where the feedback gains are given below and result in the cost matrices $\boldsymbol{W}^*_{ab}$, $\boldsymbol{W}^*_{bd}$, $\boldsymbol{W}^*_{cd}$ whose maximal eigenvalues are 18.53, 23.76 and 21.60:

$$\boldsymbol{K}_{ab} = \begin{pmatrix} -1.27 & -0.95 & -1.10 & -0.88 \\ -0.47 & -1.85 & -1.64 & -1.36 \\ -0.55 & -1.64 & -1.91 & -1.09 \\ -0.44 & -1.36 & -1.09 & -1.19 \end{pmatrix}$$

$$\boldsymbol{K}_{bd} = \begin{pmatrix} -3.18 & -2.18 & -2.32 & -2.41 \\ -1.09 & -1.88 & -1.82 & -1.49 \\ -1.16 & -1.82 & -2.23 & -1.28 \\ -1.20 & -1.49 & -1.28 & -1.63 \end{pmatrix}$$

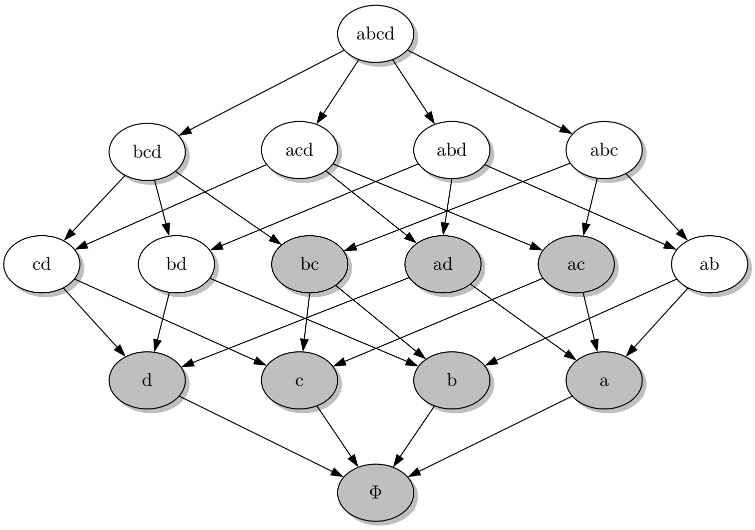

Fig. S.5. Recoverable configurations

$$\boldsymbol{K}_{cd} = \begin{pmatrix} -3.15 & -1.72 & -1.73 & -2.37 \\ -0.86 & -1.87 & -1.51 & -1.58 \\ -0.86 & -1.51 & -1.67 & -1.17 \\ -1.18 & -1.58 & -1.17 & -1.82 \end{pmatrix}$$

3. Let $\mathcal{U}$ be the reliable control bank that recovers all the recoverable configurations. List the control laws in $\mathcal{U}$. For each recoverable configuration list the control laws by which it is recovered. If several control laws allow to recover a given configuration, which one is to be selected?
4. Assume the control bank can implement only two control laws. What is the control law to be discarded? What is the influence on the coverage and the redundancy degrees? Is the system still fail-operational with respect to the first fault? □

Solution

1. The configurations ab, bd and cd are recoverable while their successors are not, hence they are minimal recoverable configurations.
2. The coverage is 0.5 since 8 configurations out of 16 are recoverable. The shortest path between $abcd$ and the set NR of non recoverable faults is 2, hence the strong redundancy degree is 2. The longest path between $abcd$ and NR is 3 hence the weak reedundancy degree. The system is fail operational with respect to the first fault, since all configurations with 3 actuators are recoverable.
3. Using the Reliable Control Theorem, a bank of three control laws, namely $u_{ab} = K_{ab}x$, $u_{bd} = K_{bd}x$ and $u_{cd} = K_{cd}x$ is able to recover all the recoverable configurations. The recovery control laws are given in Table 1.

Table S.1. Recovery control laws

i	$\mathcal{K}_i$
abcd	$\{K_{ab}, K_{bd}, K_{cd}\}$
abc	$\{K_{ab}\}$
acd	$\{K_{cd}\}$
abd	$\{K_{ab}, K_{bd}\}$
bcd	$\{K_{cd}, K_{bd}\}$
ab	$\{K_{ab}\}$
bd	$\{K_{bd}\}$
cd	$\{K_{cd}\}$

Configuration $abcd$ can be recovered by all 3 control laws, the one associated with the smallest cost is u_{ab}. Similarly, abd is best recovered by u_{ab} and bcd by u_{cd}.

