A fault tolerant control scheme based on sets separation

F. Stoican and S. Olaru

SUPELEC Systems Sciences (E3S) - Automatic Control Department
{florin.stoican,sorin.olaru}@supelec.fr

March 25, 2010

GDR-MACS (Réunion GT S3: Sûreté-Surveillance-Supervision) – *March 25, 2011 Paris, France*

Outline

Outline

Fault tolerant control (FTC)

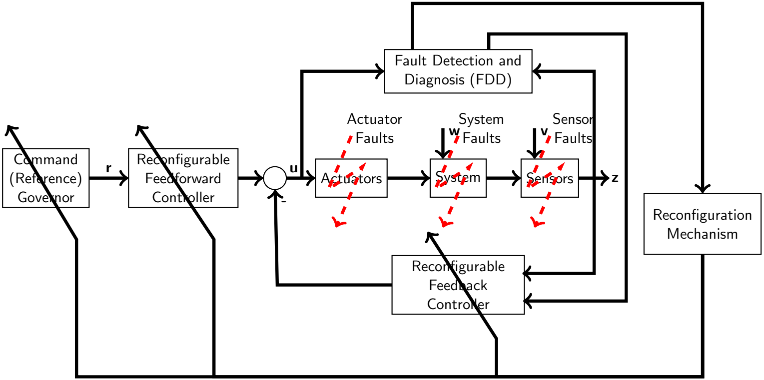
Goals

- fault detection and isolation (actuators, plant, sensors)
- control design and optimization
  - stability
  - constraints satisfaction
  - performance

Different approaches in FDI

- stochastic (Kalman filters, sensor fusion)
- set theoretic methods
- artificial intelligence

FTC – block scheme



FTC – set theoretical methods

Different approaches

- sets computed at each iteration (Planchon and Lunze [2008])
  - precise, by the consideration of current state information
  - exponential increase in complexity
- invariant sets (Seron et al. [2008], Olaru et al. [2010])
  - computed offline, online computations very simple ((real-time computational load))
  - allow discussions regarding the global stability of the system

Methodology

- off-line associate to a residual signal sets describing its healthy/faulty behavior
- test the inclusion of the residual to these sets at the runtime

Illustration of the methodology

For each fault f_i consider a residual signal r_i (Blanke et al. [2006]) which is sensible to the fault and is constructed using measurable information (state estimations, references, etc).

Assumptions:

- fault structure is known (generally abrupt faults are easier to handle)
- all exogenous signals are bounded

$$r_i = \begin{cases} r_i^H, & f_i \text{ inactive} \\ r_i^F, & f_i \text{ active} \end{cases}$$

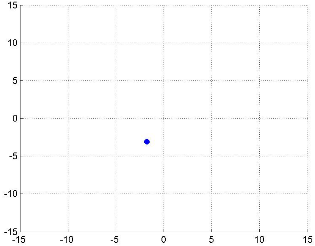
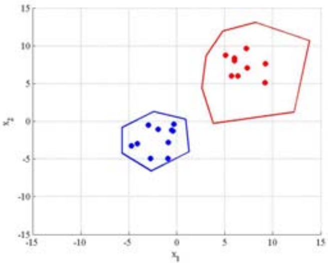


Illustration of the methodology

For each fault f_i consider a residual signal r_i (Blanke et al. [2006]) which is sensible to the fault and is constructed using measurable information (state estimations, references, etc).

Assumptions:

- fault structure is known (generally abrupt faults are easier to handle)
- all exogenous signals are bounded



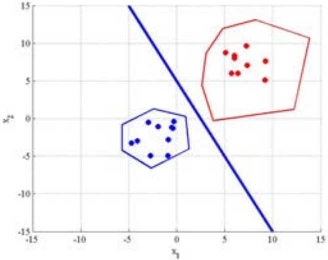
$$r_i = \begin{cases} r_i^H \in R_i^H, & f_i \text{ inactive} \\ r_i^F \in R_i^F, & f_i \text{ active} \end{cases}$$

Illustration of the methodology

For each fault f_i consider a residual signal r_i (Blanke et al. [2006]) which is sensible to the fault and is constructed using measurable information (state estimations, references, etc).

