Multisensor switching strategy for Fault-Tolerant Control

J.J. Martinez§, M. Seron‡ and J. DeDonna‡

§ Gipsa-lab UMR 5216, Grenoble-INP. St. M. d’Hères 38402, France.
‡ CDSC Centre, University of Newcastle. Callaghan 2308, NSW, Australia.

Journée GdR MACS - GT MOSAR
Grenoble, 15th February 2008
1. Motivation

2. Fault Tolerant Control (A brief introduction)

3. A multi-sensor switching scheme for FTC

4. Stability guarantees

5. A case study
Part I
Motivation
Collision Avoidance Sensor-based System:

Vehicle assistance systems require multiple sensors (sometimes redundant) to guarantee driver safety.
Several automotive control applications require multiple redundancy sensors. A sensor could fail or operate outside its specified operating conditions (*Traffic spray, Fog, Rain, Dirt on the Cover*...). Classical fusion of sensors does not work well with a failed sensor.

**Question:** How to *orchestrate* multiple redundancy sensors to make the system more robust w.r.t. a sensor failure (stability, performance, safety...).
Part II

Fault-Tolerant Control (A brief introduction)
Fault Tolerant Control (FTC)

Example of a faulty system:

- Faults are deviations from a specified mode of behaviour that can take place in different parts of a control system.
- A fault can be abrupt, intermittent or incipient.
- Systems that continue to perform adequately in the presence of faults, are called fault-tolerant control (FTC) systems.
Passive vs. Active FTC

Passive FTC:

Robust Controller \[\rightarrow\] System

- Passive FTC are mainly based on robust controller. Non require on-line detection, but very conservative, and only for small failures.

Active FTC:

Controller \[\rightarrow\] System

- Active FTC integrates a reconfigurable mechanism (adaptation) intended to preserve both stability and performance.
Approaches are focused on one of both parts, i.e. FDD and FTC separately.

- It is assumed perfect fault estimates from the FDD part (fault model).
- Most of the them do not provide any guarantee of the post-fault performance, or even stability.
Fault-Tolerant Control (New paradigm)

- The approach is based on the minimisation of a control-performance criterion.
- Faulty detection and isolation are achieved “implicitly” by avoiding the selection faulty sensors.
- Allows less conservative failure scenarios. Requiring, for example, at least one healthy sensor.
Part III
A multi-sensor switching scheme for FTC
The multi-sensor switching scheme

Key features

- The scheme switches between sensor-estimator pairs and selects the one with the “best” tracking performance to implement the control law.
- Closed-loop stability is guaranteed in the absence of faults.
- Under a set of conditions on the system parameters, closed-loop stability is preserved under faults since the switching scheme automatically avoids selecting faulty sensors.
The multi-sensor switching scheme

The plant:

\[ x^+ = Ax + Bu + Ew, \quad w \text{ bounded.} \]

The reference model to track:

\[ x_{ref}^+ = Ax_{ref} + Bu_{ref}, \quad x_{ref}, u_{ref} \text{ bounded.} \]
The multi-sensor switching scheme

Multi-sensors: \((i = 1, \ldots, N.\))

\[
\begin{align*}
\xi_i^+ &= A_{si}\xi_i + B_{si}Cx, \\
y_i &= \begin{cases} 
C_{si}\xi_i + \eta_i & \text{if healthy,} \\
\eta_i^F & \text{if faulty,} 
\end{cases} & \text{if healthy,} \\
& \quad \eta_i \text{ bounded} \\
& \quad \eta_i^F \text{ bounded}
\end{align*}
\]

Sensor “reference signals”: \((i = 1, \ldots, N.\))

\[
\xi_{i,\text{ref}}^+ = A_{si}\xi_{i,\text{ref}} + B_{si}Cx_{\text{ref}}, & \quad \xi_{i,\text{ref}} \text{ bounded}
\]
The multi-sensor switching scheme

**Estimators: \((i = 1, \ldots, N)\)**

**Filter dynamics:**
\[
\begin{bmatrix}
\hat{x}_i \\
\hat{\xi}_i
\end{bmatrix}^+ =
\begin{bmatrix}
A & -L_i C_s_i \\
B_s C & A_s_i - L_s_i C_s_i
\end{bmatrix}
\begin{bmatrix}
\hat{x}_i \\
\hat{\xi}_i
\end{bmatrix}
+ \begin{bmatrix}
B \\
L_s_i
\end{bmatrix} u
+ \begin{bmatrix}
L_i
\end{bmatrix} y_i.
\]