4. Keeping only the two control laws $u_{ab} = K_{ab}x$ and $u_{cd} = K_{cd}x$, there is only one configuration, namely bd that can no longer be recovered. The coverage is reduced from 8/16 to 7/16, while the redundancy degrees remain the same. The system is still fail-operational with respect to the first fault.

Exercise 8.3 *Sensor network design*

Consider a measurement system with four unknown variables x_1, x_2, x_3, x_4 and five sensors a, b, c, d, e that provide five measurement signals y_1, y_2, y_3, y_4, y_5. Its structure graph is given by Fig. S.6.

We are interested in the output-connection property (denoted $\mathcal{P}$), which is a very important structural property of sensor networks. A system is output-connected if there is a path in the structural graph from any unknown variable to a sensor (this is a necessary condition for the structural observability of the unknown variables). From Fig. S.6, the system is clearly output-connected when the 5 sensors are used.

1. The lattice of system configurations allows to analyse the situations in which sensors are lost or removed from the sensor network. Determine whether property $\mathcal{P}$ holds or not for all the 4 sensor configurations (the configurations where one sensor is lost from the nominal configuration).
2. We now wish to determine whether the property holds or not for the sensor configurations where 2 sensors are lost. Do we need to analyse the subsets of $bcde$?
3. What is the output connection span, what are its minimal configurations.
4. Compute the coverage, and the weak and strong redundancy degrees of the nominal configuration $abcde$. Is property $\mathcal{P}$ fail operational with respect to the first fault?
5. What are the critical sensor subsets.
6. What can be said about sensor b.
7. Note that the critical subset a is a singleton, therefore the probability to loose property $\mathcal{P}$ because of the loss of a is one order of magnitude larger than the probability to loose

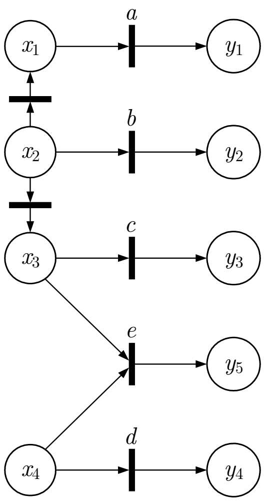

Fig. S.6. Structural graph of the measurement system

property $\mathcal{P}$ because of the loss of ce or de (assuming their failures are independent). Since b is useless, it might be interesting to remove sensor b from the sensor network and to duplicate sensor a. The new system a_1a_2cde is shown on Fig. S.7.

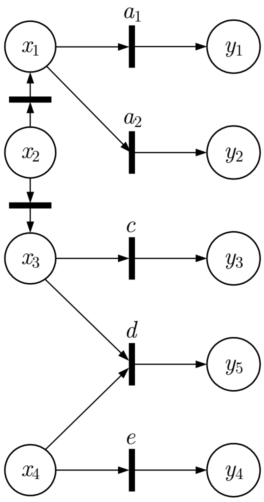

Fig. S.7. The new system with b removed and a duplicated

Go through questions 1 to 6 with the new system, and make comparisons. □

Solution

1. The property is still satisfied for configurations $abcd, abce, abde, acde$, but is no longer satisfied for configuration $bcde$.
2. No, because $bcde$ being not output-connected, its successors cannot be output-connected.
3. The lattice of sensor configurations is analysed by increasing levels.
   Level 1: $\mathcal{P}$ is satisfied for configurations $abcd, abce, abde, acde$ as seen in question 1
   Level 2: $\mathcal{P}$ is satisfied for configurations acd, abe, ace, ade
   Level 3: $\mathcal{P}$ is satisfied for configurations ae
   Levels 4 and 5 are empty.
   The minimal configurations are ae and acd. The span is given by Fig. S.8.