Assumptions:

- fault structure is known (generally abrupt faults are easier to handle)
- all exogenous signals are bounded



$$r_i = \begin{cases} r_i^H \in R_i^H, & f_i \text{ inactive} \\ r_i^F \in R_i^F, & f_i \text{ active} \end{cases}$$

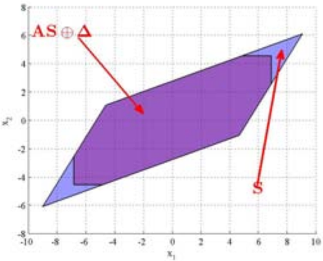
Fault detection apriori guaranteed iff:

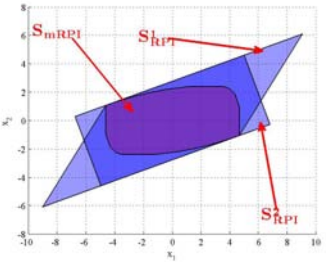
$$R_i^H \cap R_I^F = \emptyset$$

Invariance notions

Let there be a dynamic system defined by

$$x^+ = Ax + \delta, \quad \delta \in \Delta$$





Definition (RPI)

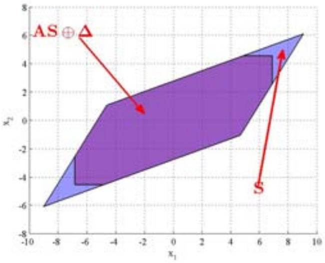
A set Ω is robust positively invariant (RPI) if and only if

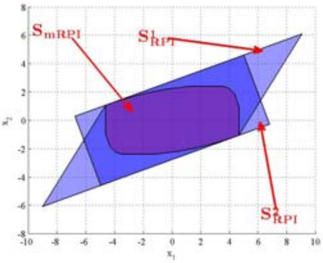
$$x \in \Omega \rightarrow x^+ \in \Omega$$

Invariance notions

Let there be a dynamic system defined by

$$x^{+} = Ax + \delta, \quad \delta \in \Delta$$





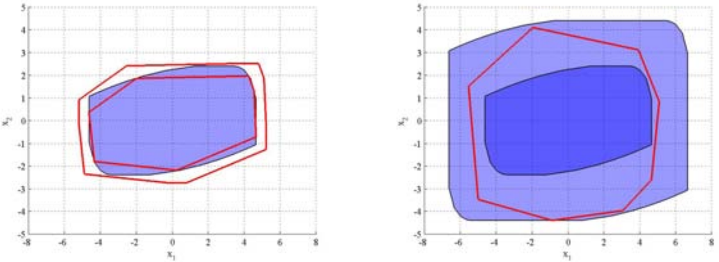
Definition (mRPI)

A set Ω is minimal robust positively invariant (mRPI) if it is contained in all RPI sets.

Invariance notions

Let there be a dynamic system defined by

$$x^+ = Ax + \delta, \quad \delta \in \Delta$$



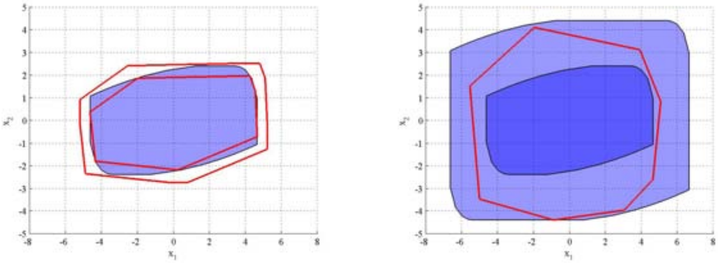
Definition (ϵ-approximations)

- ϵ-inner approximations: $\Phi \subseteq \Omega \subseteq \Phi \oplus \mathbb{B}^n_\infty(\epsilon)$
- ϵ-outer approximations: $\Omega \subseteq \Phi \subseteq \Omega \oplus \mathbb{B}^n_\infty(\epsilon)$

Invariance notions

Let there be a dynamic system defined by

$$x^+ = Ax + \delta, \quad \delta \in \Delta$$



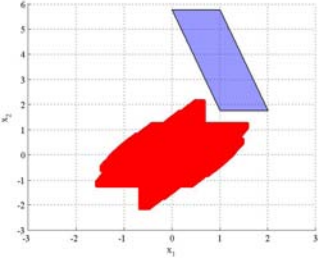
Definition (ϵ-approximations)