\(A_{L_i}\) stable

**Estimate update:**
\[
\begin{align*}
\hat{x}_i^{UP} &= \hat{x}_i + M_i (y_i - C_s_i \hat{\xi}_i), \\
\hat{\xi}_i^{UP} &= \hat{\xi}_i + M_{s_i} (y_i - C_s_i \hat{\xi}_i).
\end{align*}
\]
The multi-sensor switching scheme

The plant tracking error:

\[ z \triangleq x - x_{ref}. \]

The tracking errors for the estimates: \((i = 1, \ldots, N.)\)

\[ \hat{z}_i \triangleq \hat{x}_i - x_{ref}, \]
\[ \hat{\zeta}_i \triangleq \hat{\xi}_i - \xi_{i, ref}, \]
\[ \hat{z}_{i, UP} \triangleq \hat{x}_{i, UP} - x_{ref}. \]
The multi-sensor switching scheme

The switching control law is given by:

\[ u = u_{ref} - K \hat{z}^* \]
\[ \hat{z}^* = \arg \min_{\hat{z}} \{ \hat{z}'P\hat{z} : \hat{z} \in \{ \hat{z}_1^{UP}, \ldots, \hat{z}_N^{UP} \} \}, \]

where, given \( Q > 0 \) and \( R > 0 \), \( P > 0 \) and \( K \) are computed from the following Riccati equation:

\[ P = A'PA + Q - K'(R + B'PB)K, \]
\[ K \triangleq (R + B'PB)^{-1}B'PA. \]
Part IV
Stability guarantees
Consider the switched system
\[ x(k + 1) = Ax(k) + B_l \nu_l(k), \]
where \( l \in \{1, \ldots, N\} \), and \( A \) has eigenvalues strictly inside the unit circle. Let \( V \Lambda V^{-1} \) be the Jordan matrix decomposition of \( A \). Assume that, \( \bar{\nu} \triangleq \max_{l \in \{1, \ldots, N\}} \| V^{-1} B_l \| \bar{\nu}_l ; |\nu_l(k)| \leq \bar{\nu}_l, \bar{\nu}_l > 0 \) for all \( k \geq 0 \).

Define the set
\[ S_\epsilon \triangleq \{ x \in \mathbb{R}^n : \| V^{-1} x \| \leq (I - |\Lambda|)^{-1} \bar{\nu} + \epsilon \} . \]

Then:
1. For any \( \epsilon \geq 0 \), the set \( S_\epsilon \) is (positively) invariant. That is, if \( x(0) \in S_\epsilon \), then \( x(k) \in S_\epsilon \) for all \( k \geq 0 \).
2. Given \( \epsilon \in \mathbb{R}^n, \epsilon > 0 \), there exists \( k^* \geq 0 \) such that \( x(k) \in S_\epsilon \) for all \( k \geq k^* \).
Closed-loop analysis in the absence of faults

**Estimation errors:** \((i = 1, \ldots, N)\)

\[
\begin{bmatrix}
\tilde{x}_i \\
\tilde{\xi}_i
\end{bmatrix}
\triangleq
\begin{bmatrix}
x - \hat{x}_i \\
\xi - \hat{\xi}_i
\end{bmatrix}
= A_{Li} \begin{bmatrix}
\tilde{x}_i \\
\tilde{\xi}_i
\end{bmatrix}
+ B_i \begin{bmatrix} w_i \end{bmatrix}
\]

\[
\text{stable} \rightarrow \text{bounded} \rightarrow \text{invariant set } \tilde{S}_i
\]

**Estimator tracking errors:** \((i = 1, \ldots, N)\)

\[
\begin{bmatrix}
\hat{z}_i \\
\hat{\xi}_i
\end{bmatrix}
= A_{Li} \begin{bmatrix}
\hat{z}_i \\
\hat{\xi}_i
\end{bmatrix}
+ B_{li} \begin{bmatrix} \nu_{li} \end{bmatrix}
\]

\[
\text{stable} \rightarrow \text{bounded} \rightarrow \text{invariant set } \hat{S}_i
\]
Closed-loop analysis under faults

When a $j$ sensor fails, provided:

Only healthy sensors with estimation errors in $\tilde{S}_i$ are selected by the switching controller *working hypothesis*.

