Chapter 8
Reconfigurability Analysis

Abstract Fault-tolerant control brings together several theoretic frameworks that are needed to treat the different problems it involves. This chapter addresses these problems from a global perspective that includes the *specification* and the development of *control solutions*, as well as the *implementation* and the *evaluation* of these solutions. Among many possible control problems, this chapter uses linear quadratic control theory to illustrate the above-mentioned problems, under the two possible fault-tolerance strategies, namely *fault accommodation*, where the controller parameters are adapted to the parameters of the faulty plant, and *system reconfiguration*, where the subset of system components in operation is changed (and so is of course the control law). A variety of other control approaches will be developed in the next chapter.

8.1 The Fault-Tolerant Control Problem

8.1.1 Standard Control Problem

In order to explain the fault-tolerant control problem in more detail, the standard control problem is first stated as a problem that is defined by a given objective, a set of constraints and a set of admissible control laws. Standard control aims at finding a control law in a given set of control laws U, such that the controlled system achieves the control objectives O, while its behaviour satisfies a set of constraints C. Thus, the solution of the problem is completely defined by the triple $< O,\ C,\ U >$.

Problem 8.1 (*The control problem*)
Solve the problem $< O, C, U >$.

The following remarks should explain this problem in more detail:

- The set U of admissible control laws defines the algorithms that can be implemented, e.g. open-loop control (a mapping from the time domain to the control space), closed-loop control (a mapping from the output $\times$ reference spaces to the control space), using continuous or discrete-valued arguments for the variables,

© Springer-Verlag Berlin Heidelberg 2016

M. Blanke et al., *Diagnosis and Fault-Tolerant Control*,
DOI 10.1007/978-3-662-47943-8_8

allowing for continuous or discontinuous, differentiable or non-differentiable mappings, etc.

- The objective O defines what the system is expected to achieve, when controlled by the above-mentioned control law. It may range from very general statements (e.g. achieve closed-loop stability) to much more specific ones (e.g. reach a given point, on a given circular orbit around the earth, at a given time, for a space *rendez-vous*).
- Constraints C are functional relations that the behaviour of the controlled system must satisfy over time. They are expressed by algebraic and differential or difference equations, when continuous variables are considered, and by other models when discrete values are of interest (see Chap. 2). Inequality constraints express that some saturations act on the system admissible solutions (e.g. any trajectory which results from an admissible control law must end on a given point of a given circular orbit, at a given time, but the energy consumed all along the trajectory is limited by the capacity of the vessel's reservoirs).

Example 8.1 Control of the single-tank system
Consider the problem of filling an initially empty tank up to a certain mass m of some liquid, as fast as possible, so as to start a batch operation process in the food industry. Let $m(t)$ be the mass present in the tank at time t, and let $u(t)$ be the controlled input flow. The control problem is a very classical minimum time problem defined by the triple:

O: The objective is to change the mass $m(t)$ from its initial value $m(t_0) = 0$ to the given final value $m(t_\mathrm{f}) = M$, in minimum time, i.e. minimising the functional

$$\int_{t_0}^{t_\mathrm{f}} \mathrm{d}t.$$

C: The behaviour of the system is constrained by the state equation

$$\dot{m}(t) = u(t).$$

U: The control law belongs to the class of piecewise continuous open-loop controls with saturation

$$\begin{aligned} u:\ & |\mathcal{R}^+ \to |\mathcal{R} \\ & t \longmapsto u(t) \\ & u(t) \in [0,\ u_{\max}] \\ & u \in \mathcal{C}^0 \end{aligned}$$

Once the tank has been filled with the mass m of liquid, the production process of the batch will start. Assume that for the proper biological reaction to take place, the temperature $\eta(t)$ must be regulated around some given reference η_{ref}. The associated control problem is again well known. A PI-regulation example is given below:

O: The objective is to regulate the temperature $\eta(t)$ of the batch around the reference value η_{ref}, during the processing period $[0, T]$. It is expressed by

$$|\eta_{\text{ref}} - \eta(t)| \leq \lambda, \ \forall t \in [T_0, \ T],$$

where λ is some constant which defines the admissible temperature excursion around the reference on the time interval $[T_0, \ T]$, and $T_0 > 0$ is the time value after which the neighbourhood of the reference temperature must have been reached.

C: The behaviour of the system is described by the state and measurement equations

$$\begin{aligned}\dot{\eta}(t) &= f(\eta(t)) + \zeta(t) + v(t)\\ \dot{\zeta}(t) &= g(\eta(t), \ t)\\ y(t) &= \eta(t) + \varepsilon(t),\end{aligned}$$

which expresses that the temperature variation is the result of thermal losses $f(\eta(t))$, of the exothermic character of the biological reaction (the reaction energy is $\zeta(t)$, whose evolution is given by $g(\eta(t), t)$ in the second state equation), and of the control $v(t)$, and that the available measurement signal is the temperature, which is corrupted by some measurement error $\varepsilon(t)$.

U: The control law belongs to the class of closed-loop PI controls

$$\begin{aligned}v: \ & \Psi_{\text{ref}} \times Y \rightarrow |\mathcal{R}\\ & (\eta_{\text{ref}}, \ y(t)) \longmapsto v(t) = k_{\text{P}}(\eta_{\text{ref}} - y(t)) + k_{\text{I}} \int_0^t (\eta_{\text{ref}} - y(\tau)) \, \mathrm{d}\tau,\end{aligned}$$

where k_{P} and k_{I} are coefficients to be found as the solution of the control problem, Ψ_{ref} is the set of possible references and Y is the set of the sensor output values. □

8.1.2 Impacts of Faults on the Control Problem

Fault-tolerant control is concerned with the control of the faulty system. This can be done by changing the control law without changing the plant which is operated (this is the *fault accommodation* strategy), or by changing both the control and the system (this is the *reconfiguration* strategy). Since the control algorithm just implements the solution of a control problem for a given system, changing the control or the system means that the control problem has been changed as the result of faults. In order to understand the different strategies which can be applied to the design of fault-tolerant control, let us first consider the impact of faults on the control problem $< O, \ C(\theta), \ U >$, where $C(\theta)$ denotes the dependency of the constraint C upon the parameter θ, which in turn depends upon the fault. The different fault-tolerant control strategies will then be introduced, as a consequence of the available knowledge.

System objectives. The occurrence of faults should not change the system objectives. The objectives are associated with the users (they define what the users expect the

system to achieve), and the very nature of fault-tolerant control is to still try to achieve these objectives, *in spite* of the faults. However, this will be possible or not. Therefore, two cases have to be distinguished:

1. There is a mean of still achieving the system objectives in the presence of certain faults. The system is said to be fault tolerant, with respect to that objectives and to these faults. Equivalently, the faults are said to be recoverable. The control engineer's task is to design some control law which is able to do that.
2. The objectives cannot be achieved in the presence of the considered faults. The system is not fault tolerant with respect to that objectives and these faults, in other terms the faults are not recoverable. However, it is not enough to stand with this conclusion. The control engineer should provide, in this case, indications about what to do with the system. Since the current objectives cannot be achieved, the problem is transformed into finding new objectives that are of interest in the current situation, and to design the structure and the parameters of the new control law to achieve these new objectives.

System constraints. The occurrence of faults may obviously change the constraints $C(\theta)$ of the control problem.

- First, the constraints may remain the same but the parameters may change, thus transforming the control problem $< O, C(\theta_\mathrm{n}), U >$ into the problem $< O,\ C(\theta_\mathrm{f}),\ U >$, where θ_n (respectively θ_f) denotes the nominal (respectively the faulty) system parameters.
- Second, the constraints themselves might change, transforming the control problem $< O,\ C_\mathrm{n}(\theta_\mathrm{n}),\ U >$ into the problem $< O,\ C_\mathrm{f}(\theta_\mathrm{f}),\ U >$, where C_n is the set of nominal constraints, and $C_\mathrm{f}(\theta_\mathrm{f})$ is a set of new constraints with new associated parameters.

Both cases may be summarised by the change of $C_\mathrm{n}(\theta_\mathrm{n})$ into $C_\mathrm{f}(\theta_\mathrm{f})$ since the change of parameters only is a particular case, described by $C_\mathrm{f} = C_\mathrm{n}$.

Example 8.2 A tank with two exit pipes
Consider for example a tank with two exit pipes, respectively, situated at levels l_1 and l_2 metres. The system nominal constraints are the following:

$$\begin{aligned} x(t) \in [0,\ l_1[\ \ \dot{x}(t) &= q_i(t) \\ x(t) \in [l_1,\ l_2[\ \ \dot{x}(t) &= q_i(t) - q_1(v_1, t) \\ x(t) \geq l_2\ \ \dot{x}(t) &= q_i(t) - q_1(v_1, t) - q_2(v_2,\ t), \end{aligned}$$

where $x(t)$ is the level in the tank, $q_i(t)$ is the input flow, $q_1(v_1,\ t)$ (respectively $q_2(v_2, t)$) is the output flow through pipe 1 (respectively through pipe 2) which depends on some external variable or control signal v_1 (respectively v_2). This might be, for example, the level in another tank connected to the pipe, or the control signal of an output valve on the pipe. Suppose now that pipe 1 is clogged, then as the result of the fault, the system constraints become

$$\begin{aligned} x(t) \in [0,\ l_1[\ &\dot{x}(t) = q_i(t) \\ x(t) \in [l_1,\ l_2[\ &\dot{x}(t) = q_i(t) \quad \forall v_1(t) \\ x(t) \geq l_2\ &\dot{x}(t) = q_i(t) - q_2(v_2,\ t), \end{aligned}$$

which can also be represented by adding a fourth constraint to the three nominal ones

$$\begin{aligned} x(t) \in [0,\ l_1[\ &\dot{x}(t) = q_i(t) \\ x(t) \in [l_1,\ l_2[\ &\dot{x}(t) = q_i(t) - q_1(v_1,\ t) \\ x(t) \geq l_2\ &\dot{x}(t) = q_i(t) - q_1(v_1,\ t) - q_2(v_2,\ t) \\ &q_1(v_1,\ t) = 0, \forall v_1,\ t. \quad \square \end{aligned}$$

Admissible control laws. The occurrence of faults may also change the set of admissible control laws since faults may occur in the computing and communication devices in which they are implemented. As in the previous subsection, the new set of admissible control laws is noted U_{f} while the nominal one is U_{n}.

Example 8.1 (cont.) Control of a single-tank system
Consider the standard control problem of filling a tank in minimum time for processing a batch in food industry: find the control law in the set U_{n} of piecewise continuous functions satisfying

$$\begin{aligned} u:\ & |\mathcal{R}^+ \rightarrow |\mathcal{R} \\ & t \longmapsto u(t) \\ & u(t) \in [0,\ u_{\max}] \\ & u \in \mathcal{C}^0 \end{aligned}$$

such that the initial mass $m(t_0) = 0$ is changed into the final mass $m(t_{\mathrm{f}}) = M$, in minimum time, while satisfying the state equation $\dot{m}(t) = u(t)$. Suppose now that the pump is faulty and can only deliver a fraction of its nominal maximum output flow, namely $u_{\max}$ is changed into $u'_{\max} < u_{\max}$. The set U_{n} is changed into the set U_{f}, where the saturation level is lower (thus leading to a larger filling time for the optimal solution). $\square$

8.1.3 Passive Versus Active Fault-Tolerant Control

In the passive approach, the control algorithm is designed so that the system is able to achieve its given objectives, in healthy as well as in faulty situations, without any change in the control law. Therefore, passive fault-tolerant control sets the control problem in a context, where the ability of the system to achieve its given objective is preserved, using the same control law, whatever the system situation (healthy or faulty).

In active approaches, the control law is changed when faults occur, so that the ability of the system to achieve its given objective is preserved, using a control law adapted to each fault situation. Therefore, active fault-tolerant control algorithms

implement the solution of problems which are specifically set for each of the possible (healthy and faulty) situations.

As the result of faults, the control problem is transformed

$$\text{from} \quad < O,\ C_{\mathrm{n}}(\theta_{\mathrm{n}}),\ U_{\mathrm{n}} > \quad \text{into} \quad < O,\ C_{\mathrm{f}}(\theta_{\mathrm{f}}),\ U_{\mathrm{f}} >.$$

Suppose that both $C_{\mathrm{f}}(\theta_{\mathrm{f}})$ and U_{f} are perfectly known, then the fault-tolerant control law has to solve $< O,\ C_{\mathrm{f}}(\theta_{\mathrm{f}}),\ U_{\mathrm{f}} >$. If such a solution exists, the system is fault tolerant with respect to the objective O and the fault situation $C_{\mathrm{f}}(\theta_{\mathrm{f}}),\ U_{\mathrm{f}}$. If the problem $< O,\ C_{\mathrm{f}}(\theta_{\mathrm{f}}),\ U_{\mathrm{f}} >$ has no solution, then the system is not fault tolerant and objective reconfiguration has to be explored, as previously explained.

The difference between passive and active fault-tolerant control can now be very simply explained.

Passive fault tolerance. In passive fault tolerance, the control law is not changed when faults occur. This means that the system objectives can be obtained when the system is healthy (thus it solves $< O,\ C_{\mathrm{n}}(\theta_{\mathrm{n}}),\ U_{\mathrm{n}} >$), as well as when the system is faulty (thus it also solves $< O,\ C_{\mathrm{f}}(\theta_{\mathrm{f}}),\ U_{\mathrm{f}} >$). Implementing passive fault tolerance for a given set of faults means that there is a common solution to problem $< O,\ C_{\mathrm{n}}(\theta_{\mathrm{n}}),\ U_{\mathrm{n}} >$ and to all problems $< O,\ C_{\mathrm{f}}(\theta_{\mathrm{f}}),\ U_{\mathrm{f}} >$, $(f \in \mathcal{F})$, where $\mathcal{F}$ indexes the set of all the considered faults.

This is a very particular situation, which is fulfilled, in general, only for objectives associated with very low levels of performances (this is a so-called *conservative* approach). Note that since the control law is not changed, the passive fault-tolerance approach is similar to the robust approach when uncertain systems are considered (cf. Chap. 1). Indeed, faults can be considered as uncertainties which affect the system parameters. The difference lies not only in the size and interpretation of these changes, but also in the fact that the structure of the constraints may change as the result of faults.

Active fault tolerance. In active fault tolerance, each of the problems

$$< O,\ C_{\mathrm{n}}(\theta_{\mathrm{n}}),\ U_{\mathrm{n}} > \text{ and } < O,\ C_{\mathrm{f}}(\theta_{\mathrm{f}}),\ U_{\mathrm{f}} >,$$

$f \in \mathcal{F}$, has its own specific solution, thus allowing for much more demanding objectives. However, for each of these problems to be solved the knowledge about $C_{\mathrm{f}}(\theta_{\mathrm{f}})$ and U_{f} must be available. This is the role of fault detection and isolation algorithms. This chapter deals with active fault-tolerant control.

8.1.4 Available Knowledge

Providing information about the fault impact is the aim of the fault diagnosis algorithms. However, the power and efficiency of these algorithms are limited. Fault detection informs that the problem to solve is no longer $< O,\ C_{\mathrm{n}}(\theta_{\mathrm{n}}),\ U_{\mathrm{n}} >$. Fault

isolation informs about the subset of the constraints $C_n(\theta_n)$ which are unchanged (those associated with the still healthy components), and the subset $U_f \subseteq U_n$ of control laws which can still be used. The knowledge about the changed constraints calls for fault estimation, which is a new function to be considered for the design of fault-tolerant control. According to its performances, three cases must be considered:

1. The fault diagnosis algorithm is able to provide an estimate $\hat{C}_f(\hat{\theta}_f)$, $\hat{U}_f$ of the fault impact. Then, the problem to be solved is the standard control problem $< O, \hat{C}_f(\hat{\theta}_f), \hat{U}_f >$. Note that, when a solution exists, there is still a risk that the actual faulty system (described by $C_f(\theta_f)$ and U_f) fails to satisfy the objectives O, although the available model of the faulty system does satisfy them.
2. The fault diagnosis algorithm is able to provide an estimate $\hat{\Gamma}_f(\hat{\Theta}_f)$, U_f of the fault impact, where $\hat{\Gamma}_f$ is a set of possible constraints and $\hat{\Theta}_f$ is a set of associated parameters. Then the problem to be solved is the robust control problem $< O, \hat{\Gamma}_f(\hat{\Theta}_f), \hat{U}_f >$. When a solution exists, the actual faulty system will satisfy the objectives O provided the actual constraints $C_f(\theta_f) \in \hat{\Gamma}_f(\hat{\Theta}_f)$, otherwise, the same risk as above exists.
3. The fault diagnosis algorithm detects and isolates the faults, but it cannot provide any estimate of the fault impact. The control engineer is faced with the problem of designing the control of a completely unknown system, which is not possible. Obtaining knowledge about that system could be thought of, using e.g. learning approaches, but then an estimation of the fault impact could indeed be obtained, which would bring the problem back to case 2.