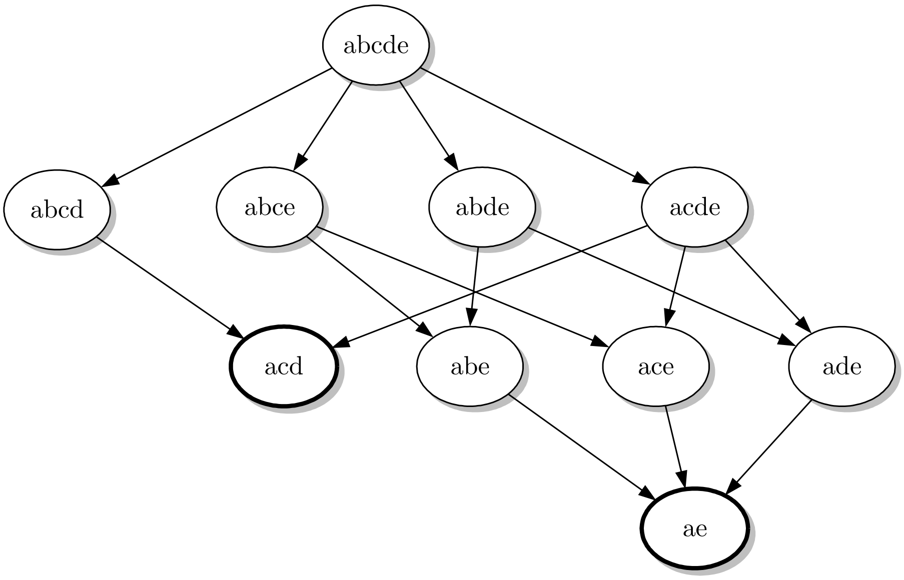

Fig. S.8. Span of the output connection property

4. The coverage is 10/32 because 10 configurations out of the 32 possible ones belong to the span of $\mathcal{P}$.
   The weak RDD is 4 which is the length of the longest path between the nominal configuration $abcde$ and the non-recoverable configurations. In this case, there are 6 such paths:
   $abcde - abce - abe - ae - NR$
   $abcde - abce - ace - ae - NR$
   $abcde - abde - abe - ae - NR$
   $abcde - abde - ace - ae - NR$
   $abcde - acde - ace - ae - NR$

$abcde - acde - ade - ae - NR$
where NR is the set of non-recoverable configurations.
The strong RDD is 1 because the shortest path is $abcde - NR$. The strong RDD = 1 shows that property $\mathcal{P}$ is not fail operational with respect to the first fault.

5. The critical sensor subsets are a, ce and de. Indeed, the loss of a gives $bcde \in NR$, the loss of ce gives $abd \in NR$ and the loss of de gives $abc \in NR$.
6. Sensor b is useless, because its loss does not change the value of the coverage.
7. Fig. S.9 gives the span of property $\mathcal{P}$ for the new system, which provides the answer to all the questions.

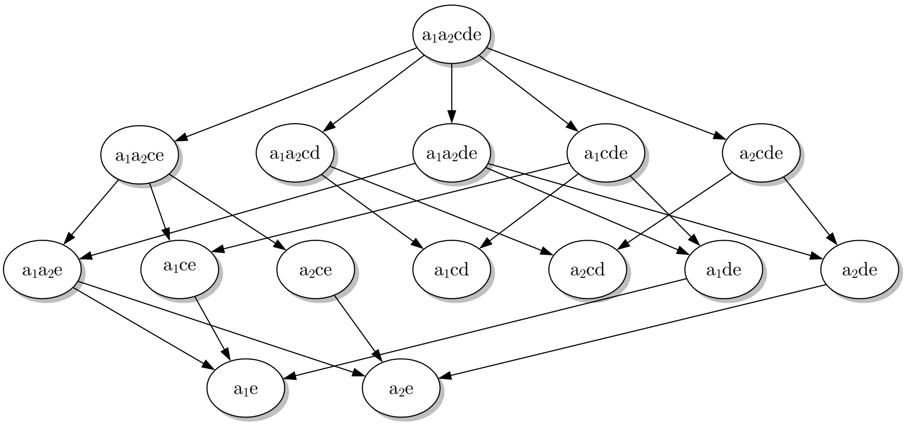

Fig. S.9. Span of the output connection property in the new system

Exercises of Chapter 10

Exercise 10.1 *Diagnosis of the two-tank system*

In this exercise we develop the complete diagnosis scheme of the two tank system in Chapter 2, where two level sensors h_{1m} and h_{2m} were implemented in addition to the flow sensor q_m. The set of constraints and unknown variables are the following:

$$\begin{aligned} \boldsymbol{f} \cup \boldsymbol{g} &= \{c_1, c_2, c_3, d_4, c_5, c_6, d_7, c_8, c_{\mathrm{m}}, c_{h1}, c_{h2}\} \\ \mathcal{X} &= \left\{q_L, q_P, h_1, \dot{h}_1, h_2, \dot{h}_2, q_2, q_{12}\right\}. \end{aligned}$$

