Controller reconfiguration based on LTR design

Niemann, Hans Henrik; Stoustrup, J.

Published in:
Proceedings of the 42nd IEEE Conference on Decision and Control

Link to article, DOI:
10.1109/CDC.2003.1272988

Publication date:
2003

Document Version
Publisher's PDF, also known as Version of record

Link back to DTU Orbit

Citation (APA):
Controller Reconfiguration based on LTR Design

Henrik Niemann
Ørsted DTU, Automation
Technical University of Denmark
Building 326, DK-2800 Lyngby, Denmark
hhn@orsted.dtu.dk

Jakob Stoustrup
Dept. of Control Engineering
Aalborg University, Fr. Bajers Vej 7C
DK-9220 Aalborg, Denmark
jakob@control.auc.dk

Abstract—Design of Controller Reconfiguration (CR) for systems with sensor faults is considered in this paper. One way to accommodate a failing sensor is by replacing it by an observer based on the remaining outputs. A similar approach can be applied for a faulty actuator by duality. By including observers in the loop to replace faulty components, the nominal feedback controller does not need to be redesigned. The CR observer design problem for the faulty sensors or actuators can be rewritten into a standard Loop Transfer Recovery (LTR) design problem, to which standard LTR design methods can be applied. Finally, it is shown that this CR architecture, where an CR observer is included in the feedback loop in between the system and the nominal controller, can be transformed into a more general fault tolerant Controller (FTC) architecture based on the Youla parameterization.

I. INTRODUCTION

The interest for using fault tolerant controllers is increasing. A number of both theoretical results as well as application examples has now been described in the literature, see e.g. [1], [2], [3], [7], [8], [11], [15], [17], [18], [20] to mention some of the relevant references in this area.

The focus in this paper will be on fault tolerance with respect to sensor faults. The dual fault case, actuator faults will not be considered in this paper. The reason is that actuator faults can be handled in the same way as sensor faults. These faults are quite common in connection with feedback control. It is therefore important that it is possible to handle these types of faults in a systematic way. Further, it is also important that the subsequent reconfiguration of the feedback controller after a fault in the system, is derived in a general and systematic way. It is further important that the applied Fault Tolerant Control (FTC) architecture is general, since else we need to derive new FTC architectures for every single type of faults. Finally, it is important that the design of the modified controller is systematic. This will make it possible to apply both standard design methods as well as to do the reconfiguration design automatically. Finally, the on-line change of the feedback controller should be done in a smooth way. This can be done by modifying the nominal feedback controller by an reconfiguration block instead of using a completely new redesigned feedback controller.

In connection with sensor faults, it is possible to handle these faults either by modifying the nominal controller, such that the faulty component is not applied in the feedback loop, or by using an estimation of the missing signals in the feedback loop. In the latter case, the nominal controller can still be applied, we only need to modify the input or output signals from the systems to remove the effect from faults in a sensor of actuator. This concept has been introduced in [2], where observers have been applied as virtual sensors.

The design of these CR observers can be derived with respect to optimizing either the performance of the observer or with respect to optimizing the performance of the closed loop system. In the first case, standard observer design methods can be applied. In the second case, the observer design needs to be designed with respect to the overall performance of the feedback system. Including an observer in a feedback loop to recover measurement signals or control signals is a well know problem in the Loop Transfer Recovery theory, see [4], [10], [12], [13], [14]. The main concept in LTR is to design a target state feedback loop, which cannot, however, be implemented in the real system due to the instrumentation. In the LTR step, the target loop is recovered by using an observer based feedback controller, which can be implemented. This is equivalent with using observers in connection with sensor faults. One of the main results in this paper is to show how it is possible to transform the CR observer design problem into standard LTR design problems.

The second result of this paper deals with the implementation of the feedback controller including an CR observer. When an CR observer needs to be included in the feedback loop, we need to break the loop to do this. This might not always be acceptable. Instead, the CR observer can be included in the feedback loop by using the FTC architecture described in [7], [8], [11], [15]. This FTC architecture is based on the Youla parameterization, which makes it possible to change/modify the nominal controller without breaking the feedback loop. The modification of the controller is derived by including an additional loop around the nominal controller. Based on this FTC architecture, it will be shown in this paper how the CR observers can be included in the feedback loop by a proper design of the additional feedback loop around the nominal controller.

II. SYSTEM SETUP

Consider the following generalized nominal $(r+m)\times(q+p)$ system $\Sigma$,

$$
\dot{x} = AX + Bd + Bu
$$

$$
\Sigma : \begin{cases} 
\dot{e} = C_{ex} + D_{ed} + D_{eu}u \\
y = C_{y}x + D_{yd}u 
\end{cases}
$$

(1)
Consider the system in (1) in the case including sensor faults. The system setup given by (5) with sensor faults. The direct controller reconfiguration design problem is as follows.