Other possible cases are those where the fault diagnosis system detects the fault, but it cannot isolate it nor is it able to provide any estimate, and the case, where the fault diagnosis system does not even detect the fault. In the first case, the only possibility to keep mastering the system is to move to a fall back mode, while in the second case, any catastrophic behaviour is possible. Active fault tolerance is only concerned with cases 1, 2 and 3.

8.1.5 Active Fault-Tolerant Control Strategies

Fault accommodation. Fault accommodation is the fault-tolerant control strategy which is associated with cases 1 and 2. It solves the problem $< O, \hat{C}_f(\hat{\theta}_f), \hat{U}_f >$ or $< O, \hat{\Gamma}_f(\hat{\Theta}_f), \hat{U}_f >$, which is associated with the control of the faulty system. The fault situation can be accommodated with respect to the objectives O when the problem has a solution.

Problem 8.2 (*Fault accommodation problem*)
Solve the control problem $< O, \hat{C}_f(\hat{\theta}_f), \hat{U}_f >$, where $\hat{C}_f(\hat{\theta}_f)$ is the estimate of the actual constraints provided by the fault diagnosis algorithms.

Note that the interpretation of fault accommodation is that it is a strategy by which the faulty system is controlled in a specific way, so as to still achieve the objectives which were (before the fault) achieved by the healthy system.

System reconfiguration. System reconfiguration is the fault-tolerant control strategy which is associated with case 3. Remind that in this case the faulty system is absolutely unknown, but the control engineer wishes to design a control that achieves the system objectives. The only means to set any control problem is to switch off the faulty components (which are known from the isolation function), and to try to achieve the objectives using only the remaining (healthy) ones. Let $C_{\mathrm{f}}(\theta_{\mathrm{f}}) = C'_{\mathrm{n}}(\theta_{\mathrm{n}}) \cup C''_{\mathrm{f}}(\theta_{\mathrm{f}})$, where $C'_{\mathrm{n}}(\theta_{\mathrm{n}})$ is the subset of the constraints which are associated with the healthy part of the system, and $C''_{\mathrm{f}}(\theta_{\mathrm{f}})$ is the subset of the constraints which are associated with the faulty part.

Problem 8.3 (*Reconfiguration problem*)
Find a new set of system constraints $C_{\mathrm{f}}(\theta_{\mathrm{f}})$ such that the control problem $< O, C_{\mathrm{f}}(\theta_{\mathrm{f}}), U >$ has a solution, find and activate this solution.

The choice of a new set of constraints will imply that the input–output relations between the controller and the plant are changed.

Note that the constraints $C'_{\mathrm{n}}(\theta_{\mathrm{n}})$ are known while $C''_{\mathrm{f}}(\theta_{\mathrm{f}})$ are unknown. Using similar notations, let $U_{\mathrm{f}} = U'_{\mathrm{n}} \cup U''_{\mathrm{f}}$. Then, the reconfiguration strategy solves the problem $< O, C'_{\mathrm{n}}(\theta_{\mathrm{n}}), U'_{\mathrm{n}} >$, i.e. it tries to achieve the system objectives by controlling only the healthy part of the system.

Fault accommodation and reconfiguration are distinguished according to whether the I/O signals between the controller and the plant are changed. Reconfiguration implies the use of different I/O relations between the controller and the system. Switching the system to a different internal structure, to change its mode of operation, is an example of such I/O switching. Accommodation does not use such means.

Both fault accommodation and system reconfiguration strategies may need new control laws in response to faults. They also have to manage transient behaviour, which result from the change of control law or change of the constraints' structure.

8.1.6 Supervision

Suppose that the accommodation and the reconfiguration strategies fail to provide a solution. This means that there is no possibility, using the faulty system (accommodation) or a subsystem of it (reconfiguration) to achieve the objective. In this case, another objective has to be provided to the system. This introduces the most general problem, defined by the 3-tuple $< \mathcal{O}, \mathcal{C}(\theta), \mathcal{U} >$, where $\mathcal{O}$ is a set of possible control objectives. This problem is called the supervision problem. It is a decision problem in which the system objective is not pre-defined, but has to be determined, according to the system possibilities at each time, taking into account the actual system possibilities.

A supervision problem is thus a fault-tolerant control problem associated with a decision problem: if faults are such that fault tolerance cannot be achieved, the system goal itself has to be changed. When far-reaching decisions with respect to the system goal have to be taken, human operators are generally involved.

It may happen that no achievable objective exists under the actual system possibilities. This can be a design error, or a deliberate choice to accept certain failure scenarios, e.g. for reasons of benefit or small likelihood of certain events. Note that fail-to-safe conditions are intended to avoid this case in some situations, since they express that for certain classes of faults, the objective of stopping the system must always be achievable.

8.2 Fault-Tolerant Control Architecture

The method to achieve fault tolerance, which is considered in this chapter, relies on employing fault diagnosis schemes on-line and on reacting to the results of the diagnosis. A discrete-event signal to a supervisor agent is generated by the diagnostic algorithm when a fault is detected, another when it is isolated. This activates an alternative control that is supposed to handle the fault. The control for the particular case could be pre-determined for each type of critical fault or obtained from real-time analysis and on-line re-design. In any event, the design process must run through a number of cases equal to the number of faults to be handled and the control system needs to be re-designed for each such case. Some types of faults in sensors and actuators are simple to handle, others require a detailed re-design. It is, thus, worthwhile to first consider the simplest possibilities, thereafter the more general and complicated case of re-design.

The architecture of a fault-tolerant control system is illustrated in Fig. 8.1. A fault is a discrete event that acts on a system and by that changes some of its properties. Having diagnosed a fault, a decision needs to be taken about a remedial action.

The goal of fault-tolerant control is to respond to the occurrence of a fault such that the faulty system still satisfies the given specifications. Due to the discrete nature of the fault occurrence and reconfiguration, fault-tolerant control systems are hybrid in nature (cf. Sect. 3.7). In the figure, σ_f denotes fault events, σ_a are control events reconfiguring the system and q_c the control mode, which selects a control law. The actual physical mode q_p of the plant may be viewed as the discrete state of an automaton which is driven by plant internal events σ_p, the fault events σ_f and the control events σ_a. While many different approaches can be used to solve the fault-tolerant control problem, it may not be possible to control the system to a desired performance for an arbitrary change of parameter or structure. A final remedial action is then to close down to a safe state should proper control not be possible. The key issue is to be able to obtain certain specified properties of the control of the faulty system, and this chapter, therefore, focusses on methods for re-design based on specifications.

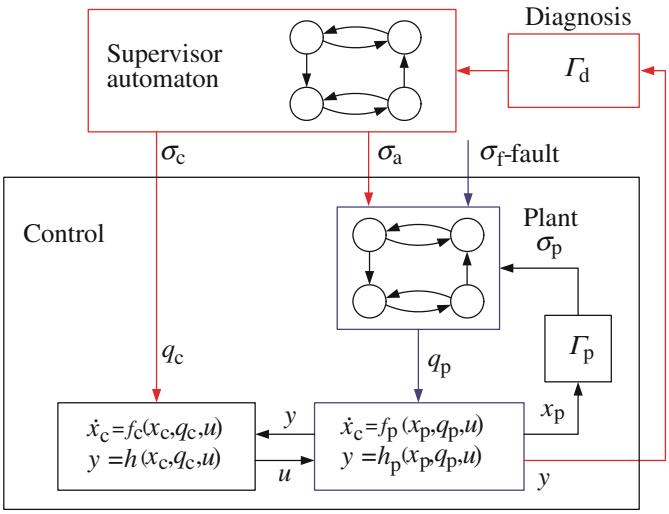

Fig. 8.1 The plant can change in a discrete way through change in states, a plant fault can cause a discrete event. Plant architecture can be changed by switch-over functions. Parameters or structure of the controller can be changed by logic in a supervisor automaton. The automaton gets its input from fault diagnosis

A fault in the plant can affect the structure and the parameters of a plant. The complexity of designing a controller for the faulty system is therefore immense, and there is no single, systematic way to design a control system with reconfiguration as depicted. Most research work deal either with diagnosis or controller reconfiguration, but not both. One approach is based on a bank of controllers, each one being associated to a healthy or a faulty plant working mode. The selection of the controller to be used for the present working mode must be assumed to be achieved with some delay and possibly false alarms.

The theory of logic-based switching control also relies on a bank of controllers (Fig. 8.2). It has recently been used for fault-tolerant control. The supervisor is made of a set of estimators, followed by performance evaluation, and a switching logic scheme (Fig. 8.3).

Each estimator reconstructs the plant output in either one of the healthy or faulty working modes. Its performance is evaluated by computing a norm of the output estimation error, and the estimator that yields the smallest performance index is assumed to correspond to the present working mode. The output of the switching logic η is the integer associated with that estimator, i.e. the estimator number. The corresponding controller is applied to the process using the switching logic.

This approach, however, presupposes that for each fault a reasonable controller has been designed before the plant is put into operation. From a practical point of view, this is not reasonable if a considerable number of faults has to be taken into account. To deal with this problem, two approaches are presented in this chapter, namely first methods that re-design the controller on-line after a fault has been identified to avoid

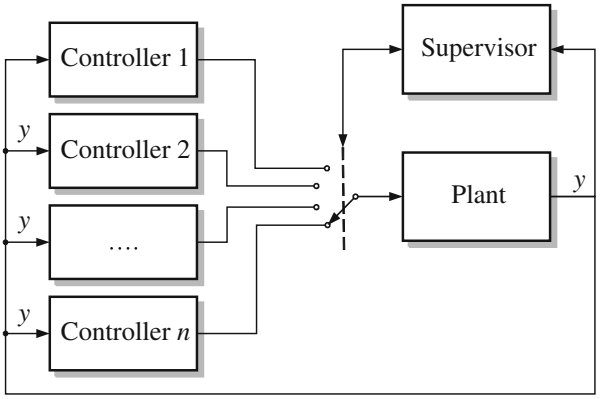

Fig. 8.2 Structure of logic-based switching controller

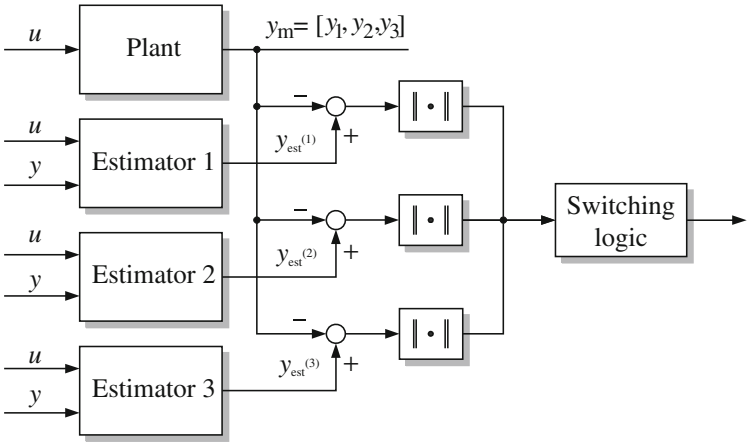

Fig. 8.3 Logic within a supervisor selects an output estimate from a bank of estimators

the use of a pre-determined bank of control laws, and second methods for reducing the size of pre-determined banks of control laws.

Note that a pre-determined bank of control laws needs possibly large memory space for their implementation but allow fast on-line reaction: once the fault has been isolated, the adequate control is just switched on, without any extra calculations. On the other hand, on-line re-design of the control law does not need extra storage but one has to wait for the design algorithm to be completed before the appropriate control law can be used.

In the sequel of this chapter, different approaches to the fault-tolerant control problem are presented, which refer to different objectives and faults. Although the presented approaches can also be used in different frames, this chapter builds on optimal control, actuator faults and the reconfiguration strategy. The linear quadratic

problem under actuator faults is considered in Sect. 8.3. Section 8.4 presents the lattice of actuator subsets whose properties are important since only the subset of healthy actuators controls the system under the reconfiguration strategy. Section 8.5 discusses the implementation problem associated with on-line re-design versus bank of control laws. The evaluation of fault tolerance is the subject of Sect. 8.6.

8.3 Fault-Tolerant Linear Quadratic Design

8.3.1 Control Problem

Linear quadratic (LQ) problems constitute a very popular frame for control design. In this section, the LQ problem is analysed with respect to the possible occurrence of actuator faults. It is shown that fault tolerance can only be achieved if admissible (rather than optimal) solutions exist. Conditions on an actuator fault to be possibly tolerated are given both for the fault accommodation and for the system reconfiguration strategies.

Consider the system whose nominal operation is modelled by

$$\dot{\boldsymbol{x}}(t) = \boldsymbol{A}\boldsymbol{x}(t) + \boldsymbol{B}\boldsymbol{u}(t) = \boldsymbol{A}\boldsymbol{x}(t) + \sum_{i \in I} \boldsymbol{B}_i \, \boldsymbol{u}_i(t). \tag{8.1}$$

$\boldsymbol{x} \in \mathcal{X} \subset |\mathcal{R}^n$ is the state vector and $\boldsymbol{u} \in \mathcal{U} \subset |\mathcal{R}^m$ is the control vector. I is the set of the actuators, $\boldsymbol{u}_i(t) \in |\mathcal{R}^{m_i}$ is the input of actuator $i \in I$, and $m = \sum_{i \in I} m_i$. $\boldsymbol{A}$ and $\boldsymbol{B}$ are constant matrices of suitable dimensions, and it is assumed that the pair $(\boldsymbol{A}, \boldsymbol{B})$ is controllable. The following optimal control problem is considered:

Problem 8.4 (*Optimal control problem*)

1. **Objective** O**:** Transfer the system state from $\boldsymbol{x}(0) = \gamma$ towards $\boldsymbol{x}(\infty) = \boldsymbol{0}$, where $\gamma \in |\mathcal{R}^n$, and $\boldsymbol{x}(\infty)$ stands for $\lim_{t \longrightarrow \infty} \boldsymbol{x}(t)$ while minimising the functional

$$J(\boldsymbol{u}, \gamma) = \frac{1}{2} \int_0^\infty (\boldsymbol{u}^{\mathrm{T}}(t) \boldsymbol{R}\boldsymbol{u}(t) + \boldsymbol{x}^{\mathrm{T}}(t) \boldsymbol{Q}\boldsymbol{x}(t)) \, \mathrm{d}t, \tag{8.2}$$

   where $\boldsymbol{Q}$ and $\boldsymbol{R}$ are symmetric matrices, and $\boldsymbol{Q} \geq 0$, $\boldsymbol{R} > 0$.
2. **Constraints** C: Equation (8.1) is satisfied $\forall t \in [0, \infty)$, $\boldsymbol{x}(t)$ and $\boldsymbol{u}(t)$ are continuous functions of time, and $\mathcal{X} = |\mathcal{R}^n, \mathcal{U} = |\mathcal{R}^m$ hold.