The correspondence with the model in Chapter 2 is as follows: c_1 is Eq. (2.7), c_2 is Eq. (2.6), c_3 is Eq. (2.1), c_5 is Eq. (2.4), c_6 is Eq. (2.2) and c_8 is Eq. (2.5). The measurement equations are c_{m} which is Eq. (2.3) and c_{h1}, c_{h2} which are respectively the added measurements of the two levels h_1 and h_2. The constraints d_4 and d_7 respectively express that $\dot{h}_1$ and $\dot{h}_2$ are the time derivatives of h_1 and h_2. The incidence matrix with respect to $\mathcal{X}$ is:

Σ_1	q_L	q_P	$\dot{h}_1$	h_1	q_{12}	h_2	$\dot{h}_2$	q_2
c_1	①			1				
c_2		①		1				
c_3	1	1		1	①			
d_4			①	1				
c_5				1	1	1		
c_{h1}				①				
c_6					1		1	1
d_7						1	①	
c_8						1		1
$c_{\rm m}$								①
c_{h2}						①		

Based on the complete matching shown by the entries ①, the over-constrained subsystem produces three residuals whose structures are

$$\begin{aligned}
\mathcal{C}\left(\rho_1\right) &= \{c_1, c_2, c_3, c_5, c_{h1}, c_{h2}\} \\
\mathcal{C}\left(\rho_2\right) &= \{c_1, c_2, c_3, c_6, d_7, c_{\rm m}, c_{h1}, c_{h2}\} \\
\mathcal{C}\left(\rho_3\right) &= \{c_8, c_{\rm m}, c_{h2}\}\,.
\end{aligned}$$

1. What is the residuals' signature table.
2. The mathematical constraints d_4 and d_7 specify that $\dot{h}_1$ and $\dot{h}_2$ are the derivatives of h_1 and h_2. Discarding them (since they cannot be faulty), determine the system's distinguishability classes and draw the distinguishability table.
3. For each of the eight possible residual configurations, find the minimal hitting sets and draw the diagnosis table. □

Solution

1. The signature table is:

	OK	c_1	c_2	c_3	d_4	c_5	c_6	d_7	c_8	c_m	c_{h1}	c_{h2}
ρ_1		1	1	1		1					1	1
ρ_2		1	1	1			1	1		1	1	1
ρ_3									1	1		1

2. The distinguishability classes are $\mathcal{D}^0 = \{OK\}$,$\mathcal{D}^1 = \{c_1, c_2, c_3, c_{h1}\}$,$\mathcal{D}^2 = \{c_5\}$, $\mathcal{D}^3 = \{c_6\}$, $\mathcal{D}^4 = \{c_8\}$, $\mathcal{D}^5 = \{c_m\}$, and $\mathcal{D}^6 = \{c_{h2}\}$ that give the distinguishability table:

	$\mathcal{D}^0$	$\mathcal{D}^1$	$\mathcal{D}^2$	$\mathcal{D}^3$	$\mathcal{D}^4$	$\mathcal{D}^5$	$\mathcal{D}^6$
ρ_1		1	1				1
ρ_2		1		1		1	1
ρ_3					1	1	1

3. The diagnosis table is:

$\rho_1\rho_2\rho_3$	Diagnosis
000	$\mathcal{D}^0$
001	$\mathcal{D}^4$
010	$\mathcal{D}^3$
011	$\mathcal{D}^5 \cup \left(\mathcal{D}^3 \times \mathcal{D}^4\right)$
100	$\mathcal{D}^2$
101	$\mathcal{D}^2 \times \mathcal{D}^4$
110	$\mathcal{D}^1 \cup \left(\mathcal{D}^2 \times \mathcal{D}^3\right)$
111	$\mathcal{D}^6 \cup \left(\mathcal{D}^1 \times \mathcal{D}^4\right) \cup \left(\mathcal{D}^1 \times \mathcal{D}^5\right) \cup \left(\mathcal{D}^2 \times \mathcal{D}^5\right) \cup \left(\mathcal{D}^2 \times \mathcal{D}^3 \times \mathcal{D}^4\right)$