**Problem 1 Direct controller reconfiguration design.** Let a faulty system be given by (5). Design a stabilizing controller $K_{sen}$, if it exist, such that a suitable norm of the closed loop system $T_{ed,sen}$ is minimized.

The advantages with this design problem is that the controller is optimized with respect to the original performance condition. The disadvantage with this design is that we get a new controller that will in general be completely different compared with the nominal controller.

Instead of making a direct design of $K_{sen}$, let us consider the difference between the nominal closed loop system and the faulty closed loop system given by

$$E_{ed,sen} = T_{ed,nom} - T_{ed,sen}$$

$$E_{ed,sen} = G_{eu} [K(I - G_{yu}K)^{-1}G_{yd}]$$

(10)

and try to minimize this difference in a suitable sense by the design of $K_{sen}$. However, a direct optimization of (10) will not result in an optimal controller with respect to minimizing the effect from the external input $d$ to the external output $e$.

The reason is that the external disturbance input consist of sensor faults and actuator faults. Sensor faults are modeled as change in the output matrices $C_y$ and $D_{yd}$. In many cases a sensor fault will result in a reduction of the number of measurement signals, i.e. in a rank drop in the said matrices. In case of sensor faults, the system in (1) is given by,

$$\dot{x} = Ax + Bd + Bu$$

(4)

where $x_e \in \mathbb{R}^{n_e}$ is the controller state vector.

Let us consider the system given by (1) in the case of sensor faults and actuator faults. Sensor faults are modeled as a change in the output matrices $C_y$ and $D_{yd}$. In many cases, a sensor fault will result in a reduction of the number of measurement signals, i.e. in a rank drop in the said matrices. In case of sensor faults, the system in (1) is given by,

$$\dot{x} = Ax + Bd + Bu$$

(4)

and where $x_e \in \mathbb{R}^{n_e}$ is the controller state vector.

Let us consider the system given by (1) in the case of sensor faults and actuator faults. Sensor faults are modeled as a change in the output matrices $C_y$ and $D_{yd}$. In many cases, a sensor fault will result in a reduction of the number of measurement signals, i.e. in a rank drop in the said matrices. In case of sensor faults, the system in (1) is given by,

$$\dot{x} = Ax + Bd + Bu$$

(4)

and where $x_e \in \mathbb{R}^{n_e}$ is the controller state vector.

Let us consider the system given by (1) in the case of sensor faults and actuator faults. Sensor faults are modeled as a change in the output matrices $C_y$ and $D_{yd}$. In many cases, a sensor fault will result in a reduction of the number of measurement signals, i.e. in a rank drop in the said matrices. In case of sensor faults, the system in (1) is given by,

$$\dot{x} = Ax + Bd + Bu$$

(4)

and where $x_e \in \mathbb{R}^{n_e}$ is the controller state vector.

Let us consider the system given by (1) in the case of sensor faults and actuator faults. Sensor faults are modeled as a change in the output matrices $C_y$ and $D_{yd}$. In many cases, a sensor fault will result in a reduction of the number of measurement signals, i.e. in a rank drop in the said matrices. In case of sensor faults, the system in (1) is given by,

$$\dot{x} = Ax + Bd + Bu$$

(4)

and where $x_e \in \mathbb{R}^{n_e}$ is the controller state vector.

Let us consider the system given by (1) in the case of sensor faults and actuator faults. Sensor faults are modeled as a change in the output matrices $C_y$ and $D_{yd}$. In many cases, a sensor fault will result in a reduction of the number of measurement signals, i.e. in a rank drop in the said matrices. In case of sensor faults, the system in (1) is given by,

$$\dot{x} = Ax + Bd + Bu$$

(4)

and where $x_e \in \mathbb{R}^{n_e}$ is the controller state vector.