- ϵ-inner approximations: $\Phi \subseteq \Omega \subseteq \Phi \oplus \mathbb{B}^n_\infty(\epsilon)$
- ϵ-outer approximations: $\Omega \subseteq \Phi \subseteq \Omega \oplus \mathbb{B}^n_\infty(\epsilon)$

Set primitives

Families of sets:

- convex sets
  - ellipsoids
  - polyhedra
  - zonotopes
- non-convex sets
  - star-shaped sets



Polyhedral approximations of the mRPI set:

- ultimate bounds (Kofman et al. [2007])
- RPI ϵ-approximations of the mRPI set
  - inner approximations (Raković et al. [2005])
  - outer approximations (Olaru et al. [2010])

Ultimate bounds

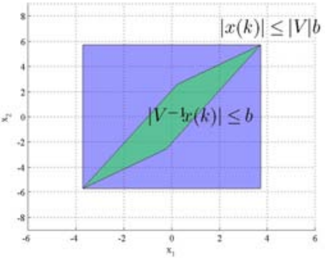
Theorem (Ultimate bounds – discrete case)

Consider the stable system $x^+ = Ax + Bu$. Let there be the Jordan decomposition $A = V\Lambda V^{-1}$ and assume that $\left|u(k)\right| \leq \bar{u}, \forall k \geq 0$. Then there exists $l(\epsilon)$ such that for all $k \geq l$:

$$\begin{aligned} |V^{-1}x(k)| &\leq (I - |\Lambda|)^{-1}|V^{-1}B|\bar{u} + \epsilon \\ |x(k)| &\leq |V|(I - |\Lambda|)^{-1}|V^{-1}B|\bar{u} + |V|\epsilon \end{aligned}$$

$$x(k+1) = Ax(k) + Bu(k)$$

where $\left|u(k)\right| \leq 1$



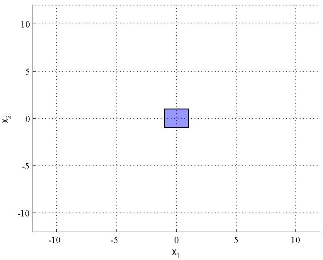
mRPI inner approximations

Note: An alternative formulation of a mRPI set can be given

$$\Omega = \bigoplus_{i=0}^{i=\infty} A^i \Delta$$

This permits the computation of a sequence of RPI inner approximations of the mRPI set

$$\Phi_{k+1} = A\Phi_k \oplus \Delta, \quad \Phi_0 = \{0\}$$



Theorem (Raković et al. [2005])

For any $\epsilon \geq 0$ exists $s \in \mathbb{N}^+$ such that the following relation is true

$$\Phi_s \subset \Omega \subset (1 - \alpha(s))^{-1} \Phi_s(\epsilon)$$

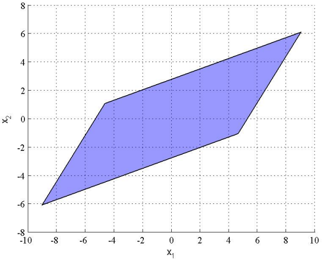
mRPI outer approximations

Note: An alternative formulation of a mRPI set can be given

$$\Omega = \bigoplus_{i=0}^{i=\infty} A^i \Delta$$

This permits the computation of a sequence of RPI outer approximations of the mRPI set

$$\Phi_{k+1} = A\Phi_k \oplus \Delta, \quad \Phi_0 = \Psi$$



Theorem (Olaru et al. [2010])

For any $\epsilon \geq 0$ exists $s \in \mathbb{N}^+$ such that the following relation is true

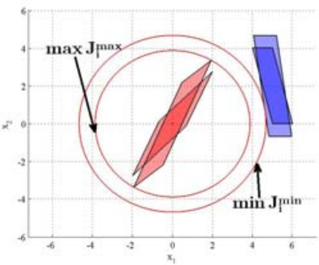
$$\Omega \subset \Phi_s \subset \Omega \oplus \mathbb{B}_p^n(\epsilon)$$