8.3.2 Control of the Nominal Plant

The solution of Problem 8.4 is well known from the classical theory of optimal control. Let $H(\boldsymbol{x}, \boldsymbol{u}, \boldsymbol{p}, t)$ be the system Hamiltonian

$$H(\boldsymbol{x}(t),\ \boldsymbol{u}(t),\ \boldsymbol{p}(t),\ t) = -\frac{1}{2}\left(\boldsymbol{u}^{\mathrm{T}}(t)\boldsymbol{R}\boldsymbol{u}(t) + \boldsymbol{x}^{\mathrm{T}}(t)\boldsymbol{Q}\boldsymbol{x}(t)\right) + \boldsymbol{p}^{\mathrm{T}}(t)\left(\boldsymbol{A}\boldsymbol{x}(t) + \boldsymbol{B}\boldsymbol{u}(t)\right),$$

where $\boldsymbol{p}(t)$ is the adjoint state vector, then the necessary optimality condition is

$$\dot{\boldsymbol{x}}(t) = \frac{\partial H}{\partial \boldsymbol{p}}(\boldsymbol{x}(t),\ \boldsymbol{u}(t),\ \boldsymbol{p}(t),\ t) = \boldsymbol{A}\boldsymbol{x}(t) + \boldsymbol{B}\boldsymbol{u}(t) \tag{8.3}$$

$$\dot{\boldsymbol{p}}(t) = -\frac{\partial H}{\partial \boldsymbol{x}}(\boldsymbol{x}(t),\ \boldsymbol{u}(t),\ \boldsymbol{p}(t),\ t) = \boldsymbol{Q}\boldsymbol{x}(t) - \boldsymbol{A}^{\mathrm{T}}\boldsymbol{p}(t) \tag{8.4}$$

$$\boldsymbol{0} = \frac{\partial H}{\partial \boldsymbol{u}}(\boldsymbol{x}(t),\ \boldsymbol{u}(t),\ \boldsymbol{p}(t),\ t) = \boldsymbol{u}(t) - \boldsymbol{R}^{-1}\boldsymbol{B}^{\mathrm{T}}\boldsymbol{p}(t).$$

It is easy to show that the optimal solution is given by

$$\begin{aligned}\boldsymbol{p}(t) &= -\boldsymbol{P}\boldsymbol{x}(t)\\ \boldsymbol{u}(t) &= -\boldsymbol{R}^{-1}\boldsymbol{B}^{\mathrm{T}}\boldsymbol{P}\boldsymbol{x}(t),\end{aligned}$$

where $\boldsymbol{P}$ is the (symmetric) solution of the algebraic Riccati equation

$$\boldsymbol{Q} + \boldsymbol{A}^{\mathrm{T}}\boldsymbol{P} + \boldsymbol{P}\boldsymbol{A} - \boldsymbol{P}\boldsymbol{B}\boldsymbol{R}^{-1}\boldsymbol{B}^{\mathrm{T}}\boldsymbol{P} = \boldsymbol{0}$$

such that the closed-loop system

$$\dot{\boldsymbol{x}}(t) = \left(\boldsymbol{A} - \boldsymbol{B}\boldsymbol{R}^{-1}\boldsymbol{B}^{\mathrm{T}}\boldsymbol{P}\right)\boldsymbol{x}(t)$$

is stable. The solution exists since the pair $(\boldsymbol{A}, \boldsymbol{B})$ is controllable, and the optimal value of the criterion is given by

$$J(0,\ \emptyset,\ \gamma) = \frac{1}{2}\gamma^{\mathrm{T}}\boldsymbol{P}\gamma, \tag{8.5}$$

where the argument $0,\ \emptyset$ recalls that there is no faulty actuator on the time window $[0,\ \infty)$.

Nominal performances. Equation (8.5) shows that the nominal performance of the actuator set I depends on the value of γ.

$$\Gamma = \{\gamma \in |\mathcal{R}^n,\ \text{s.t.}\ \frac{1}{2}\gamma^{\mathrm{T}}\boldsymbol{P}\gamma \leq 1\}$$

represents the set of points in the state space from which the origin can be reached with a cost less than 1. The characterisation of the actuation scheme I independently of the control objective γ leads to consider the worst control problem from the quadratic criterion point of view: transfer the system state from $\boldsymbol{x}(0) = \gamma^*$ to $\boldsymbol{x}(\infty) = \boldsymbol{0}$,

where

$$\gamma^* = \arg\max_{|\gamma|=1} J\,(0, \emptyset, \gamma).$$

The set of actuators I is thus characterised by the maximum eigenvalue of $\boldsymbol{P}$ which is interpreted as the maximum cost which might be spent in transferring the system state from $\boldsymbol{x}(0) = \gamma$ to $\boldsymbol{x}(\infty) = \boldsymbol{0}$ for some $\gamma \in |\mathcal{R}^n$ such that $|\gamma| = 1$

$$J\left(0, \emptyset, \gamma^*\right) = \frac{1}{2}\lambda_{\max}(\boldsymbol{P}). \tag{8.6}$$

8.3.3 Fault Tolerance with Respect to Actuator Faults

This section considers the situation in which the system is faultless until the time instant t_f and has afterwards a fault in one or several actuators. Hence, the whole set of actuators I is healthy in the time interval $(0,\ t_\mathrm{f}[$ while there is a subset I_F of faulty actuators in the interval $[t_\mathrm{f},\ \infty)$. Let $I = I_\mathrm{N} \cup I_\mathrm{F}$, where I_N is the subset of the still normal actuators. After t_f the faulty system behaviour is described by

$$\dot{\boldsymbol{x}}(t) = \boldsymbol{A}\boldsymbol{x}(t) + \sum_{i \in I_\mathrm{N}} \boldsymbol{B}_i\, \boldsymbol{u}_i\,(t) + \sum_{i \in I_\mathrm{F}} \boldsymbol{\beta}_i\ (\boldsymbol{u}_i(t),\ \theta_i), \tag{8.7}$$

where $\boldsymbol{\beta}_i\ (\boldsymbol{u}_i(t),\ \theta_i)$ describes the contribution of the faulty actuator i. This vector may be known, known with unknown parameters θ_i or completely unknown, depending on the faults which are considered, and of the capability of the fault diagnostic algorithm to estimate them. The objective, constraints and criterion of the fault-tolerant control problem are identical to those of the control problem, with the exception of constraint (8.1) being valid on $(0,\ t_\mathrm{f}[$ and being replaced by constraint (8.7) on $[t_\mathrm{f},\ \infty)$.

Problem constraints. Two cases can be considered as far as the status of constraint (8.7) is concerned.

1. In the first case, the fault tolerance analysis is done (off-line) for given faults, which are known to possibly occur in the considered system (from the failure-modes and effect analysis, for example). Therefore, constraint (8.7) *is known* and the fault-tolerant control can be designed beforehand (but it can be applied on-line only when the actual fault matches the fault for which it has been designed, which needs the actual fault to be identified).
2. In the second case, the analysis is done for any kind of fault which might occur during the system operation and, therefore, constraint (8.7) *being not known* has again to be identified (or replaced by another constraint if identification is impossible or not available). The identification of the subset I_F of faulty actuators is normally done by the fault diagnostic algorithm, which detects and isolates the faults. Defining the constraints resumes to identifying the functions

$\boldsymbol{\beta}_i(\boldsymbol{u}_i(t), \theta_i), i \in I_F$. This is not usually done by fault diagnostic algorithms, and could be referred to as a *diagnostic* (or fault estimation) possibility, which rests on fault modelling and on fault parameter identification, and it could be—or not—provided by the fault diagnostic system.

Therefore, the two approaches to fault-tolerant control can be applied in dependence upon the situation. Fault accommodation consists of controlling the faulty system after replacing Eq. (8.7) by

$$\dot{\boldsymbol{x}}(t) = \boldsymbol{A}\boldsymbol{x}(t) + \sum_{i \in I_N} \boldsymbol{B}_i \, \boldsymbol{u}_i(t) + \sum_{i \in I_F} \hat{\boldsymbol{\beta}}_i \left(\boldsymbol{u}_i(t), \, \hat{\boldsymbol{\theta}}_i \right), \tag{8.8}$$

where the functions $\hat{\boldsymbol{\beta}}_i \, (\boldsymbol{u}_i(t), \, \hat{\boldsymbol{\theta}}_i)$ and parameters $\hat{\boldsymbol{\theta}}_i, i \in I_F$ are estimated. System reconfiguration consists of controlling only the healthy part of the system (thus switching off the faulty actuators), which means replacing Eq. (8.7) by

$$\dot{\boldsymbol{x}}(t) = \boldsymbol{A}\boldsymbol{x}(t) + \sum_{i \in I_N} \boldsymbol{B}_i \, \boldsymbol{u}_i(t). \tag{8.9}$$

Admissible solutions. Whatever the selected strategy, a solution to the fault-tolerant control problem exists provided the objective $\boldsymbol{x}(\infty) = \boldsymbol{0}$ can still be reached from the initial state $\boldsymbol{x}(0) = \boldsymbol{\gamma}$. When solutions are needed to exist for any objective $\boldsymbol{\gamma}$, it is obviously necessary that the system (8.7) or (8.9) is still controllable.

Suppose that the fault-tolerant control problem has a solution, i.e. the system state can be transferred from $\boldsymbol{x}(0) = \boldsymbol{\gamma}$ to $\boldsymbol{x}(\infty) = \boldsymbol{0}$, and introduce the notation

$$J \, ((0, \, t_f), \, (\emptyset, \, I_F), \, \boldsymbol{\gamma}) \tag{8.10}$$

for the minimal cost associated with the two time instants $(0, \, t_f)$ at which the failed actuators are respectively $(\emptyset, \, I_F)$. Obviously, the fact that a solution exists does not mean that it is satisfactory. Two cases can be distinguished.

- The cost is of no importance provided the system objective is achieved in spite of the fault. In this case, the actuation scheme I is fault tolerant with respect to the situation I_F occurring at time t_f if and only if system (8.8)—when accommodation is used—or (8.9)—when reconfiguration is concerned—is controllable.
- Some cost limitation is considered. Although optimal, the cost might be too high, thus denying the actuation scheme I to deserve the "fault-tolerant" label with respect to the situation I_F.

Definition 8.1 (*Admissibility*) Let I_F be a fault situation occurring at time t_f. The solution of the fault-tolerant control problem is admissible with respect to the control objective $\boldsymbol{\gamma}$ if and only if

$$J\left((0,\ t_{\mathrm{f}}),\ (\emptyset,\ I_{\mathrm{F}}),\ \gamma\right) \leq \rho(\gamma) J\left(0,\ \emptyset,\ \gamma\right), \tag{8.11}$$

where $\rho(\gamma) \geq 1$ is some pre-defined function.

In Eq. (8.11), $\rho(\gamma)$ is the maximal loss of efficiency which is allowed when a control solution, which still achieves the objective γ but under the situation where the fault I_{F} occurs at time t_{f}, is used. Three special choices of $\rho(\gamma)$ may be of interest.

- $\rho(\gamma) = \infty,\ \forall \gamma \in |\mathcal{R}^n$.
  In this case, fault tolerance is only concerned with the existence of an optimal solution, whatever its cost, thus reducing the fault-tolerance property to the permanence of the controllability property: any fault such that the system remains controllable is recoverable,
- $\rho(\gamma) = \frac{\sigma}{\gamma^{\mathrm{T}} \boldsymbol{P} \gamma},\ \forall \gamma \in |\mathcal{R}^n,\ |\gamma| \leq 1$
  defines a uniform bound σ for the cost of controlling the faulty system, whatever the initial state in the unit sphere: any fault such that there exists a stabilising control whose cost is less than σ is recoverable,
- $\rho(\gamma) = \rho^*,\ \forall \gamma \in |\mathcal{R}^n$
  defines a uniform bound for the loss of efficiency in the control of the faulty system, whatever the control objective: any fault such that there exists a stabilising control associated with a cost degradation factor less than ρ^* is recoverable.

Based on the definition of admissibility, fault tolerance can be defined as follows.

Definition 8.2 (*Fault tolerance of a system subject to actuator faults*) The actuation scheme I is fault tolerant with respect to the fault I_{F} occurring at time t_{f} for the control objective γ if the accommodation or the reconfiguration problem has an admissible solution (equivalently, fault I_{F} occurring at time t_{f} is said to be recoverable).

8.3.4 Fault Accommodation

The accommodation strategy is now analysed for the system described by

$$\dot{\boldsymbol{x}}(t) = \boldsymbol{A}\boldsymbol{x}(t) + \sum_{i \in I} \boldsymbol{B}_i\, \boldsymbol{u}_i(t) \quad \text{for } t \in [0,\ t_{\mathrm{f}}[$$

$$\dot{\boldsymbol{x}}(t) = \boldsymbol{A}\boldsymbol{x}(t) + \sum_{i \in I_{\mathrm{N}}} \boldsymbol{B}_i\, \boldsymbol{u}_i(t) + \sum_{i \in I_{\mathrm{F}}} \boldsymbol{\beta}_i\ (\boldsymbol{u}_i(t),\ \theta_i), \quad \boldsymbol{x}(t_{\mathrm{f}}) = \boldsymbol{x}_{\mathrm{f}},$$

$$\text{for } t \in [t_{\mathrm{f}},\ \infty).$$

Identifying the faulty system. Since the functions $\boldsymbol{\beta}_i\ (\boldsymbol{u}_i(t),\ \theta_i)$ and parameters θ_i, $i \in I_{\mathrm{F}}$ are not known, they must be estimated, and therefore the LQ control problem is set for the model

$$\dot{\boldsymbol{x}}(t) = \boldsymbol{A}\boldsymbol{x}(t) + \sum_{i \in I} \boldsymbol{B}_i \, \boldsymbol{u}_i(t) \quad \text{for } t \in [0, \, t_\mathrm{f}[$$

$$\dot{\boldsymbol{x}}(t) = \boldsymbol{A}\boldsymbol{x}(t) + \sum_{i \in I_\mathrm{N}} \boldsymbol{B}_i \, \boldsymbol{u}_i(t) + \sum_{i \in I_\mathrm{F}} \hat{\beta}_i \, \left(\boldsymbol{u}_i(t), \, \hat{\theta}_i\right) \quad \text{for } t \in [t_\mathrm{f}, \, \infty),$$

where the functions $\hat{\beta}_i \, \left(\boldsymbol{u}_i(t), \, \hat{\boldsymbol{\theta}}_i\right)$ and parameters $\hat{\boldsymbol{\theta}}_i$, $i \in I_\mathrm{F}$ are known. This approach obviously needs some fault model to be defined, and its parameters to be identified.

Assume it is known that the faulty actuators can still be described by a linear model

$$\hat{\beta}_i \, \left(\boldsymbol{u}_i(t), \, \hat{\boldsymbol{\theta}}_i\right) = \hat{\boldsymbol{B}}_i \, \boldsymbol{u}_i(t), \, i \in I_\mathrm{F}$$

and, therefore, the model of the faulty system is

$$\begin{aligned} \dot{\boldsymbol{x}}(t) &= \boldsymbol{A}\boldsymbol{x}(t) + \sum_{i \in I_\mathrm{N}} \boldsymbol{B}_i \boldsymbol{u}_i(t) + \sum_{j \in I_\mathrm{F}} \hat{\boldsymbol{B}}_j \boldsymbol{u}_j(t) \\ &= \boldsymbol{A}\boldsymbol{x}(t) + \boldsymbol{B}_\mathrm{f} \boldsymbol{u}(t), \end{aligned} \tag{8.12}$$

where $\boldsymbol{B}_\mathrm{f} = (\boldsymbol{B}_\mathrm{N}, \hat{\boldsymbol{B}}_\mathrm{F})$ is the new actuator matrix, formed by the concatenation of the $\boldsymbol{B}_i$ matrices associated with the healthy actuators $\boldsymbol{B}_\mathrm{N} = (\boldsymbol{B}_i, i \in I_\mathrm{N})$ and the $\hat{\boldsymbol{B}}_j$ matrices associated with the faulty actuators $\hat{\boldsymbol{B}}_\mathrm{F} = (\hat{\boldsymbol{B}}_j, j \in I_\mathrm{F})$.