Let us consider the system given by (1) in the case of sensor faults and actuator faults. Sensor faults are modeled as a change in the output matrices $C_y$ and $D_{yd}$. In many cases, a sensor fault will result in a reduction of the number of measurement signals, i.e. in a rank drop in the said matrices. In case of sensor faults, the system in (1) is given by,

$$\dot{x} = Ax + Bd + Bu$$

(4)

and where $x_e \in \mathbb{R}^{n_e}$ is the controller state vector.
the measurement noise from the nominal closed loop system, we get the following nominal closed loop system

\[ \dot{T}_{ed,nom} = (C_e + D_{en}KC_y)(sI - A - B_uKC_y)^{-1}B_d + D_{ed} \]

(11)

Using \( \dot{T}_{ed,nom} \) from (11) in the closed loop error \( E_{ed,sen} \) in (10) gives the following modified closed loop transfer error \( \tilde{E}_{ed,sen} \)

\[ \tilde{E}_{ed,sen} = \dot{T}_{ed,nom} - T_{ed,sen} \]

(12)

Based on the above closed loop transfer error, we have the following direct CR recover design

**Problem 2 Direct CR recovery design.** Let a faulty system be given by (5) and let the associated closed loop transfer error be given by (12). Design a stabilizing controller \( K_{sen} \) if it exist, such that a suitable norm of the closed loop transfer error \( \tilde{E}_{ed,sen} \) is minimized.

Again, we will get a new controller that will in general be a completely different controller compared with the nominal controller. This means that there are no advantages in implementation of the CR controller \( K_{sen} \) with respect to the nominal controller. Further, it can not be seen directly from the design problem, how well the nominal closed loop can be recovered. In principle, it is possible to analyze this problem directly. It is much easier, however, to analyze when a specific controller architecture is applied for the CR controller \( K_{sen} \).

Let us include an observer in the loop as described in e.g. [2] when sensor faults appear. The observer will estimate the missing measurement signals and, thus, the nominal feedback controller can still be applied. The design of the observer can be derived in two ways: either by optimizing the observer to give a good estimate of the missing measurement signals or by optimizing in order to minimize a suitable norm of the closed loop transfer error given by (12). The first method is a standard observer design and will not be considered further in this paper. The second method is equivalent with the well known Loop Transfer Recovery design method, [10], [12], [14].

Let a full order observer be included in the feedback controller to estimate all measurement signals be given by

\[ \dot{x} = A\dot{x} + Bu - L(y_f - C_{y,f}\dot{x}) \]

\[ y = C_y\dot{x} \]

where \( L \) is the observer gain. Including the nominal feedback controller in the observer, we get the following fault tolerant controller

\[ K_{sen} = KC_y(sI - A - BuKC_y - LC_{y,f})^{-1}L \]

(14)

Based on the full order observer based feedback controller given by (14), it is possible to rewrite \( \tilde{E}_{ed,sen} \). Using the results from LTR, [10], [12], [14], \( \tilde{E}_{ed,sen} \) can be written as:

\[ \tilde{E}_{ed,sen} = \dot{T}_{ed,nom}M_{sen} \]

(15)

where \( \dot{T}_{ed,nom} \) is the nominal closed loop transfer function from measurement signal \( y \) to the external output \( e \) without disturbances

\[ \dot{T}_{ed,nom} = (C_e + D_{en}KC_y)(sI - A - BuKC_y)^{-1}B_u + D_{ed}K \]

(16)

and \( M_{sen} \) is given by

\[ M_{sen} = C_y(sI - A - LC_{y,f})^{-1}(B_d + LD_{y,f}) \]

(17)

and is called the sensor recovery matrix, inspired by the classical LTR theory, where it is simply called the recovery matrix. Note that \( \dot{T}_{ed,nom} \) is independent of the observer design. It depends only on the nominal feedback controller and the sensor recovery matrix \( M_{sen} \) depend on the observer design.

Based on (15), it is possible to minimize the closed loop transfer error either directly by minimizing \( \dot{T}_{ed,nom}M_{sen} \) or indirectly by minimizing the sensor recovery matrix \( M_{sen} \) for the design of the observer. Let us consider the following indirect CR design problem for the sensor fault problem

**Problem 3 Indirect CR recovery design.** Let a faulty system be given by (5) and let the associated closed loop transfer error be given by (12). Design a stabilizing observer based controller \( K_{sen} \) given by (14), if it exists, such that a suitable norm of the sensor recovery matrix \( M_{sen} \) is minimized.

The CR design problem for systems with sensor faults has now been transformed into a standard LTR design problem. It is therefore possible to use all the analysis and design methods known from LTR in connection with CR design for systems with sensor faults.

There exist a number of different methods for design of LTR controllers that can be applied directly in connection with an optimization of the sensor recovery matrix.