Set separation

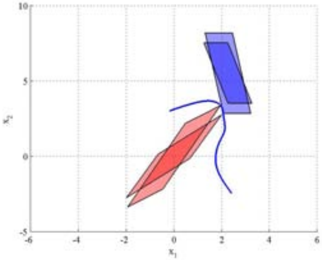
- implicit: there exists a function $J(*)$ such that

$$\max_i J(r_i^H) < \min_i J(r_i^F), \quad r_i^H \in R_i^H,\ r_i^F \in R_i^F$$

quadratic function



barrier function

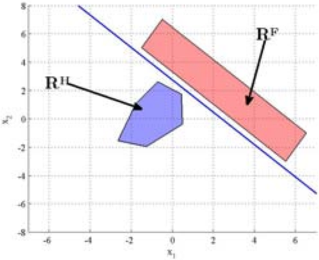


Set separation

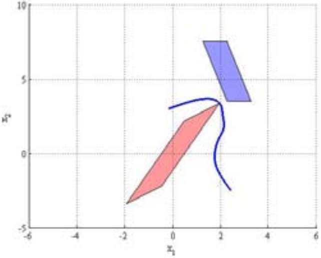
- explicit: there exists a function $J_i(*)$ for each residual r_i such that

$$J_i(r_i^H) < J_i(r_i^F), \quad r_i^H \in R_i^H, \; r_i^F \in R_i^F$$

separating hyperplane

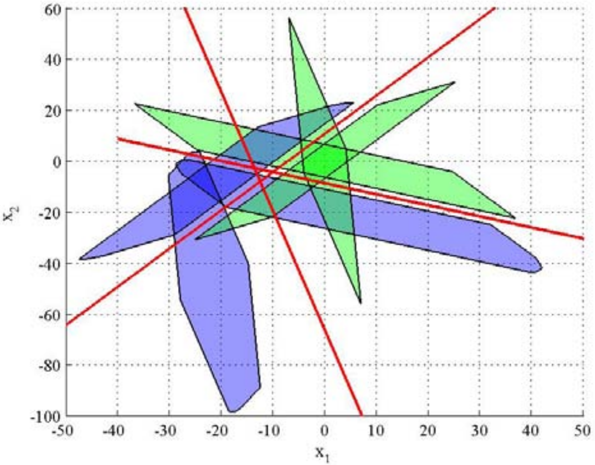


barrier function



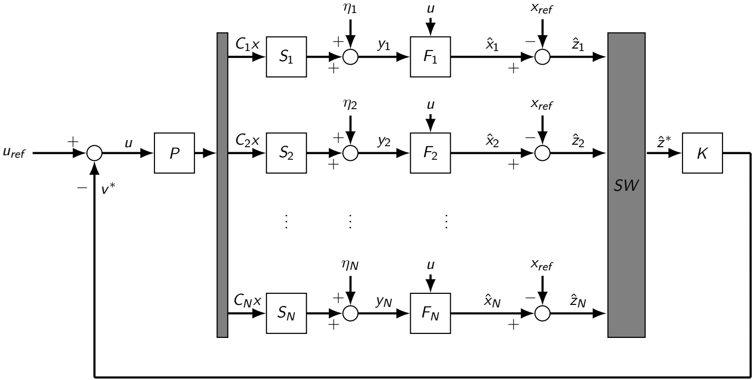
Set separation

Explicit separation is sometimes the only solution:



Outline

Multisensor scheme



Assumptions

- A is stabilizable and pair (A, B) is controllable
- pairs (A, C_i) are detectable for $i = 1, \dots, N$
- additive disturbances and the measurements perturbations are considered to be delimited by bounded polyhedral sets

Modeling equations

- plant dynamics

$$x^+ = Ax + Bu + Ew$$

- reference signal

$$x^+_{ref} = Ax_{ref} + Bu_{ref}$$

- plant tracking error

$$z^+ = x - x_{ref} = Az + B\underbrace{(u - u_{ref})}_{v} + Ew$$

- estimations of the state

$$\hat{x}_i^+ = (A - L_i C_i)\,\hat{x}_i + Bu + L_i\,(y_i - C_i\hat{x}_i)$$

- estimations of the tracking error

$$\hat{z}_i = \hat{x}_i - x_{ref}$$

Switching criteria

At every step a pair sensor-estimator is selected to compute the command action s.t. the following cost function is minimized

$$J(\hat{z}, v) = (\hat{z})' Q\hat{z} + (A\hat{z} + Bv)' P (A\hat{z} + Bv)$$

for the tracking error estimation $\hat{z} \in \{\hat{z}_i\}_{i\in\mathcal{I}}$ with $\mathcal{I} = \{1 \ldots N\}$.
The control action is then defined as

$$u^* = u_{ref} - K\hat{z}^*$$

with

$$\hat{z}^* = \arg\min_{\hat{z}} \left\{J(\hat{z}, v);\ \hat{z} \in \{\hat{z}_i\}_{i\in\mathcal{I}}, v \in \mathbb{R}^m\right\}$$