Exercise 10.2 *Two-tank system decomposition*

This exercise illustrates Remark 10.5 still with the two tank system. Assume each tank is a subsystem with the structures:

$$\begin{aligned} \boldsymbol{f}_1 \cup \boldsymbol{g}_1 &= \{c_1, c_2, c_3, d_4, c_5, c_{h1}\} \\ \boldsymbol{x}_1 &= \left\{q_L, q_P, h_1, \dot{h}_1, q_{12}\right\} \\ \overline{\boldsymbol{x}}_1 &= \{h_2\} \\ \boldsymbol{f}_2 \cup \boldsymbol{g}_2 &= \{c_6, d_7, c_8, c_{\mathrm{m}}, c_{h2}\} \\ \boldsymbol{x}_2 &= \left\{h_2, \dot{h}_2, q_2\right\} \\ \overline{\boldsymbol{x}}_2 &= \{q_{12}\}\,. \end{aligned}$$

The global incidence matrix is decomposed as follows:

Σ_1	q_L	q_P	$\dot{h}_1$	h_1	q_{12}	h_2
c_1	①			1		
c_2		①		1		
c_3	1	1		1	①	
d_4			①	1		
c_5				1	1	①
c_{h1}				①		

Σ_2	$\dot{h}_2$	h_2	q_2	q_{12}
c_6	1		1	①
d_7	①	1		
c_8		1	1	
c_{m}			①	
c_{h2}		①		

and two complete matchings with respect to the unknown variables are shown by ①.

1. How many local residuals are respectively provided by Σ_1 and Σ_2 and what are their structures?
2. Can you explain why there are less local residuals than when considering the global structure? □

Solution

1. There is no over-constrained subsystem in Σ_1 and there is only one local residual in Σ_2 with the structure $\{c_{h2}, c_m, c_8\}$.
2. Two of the three residuals exhibited by the global structure have disappeared. Indeed, a closer look at the two local structures shows that in Σ_1 the external variable h_2 can be computed using $\{c_1, c_2, c_3, c_5, c_{h1}\}$ while in Σ_2, h_2 is an internal variable that can be computed using c_{h_2}. Equating these two results would give a global residual with the structure $\{c_1, c_2, c_3, c_5, c_{h1}, c_{h2}\}$ that includes constraints from the two subsystems. This follows from the fact that in the structural analysis of the global model h_2 is over-constrained, while it is just-constrained in each of the two local structural analysis. Similarly, q_{12} can be computed in Σ_1 from $\{c_1, c_2, c_3, c_{h1}\}$ and in Σ_2 from $\{c_6, d_7, c_m, c_{h2}\}$ so the structure of the global residual obtained by equating these two results would be the union of these two structures.

Exercise 10.3 *Coordination of local diagnosis*

Consider a system in which there are 3 different estimation versions of an unknown variable x from the known variables $u' \cup y'$ (remember that the notation u', y' means u, y and a number of their time derivatives):

$$\begin{aligned} x &= f_1\left(u', y'\right) \quad \text{using the subset of constraints } C_1 = \{a, b, c, d\} \\ x &= f_2\left(u', y'\right) \quad \text{using the subset of constraints } C_2 = \{e, f\} \\ x &= f_3\left(u', y'\right) \quad \text{using the subset of constraints } C_3 = \{b, f, g, h\}. \end{aligned}$$

Three residuals are obtained:

$$\begin{aligned} \rho_1 &= f_1\left(u', y'\right) - f_2\left(u', y'\right) \\ \rho_2 &= f_1\left(u', y'\right) - f_3\left(u', y'\right) \\ \rho_3 &= f_2\left(u', y'\right) - f_3\left(u', y'\right). \end{aligned}$$

1. What are the structures of the residuals?
2. What is the distinguishability table?
3. Assuming there are three subsystems that run one residual each, what are the local diagnosis tables?
4. What is the coordinated diagnosis table? □

Solution

1. The structure of the residuals are:

$$C(\rho_1) = \{a, b, c, d, e, f\}$$
$$C(\rho_2) = \{a, b, c, d, f, g, h\}$$
$$C(\rho_3) = \{b, e, f, g, h\}$$

2. The distinguishibility table is:

	OK	a, c, d	b, f	e	g, h
ρ_1	0	1	1	1	0
ρ_2	0	1	1	0	1
ρ_3	0	0	1	1	1

3. The local diagnosis tables are:

ρ_1	Δ_1	ρ_2	Δ_2	ρ_3	Δ_3
0	$OK \cup \{g, h\}$	0	$OK \cup \{e\}$	0	$OK \cup \{a, c, d\}$
1	$\{a, b, c, d, e, f\}$	1	$\{a, b, c, d, f, g, h\}$	1	$\{b, e, f, g, h\}$