Finally, let us consider a few design methods for the CR observer. All the well known design methods from LTR can be applied directly. For a description of LTR design methods, see e.g. [10], [12], [14]. The most well-known LTR design method is the LQG/LTR design method. It is based on the classical LQG design method with a special selection of the covariance matrices, see e.g. [4], [13]. It is also possible to use \( \mathcal{H}_2 \) or \( \mathcal{H}_\infty \) methods for optimization of the recovery matrix, i.e. \( \mathcal{H}_2/LTR \) and \( \mathcal{H}_\infty/LTR \) design, see [10], [12], [14]. These two design methods are based on a minimization of the \( \mathcal{H}_2 \) norm or the \( \mathcal{H}_\infty \) norm of the recovery matrix with the design of the observer gain. These two design problems can be formulated as a standard design problem. Using the standard setup, the CR recovery design problem can be transformed into the setup shown in Figure 1, where \( P_{M_{sen}} \) is given by

\[ P_{M_{sen}} = \begin{pmatrix} A & B_d & I \\ C_y & 0 & 0 \\ C_{y,f} & D_{y,f} & 0 \end{pmatrix} \]

(18)
Problem 4 CR recovery design. Let the recovery matrix \( M_{sen} \) be given by:
\[
M_{sen} = C_y(sI - A - LC_y,f)^{-1}(B_d + LD_yd,f)
\]
The CR recovery design problem is to design a proper, real-rational controller \( L \), if such exist, which stabilizes \( P_{M_{sen}} \) internally and minimize a suitable norm of the \( M_{sen} \).

IV. IMPLEMENTATION OF CONTROLLER RECONFIGURATION

The implementation of the CR controllers will be considered in the following. A direct method to implement the CR part of the feedback controller considered in Section III is to include an observer (for sensor faults) or a dual observer (for actuator faults) in between the system and the nominal controller. This CR architecture has been considered in [2], where a reconfiguration block is included between the system and the nominal controller.

This architecture modifies the input/outputs from the system such that the nominal controller does not need to be modified. This mean that the reconfiguration block will depend strongly on the type of faults appearing in the system.

Another architecture has been considered in [7], [11], [15]. This architecture is based on the Youla parameterization. In contrast with the setup used in [2], the nominal controller is applied directly on the faulty system. Instead, the nominal controller is modified by a CR block that is connected to the nominal controller. This CR block is a general block where the structure does not depend on the fault case.

Before this FTC architecture is described in more details, the Youla parameterization is shortly introduced.

A. The Youla Parameterization

Let a coprime factorization of the system \( G_{yu}(s) \) from (2) and a stabilizing controller \( K(s) \) from (4) be given by:
\[
\begin{align*}
G_{yu} &= NM^{-1} = \hat{M}^{-1}\hat{N}, \quad N, M, \hat{N}, \hat{M} \in \mathbb{RH}_\infty \\
K &= UV^{-1} = \hat{V}^{-1}\hat{U}, \quad U, V, \hat{U}, \hat{V} \in \mathbb{RH}_\infty
\end{align*}
\]
where the eight matrices in (19) must satisfy the double Bezout equation given by, see [19]:
\[
\begin{pmatrix}
1 & 0 \\
0 & 1
\end{pmatrix}
= \begin{pmatrix}
\hat{V} & -\hat{U} \\
-\hat{N} & \hat{M}
\end{pmatrix}
\begin{pmatrix}
M & U \\
N & V
\end{pmatrix}
= \begin{pmatrix}
M & U \\
N & V
\end{pmatrix}
\begin{pmatrix}
\hat{V} & -\hat{U} \\
-\hat{N} & \hat{M}
\end{pmatrix}
\]

Based on the above coprime factorization of the system \( G_{yu}(s) \) and the controller \( K(s) \), we can give a parameterization of all controllers that stabilize the system in terms of a stable parameter \( Q(s) \), i.e. all stabilizing controllers are given by [16]:
\[
K(Q) = U(Q)V(Q)^{-1}
\]

where
\[
U(Q) = U + MQ, \quad V(Q) = V + NQ, \quad Q \in \mathbb{RH}_\infty
\]

Using the Bezout equation, the controller given either by (21) can be realized as an LFT in the parameter \( Q \),
\[
K(Q) = \mathcal{F}_l(J_K, Q)
\]
where \( J_K \) is given by
\[
J_K = \begin{pmatrix}
UV^{-1} & \hat{V}^{-1} \\
V^{-1} & -V^{-1}N
\end{pmatrix}
\]

Reorganizing the controller \( K(Q) \) given by (22) results in the closed loop system depicted in Figure 2, [16].

An important observation is the following relatively simple expression for the transfer function from the external input \( d \) to the external output \( e \) terms of the parameter \( Q \):
\[
e = (G_{ed} + G_{eu}K(Q)(I - G_{yu}K(Q))^{-1}G_{yd})d
= (G_{ed} + G_{eu}U\hat{M}G_{yd} + G_{eu}MQ\hat{M}G_{yd})d
\]
where (20) has been exploited. Note, that the transfer function relating \( d \) and \( e \) is affine in \( Q \).