Then, the healthy sensor trajectories remain in the invariant sets; however:

**Estimator tracking error for the failed sensor**

$$\begin{bmatrix} \hat{z}_j \\ \hat{\zeta}_j \end{bmatrix}^+ = A_{Lj} \begin{bmatrix} \hat{z}_j \\ \hat{\zeta}_j \end{bmatrix} + B_{lj} \nu_{ij}^F$$

stable \hspace{1cm} bounded \quad \longrightarrow \quad \text{invariant set} \quad \hat{S}_j^F \supset \hat{S}_j$$

$$\begin{bmatrix} \tilde{x}_j \\ \tilde{\xi}_j \end{bmatrix}$$
Stability guarantees

Under the following:

**Failure Scenario**

- There is at least one healthy sensor.
- All healthy sensors have estimation errors in $\tilde{S}_i$.
- At least one healthy sensor has tracking error in $\hat{S}_i$.

The switching scheme selects a healthy $i$th sensor over the faulty $j$th sensor at the time of the fault and while the sensor remains failed provided:

**Conditions for healthy sensor selection**

$$J_{i}^{\text{max}} < J_{j}^{\text{min}} \quad \text{for all } i = 1, \ldots, N, \ i \neq j,$$

where

$$J_{i}^{\text{max}} \triangleq \max \left\{ (\hat{z}_i^{UP})' P_{\hat{z}_i^{UP}} : \hat{z}_i^{UP} \in T_i(\hat{S}_i \times W_i) \right\},$$

$$J_{j}^{\text{min}} \triangleq \min \left\{ (\hat{z}_j^{UP})' P_{\hat{z}_j^{UP}} : \hat{z}_j^{UP} \in T_j(\hat{S}_j^F \times W_j^F) \right\}.$$
Stability guarantees

Geometric interpretation of the conditions: for all \( i = 1, \ldots, N, i \neq j \)

\[
J_{i}^{\text{max}} \triangleq \max \left\{ (P^{1/2} \hat{z}_i^{UP})' (P^{1/2} \hat{z}_i^{UP}) : \hat{z}_i^{UP} \in T_i(\hat{S}_i \times W_i) \right\} < P^{-1/2} S_{i}^{\text{max}}
\]

\[
J_{j}^{\text{min}} \triangleq \min \left\{ (P^{1/2} \hat{z}_j^{UP})' (P^{1/2} \hat{z}_j^{UP}) : \hat{z}_j^{UP} \in T_j(\hat{S}_j^F \times W_j^F) \right\}.
\]

\[\|s\|^2 = J_{i}^{\text{max}}\]

\[\|s\|^2 = J_{j}^{\text{min}}\]
Part V

A case study: Multisensor automotive control
Simulation example

The inter-distance dynamics is taken as a double integrator ($T_s = 0.1s$):

$$A = \begin{bmatrix} 1 & 0.1 \\ 0 & 1 \end{bmatrix}, \quad B = \begin{bmatrix} 0 \\ 0.1 \end{bmatrix}, \quad C = \begin{bmatrix} 1 & 0 \end{bmatrix}, \quad \sigma^2_w = 0.01.$$ 

The two sensors are modelled with the following numerical values:

$$A_{s1} = 0.6065, \quad B_{s1} = 0.5, \quad C_{s1} = 0.7869, \quad \sigma^2_{s1} = 1,$$

$$A_{s2} = 0.9048, \quad B_{s2} = 0.25, \quad C_{s2} = 0.3807, \quad \sigma^2_{s2} = 0.5.$$ 

Comparison: LQG vs Switching, with matrices $Q = I_2$ and $R = 1$. We simulate a Stop-and-go scenario.
Simulation example (Off-line verification of stability conditions)

Geometric interpretation of the multisensor switching stability conditions for longitudinal control:

With the system data, the stability conditions are satisfied. Hence the system is guaranteed to be closed-loop stable under sensor fault.
Simulation example (Nominal operation)
Simulation example (A noisy sensor at 25s)

- Reference
- LQG
- Switching

Inter-distance $d$ (m)

Switch sequence

Stage cost

Journée MOSAR 28 / 32
Simulation example (Outage of a sensor at $25s$)
Conclusions and future directions

- We have investigated the fault tolerance properties of a multisensor switching strategy.

- The switching scheme is motivated by a control performance criterion and has a good performance in the absence of sensor failure.