4. The coordinated diagnosis table is:

$\rho_1\rho_2\rho_3$	Δ_1	Δ_2	Δ_3	Δ
000	$OK \cup \{g, h\}$	$OK \cup \{e\}$	$OK \cup \{a, c, d\}$	$OK \cup \{g, h\}$ $\times \{e\} \times \{a, c, d\}$
001	$OK \cup \{g, h\}$	$OK \cup \{e\}$	$\{b, e, f, g, h\}$	$\{g, h\} \times \{e\}$
010	$OK \cup \{g, h\}$	$\{a, b, c, d, f, g, h\}$	$OK \cup \{a, c, d\}$	$\{g, h\} \times \{a, c, d\}$
011	$OK \cup \{g, h\}$	$\{a, b, c, d, f, g, h\}$	$\{b, e, f, g, h\}$	$\{g, h\}$
100	$\{a, b, c, d, e, f\}$	$OK \cup \{e\}$	$OK \cup \{a, c, d\}$	Cannot happen
101	$\{a, b, c, d, e, f\}$	$OK \cup \{e\}$	$\{b, e, f, g, h\}$	$\{e\}$
110	$\{a, b, c, d, e, f\}$	$\{a, b, c, d, f, g, h\}$	$OK \cup \{a, c, d\}$	$\{a, c, d\}$
111	$\{a, b, c, d, e, f\}$	$\{a, b, c, d, f, g, h\}$	$\{b, e, f, g, h\}$	$\{b, f\} \cup \{a, c, d\}$ $\times \{e, g, h\}$ $\cup \{e\} \times \{g, h\}$

Exercises of Chapter 12

Exercise 12.2 *Diagnosis of an interconnected discrete-event system*

Consider the system modelled by the I/O automata network shown in Fig. S.10. The system is designed so that the two subsystems represented by the automata $\mathcal{A}_1$ and $\mathcal{A}_2$ cannot reach the state 2 and 4 simultaneously.

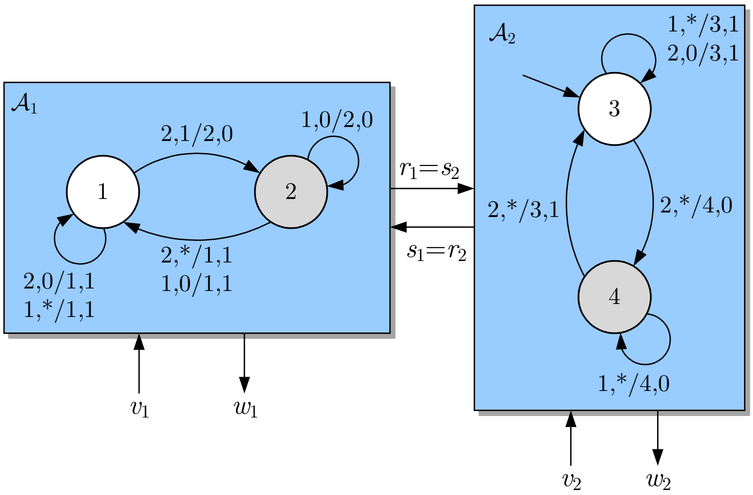

Fig. S.10. Composite system model

1. Combine the models shown in the figure to get a determinstic automaton of the overall system. Show that the specification mentioned above is satisfied.
2. The fault f_2 appearing in the automaton $\mathcal{A}_2$ makes the coupling output r_2 identical to 1 ($r_2(k) = 1$) independently of the automaton state. Change the model $\mathcal{A}_2$ accordingly. What happens in the model of the overall system?
3. Use decentralised diagnosers to detect the fault f_2. Is it possible to select an input sequence for both subsystems such that the fault is detected before the subsystems reach simultaneously the states 2 and 4?
4. Consider now a sensor fault, which makes the output of the automaton $\mathcal{A}_1$ constant: $w_1(k) = 1$. Can decentralised diagnosers detect this fault? Select, if possible, distinguishing input sequences for both subsystems. □

Solution

1. The overall system is described by the I/O automaton shown in Fig. S.11. The model shows that indeed the state $(2 \;\; 4)^{\mathrm{T}}$ is not reachable.
2. The faulty overall system can reach the state $(2 \;\; 4)^{\mathrm{T}}$ as shown in Fig. S.12.