Accomodating the control to the faulty system. From Bellman's optimality principle, the accommodation strategy consists of applying the optimal control solution to system (8.12), with initial condition $\boldsymbol{x}_\mathrm{f} = \boldsymbol{x}(t_\mathrm{f})$, on the time interval $[t_\mathrm{f}, \, \infty)$, thus leading to compute the accommodated control and trajectories as the solution of

$$\begin{aligned} \dot{\boldsymbol{x}}(t) &= \boldsymbol{A}\boldsymbol{x}(t) + \boldsymbol{B}_\mathrm{f} \boldsymbol{u}(t) \\ \dot{\boldsymbol{p}}(t) &= \boldsymbol{Q}\boldsymbol{x}(t) - \boldsymbol{A}^\mathrm{T} \boldsymbol{p}(t) \\ \boldsymbol{u}(t) &= \boldsymbol{R}^{-1} \, \boldsymbol{B}_\mathrm{f}^\mathrm{T} \boldsymbol{P} \boldsymbol{x}(t) \end{aligned} \tag{8.13}$$

with the result that the value of the criterion is now

$$J\left((0, \, t_\mathrm{f}), \, (\emptyset, \, I_\mathrm{F}), \, \boldsymbol{\gamma}\right)\right) = J_{0f} + \frac{1}{2} \boldsymbol{x}_\mathrm{f}^\mathrm{T} \boldsymbol{P}_\mathrm{f} \boldsymbol{x}_\mathrm{f} \tag{8.14}$$

instead of

$$J(0, \, \emptyset, \, \boldsymbol{\gamma}) = \frac{1}{2} \boldsymbol{\gamma}^\mathrm{T} \boldsymbol{P} \boldsymbol{\gamma},$$

where J_{0f} is the cost already spent between $t = 0$ and $t = t_\mathrm{f}$ and $\boldsymbol{P}_\mathrm{f}$ is the solution of the algebraic Riccati equation in which $\boldsymbol{B}$ has been replaced by $\boldsymbol{B}_\mathrm{f}$, namely

$$\boldsymbol{Q} + \boldsymbol{A}^\mathrm{T} \boldsymbol{P}_\mathrm{f} + \boldsymbol{P}_\mathrm{f} \, \boldsymbol{A} - \boldsymbol{P}_\mathrm{f} \, \boldsymbol{B}_\mathrm{f} \, \boldsymbol{R}^{-1} \, \boldsymbol{B}_\mathrm{f}^\mathrm{T} \, \boldsymbol{P}_\mathrm{f} = \boldsymbol{0}. \tag{8.15}$$

Testing the admissibility of the accommodated control. From simple calculations, and taking into account that

$$J(0,\ \emptyset,\ \gamma) = J_{0f} + \frac{1}{2}\boldsymbol{x}_{\mathrm{f}}^{\mathrm{T}}\,\boldsymbol{P}\boldsymbol{x}_{\mathrm{f}}$$

one has

$$J_{0f} = \frac{1}{2}\gamma^{\mathrm{T}}\boldsymbol{P}\gamma - \frac{1}{2}\boldsymbol{x}_{\mathrm{f}}^{\mathrm{T}}\,\boldsymbol{P}\boldsymbol{x}_{\mathrm{f}}$$

and therefore

$$J\left((0,\ t_{\mathrm{f}}),\ (\emptyset,\ I_{\mathrm{F}}),\ \gamma\right)) = \frac{1}{2}\gamma^{\mathrm{T}}\boldsymbol{P}\gamma + \frac{1}{2}\boldsymbol{x}_{\mathrm{f}}^{\mathrm{T}}\,(\boldsymbol{P}_{\mathrm{f}} - \boldsymbol{P})\,\boldsymbol{x}_{\mathrm{f}}. \tag{8.16}$$

From (8.14) and the different definitions of admissibility, the set of triples

$$(\boldsymbol{B}_{\mathrm{f}}, t_{\mathrm{f}}, \gamma)$$

which can be tolerated by an accommodation strategy are characterised as follows:

- $\rho(\gamma) = \infty,\ \forall\gamma \in |\mathcal{R}^n$

$$(\boldsymbol{A},\ \boldsymbol{B}_{\mathrm{f}})\ \text{controllable} \tag{8.17}$$

- $\rho(\gamma) = \frac{\sigma}{\gamma^{\mathrm{T}}\boldsymbol{P}\gamma},\ \forall\gamma \in |\mathcal{R}^n,\ |\gamma| \leq 1$

$$\begin{array}{c}(\boldsymbol{A},\ \boldsymbol{B}_{\mathrm{f}})\ \text{controllable}\\ \boldsymbol{x}_{\mathrm{f}}^{\mathrm{T}}\,(\boldsymbol{P}_{\mathrm{f}} - \boldsymbol{P})\,\boldsymbol{x}_{\mathrm{f}} \leq \sigma - \gamma^{\mathrm{T}}\boldsymbol{P}\gamma\end{array} \tag{8.18}$$

- $\rho(\gamma) = \rho^*,\ \forall\gamma \in |\mathcal{R}^n$

$$\begin{array}{c}(\boldsymbol{A},\ \boldsymbol{B}_{\mathrm{f}})\ \text{controllable}\\ \boldsymbol{x}_{\mathrm{f}}^{\mathrm{T}}\,(\boldsymbol{P}_{\mathrm{f}} - \boldsymbol{P})\,\boldsymbol{x}_{\mathrm{f}} \leq (\rho^* - 1)\,\gamma^{\mathrm{T}}K\gamma\end{array} \tag{8.19}$$

Note that these conditions depend on the value of the state $\boldsymbol{x}_{\mathrm{f}}$ at the time of the fault occurrence, which is computed by

$$\boldsymbol{x}_{\mathrm{f}}(t) = \mathrm{e}^{\,\boldsymbol{A}t_{\mathrm{f}}}\,\gamma + \int_0^{t_{\mathrm{f}}} e^{\boldsymbol{A}(t_{\mathrm{f}}-t)}\,\boldsymbol{B}\boldsymbol{u}(t)\,\mathrm{d}t,$$

where $\boldsymbol{u}(t)$ is the optimal control computed from (8.4), and can also be expressed as

$$\boldsymbol{x}_{\mathrm{f}} = \mathrm{e}^{\left(\boldsymbol{A}-\boldsymbol{B}\boldsymbol{R}^{-1}\,\boldsymbol{B}^{\mathrm{T}}\boldsymbol{P}\right)t_{\mathrm{f}}}\gamma.$$

Since t_{f} is unknown beforehand, these conditions can only be checked on-line, at time t_{f} when the fault is detected, isolated and diagnosed. Of course, it might be

unpleasant to discover on-line that the fault that just occurred cannot be accommodated. Therefore, it is interesting to look for sufficient conditions, which could be checked off-line. Such conditions can be found under the reasonable assumption that if the objective can be reached by an admissible control using the faulty system from the beginning, then it can also be reached by an admissible control when the nominal system is first used and replaced (at an unknown time) by the faulty one.

This assumption is satisfied as it can be seen by considering the worst case value of $\boldsymbol{x}_{\mathrm{f}}$ in the previous conditions. Under the assumption that $(\boldsymbol{P}_{\mathrm{f}} - \boldsymbol{P}) \geq 0$ (which is reasonable since it states that the faulty actuators are less efficient than the healthy ones), the worst case situation is that in which the fault occurs right at time $t_{\mathrm{f}} = 0$, and therefore one has $\boldsymbol{x}_{\mathrm{f}} = \boldsymbol{\gamma}$, which leads to the sufficient conditions (8.20)–(8.22) for the fault I_{F} to be tolerated using an accommodation strategy. Note that these conditions characterise all the pairs $(\boldsymbol{B}_{\mathrm{f}}, \boldsymbol{\gamma})$ for which the system is fault tolerant, whatever the time at which the fault $\boldsymbol{B}_{\mathrm{f}}$ occurs.

- $\rho(\boldsymbol{\gamma}) = \infty, \forall \boldsymbol{\gamma} \in |\mathcal{R}^n$

$$(\boldsymbol{A},\ \boldsymbol{B}_{\mathrm{f}})\ \text{controllable} \tag{8.20}$$

- $\rho(\boldsymbol{\gamma}) = \frac{\sigma}{\boldsymbol{\gamma}^{\mathrm{T}} \boldsymbol{P} \boldsymbol{\gamma}},\ \forall \boldsymbol{\gamma} \in |\mathcal{R}^n,\ |\boldsymbol{\gamma}| \leq 1$

$$\begin{array}{c} (\boldsymbol{A},\ \boldsymbol{B}_{\mathrm{f}})\ \text{controllable} \\ \boldsymbol{\gamma}^{\mathrm{T}} \boldsymbol{P}_{\mathrm{f}} \boldsymbol{\gamma} \leq \sigma \end{array} \tag{8.21}$$

- $\rho(\boldsymbol{\gamma}) = \rho^*,\ \forall \boldsymbol{\gamma} \in |\mathcal{R}^n$

$$\begin{array}{c} (\boldsymbol{A},\ \boldsymbol{B}_{\mathrm{f}})\ \text{controllable} \\ \boldsymbol{\gamma}^{\mathrm{T}} \left(\boldsymbol{P}_{\mathrm{f}} - \rho^* \cdot \boldsymbol{P}\right) \boldsymbol{\gamma} \leq 0 \end{array} \tag{8.22}$$

The conditions under which the fault $\boldsymbol{B}_{\mathrm{f}}$ can be tolerated for any objective $\boldsymbol{\gamma}$, whatever the time at which it occurs, are given by

- $\rho(\boldsymbol{\gamma}) = \infty,\ \forall \boldsymbol{\gamma} \in |\mathcal{R}^n$

$$(\boldsymbol{A},\ \boldsymbol{B}_{\mathrm{f}})\ \text{controllable}, \tag{8.23}$$

- $\rho(\boldsymbol{\gamma}) = \frac{\sigma}{\boldsymbol{\gamma}^{\mathrm{T}} \boldsymbol{P} \boldsymbol{\gamma}},\ \forall \boldsymbol{\gamma} \in |\mathcal{R}^n,\ |\boldsymbol{\gamma}| \leq 1$

$$\begin{array}{c} (\boldsymbol{A},\ \boldsymbol{B}_{\mathrm{f}})\ \text{controllable} \\ \lambda_{\max}\left(\boldsymbol{P}_{\mathrm{f}}\right) \leq \sigma, \end{array} \tag{8.24}$$

- $\rho(\boldsymbol{\gamma}) = \rho^*,\ \forall \boldsymbol{\gamma} \in |\mathcal{R}^n$

$$\begin{array}{c} (\boldsymbol{A},\ \boldsymbol{B}_{\mathrm{f}})\ \text{controllable} \\ \lambda_{\max}\left(\boldsymbol{P}_{\mathrm{f}} - \rho^* \cdot \boldsymbol{P}\right) \leq 0. \end{array} \tag{8.25}$$

8.3.5 Control Reconfiguration

Reconfiguration strategies set the control problem of a system in which the faulty part has been switched off. The choice of a reconfiguration strategy might follow from the impossibility of estimating the fault, or it can be deliberate, so as to implement fault-tolerant strategies which provide guaranteed results, and are as simple and as understandable as possible by operators. In many cases, reconfiguration is understood as the replacement of the faulty part by some non-faulty one. Considering the problem under investigation, this means that some actuators were not in service before the fault occurrence and that they can be switched on after the fault.

Let I_{off} be the set of those actuators, which are assumed without loss of generality to be non-faulty. It obviously follows that considering from the beginning the whole set of actuators $I \cup I_{\text{off}}$ reduces the problem to that of reconfiguring the system $I_{\text{off}} \cup I_{\text{N}} \cup I_{\text{F}}$ by simply removing the faulty part. Thus, including I_{off} within I (namely, into I_{N}), one can go on with unchanged notations. In this situation, the fault-tolerant control problem has to be analysed replacing Eq. (8.7) by

$$\dot{\boldsymbol{x}}(t) = \boldsymbol{A}\boldsymbol{x}(t) + \sum_{i \in I_{\text{N}}} \boldsymbol{B}_i \, \boldsymbol{u}_i(t).$$

Therefore, all the previous results and statements also apply to the reconfiguration strategy, provided $\boldsymbol{B}_{\text{f}} = \left(\boldsymbol{B}_{\text{N}},\ \hat{\boldsymbol{B}}_{\text{F}}\right)$ is replaced by $\boldsymbol{B}_{\text{f}} = (\boldsymbol{B}_{\text{N}},\ \boldsymbol{O})$.

It is easily seen that $\boldsymbol{B}_{\text{f}}$ only depends on the subset of actuators I_{N} whatever the faults that act on the subset of actuators I_{F}. Therefore, neither is it needed to assume that the faulty actuators be described by a linear model $\hat{\boldsymbol{B}}_{\text{f}}$, nor is it needed to identify this model. Moreover, since there is only a finite number of actuator subsets, the reconfigured controls can be computed off-line for each possible subset I_{F}, and the solution can be switched on-line as soon as the FDI has provided the current subset of faulty actuators (this needs only fault detection and isolation). Note that for some subsets I_{F} an admissible solution will not exist, therefore it is of interest to analyse off-line all the possible subsets of faulty actuators.

8.4 The Lattice of Actuator Subsets

The accommodation and reconfiguration strategies have been presented in the previous section for the case of actuator faults in the Linear Quadratic problem. However, whatever the control objectives, the reconfiguration strategy always deals with controlling only the subset of the system's healthy components (the faulty ones are switched off) and therefore, the analysis of the system's component subsets is the general frame in which the reconfiguration problem is to be considered. This is the goal of this section.

8.4.1 Actuator Configurations

Since I is the set of all actuators in the system, the power set 2^I is the set of all possible actuator subsets, also named *actuator configurations*. According to the fact that the pair $(\boldsymbol{A},\ \boldsymbol{B}_{\mathrm{f}})$ associated with a given configuration I_{N} satisfies or not the admissibility conditions, 2^I can be partitioned into

$$2^I = \mathcal{R} \cup \overline{\mathcal{R}}$$

where

$$\mathcal{R} = \{I_{\mathrm{N}} \subseteq I :\ \text{the fault } I_{\mathrm{F}} = I \backslash I_{\mathrm{N}} \text{ can be tolerated}\}$$
$$\overline{\mathcal{R}} = \{J \subset I :\ \text{the fault } I_{\mathrm{F}} = I \backslash I_{\mathrm{N}} \text{ cannot be tolerated}\}.$$

Definition 8.3 (*Recoverable fault, recoverable configuration*) A fault I_{F} is said to be recoverable if configuration $I_{\mathrm{N}} \in \mathcal{R}$. It is non-recoverable if configuration $I_{\mathrm{N}} \in \overline{\mathcal{R}}$. In the sequel we also use the wording *recoverable/non-recoverable configuration*.

It is well known that power sets have a lattice structure. That means that 2^I can be represented by a hierarchical graph, where nodes are actuator configurations organised into levels as follows:

- level 0 contains only I,
- level 1 contains all configurations I_{N} such that I_{F} has only one element,
- level 2 contains all configurations I_{N} such that I_{F} has two elements,
- etc. ...
- the last level is the empty set (I_{F} contains all actuators I).

Each configuration at a given level belongs either to $\mathcal{R}$ or to $\overline{\mathcal{R}}$. Edges connect configurations which belong to adjacent levels and differ by only one actuator.

Definition 8.4 (*Successors, predecessors*) Let I_{N} be a configuration, $\mathcal{S}(I_{\mathrm{N}})$ the set of its successors and $\mathcal{P}(I_{\mathrm{N}})$ the set of its predecessors are defined as

$$\mathcal{S}(I_{\mathrm{N}}) = \{I' \in 2^I :\ I' \subseteq I_{\mathrm{N}}\}$$
$$\mathcal{P}(I_{\mathrm{N}}) = \{I'' \in 2^I :\ I'' \supseteq I_{\mathrm{N}}\}.$$

Note that from this definition, any configuration I_{N} belongs both to $\mathcal{S}(I_{\mathrm{N}})$ and $\mathcal{P}(I_{\mathrm{N}})$. Remark also that since a successor of I_{N} is included in I_{N} it represents a configuration with more faulty actuators while a predecessor of I_{N} represents a configuration with less faulty actuators.

Example 8.3 Reconfiguration after actuator faults
Consider a system with 7 states, and 4 actuators: $I = \{1,\ 2,\ 3,\ 4\}$. The matrices $\boldsymbol{A}$ and $\boldsymbol{B}^{\mathrm{T}}$ are as follows:

$$\boldsymbol{A} = \text{diag}\ \{-1,\ -0.5,\ -3,\ -4,\ -2,\ -1.5,\ -2.5\},$$
$$\boldsymbol{B}^{\mathrm{T}} = \begin{pmatrix} 0\ 1\ 1\ 1\ 1\ 1\ 0 \\ 1\ 0\ 1\ 1\ 1\ 0\ 1 \\ 1\ 1\ 0\ 1\ 0\ 1\ 1 \\ 1\ 0\ 1\ 0\ 1\ 1\ 1 \end{pmatrix}.$$

The considered criterion is

$$J(\boldsymbol{u},\ \gamma) = \frac{1}{2}\int_0^{\infty} \boldsymbol{u}^{\mathrm{T}}(t)\boldsymbol{u}(t)\,\mathrm{d}t,$$

which means that only the control energy is of interest and $\boldsymbol{R}$ is the identity matrix. In that case, it is known that

$$J(I,\ 0,\ \gamma) = \gamma^{\mathrm{T}}\boldsymbol{W}_{\mathrm{c}}^{-1}\gamma,$$

where $\boldsymbol{W}_{\mathrm{c}}$ is the Gramian associated with the pair $(\boldsymbol{A},\ \boldsymbol{B})$, i.e.

$$\boldsymbol{W}_{\mathrm{c}} = \int_0^{\infty} \mathrm{e}^{\boldsymbol{A}t}\,\boldsymbol{B}\boldsymbol{B}^{\mathrm{T}}\left(\mathrm{e}^{\boldsymbol{A}t}\right)^{\mathrm{T}}\,\mathrm{d}t.$$

The maximal eigenvalue is $\lambda_{\max}\left(\boldsymbol{W}_{\mathrm{c}}^{-1}\,(I)\right) = 0.4357$ energy units.

Assume that admissible solutions are defined such that the worst situation control cost should not exceed 1.125 energy units. Then, there are 10 fault situations in which the system is controllable by reconfiguration, namely when only actuators 1234, 234, 134, 124, 123, 34, 23, 14, 12, 13 remain available (using the short notations 1234 for {1, 2, 3, 4}, 24 for {2, 4}, etc.) but only 6 of them are admissible when energy limitation is considered, as shown by Table 8.1.