- Closed-loop stability is guaranteed under a multiple failure scenario if a set of conditions on the parameters of the problem is satisfied. These conditions can be tested off line.

- Faulty sensor detection and isolation is achieved “implicitly” by guaranteeing that the switching cost avoids selecting faulty sensors. This feature departs from other available techniques.

- The on-line implementation of the scheme is simple, requiring only to compare cost values.

- Future work includes relaxing the failure scenario and the conditions for healthy sensor selection.
Conclusions and future directions

- We have investigated the fault tolerance properties of a multisensor switching strategy.

- The switching scheme is motivated by a control performance criterion and has a good performance in the absence of sensor failure.

- Closed-loop stability is guaranteed under a multiple failure scenario if a set of conditions on the parameters of the problem is satisfied. These conditions can be tested off line.

- Faulty sensor detection and isolation is achieved “implicitly” by guaranteeing that the switching cost avoids selecting faulty sensors. This feature departs from other available techniques.

- The on-line implementation of the scheme is simple, requiring only to compare cost values.

- Future work includes relaxing the failure scenario and the conditions for healthy sensor selection.
Conclusions and future directions

- We have investigated the fault tolerance properties of a multisensor switching strategy.

- The switching scheme is motivated by a control performance criterion and has a good performance in the absence of sensor failure.

- Closed-loop stability is guaranteed under a multiple failure scenario if a set of conditions on the parameters of the problem is satisfied. These conditions can be tested off line.

- Faulty sensor detection and isolation is achieved “implicitly” by guaranteeing that the switching cost avoids selecting faulty sensors. This feature departs from other available techniques.

- The on-line implementation of the scheme is simple, requiring only to compare cost values.

- Future work includes relaxing the failure scenario and the conditions for healthy sensor selection.
Conclusions and future directions

- We have investigated the fault tolerance properties of a multisensor switching strategy.

- The switching scheme is motivated by a control performance criterion and has a good performance in the absence of sensor failure.

- Closed-loop stability is guaranteed under a multiple failure scenario if a set of conditions on the parameters of the problem is satisfied. These conditions can be tested off line.

- Faulty sensor detection and isolation is achieved “implicitly” by guaranteeing that the switching cost avoids selecting faulty sensors. This feature departs from other available techniques.

- The on-line implementation of the scheme is simple, requiring only to compare cost values.

- Future work includes relaxing the failure scenario and the conditions for healthy sensor selection.
Conclusions and future directions

- We have investigated the fault tolerance properties of a multisensor switching strategy.

- The switching scheme is motivated by a control performance criterion and has a good performance in the absence of sensor failure.

- Closed-loop stability is guaranteed under a multiple failure scenario if a set of conditions on the parameters of the problem is satisfied. These conditions can be tested off line.

- Faulty sensor detection and isolation is achieved “implicitly” by guaranteeing that the switching cost avoids selecting faulty sensors. This feature departs from other available techniques.

- The on-line implementation of the scheme is simple, requiring only to compare cost values.

- Future work includes relaxing the failure scenario and the conditions for healthy sensor selection.
Conclusions and future directions

- We have investigated the fault tolerance properties of a multisensor switching strategy.

- The switching scheme is motivated by a control performance criterion and has a good performance in the absence of sensor failure.

- Closed-loop stability is guaranteed under a multiple failure scenario if a set of conditions on the parameters of the problem is satisfied. These conditions can be tested off line.

- Faulty sensor detection and isolation is achieved “implicitly” by guaranteeing that the switching cost avoids selecting faulty sensors. This feature departs from other available techniques.

- The on-line implementation of the scheme is simple, requiring only to compare cost values.

- Future work includes relaxing the failure scenario and the conditions for healthy sensor selection.
Martinez J., Seron M. and De-Dona J.  
“Fault-Tolerant Switching Scheme with Multiple Sensor-Controller Pairs”.  
IFAC World Congress (Accepted) - Seoul, Korea. July, 2008.

Seron M., Zhuo X., De-Dona J. and Martinez J.  
“Multi-sensor switching control strategy with fault tolerance guarantees”.  

Seron M., Zhuo X., De-Dona J. and Martinez J.  
“Fault Tolerant Multi-Sensor Switching Control Strategy”.  

Martinez J., Zhuo X., De-Dona J. and Seron M.  
“Multi-sensor switching strategy for automotive longitudinal control”.  
Thanks you for your attention!