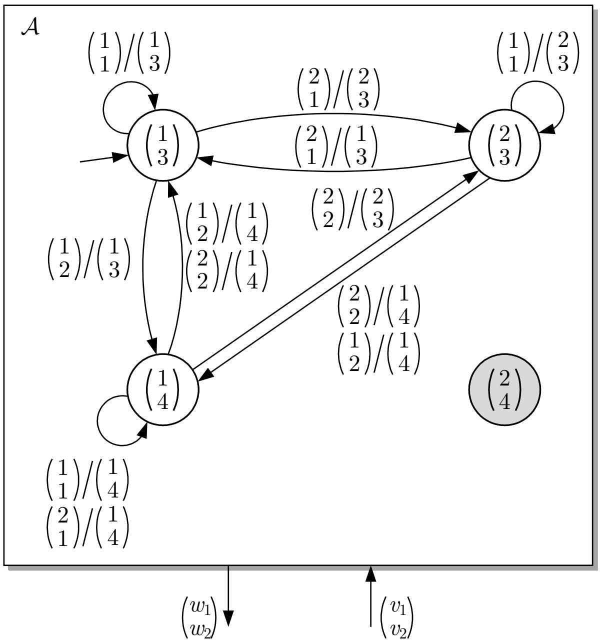
$\mathcal{A}$
$\binom{1}{1}/\binom{1}{3}$
$\binom{2}{1}/\binom{2}{3}$
$\binom{1}{1}/\binom{2}{3}$
$\binom{1}{3}$
$\binom{2}{1}/\binom{1}{3}$
$\binom{2}{3}$
$\binom{2}{2}/\binom{2}{3}$
$\binom{1}{2}/\binom{1}{4}$
$\binom{1}{2}/\binom{1}{3}$
$\binom{2}{2}/\binom{1}{4}$
$\binom{2}{2}/\binom{1}{4}$
$\binom{1}{2}/\binom{1}{4}$
$\binom{1}{4}$
$\binom{2}{4}$
$\binom{1}{1}/\binom{1}{4}$
$\binom{2}{1}/\binom{1}{4}$
$\binom{w_1}{w_2}$
$\binom{v_1}{v_2}$

Fig. S.11. Overall system model

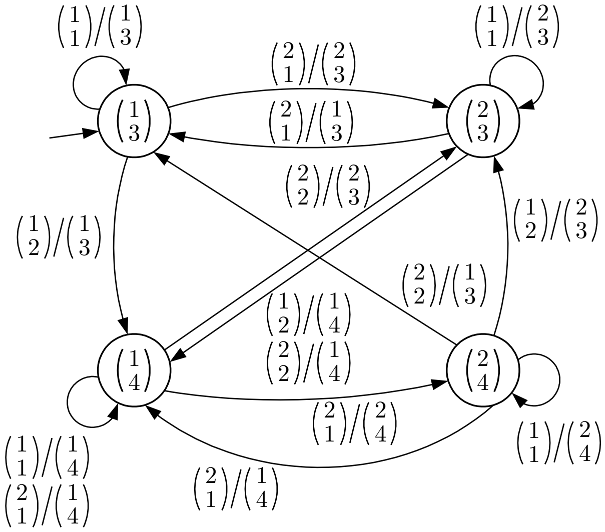
$\binom{1}{1}/\binom{1}{3}$
$\binom{1}{1}/\binom{2}{3}$
$\binom{2}{1}/\binom{2}{3}$
$\binom{1}{3}$
$\binom{2}{1}/\binom{1}{3}$
$\binom{2}{3}$
$\binom{2}{2}/\binom{2}{3}$
$\binom{1}{2}/\binom{1}{3}$
$\binom{1}{2}/\binom{2}{3}$
$\binom{2}{2}/\binom{1}{3}$
$\binom{1}{2}/\binom{1}{4}$
$\binom{2}{2}/\binom{1}{4}$
$\binom{1}{4}$
$\binom{2}{4}$
$\binom{2}{1}/\binom{2}{4}$
$\binom{1}{1}/\binom{2}{4}$
$\binom{1}{1}/\binom{1}{4}$
$\binom{2}{1}/\binom{1}{4}$
$\binom{2}{1}/\binom{1}{4}$

Fig. S.12. Model of the faulty overall system