Table 8.1 Admissible actuators subsets and associated characteristics

Actuator subsets	$\lambda_{\max}$ (energy units)
1234	0.4357
234	1.1197
134	0.4676
124	0.8274
123	0.4778
34	**3.0201**
23	**1.3948**
14	**2.2576**
12	1.0612
13	**1.1452**

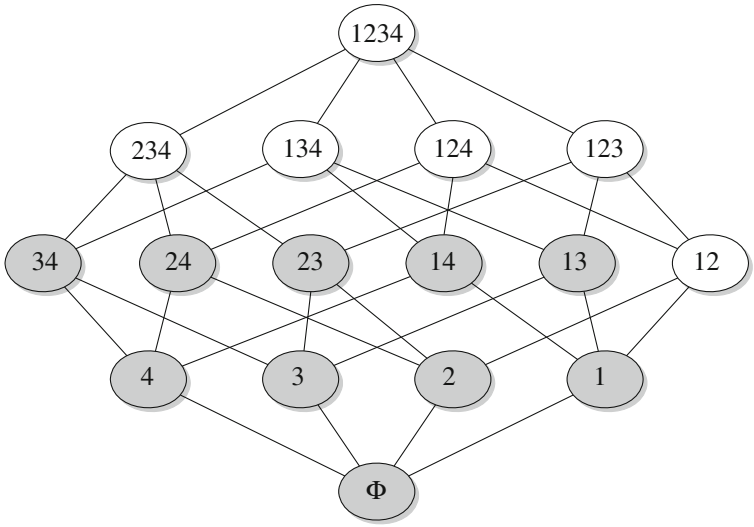

Fig. 8.4 The lattice of the actuators subsets in the example

Figure 8.4 shows the actuators lattice and its five levels. Dark grey nodes are configurations that cannot control the system (the corresponding pair $(\boldsymbol{A},\ \boldsymbol{B}_{\mathrm{f}})$ is not controllable), light grey nodes are configurations by which the system is controllable, but energy limitations are not met, white nodes are configurations which allow to control the system in an admissible way, i.e. they are recoverable. Grey nodes correspond to faults that cannot be tolerated, i.e. they represent non-recoverable configurations. □

Discrete state behaviour of the actuation system. Define the discrete state of the actuation system as the subset of actuators $I_{\mathrm{N}}(t)$, that are healthy at time t and assume, without loss of generality, that $I_{\mathrm{N}}(0) = I$. Assume that at time t_1 actuator σ_1 becomes faulty, then the reconfiguration mechanism, by discarding actuator σ_1, results in the discrete state $I_{\mathrm{N}}(t_1) = I \setminus \{\sigma_1\}$ which belongs to $\mathcal{S}(I)$. Further faults will result in discrete states $I_{\mathrm{N}}(t)$ moving to lower levels in the lattice, according to the dynamical dicrete state equation

$$I_{\mathrm{N}}(t^+) = I_{\mathrm{N}}(t^-) \setminus \Sigma_{\mathrm{f}}(t),$$

where $I_{\mathrm{N}}(t^-)$ is the discrete state before the fault, $\Sigma_{\mathrm{f}}(t) \subseteq I_{\mathrm{N}}(t^-)$ is the subset of actuators that become faulty at time t, and $I_{\mathrm{N}}(t^+)$ is the discrete state after the system reconfiguration. Symmetrically, repair operations move the discrete state to higher levels, according to

$$I_{\mathrm{N}}(t^{+}) = I_{\mathrm{N}}(t^{-}) \cup \Sigma_{\mathrm{r}}(t),$$

where $\Sigma_r(t) \subseteq I \setminus I_{\mathrm{N}}(t^{-})$ is the subset of actuators that have been repaired at time t (it can be checked that subsets of faulty or repaired actuators can be treated one by one, in an arbitrary order, resulting in the same post-fault or post-maintenance configuration in the lattice). Repair operations have an important impact on system reliability (by means of fault avoidance), but they are not considered here.

8.4.2 Critical Actuator Subsets and Minimal Recoverable Configurations

Consider a recoverable configuration $I_{\mathrm{N}} \in \mathcal{R}$. Loosing a subset of actuators $\Sigma \subset I_{\mathrm{N}}$ can be tolerated as long as the resulting configuration $I_{\mathrm{N}} \setminus \Sigma$ is still recoverable.

Definition 8.5 (*Critical actuator subsets*) A critical actuator subset associated with the recoverable configuration I_{N} is a minimal subset $\Sigma \subset I_{\mathrm{N}}$ such that $I_{\mathrm{N}} \setminus \Sigma \in \overline{\mathcal{R}}$.

Critical subsets are in general not unique. Let $C(I_{\mathrm{N}})$ be the ones associated with configuration I_{N}. Note that minimality is required in the definition because the loss of any superset of a critical actuator subset could obviously not be tolerated.

Definition 8.6 (*Minimal recoverable configuration*) A minimal recoverable configuration is a configuration that belongs to $\mathcal{R}$ while all its successors belong to $\overline{\mathcal{R}}$.

This is a very interesting property: in spite of those actuators already switched off, a minimal recoverable configuration is indeed recoverable, and so are all its predecessors, but loosing any extra actuator results in a non-recoverable configuration. As a result, the set of all recoverable configurations is completely known once the minimal recoverable ones have been found. Note also that the critical actuator subsets associated with a minimal recoverable configuration are the singletons formed with each actuator in the configuration.

Example 8.4 Critical subsets, Minimal recoverable configurations
It is easily seen on Fig. 8.4 that the set of recoverable configurations is

$$\mathcal{R} = \{1234,\ 123,\ 124,\ 134,\ 234,\ 12\}$$

The minimal recoverable configurations are therefore {12, 134, 234}. Indeed, loosing one more actuator in any of these configurations moves the system to a non-recoverable configuration, whatever the lost actuator. Note that any subset of a non-recoverable configuration is non-recoverable, while any superset of a recoverable configuration is recoverable. The critical actuator subsets associated with the nominal configuration 1234 are $C(1234) = \{24,\ 23,\ 14,\ 13,\ 12\}$, while the critical actuator subsets associated with configuration 234 are $C(234) = \{2,\ 3,\ 4\}$, which is not a surprise since 234 is a minimal recoverable configuration. □

8.5 Implementational Issues of Fault-Tolerant Control

8.5.1 On-Line Re-design Versus Bank of Control Laws

In the Fault-Tolerant Linear Quadratic problem, on-line re-design computes the control law $\boldsymbol{u}(t) = -\boldsymbol{R}^{-1}\boldsymbol{B}_{\mathrm{f}}^{\mathrm{T}}\boldsymbol{P}_{\mathrm{f}}\boldsymbol{x}(t)$ adapted to the faulty system by solving the Riccati equation

$$\boldsymbol{Q} + \boldsymbol{A}^{\mathrm{T}}\boldsymbol{P}_{\mathrm{f}} + \boldsymbol{P}_{\mathrm{f}}\boldsymbol{A} - \boldsymbol{P}_{\mathrm{f}}\boldsymbol{B}_{\mathrm{f}}\boldsymbol{R}^{-1}\boldsymbol{B}_{\mathrm{f}}^{\mathrm{T}}\boldsymbol{P}_{\mathrm{f}} = \boldsymbol{O}$$

where the post-fault actuation matrix $\boldsymbol{B}_{\mathrm{f}}$ is known from a fault estimation procedure when accommodation is applied or from zeroing the columns associated with the faulty actuators when reconfiguration is used. Note that a solution exists under the condition that the fault is recoverable, but the delay between the occurrence of the fault and the availability of the re-designed control law may lead to possibly unpleasant transient behaviours, during the time when the faulty system is still controlled by the nominal control law (an approach to this problem will be presented in Chap. 9). While on-line re-design is compulsory in fault accommodation because $\boldsymbol{B}_{\mathrm{f}}$ is not known in advance, it is optional in system reconfiguration. Indeed, since there is a limited number of possible $\boldsymbol{B}_{\mathrm{f}}$ matrices (each one is associated with an actuator configuration), the control law associated with each of them can be designed off-line, and stored in a control bank from which the appropriate one is selected as soon as the faulty actuators have been isolated, i.e. the current configuration is known. The control bank contains as many control laws as the number of recoverable configurations, which may be unpractical if this number is large. A solution to this problem, the so-called Passive–Active approach, is presented now.

8.5.2 The Passive–Active Approach

The Passive–Active (PACT) approach is intended to decrease the number of control laws that allow to recover all the recoverable faults. It is based on a result known as the "Reliable Control Theorem".

Theorem 8.1 (Reliable Control) *Consider the Linear Quadratic problem associated with the nominal system*

$$\dot{\boldsymbol{x}}(t) = \boldsymbol{A}\boldsymbol{x}(t) + \boldsymbol{B}\boldsymbol{u}(t), \quad \boldsymbol{x}(0) = \boldsymbol{\gamma}$$
$$J(\boldsymbol{u}, \boldsymbol{\gamma}) = \frac{1}{2}\int_0^{\infty} \left[\boldsymbol{x}^{\mathrm{T}}(t)\,\boldsymbol{Q}\boldsymbol{x}(t) + \boldsymbol{u}^{\mathrm{T}}(t)\boldsymbol{R}\boldsymbol{u}(t)\right] \mathrm{d}t$$

where matrices $\boldsymbol{A}$, $\boldsymbol{B}$, $\boldsymbol{R}$, $\boldsymbol{Q}$ *are given (*$\boldsymbol{R}$ *is assumed to be diagonal) and such that the Riccati equation*

$$\boldsymbol{Q} + \boldsymbol{A}^{\mathrm{T}}\boldsymbol{P} + \boldsymbol{P}\boldsymbol{A} - \boldsymbol{P}\boldsymbol{B}\boldsymbol{R}^{-1}\boldsymbol{B}^{\mathrm{T}}\boldsymbol{P} = \boldsymbol{O}$$

has a unique positive definite stabilising solution. The optimal control law is therefore $\boldsymbol{u}(t) = -\boldsymbol{R}^{-1}\boldsymbol{B}^{\mathrm{T}}\boldsymbol{P}\boldsymbol{x}(t)$. *Let* $\{I_{\mathrm{N}}, I_{\mathrm{F}}\}$ *be a partition of the set of actuators* I *and let* $\boldsymbol{B} = \boldsymbol{B}_{\mathrm{N}} + \boldsymbol{B}_{\mathrm{F}}$ *where* $\boldsymbol{B}_{\mathrm{N}}$ *(resp.* $\boldsymbol{B}_{\mathrm{F}}$*) is obtained by zeroing those columns in* $\boldsymbol{B}$ *that are associated with the actuators in* I_{F} *(resp.* I_{N}*). Assume that the Riccati equation*

$$\boldsymbol{Q} + \boldsymbol{A}^{\mathrm{T}}\boldsymbol{P}_{\mathrm{N}} + \boldsymbol{P}_{\mathrm{N}}\boldsymbol{A} - \boldsymbol{P}_{\mathrm{N}}\boldsymbol{B}_{\mathrm{N}}\boldsymbol{R}^{-1}\boldsymbol{B}_{\mathrm{N}}^{\mathrm{T}}\boldsymbol{P}_{\mathrm{N}} = \boldsymbol{O} \tag{8.26}$$

has a unique definite positive stabilising solution, then the control law $\boldsymbol{u}_{\mathrm{N}}(t) = -\boldsymbol{R}^{-1}\boldsymbol{B}^{\mathrm{T}}\boldsymbol{P}_{\mathrm{N}}\boldsymbol{x}(t)$ *has the following properties:*

1. *It stabilises the system when only controlled by the actuators in* I_{N}*, at the quadratic cost*
$$J(\boldsymbol{u}_{\mathrm{N}}, \gamma) = \frac{1}{2}\gamma^{\mathrm{T}}\boldsymbol{P}_{\mathrm{N}}\gamma$$
2. *It also stabilises the system when controlled by the actuators in* $I_{\mathrm{N}} \cup I_{\mathrm{f}}$ *where* I_{f} *is any subset of* I_{F}*, at a quadratic cost less than or equal to* $\frac{1}{2}\gamma^{\mathrm{T}}\boldsymbol{P}_{\mathrm{N}}\gamma$.

Discussion. Let $\{I_{\mathrm{N}}, I_{\mathrm{F}}\}$ be a partition of the set of actuators I such that I_{N} is a minimal recoverable configuration. It follows that the control law $\boldsymbol{u}_{\mathrm{N}}(t) = -\boldsymbol{R}^{-1}\boldsymbol{B}^{\mathrm{T}}\boldsymbol{P}_{\mathrm{N}}\boldsymbol{x}(t)$ where $\boldsymbol{P}_{\mathrm{N}}$ is the unique stabilising solution of Eq. (8.26) is admissible, i.e. the quadratic cost $\frac{1}{2}\gamma^{\mathrm{T}}\boldsymbol{P}_{\mathrm{N}}\gamma$ associated with the stable closed-loop system

$$\dot{\boldsymbol{x}}(t) = \left[\boldsymbol{A} - \boldsymbol{B}_{\mathrm{N}}\boldsymbol{R}^{-1}\boldsymbol{B}^{\mathrm{T}}\boldsymbol{P}_{\mathrm{N}}\right]\boldsymbol{x}(t)$$

satisfies the cost constraint. From the second property of the Reliable Control Theorem, this control law is also admissible for any system configuration $I_N \cup I_{\mathrm{f}}$ where $I_{\mathrm{f}} \subseteq I_{\mathrm{F}}$. It is therefore concluded that under this control law, the system is passively fault tolerant with respect to all faults that are "smaller" than I_{F} (i.e. the set of faulty actuators is included in I_{F}). Since the set of those faults corresponds to the set of configurations that are the predecessors of configuration I_{N}, the Reliable Control Theorem can be reformulated as follows.

Theorem 8.2 (Reliable Control reformulated) *Let* I_{N} *be a minimal recoverable configuration. Then, the control law* $\boldsymbol{u}_{\mathrm{N}}(t) = -\boldsymbol{R}^{-1}\boldsymbol{B}^{\mathrm{T}}\boldsymbol{P}_{\mathrm{N}}\boldsymbol{x}(t)$ *where* $\boldsymbol{P}_{\mathrm{N}}$ *is the unique definite positive stabilising solution of Eq. (8.26) is admissible for all its predecessors.*

Practical implementation. This new formulation shows that a mix of passive and active fault tolerance is able to cope with all the recoverable configurations: each minimal recoverable configuration is associated with its own control law (the active part of the strategy), and this control law recovers the set of all its predecessors (the passive part). The result is that instead of containing as many control laws as the number of recoverable configurations, the control bank now contains as many control laws as the number of minimal recoverable configurations, which may be

much smaller. However, there is a non-uniqueness problem to be dealt with, since a recoverable configuration may belong to the predecessors of more than one minimal recoverable configuration, hence several control laws are available for its recovery. Since all of them are admissible the designer is free to select the one that best fits some extra design criterion, for example selecting the one associated with the minimal cost.

Example 8.5 PACT control bank
Consider the linear quadratic problem associated with a system with 6 states and 4 actuators $I = \{1,\ 2,\ 3,\ 4\}$ where the matrices $\boldsymbol{A}$ and $\boldsymbol{B}$ are as follows

$$\boldsymbol{A} = \begin{pmatrix} 0 & 1 & 1 & 2 & 0 & 0 \\ -1 & 1 & 1 & 0 & 0 & 0 \\ 2 & 2 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & 1 & -1 \end{pmatrix}, \quad \boldsymbol{B}^{\mathrm{T}} = \begin{pmatrix} 1\,0\,1\,0\,1\,1 \\ 1\,1\,1\,0\,0\,0 \\ 1\,0\,0\,0\,1\,0 \\ 0\,0\,1\,1\,1\,0 \end{pmatrix}$$

and the cost is defined by

$$J(\boldsymbol{x}_0,\ \boldsymbol{u}) = \frac{1}{2}\int_0^\infty \left[\boldsymbol{x}(t)^{\mathrm{T}}\boldsymbol{Q}\boldsymbol{x}(t) + \boldsymbol{u}(t)^{\mathrm{T}}\boldsymbol{R}\boldsymbol{u}(t)\right]\mathrm{d}t.$$

Let $\boldsymbol{Q}$ and $\boldsymbol{R}$ be identity matrices of appropriate dimensions. The optimal control of the nominal system is $\boldsymbol{u}^*(t) = -\boldsymbol{R}^{-1}\boldsymbol{B}^{\mathrm{T}}\boldsymbol{P}\boldsymbol{x}(t)$. It results in the minimal cost $J(\gamma) = \frac{1}{2}\gamma^{\mathrm{T}}\boldsymbol{P}\gamma$ where γ is the initial condition and $\boldsymbol{P}$ is the unique symmetric positive definite stabilising solution of the Riccati equation associated with the nominal system. It can be checked that for the nominal configuration, the optimal state-feedback control results in a cost matrix $\boldsymbol{P}$ whose maximal eigenvalue is $\lambda_{\max}(\boldsymbol{P}) = 7.3554$.