**B. Fault Tolerant Controller Architecture**

An architecture for fault tolerant controllers will now be proposed, based on the Youla parameterization shown in the block diagram in Figure 2. There is a number of reasons for using the architecture from the Youla parameterization in connection with FTC. Using this architecture, the \( Q \) parameter will be the CR part of the controller. This means that the CR part of the feedback controller is a modification of the existing controller. Thus, a controller change when a fault appears in the system is not a complete shift to another controller, but only a modification of the existing controller by adding a correction signal in the nominal controller, the \( r \) signal in Figure 2. However, it should be pointed out that it is possible to modify the controller arbitrarily by designing the Youla parameter \( Q \), see e.g. [9], [16], since this parameterization eventually yields any stabilizing compensator.

Another important thing is that the architecture includes also a parameterization of all residual generators. All residual signals can be described by, [5], [6]

\[
\tau_{FDI} = Q_{FDI} \tilde{r} = Q_{FDI}(M_y - \bar{N}u) \quad (24)
\]

This means that it is possible to combine both fault diagnosis and fault tolerant control in the same architecture without any problems. A block diagram for this combined FDI and CR architecture (FTC architecture) based on the Youla parameterization is shown in Figure 3 for three potential faults - the generalization to any number of faults should be obvious.

**C. Implementation of Fault Tolerant Controllers**

The FTC architecture shown in Figure 3 will now be applied for the implementation of the CR controller considered in Section III. The implementation of the observer based feedback controller based on the FTC architecture can be derived by using the following result from [9]:

**Theorem IV.1** Let a system be given by (1) and let two stabilizing controllers for the system be given by \( K_0 = U_0V_0^{-1} \) and \( K_1 = \tilde{V}_1^{-1}\tilde{U}_1 \). Then \( K_1 \) can be implemented as \( K_0(Q) \) where the stable \( Q \) parameter is given by:

\[
Q = X(\tilde{U}_1V_0 - \tilde{V}_1U_0) = X\bar{Q},
\]

or

\[
Q = X(\tilde{V}_1(K_1 - K_0)V_0)
\]

where

\[
X = M_0^{-1}M_1
\]

**Proof:** See [9].

Using the above theorem, we have directly that it is possible to implement the CR controller given by (14) as function of the nominal controller \( K \) and a CR parameter \( Q_{CR} \). Let the CR controllers for the sensor faults given in (14), and the faulty system have the following coprime factorization

\[
K_{sen} = \tilde{V}_{sen}^{-1}\tilde{U}_{sen} = U_{sen}V_{sen}^{-1}
\]

\[
G_{yu} = N_{sen}M_{sen}^{-1} = \bar{N}_{sen}^{-1}\bar{N}_{sen}
\]

where the \( S \) stable coprime factors satisfies the double Bezout equation (20).

Based on Theorem IV.1 and the coprime factorization of the CR controllers given by (25), we have the following result.

**Theorem IV.2** Let the CR controllers for the sensor fault case be given by \( K_{sen} \), with the coprime factorization given by (25). The implementation of the controller in the general FTC architecture is possible by using

\[
Q_{CR,sen} = M_{sen}^{-1}M_{sen}(\tilde{U}_{sen}V - \tilde{V}_{sen}U)
\]

![Fig. 3. Fault tolerant scheme with three potential faults. The residual signal is used both for isolation and for feedforward in the fault handling.](image)
for the sensor fault case.

In connection with the above theorem, it is important to note that in contrast to the nominal controller, the final controller $K_{\text{sen}}(Q_{\text{CR, sen}})$ will not depend on the faulty signals at all.

V. Conclusion

The controller reconfiguration problem for systems with sensor faults has been considered in this paper. The CR problem can be solved by including an observer in the feedback loop to compensate the missing sensor signals. The design of the CR observers is based on the criterion that the fault free nominal feedback loop must be recovered as good as possible. Based on this criterion, the design problem is equivalent with the well known LTR design of observer based feedback controllers. All the standard LTR design methods can be applied for the design of the FTC observers.

Further, it is shown that including an CR observer in the feedback loop to compensate for sensor faults can be implemented by using the general FTC architecture. The CR observer can be included in the feedback loop by including an additional loop around the nominal feedback controller, i.e. using the Youla parameterization. As a consequence of this, we do not need to break the loop to include CR observers in the feedback loop - the fault tolerance is achieved by an additive correction signal. The actuator fault case can be handled in the same way.

VI. References