Now, controlling a configuration $I_{\mathrm{N}} \subseteq I$ by some control law u results in the cost

$$J_{\mathrm{N}}(\gamma,\ \boldsymbol{u}) = \frac{1}{2}\int_0^\infty \left[\boldsymbol{x}(t)^{\mathrm{T}}\boldsymbol{Q}\boldsymbol{x}(t) + \boldsymbol{u}(t)^{\mathrm{T}}\boldsymbol{R}_{\mathrm{N}}\boldsymbol{u}(t)\right]\mathrm{d}t$$

where $\boldsymbol{R}_{\mathrm{N}} = diag\,\{r_i,\ i = 1, 2, 3, 4\}$ and $r_i \in \{0, 1\}$ according to the fact that actuator i is present or not in configuration I_{N} (indeed, switched off actuators do not imply any energy cost, whatever the control signal that is sent to them). The specification is that a control law $\boldsymbol{u}$ is admissible if it satisfies

$$\forall\gamma \in R^n :\ J_{\mathrm{N}}(\gamma,\ \boldsymbol{u}) \leq \frac{1}{2}\rho\gamma^{\mathrm{T}}\boldsymbol{P}\gamma \tag{8.27}$$

where $\rho > 1$ is the admissible performance degradation factor, meaning that performance degradation is accepted as long as the degraded cost does not exceed ρ times the optimal nominal cost. It follows that a recoverable configuration I_{N} is such that there exists a unique symmetric positive definite stabilising solution $\boldsymbol{P}_{\mathrm{N}}$ to the Riccati equation associated with I_{N} which satisfies:

$$\forall\gamma :\ \gamma^{\mathrm{T}}(\boldsymbol{P}_{\mathrm{N}} - \rho\boldsymbol{P})\gamma \leq 0$$

(indeed, the minimal cost achievable by configuration I_{N} is $\frac{1}{2}\gamma^{\mathrm{T}}\boldsymbol{P}_{\mathrm{N}}\gamma$).

Let the specification be defined by $\rho = 15$. Still naming the configurations after the actuators they contain, e.g. the nominal configuration I is 1234, the failure of actuator 2 results in configuration 134, etc., the set of recoverable configurations is

$$\mathcal{R}_{\rho=15} = \{1234,\ 123,\ 124,\ 12,\ 134,\ 234,\ 23,\ 24\}$$

while the minimal recoverable configurations are $\mathcal{M}_{\rho=15} = \{12,\ 134,\ 23,\ 24\}$. Figure 8.5 shows the lattice of configurations where recoverable configurations are white, non-recoverable configurations are grey, and minimal recoverable ones have a bold contour.

Active control bank. Each recoverable configuration being associated with its own control law, the active control bank contains 8 laws, for example the 8 optimal state feedbacks associated with the 8 recoverable configurations:

$$\mathcal{U}_{\text{active}} = \left\{ \boldsymbol{u}_{\text{N}}(t) = -\boldsymbol{R}^{-1}\boldsymbol{B}_{\text{N}}^{\text{T}}\boldsymbol{P}_{\text{N}}\boldsymbol{x}(t),\ I_{\text{N}} \in \mathcal{R}_{\rho=15} \right\}$$

Note that choosing the optimal control law associated with each configuration insures the minimal cost is obtained when this configuration occurs as the result of faults, but there is no need for the control laws to be optimal: they might be chosen arbitrarily provided they satisfy the admissibility constraints.

Passive–active control bank. In this scheme, each minimal recoverable configuration is associated with a control law that is admissible for all its predecessors. The bank now contains only 4 control laws, namely,

$$\mathcal{U}_{\text{PACT}} = \left\{ \boldsymbol{u}_{\text{N}}(t) = -\boldsymbol{R}^{-1}\boldsymbol{B}^{\text{T}}\boldsymbol{P}_{\text{N}}\boldsymbol{x}(t),\ I_{\text{N}} \in \mathcal{M}_{\rho=15} \right\}. \tag{8.28}$$

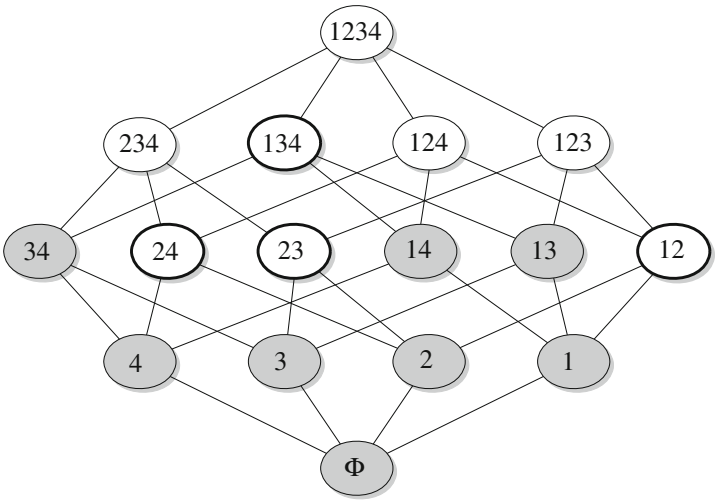

Fig. 8.5 The lattice of actuator configurations

Note that the law $\boldsymbol{u}_{\mathrm{N}}(t)$ is optimal for configuration $I_{\mathrm{N}} \in \mathcal{M}_{\rho=15}$ but is only admissible for the predecessors $\mathcal{P}(I_{\mathrm{N}}) \setminus I_{\mathrm{N}}$. The respective performance indexes are

$$\begin{aligned}\lambda_{\max}(P_{12}) &= 17.4285\\ \lambda_{\max}(P_{134}) &= 32.9450\\ \lambda_{\max}(P_{23}) &= 16.5649\\ \lambda_{\max}(P_{24}) &= 18.6938.\end{aligned}$$

Let $\mathcal{R}(u)$ be the set of configurations recovered by the control law u, one has

$$\begin{aligned}\mathcal{R}(u_{12}) &= \left\{1234,\ 123,\ 124,\ 12,\ \underline{234},\ \underline{23}\right\}\\ \mathcal{R}(u_{134}) &= \left\{1234,\ \underline{123},\ 134,\ \underline{234}\right\}\\ \mathcal{R}(u_{23}) &: \{1234,\ 123,\ 234,\ 23\}\\ \mathcal{R}(u_{24}) &: \{1234,\ 124,\ 234,\ 24\}.\end{aligned}$$

One remarks that $\mathcal{R}\left(u_{I_{\mathrm{N}}}\right)$ indeed not only includes, for each minimal recoverable configuration I_{N}, all its predecessors, but it may also include more (those that are underlined). Another remark is that non-minimal recoverable configurations can be recovered by several control laws, hence the need for a decision procedure.

Table 8.2 gives, for each recoverable configuration, the list of control laws by which it can be recovered. The simplest decision procedure selects the one with the best performance (underlined). □

Reducing the control bank size. Let $\mathcal{U}$ be a passive–active control bank that recovers all the recoverable faults. It may happen that the designer is happy with a bank $\mathcal{U}_{\text{smaller}}$ that contains a smaller number of laws at the price of recovering only a subset of recoverable faults (i.e. at the price of being less fault-tolerant). This trade-off will be considered later since it is connected with the evaluation of fault tolerance, as one can guess from the wording "*being less fault-tolerant*". This section investigates the minimality of the control bank for a given subset of faults to be recovered.

Table 8.2 Control laws for recovery

Configurations	1234	123	124	12	134	234	23	24
Admissible control laws	u_{12} u_{134} $\underline{u_{23}}$ u_{24}	u_{12} u_{134} $\underline{u_{23}}$	$\underline{u_{12}}$ u_{24}	u_{12}	u_{134}	u_{12} u_{134} $\underline{u_{23}}$ u_{24}	u_{12} $\underline{u_{23}}$	u_{24}

Definition 8.7 (*Minimal Control bank*) A control bank $\mathcal{U}$ is minimal with respect to a given set of faults if there is no proper subset of $\mathcal{U}$ that recovers all these faults.

Given a passive–active control bank $\mathcal{U}$ that recovers a set of faults $\mathcal{R}(\mathcal{U})$ the reduction to a minimal control bank problem has to be found in the following problem:

Problem 8.5 (*Reduction problem*)

1. Check whether $\mathcal{U}$ is minimal or not,
2. if not, find a minimal control bank $\mathcal{U}_{\min}$.

Let $\mathcal{R}(\mathcal{U})$ be the set of faults recovered by all the control laws in the bank $\mathcal{U}$ then one has

$$\mathcal{R}(\mathcal{U}) = \cup_{u \in \mathcal{U}} \mathcal{R}(u).$$

Let $U \subset \mathcal{U}$ be a proper subset of control laws. It recovers the set of faults:

$$\mathcal{R}(U) = \cup_{u \in U} \mathcal{R}(u).$$

By comparing $\mathcal{R}(\mathcal{U})$ and $\mathcal{R}(U)$, it is concluded that if $\mathcal{R}(U) = \mathcal{R}(\mathcal{U})$ then $\mathcal{U}$ is not minimal (indeed U is a proper subset that recovers the same faults), and either U or some subsets of U are minimal. On the contrary, if $\mathcal{R}(U) \subset \mathcal{R}(\mathcal{U})$ then neither U nor any of its successors can recover all the faults to be recovered. This remark leads to the following algorithm for the determination of the minimal control banks that recover the same set if faults as a given PACT control bank.

Algorithm 8.1 *Reduction of a PACT bank of control laws*

Given: Bank of control laws $\mathcal{U}$
Recovered faults $\mathcal{R}(\mathcal{U})$.
Initialisation: Put $\mathcal{U}$ into the list "possible", initialize two empty lists "minimal" and "impossible"
While the list "Possible" is not empty
For each member $\mathcal{V}$ of this list
If all its direct successors U are such that $\mathcal{R}(U) \subset \mathcal{R}(\mathcal{U})$
then remove $\mathcal{V}$ from the list "possible" and move it into the list "minimal"
else give the direct successors that satisfy $\mathcal{R}(U) = \mathcal{R}(\mathcal{V})$ the label "possible" and change the label of $\mathcal{V}$ into "impossible"
Result: list of minimal banks that recover all the faults $\mathcal{R}(\mathcal{U})$.

Example 8.6 Minimal control bank
The passive–active control bank of Example 8.5 resulted in a control bank with four control laws:

$$\mathcal{U}_{\text{PACT}} = \{u_{12}, u_{134}, u_{23}, u_{24}\}$$

Table 8.3 Level 1 subsets

Subsets	Recovered faults	Comment
$\{u_{12}, u_{134}, u_{23}\}$	{1234, 123, 124, 12, 234, 23, 134, 24}	Possibly minimal
$\{u_{12}, u_{134}, u_{24}\}$	{1234, 123, 124, 12, 234, 23, 134, 24}	Possibly minimal
$\{u_{12}, u_{23}, u_{24}\}$	{1234, 123, 124, 12, 234, 23, 24}	Impossible
$\{u_{134}, u_{23}, u_{24}\}$	{1234, 123, 134, 234, 23, 124, 24}	Impossible

Table 8.4 Level 2 subsets

Subsets	Recovered faults	Comment
$\{u_{12}, u_{134}\}$	{1234, 123, 124, 12, 234, 23, 134}	Impossible
$\{u_{12}, u_{23}\}$	{1234, 123, 124, 12, 234, 23}	Impossible
$\{u_{134}, u_{23}\}$	{1234, 134, 123, 234, 23}	Impossible

that were able to recover all the recoverable faults { 1234, 123, 124, 12, 134, 234, 23, 24 } according to the following list:

$$\begin{aligned}\mathcal{R}(u_{12}) &= \{1234,\ 123,\ 124,\ 12,\ \underline{234},\ \underline{23}\}\\ \mathcal{R}(u_{134}) &= \{1234,\ \underline{123},\ 134,\ \underline{234}\}\\ \mathcal{R}(u_{23}) &= \{1234,\ 123,\ 234,\ 23\}\\ \mathcal{R}(u_{24}) &= \{1234,\ 124,\ 234,\ 24\}\end{aligned}$$

Exploring the Level 1 subsets of $\mathcal{U}_{\text{PACT}}$ shows that two banks with 3 control laws, namely $\{u_{12}, u_{134}, u_{23}\}$ and $\{u_{12}, u_{134}, u_{24}\}$ are able to recover all the recoverable faults (Table 8.3).

Analysing the subsets of $\{u_{12}, u_{134}, u_{23}\}$ and $\{u_{12}, u_{134}, u_{24}\}$ shows that none of them can recover all the faults (Table 8.4 shows the results for $\{u_{12}, u_{134}, u_{23}\}$).

It is, therefore, concluded that the PACT control bank $\mathcal{U}_{\text{PACT}} = \{u_{12}, u_{134}, u_{23}, u_{24}\}$ can be replaced with no loss of recoverability by a 3-laws control bank: either $\{u_{12}, u_{134}, u_{23}\}$ or $\{u_{12}, u_{134}, u_{24}\}$. □

8.5.3 Reducing the Reliability Over-Cost

Let $\mathcal{M}$ be the set of minimal recoverable configurations of a given system, and let $\mathcal{U}$ be the PACT control bank where each control law $\boldsymbol{u}_{\text{N}}(t) \in \mathcal{U}$ is associated with one minimal recoverable configuration $I_{\text{N}} \in \mathcal{M}$.

Reliability over-cost. As already noted, $\boldsymbol{u}_{\text{N}}(t)$ is optimal for configuration I_{N}, but for any other configuration $I_K \in \mathcal{P}(I_{\text{N}})$ it is only admissible. Indeed, configuration I_K achieves the minimal cost $\frac{1}{2}\gamma^{\text{T}}\boldsymbol{P}_K\gamma$ under the control law $\boldsymbol{u}_K(t) = -\boldsymbol{R}^{-1}\boldsymbol{B}^{\text{T}}\boldsymbol{P}_K\boldsymbol{x}(t)$ where $\boldsymbol{P}_K$ is the unique solution of the Riccati equation

$$\boldsymbol{Q} + \boldsymbol{A}^{\text{T}}\boldsymbol{P}_K + \boldsymbol{P}_K\boldsymbol{A} - \boldsymbol{P}_K\boldsymbol{B}_K\boldsymbol{R}^{-1}\boldsymbol{B}_K^{\text{T}}\boldsymbol{P}_K = \boldsymbol{O}$$

while it is well known that under the (non-optimal) control law

$$\boldsymbol{u}_{\mathrm{N}}(t) = -\boldsymbol{R}^{-1}\boldsymbol{B}^{\mathrm{T}}\boldsymbol{P}_{\mathrm{N}}\boldsymbol{x}(t)$$

the cost is $\frac{1}{2}\gamma^{\mathrm{T}}\boldsymbol{P}_{\mathrm{N,K}}\gamma$ where $P_{\mathrm{N,K}}$ is symmetric positive definite and given by the Lyapunov equation:

$$\boldsymbol{Q} + \boldsymbol{P}_{\mathrm{N}}\boldsymbol{B}\boldsymbol{R}^{-1}\boldsymbol{B}^{\mathrm{T}}\boldsymbol{P}_{\mathrm{N}} + \boldsymbol{P}_{\mathrm{N,K}}\left(\boldsymbol{A} - \boldsymbol{B}_K\boldsymbol{R}^{-1}\boldsymbol{B}^{\mathrm{T}}\boldsymbol{P}_{\mathrm{N}}\right) + \left(\boldsymbol{A} - \boldsymbol{B}_K\boldsymbol{R}^{-1}\boldsymbol{B}^{\mathrm{T}}\boldsymbol{P}_{\mathrm{N}}\right)^{\mathrm{T}}\boldsymbol{P}_{\mathrm{N,K}} = \boldsymbol{O}$$

It is concluded that for configuration I_K, the reliability over-cost to be paid for using $\boldsymbol{u}_{\mathrm{N}}(t)$ instead of $\boldsymbol{u}_K(t)$ is $\frac{1}{2}\gamma^{\mathrm{T}}\left[\boldsymbol{P}_{\mathrm{N,K}} - \boldsymbol{P}_K\right]\gamma$.

Trade-off control bank. Since the nominal configuration I is expected to occur most of the time, it may be sensible to add the nominal control law to the minimal PACT bank. It follows that no reliability over-cost is paid in the nominal configuration, at the cost of abandoning the minimality of the control bank.

Example 8.7 Trade-off control bank
In Example 8.6, a minimal control bank with three laws, namely $\{u_{12}, u_{134}, u_{23}\}$ or $\{u_{12}, u_{134}, u_{24}\}$ was able to recover all the recoverable configurations. In this case, one would have chosen the first bank, since it contains u_{23} which gives the smallest cost

$$\frac{1}{2}\gamma^{\mathrm{T}}\boldsymbol{P}_{23,1234}\gamma$$

in the nominal situation, as highlighted in Table 8.2. However, implementing the trade-off bank $\{u_{1234}, u_{12}, u_{134}, u_{23}\}$ results in an optimal cost for the nominal system and a minimal number of control laws to obtain an admissible cost for the other (recoverable) configurations. □

More generally, a trade-off control bank can be designed by associating some recoverable configurations (Subset1) with their optimal control law, while the rest (Subset2) is controlled by the PACT bank associated with the minimal recoverable configurations. The system performances are optimal as long as the current configuration belongs to Subset1, at the cost of increasing the number of control laws in the overall control bank. For Subset2, the cost reduction problem can be stated as follows:

Problem 8.6 (*Cost reduction problem*)
Given a minimal recoverable configuration I_{N}, find a control law that minimises the cost achieved by some pre-selected configuration $I_L \in \mathcal{P}(I_{\mathrm{N}})$ under the constraint that it is admissible for all the configurations in $\mathcal{P}(I_{\mathrm{N}})$.

Note that the optimal control of configuration I_L indeed minimises the cost achieved by this configuration, but there is no reason for it to be admissible for all the

configurations in $\mathcal{P}(I_N)$. Conversely, the reliable control $\boldsymbol{u}_N(t) = -\boldsymbol{R}^{-1}\boldsymbol{B}^T\boldsymbol{P}_N\boldsymbol{x}(t)$ is admissible for all the configurations in $\mathcal{P}(I_N)$ but there is no reason for it to yield the minimal cost when applied to I_L.

The cost reduction problem can be addressed by introducing a degree of freedom $\boldsymbol{H}$ in the control law, namely $\boldsymbol{u}(t) = -\boldsymbol{R}^{-1}\boldsymbol{B}^T\boldsymbol{H}\boldsymbol{x}(t)$ instead of $\boldsymbol{u}(t) = -\boldsymbol{R}^{-1}\boldsymbol{B}^T\boldsymbol{P}_N\boldsymbol{x}(t)$, where $\boldsymbol{H}$ is symmetric positive definite. Applying this control law to a configuration $I_K \in \mathcal{P}(I_N)$ results in the closed-loop matrix $\boldsymbol{A} - \boldsymbol{B}_K\boldsymbol{R}^{-1}\boldsymbol{B}^T\boldsymbol{H}$ and (assuming it is stable), in the cost $\frac{1}{2}\gamma^T\boldsymbol{W}_K\gamma$ where $\boldsymbol{W}_K$ is symmetric positive definite and given by the Lyapunov equation:

$$\boldsymbol{Q} + \boldsymbol{H}\boldsymbol{B}\boldsymbol{R}^{-1}\boldsymbol{B}^T\boldsymbol{H} + \boldsymbol{W}_K\left(\boldsymbol{A} - \boldsymbol{B}_K\boldsymbol{R}^{-1}\boldsymbol{B}^T\boldsymbol{H}\right) + \left(\boldsymbol{A} - \boldsymbol{B}_K\boldsymbol{R}^{-1}\boldsymbol{B}^T\boldsymbol{H}\right)^T\boldsymbol{W}_K = \boldsymbol{O} \tag{8.29}$$

Let $\mathcal{H}$ be the set of symmetric positive definite matrices $\boldsymbol{H}$ that satisfy the conditions that $\boldsymbol{A} - \boldsymbol{B}_K\boldsymbol{R}^{-1}\boldsymbol{B}^T\boldsymbol{H}$ is stable and $\forall I_K \in \mathcal{P}(I_N)$, $\frac{1}{2}\gamma^T\boldsymbol{W}_K\gamma$ is admissible.

Applying the control law $\boldsymbol{u}(t) = -\boldsymbol{R}^{-1}\boldsymbol{B}^T\boldsymbol{H}\boldsymbol{x}(t)$ to configuration I_L results in the cost $\frac{1}{2}\gamma^T\boldsymbol{W}_L\gamma$ and therefore, the cost reduction problem is nothing but the optimisation problem: find $\boldsymbol{H}$ so as to minimise $\lambda_{\max}(\boldsymbol{W}_L)$ under the constraints $\boldsymbol{H} \in \mathcal{H}$.

Unfortunately, this problem appears to be non-convex and difficult to solve. However, it is possible to build a sequence of control laws $\boldsymbol{u}^k(t) = -\boldsymbol{R}^{-1}\boldsymbol{B}^T\boldsymbol{H}^k\boldsymbol{x}(t)$, $(k = 1, 2, \ldots)$ that improve the cost of the selected configuration while satisfying the constraints. The following algorithm is based on an adaptation of the Newton-Kleinman procedure. It can be shown that it produces a converging sequence of control laws $\boldsymbol{u}^k(t) = -\boldsymbol{R}^{-1}\boldsymbol{B}^T\boldsymbol{H}^k\boldsymbol{x}(t)$, $(k = 1, 2, \ldots)$ that stabilise all the configurations in $\mathcal{P}(I_N)$ and are such that $\boldsymbol{P}_L \leq \cdots \leq \boldsymbol{W}_L^{k+1} \leq \boldsymbol{W}^k \leq \cdots \leq \boldsymbol{P}_N$ where $\boldsymbol{W}_L^{k+1} \leq \boldsymbol{W}^k$ means that for any initial condition γ, the quadratic form $\gamma^T\boldsymbol{W}^k\gamma$ is a decreasing function of k.

Algorithm 8.2 *Cost reduction problem*

Given: A minimal recoverable configuration I_N
a pre-selected configuration $I_L \in \mathcal{P}(I_N)$
an arbitrary small positive number ε, a matrix norm $\|.\|$

Initialisation: $\boldsymbol{H}^0 = \boldsymbol{P}_N$ and $\boldsymbol{W}_L^{-1} = \infty$

While: STOP condition not fulfilled

1. Solve the Lyapunov equation $\boldsymbol{Q} + \boldsymbol{H}^k\boldsymbol{B}\boldsymbol{R}^{-1}\boldsymbol{B}^T\boldsymbol{H}^k + \boldsymbol{W}^k\left(\boldsymbol{A} - \boldsymbol{B}_L\boldsymbol{R}^{-1}\boldsymbol{B}^T\boldsymbol{H}^k\right) + \left(\boldsymbol{A} - \boldsymbol{B}_L\boldsymbol{R}^{-1}\boldsymbol{B}^T\boldsymbol{H}^k\right)^T\boldsymbol{W}^k = \boldsymbol{O}$ for $\boldsymbol{W}^k$
2. Update $\boldsymbol{H}^{k+1} = p^k\boldsymbol{H}^k + q^k\boldsymbol{W}^k$, where $q^k = \max\left\{\zeta : \zeta \in [0, 1],\ \boldsymbol{H}^{k+1} \in \mathcal{H}\right\}$ and $p^k = 1 - q^k$

3. Check the STOP condition $\left\| \boldsymbol{W}_L^{k+1} - \boldsymbol{W}^k \right\| \leq \varepsilon$

Result: a convergent sequence of control laws $\boldsymbol{u}^k(t) = -\boldsymbol{R}^{-1}\boldsymbol{B}^{\mathrm{T}}\boldsymbol{H}^k\boldsymbol{x}(t)$, $(k = 1, 2, \ldots)$ that satisfy the admissibility constraints for all configurations in $\mathcal{P}(I_{\mathrm{N}})$ and decrease the quadratic cost associated with configuration I_L.

Notice that the pure Newton-Kleinman scheme is obtained if the updating procedure in Step 2 is applied with $p^k = 0$ and $q^k = 1$ for all k. This scheme produces the optimal control matrix associated with configuration I_L under no constraint. The updating procedure in Step 2 is aimed at satisfying the constraints $\boldsymbol{H} \in \mathcal{H}$.

Example 8.8 Cost reduction
In Example 8.7, consider the minimal recoverable configuration 12. The control law u_{12} is admissible for configurations $\{1234,\ 123, 124,\ 12,\ \underline{234},\ \underline{23}\}$ but using it in the nominal configuration 1234 gives the cost matrix $P_{12,1234}$ whose maximal eigenvalue is $\lambda_{\max}\left(P_{12,1234}\right) = 12.267$. However, any control law $\boldsymbol{u}(t) = -\boldsymbol{R}^{-1}\boldsymbol{B}^{\mathrm{T}}\boldsymbol{H}\boldsymbol{x}(t)$, where $\boldsymbol{H} = \boldsymbol{H}^{\mathrm{T}} > 0$ is better than u_{12} and admissible for all configurations in $\mathcal{P}(12)$ if it satisfies the following conditions:

- the predecessors are stable: $\forall I_K \in \{1234,\ 123,\ 124,\ 12\}$, $\boldsymbol{A} - \boldsymbol{B}_K\boldsymbol{R}^{-1}\boldsymbol{B}^{\mathrm{T}}\boldsymbol{H}$ is Hurwitz,
- the predecessors are admissible: $\forall I_K \in \{1234,\ 123,\ 124,\ 12\}$, $W_K \leq 15P_{1234}$, where W_K is the solution of Eq. (8.29)
- for any initial condition the cost associated with the nominal configuration $\frac{1}{2}\gamma^{\mathrm{T}}\boldsymbol{W}_{1234}\gamma$ is smaller than $\frac{1}{2}\gamma^{\mathrm{T}}\boldsymbol{P}_{12,1234}\gamma$.

It can be checked that, applying the pure Newton-Kleinman algorithm $p^k = 0$, $q^k = 1$ for all k, results in a sequence of cost matrices $\boldsymbol{W}_{1234}^k$ that decrease from the solution $\boldsymbol{W}_{1234}^0 = \boldsymbol{P}_{12,1234}$ of the Lyapunov equation

$$\boldsymbol{Q} + \boldsymbol{P}_{12}\boldsymbol{B}\boldsymbol{R}^{-1}\boldsymbol{B}^{\mathrm{T}}\boldsymbol{P}_{12} + \boldsymbol{W}_{1234}^0\left(\boldsymbol{A} - \boldsymbol{B}\boldsymbol{R}^{-1}\boldsymbol{B}^{\mathrm{T}}\boldsymbol{P}_{12}\right) + \left(\boldsymbol{A} - \boldsymbol{B}\boldsymbol{R}^{-1}\boldsymbol{B}^{\mathrm{T}}\boldsymbol{P}_{12}\right)^{\mathrm{T}}\boldsymbol{W}_{1234}^0 = \boldsymbol{O}$$

to the optimal solution $\boldsymbol{W}_{1234}^{\infty} = \boldsymbol{P}_{1234}$ associated with the nominal system. However, as soon as the first iteration, $\boldsymbol{H}^1$ violates the admissibility constraint, so the update law in the algorithm must be used. The result is displayed in Table 8.5. The control $\boldsymbol{u}(t) = -\boldsymbol{R}^{-1}\boldsymbol{B}^{\mathrm{T}}\boldsymbol{H}^2\boldsymbol{x}(t)$ is

Table 8.5 Results for configuration 12

Iteration	0	1	2
$\lambda_{\max}\left(W_{1234}^k\right)$	12.267	10.159	10.159
$q_{\max}$	0.648	0.000	0.000

Table 8.6 Results for all configurations

	Reliable control	Cost reduction	Decrease
Configuration 12	12.267	10.159	17.18%
Configuration 134	19.340	15.892	17.83%
Configuration 23	12.743	7.873	38.22%
Configuration 24	10.869	9.182	15.53%

admissible for all the predecessors $\mathcal{P}$ (12), and decreases the nominal configuration cost by 17.18 % when compared with the reliable control u_{12}.

Table 8.6 compares the nominal configuration costs achieved by the control law associated with each configuration in $\mathcal{M}_{\rho=15}$ respectively for the reliable control and the cost reduced control. □

8.6 Fault-Tolerance Evaluation

The system is tolerant to actuator faults, when the reconfiguration strategy is used, as long as the current configuration $I_N(t)$ belongs to the set of recoverable configurations $\mathcal{R}$. Introducing some measure $\mu(\mathcal{R})$ of this set should therefore give an idea about the overall system fault tolerance. On another hand, let the system configuration be $I_N(t)$ at time t and assume there is no repair during its operation, then actuator failures can only move the discrete state to configurations within the set of successors $\mathcal{S}(I_N(t))$, among which only those in the intersection $\mathcal{R} \cap \mathcal{S}(I_N(t))$ are recoverable. The "remaining" fault tolerance at time t can therefore be evaluated by the measure $\mu(\mathcal{R} \cap \mathcal{S}(I_N(t)))$. Note that $\mathcal{R} = \mathcal{R} \cap \mathcal{S}(I)$ because $\mathcal{S}(I) = 2^I$, and therefore the measure $\mu(\mathcal{R})$ is the "remaining" fault tolerance at the initial time, assuming that the system is then in its nominal configuration. Two kinds of measures, namely deterministic or probabilistic measures can be used.

8.6.1 Deterministic Measures

Deterministic measures do not use any model of the transitions from one configuration to another. The most important ones are the redundancy degrees which are based on the number of levels, in the lattice of system configurations, between a recoverable configuration $I_N(t)$ and the set of non-recoverable ones.

Definition 8.8 (*Strong redundancy degree*) The strong redundancy degree is the measure $\mu(\mathcal{R} \cap \mathcal{S}(I_N(t)))$ defined by:

$$k_{\text{strong}}[I_N(t)] = \min\left\{|\Sigma| : \Sigma \subseteq I_N(t) \wedge I_N(t) \setminus \Sigma \in \overline{\mathcal{R}}\right\}, \tag{8.30}$$

where $|\Sigma|$ is the cardinal number of the set Σ.

$k_{\text{strong}}[I_{\text{N}}(t)]$ is the length of the shortest path, in the lattice of system configurations, between a recoverable configuration $I_{\text{N}}(t)$ and the set of non-recoverable configurations. In other words, no matter which actuators are lost, as long as their number does not exceed $k_{\text{strong}}[I_{\text{N}}(t)] - 1$, the fault is recoverable.

Definition 8.9 (*Weak redundancy degree*) The weak redundancy degree is the measure $\mu(\mathcal{R} \cap \mathcal{S}(I_{\text{N}}(t)))$ defined by:

$$k_{\text{weak}}[I_{\text{N}}(t)] = \max\{|\Sigma| : \Sigma \subseteq I_{\text{N}}(t) \wedge I_{\text{N}}(t) \setminus \Sigma \in \mathcal{R}\} \tag{8.31}$$

It is the length of the longest path, in the lattice of system configurations, between a recoverable configuration $I_{\text{N}}(t)$ and the set of non-recoverable ones. In other words, the largest set of actuators whose loss can be tolerated from the current configuration $I_{\text{N}}(t)$ is of size $k_{\text{weak}}[I_{\text{N}}(t)]$.

The redundancy degrees enjoy nice practical interpretations. It follows from their definition that

$$\forall I_{\text{n}}(t) \in \mathcal{R},\ k_{\text{strong}}[I_{\text{N}}(t)] \leq k_{\text{weak}}[I_{\text{N}}(t)].$$

The *coverage* is another deterministic measure that is sometimes used in addition to the redundancy degrees.

Definition 8.10 (*Coverage*) The coverage is the measure $\mu(\mathcal{R} \cap \mathcal{S}(I_{\text{N}}(t)))$ defined by the ratio between the number of recoverable configurations and the total number of possible configurations.

Its interpretation is not so straightforward as that of the redundancy degrees, but it is easy to compute, and it may provide some useful insight with respect to the usefulness of the individual system components. For example, it allows a quick evaluation of the individual components usefulness, as discussed in Sect. 8.6.3.

8.6.2 Probabilistic Measures

Probabilistic measures assume that a model that governs the transitions from one configuration to another one is available. Then, the set $\mathcal{R} \cap \mathcal{S}(I_{\text{N}}(t))$ can be measured using reliability concepts. Indeed, for any pair of time instants t_1, t_2 such that $t_2 > t_1$ let $\pi_\sigma(t_1, t_2)$ be the probability for actuator σ to be healthy at time t_2 subject to the condition that it was healthy at time t_1. Assume this function is known for all actuators, that actuators faults are independent, and that the nominal configuration I is the current one at the initial time. Then, the probability for the system discrete state to be I_{N} at time t is given by

$$\Pr[I_{\text{N}},\ 0,\ t] = \prod_{\sigma \in I_{\text{N}}} \pi_\sigma(t,\ 0) \prod_{\sigma \notin I_{\text{N}}} [1 - \pi_\sigma(t,\ 0)]. \tag{8.32}$$

Let the time window $[0,\ T]$ define the duration of the system mission, then fault tolerance is guaranteed provided no configuration in $\overline{\mathcal{R}}$ becomes active on $[0,\ T]$ (indeed, the specification is satisfied as long as the current configuration belongs to $\mathcal{R}$). It follows that the success probability on $[0,\ T]$ is given by

$$\Pr[I,\ 0,\ T] = \sum_{I_{\mathrm{N}} \in \mathcal{R}} \Pr[I_{\mathrm{N}},\ 0,\ T]. \tag{8.33}$$

Starting with the nominal configuration I at the initial time, the time during which the system will operate successfully is the time before it enters a configuration in $\overline{\mathcal{R}}$. This is a random variable, whose probability distribution is given by Eq. (8.33). A possible alternative measure of the fault-tolerance capability is the mean-time to failure:

$$MTTF(I,\ 0) = \int_0^{\infty} \Pr[I,\ 0,\ T]\,\mathrm{d}T. \tag{8.34}$$

8.6.3 Sensitivity

The size of $\mathcal{R}$ (and consequently the size of $\mathcal{R} \cap \mathcal{S}(I_{\mathrm{N}}(t))$ depends on the difficulty for the specification to be satisfied and on the size of I. It follows that two kinds of sensitivities can be considered.

Sensitivity with respect to the specifications. Consider the triple $(I,\ \mathrm{Spec1},\ \mathrm{Spec2})$, where Spec1 and Spec2 are two specifications, then one has

$$(\mathrm{Spec1} \Rightarrow \mathrm{Spec2}) \Rightarrow \mathcal{R}_{\mathrm{Spec1}} \subseteq \mathcal{R}_{\mathrm{Spec2}}, \tag{8.35}$$

where Spec1 $\Rightarrow$ Spec2 means that Specification 2 is *weaker* than—or is a *degraded* specification with respect to—Specification 1, and $\mathcal{R}_{\mathrm{Spec1}}$ (resp. $\mathcal{R}_{\mathrm{Spec2}}$) is the set of configurations that are recoverable when the nominal set of actuators is I and the specification is Spec1 (resp. Spec2). Indeed, any configuration that satisfies Spec1 also satisfies Spec2.

The sensitivity with respect to the specifications is easily evaluated from the difference of the above deterministic or probabilistic measures associated with each set of recoverable configurations. For example, the strong redundancy degree of a given configuration $I_{\mathrm{N}}(t)$ is

$$k_{\mathrm{strong}}[I_{\mathrm{N}}(t)] = \min\left\{|\Sigma| : \Sigma \subseteq I_{\mathrm{N}}(t) \wedge I_{\mathrm{N}}(t) \setminus \Sigma \in \overline{\mathcal{R}}_{\mathrm{Spec1}}\right\}$$

or

$$k_{\mathrm{strong}}[I_{\mathrm{N}}(t)] = \min\left\{|\Sigma| : \Sigma \subseteq I_{\mathrm{N}}(t) \wedge I_{\mathrm{N}}(t) \setminus \Sigma \in \overline{\mathcal{R}}_{\mathrm{Spec2}}\right\}$$

according to the selected specifications.

An interesting development is associated with specifications Spec (θ) that are monotonous with respect to some parameter θ in the following sense:

$$\theta_1 \leq \theta_2 \Rightarrow \mathcal{R}_{\text{Spec}(\theta_1)} \subseteq \mathcal{R}_{\text{Spec}(\theta_2)}$$

θ may for example be interpreted as a cost: the more one is ready to spend, the larger the set of recoverable configurations. With this interpretation in mind, let $\mathcal{R}_{\text{wish}}$ be a set of configurations that are wished to be recoverable. The value

$$\theta_{\text{optimal}} = \min \left\{ \theta : \mathcal{R}_{\text{Spec}(\theta)} \supseteq \mathcal{R}_{\text{wish}} \right\}$$

is the minimal cost at which the wished fault-tolerance specifications are achieved.

Note that the particular value θ_{critical} associated with $\mathcal{R}_{\text{wish}} = \{ I \}$ appears as the minimal cost to be paid for the existence of at least one solution (the nominal one) to the specification satisfaction problem.

Sensitivity with respect to the components. Similarly, for a given specification Spec let I_{Comp1} and I_{Comp2} be two sets of actuators (more generally two sets of components), then:

$$\left(I_{\text{Comp1}} \subseteq I_{\text{Comp2}} \right) \Rightarrow \mathcal{R}_{\text{Comp1}} \subseteq \mathcal{R}_{\text{Comp2}}, \tag{8.36}$$

where $\mathcal{R}_{\text{Comp1}}$ (resp. $\mathcal{R}_{\text{Comp2}}$) is the set of configurations that are recoverable when the nominal set of actuators is I_{Comp1} (resp. I_{Comp2}). The sensitivity with respect to the components is easily evaluated from the difference of the above deterministic or probabilistic measures associated with the sets I_{Comp1} and I_{Comp2}.

Two consequences of Eq. (8.36) may be of interest:

- Assume that two sets of components are such that $I_{\text{Comp1}} \subset I_{\text{Comp2}}$ and $\mathcal{R}_{\text{Comp1}} = \mathcal{R}_{\text{Comp2}}$. Then the components in $I_{\text{Comp2}} \setminus I_{\text{Comp1}}$ are useless for achieving the system objectives. It is concluded that the difference of the measures associated with $\mathcal{R}_{\text{Comp1}}$ and $\mathcal{R}_{\text{Comp2}}$ gives an idea of the usefulness of the subset of components $I_{\text{Comp2}} \setminus I_{\text{Comp1}}$.
- Assume that two sets of components are such that $I_{\text{Comp1}} \subset I_{\text{Comp2}}$ and that $\mathcal{R}_{\text{Comp1}} = \emptyset$ while $\mathcal{R}_{\text{Comp2}} \neq \emptyset$, then the subset $I_{\text{Comp2}} \setminus I_{\text{Comp1}}$ is (or contains) a critical component subset. Therefore, its removal from I_{Comp2} implies the impossibility that it will be impossible to satisfy the system specifications.

Example 8.9 Fault-tolerance evaluation

Assume the system in the previous example is expected to operate on the time interval $[0, T]$ with $T = 10^5$ h. Actuators 1 and 2 reliability data are $r_1(t, 0) = r_2(t, 0) = \exp\left(-4 \times 10^{-6} t\right)$, while actuators 3 and 4 are less prone to failures, namely $r_3(t, 0) = r_4(t, 0) = \exp\left(-4 \times 10^{-7} t\right)$.

Starting with the nominal configuration 1234 at the initial time, the PACT control bank $\mathcal{U}_{\text{PACT}} = \{u_{12}, u_{134}, u_{23}, u_{24}\}$ allows to recover all recoverable configurations. This results

in the redundancy degrees $k_{\text{strong}}\,[1234] = 1$, and $k_{\text{weak}}\,[1234] = 2$, meaning that the system operation can go on in the single failure case, whatever the failed actuator (the system is said to be fail-operational with respect to the first fault), and still works when some double faults occur. Note that using the smaller control bank $\mathcal{U} = \{u_{12},\ u_{134},\ u_{23}\}$ does not change the redundancy degrees, since the set of recoverable configurations remains unchanged (however, the performance of some configurations will be lower, although still admissible).

Using $\mathcal{U}_{\text{PACT}} = \{u_{12},\ u_{134},\ u_{23},\ u_{24}\}$, and assuming actuator failures are independent, the success probability computed from Eq. (8.33) is $\Pr\left[1234,\ 0,\ 10^5\right] = 0.8740$. Decreasing $\mathcal{U}_{\text{PACT}}$ to $\mathcal{U} = \{u_{12},\ u_{134},\ u_{23}\}$ does not change this figure.

Assuming the minimality of the control bank is an important point, note that if the bank $\{u_{12},\ u_{134},\ u_{23}\}$ is further decreased to $\{u_{12},\ u_{134}\}$ the recoverable configuration 24 cannot be recovered anymore. However, the probability for this configuration to occur within the mission time is so small (0.0083) that one could decide to implement the bank $\{u_{12}, u_{134}\}$ at the cost of not recovering fault 24 should it occur. Note that in this case, the redundancy degrees are still $k_{\text{strong}}\,[1234] = 1$ and $k_{\text{weak}}\,[1234] = 2$, but the success probability decreases from 0.8740 to 0.8657.

The admissible cost specification was defined by $\rho = 15$: a configuration is recoverable if there exists a control law such that the quadratic cost does not exceed 15 times the optimal cost of the nominal configuration. Table 8.7 shows the results obtained for different values of the cost parameter $\rho \in \{1, 2, \ldots, 7\}$. Only the values at which changes occur are displayed, and the last column recalls the results for $\rho = 15$.

To evaluate the sensitivity with respect to components, the effect of removing actuator subsets from I is computed. Table 8.8 shows the results for $\rho = 15$. Subsets whose removal results in $\mathcal{R} = \emptyset$ are not shown.

It is clearly seen that there is no useless component and that the critical component subsets are $\{12,\ 23,\ 24\}$: the failure of any of these subsets results in a non-recoverable configuration. This analysis is very useful for the architecture design problem, which consists in selecting the appropriate actuators to control the system in a fault tolerant way. For example, implementing only actuators123 would give $\mathcal{R} = \{123,\ 12,\ 23\}$, $k_{\max}\,[123] = 0$ and $k_{\min}\,[123] = 1$, meaning that the single fault fail operational property is lost. The success probability is drastically decreased to 0.0259. □

Table 8.7 Sensitivity to cost specification

ρ	1	2	4	5	15
Minimal recoverable configurations	1234	234	123 124 234	124 23	12 134 23 24
Strong redundancy degree	0	0	0	0	1
Weak redundancy degree	0	1	1	2	2
Success probability	0.4148	0.6188	0.6526	0.6609	0.8740

Table 8.8 Sensitivity to components

Removed subsets	1	2	3	4	13	14	34
Recoverable configurations	234 24 23	134	124 24 12	123 12 23	24	23	12
Strong redundancy degree	0	0	0	0	0	0	0
Weak redundancy degree	1	0	1	1	0	0	0
Success probability ($\times 10^2$)	21.06	20.40	2.59	2.59	0.83	0.83	0.07

8.7 Exercises

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? □

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 four times the optimal cost of the healthy system, all configurations are recoverable except $\{ac, ad, bc, a, b, c, d\}$ as shown in Fig. 8.6, where the white nodes are recoverable while the grey nodes are not.

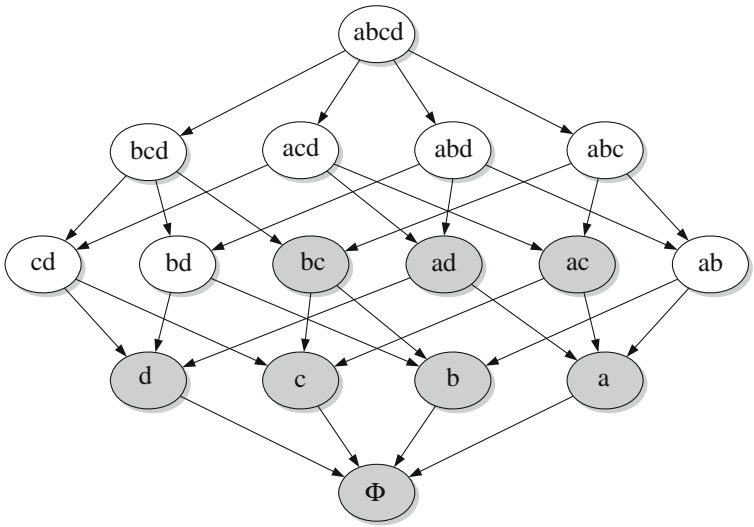

Fig. 8.6 Recoverable configurations

1. From Fig. 8.6 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:

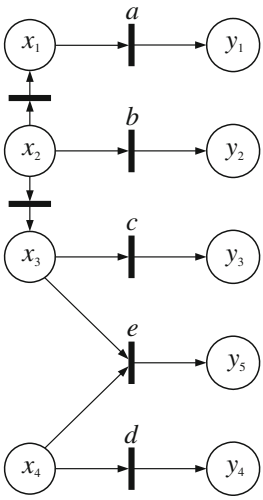

Fig. 8.7 Structural graph of the measurement system

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

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

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

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? □

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. 8.7.

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

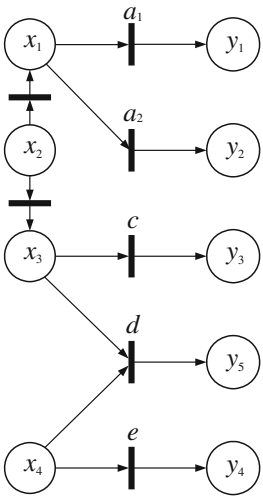

Fig. 8.8 The new system with b removed and a duplicated

structural graph from any unknown variable to a sensor (this is a necessary condition for the structural observability of the unknown variables). From Fig. 8.7, the system is clearly output-connected when the five 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 two 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 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. 8.8.

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

8.8 Bibliographical Notes

The fault-tolerant control problem. Defining the fault-tolerant control problem and understanding the differences with the classical control problem has motivated many early works [30, 32]. A formalisation of the problem can be found in [122, 329].

Recoverability is concerned with the possibility either to accommodate the faults or to reconfigure the system when faults occur. Early works on the recoverability problem are [113, 121, 170, 392] for a class of switched systems.

Recoverable faults can be handled by fault accommodation or system reconfiguration. A survey on fault accommodation is given in [264, 285], and interesting results can be found in [172, 327]. Many approaches have been developed to provide the model of the faulty system that is required by fault accommodation, most of them based on the development of adaptive or learning observers [171, 335, 336]. A control mixer approach to deal with actuator faults was pursued by [400, 401]. A wider area of reconfiguration was studied in [393, 399]. The general model of reconfiguration based fault tolerance was introduced in [330] and the use of generic models for reconfiguration analysis was considered in [331].

When faults are not recoverable, human intervention is most commonly needed to find another achievable system objective, using decision support from the diagnosis and overall goals for the plant [199]. Appropriate switching of the system operating mode is the goal of the supervisory system [169]. In fact, due to the discrete nature of fault occurrence and reconfiguration, fault-tolerant control systems are hybrid in nature according to [112, 113].

The properties of combined fault diagnosis and control were treated in [264].

Fault-tolerant linear quadratic design. The fault-tolerant linear quadratic design problem was introduced in [321] for actuator faults. Sensor faults and sensor network design were addressed in [149].

The model-predictive control technique allows to take into account inequality constraints, that are rather difficult to consider in linear quadratic control, at the price of an increased on-line computing power. This technique was used in [223] for fault accommodation and reconfiguration. The model-predictive controller uses all available input signals u_i and measurable output signals y_i which comprise the vectors $\boldsymbol{u}$ and $\boldsymbol{y}$ as before rather than only those input and output signals are used in the nominal feedback loop. If on the supervision level a fault f is detected, the inequality constraints included in the optimisation problem can be changed so that the model-predictive controller adapts to the faulty system. This can be done in a very easy way for actuator faults. If the diagnostic algorithm shows that the jth actuator is faulty, the equality constraint $u_j = 0$ is included in the optimisation problem in order to ensure that the controller does not really use the jth input. Then the model-predictive controller moves its control activity towards the available actuators, which can be interpreted as an on-line reconfiguration of the control loop.

As model-predictive control necessitates a rather large on-line computing capacity and as its reconfigurability property is, more or less, restricted to actuator faults this

method should be used for ensuring fault tolerance only if the advantages of model-predictive control have to be exploited for the faultless plant as well. For applications, where a fixed (linear) controller is sufficient for satisfying the control requirements for the faultless plant, the reconfiguration should be carried out by methods described in the earlier sections, which eventually result in a new fixed control law.

Implementation issues. The general theory of reconfiguration-based fault tolerance, including the passive–active design, was developed in [333]. The optimisation of the reliable control specifications was analysed in [332] while the reduction of the reliability over-cost was first presented in [16].

Fault-tolerance evaluation. Fault-tolerance evaluation is in some sense a measure of how many faults are or are not recoverable. It has been considered from the point of view of the system structural properties, e.g. observability or controllability, extending the evaluation of these properties to the faulty system. For example, the smallest second-order mode, first introduced in [231], has been proposed as a reconfigurability measure in [392]. A general approach to fault-tolerance evaluation under the reconfiguration strategy was presented in [68] with application to the measure of the system components' usefulness, and specification to the structural analysis approach.