Outline

Fault scenarios

- total output outages

$$y_i = C_i x + \eta_i \xrightarrow{\text{FAULT}} y_i = 0 \cdot x + \eta_i^F$$
$$y_i = C_i x + \eta_i \xleftarrow{\text{RECOVERY}} y_i = 0 \cdot x + \eta_i^F$$

- more complex fault scenarios (a signature matrix for each type of fault)

$$y_i = N_i \left[C_i x + \eta_i \right] + \left[I - N_i \right] \eta_i^F$$

Auxiliary sets

- N_i, N_i^F, W – bounding boxes for sensor and plant noises
- X_{ref} – set for the reference signal
- $\tilde{S}_i$ – invariant set for the state estimation error
- S_z – invariant set for the plant tracking error

State estimation error:

$$\tilde{x}_i^+ = x^+ - \hat{x}_i^+ = (A - L_i C_i)\,\tilde{x}_i + \begin{bmatrix} E & -L_i \end{bmatrix} \begin{bmatrix} w \\ \eta_i \end{bmatrix}$$

Plant tracking error:

$$z^+ = (A - BK)\,z + \begin{bmatrix} E & BK \end{bmatrix} \begin{bmatrix} w \\ \tilde{x}_l \end{bmatrix}$$

Auxiliary sets

- N_i, N_i^F, W – bounding boxes for sensor and plant noises
- X_{ref} – set for the reference signal
- $\tilde{S}_i$ – invariant set for the state estimation error
- S_z – invariant set for the plant tracking error

State estimation error:

$$\tilde{x}_i^+ = x^+ - \hat{x}_i^+ = (A - L_i C_i)\,\tilde{x}_i + \begin{bmatrix} E & -L_i \end{bmatrix} \begin{bmatrix} w \\ \eta_i \end{bmatrix}$$

Plant tracking error:

$$z^+ = (A - BK)\,z + \begin{bmatrix} E & BK \end{bmatrix} \begin{bmatrix} w \\ \tilde{x}_l \end{bmatrix}$$

Auxiliary sets

- N_i, N_i^F, W – bounding boxes for sensor and plant noises
- X_{ref} – set for the reference signal
- $\tilde{S}_i$ – invariant set for the state estimation error
- S_z – invariant set for the plant tracking error

State estimation error:

$$\tilde{x}_i^+ = x^+ - \hat{x}_i^+ = (A - L_i C_i)\,\tilde{x}_i + \begin{bmatrix} E & -L_i \end{bmatrix} \begin{bmatrix} w \\ \eta_i \end{bmatrix}$$

Plant tracking error:

$$z^+ = (A - BK)\,z + \begin{bmatrix} E & BK \end{bmatrix} \begin{bmatrix} w \\ \tilde{x}_l \end{bmatrix}$$

Residual signals

The residual signal associated to the i^{th} sensor can be defined as:

$$r_i = y_i - C_i x_{ref}$$

Reminder:

- $z = x - x_{ref}$
- $y_i = \begin{cases} C_i x + \eta_i, \\ \eta_i^F \end{cases}$

Residual values for sensor i:

- healthy case:

$$r_i^H = C_i z + \eta_i$$

- faulty case:

$$r_i^F = -C_i x_{ref} + \eta_i^F$$

Residual signals

The residual signal associated to the i^{th} sensor can be defined as:

$$r_i = y_i - C_i x_{ref}$$

Reminder:

- $z = x - x_{ref}$
- $y_i = \begin{cases} C_i x + \eta_i, \\ \eta_i^F \end{cases}$

Residual values for sensor i:

- healthy case:

$$R_i^H = C_i S_z \oplus N_i$$

- faulty case:

$$R_i^F = -C_i X_{ref} \oplus N_i^F$$

Sensor partitioning

Using the previous results we can partition the sensors after their

- healthy functioning ($y_i = C_i x + \eta_i$)
- estimation error ($\tilde{x}_i \in \tilde{S}_i$)

into

- $\mathcal{I}_H$: healthy sensors

$$\mathcal{I}_H = \left\{ i \in \mathcal{I}_H^- : r_i \in R_i^H \right\} \cup \left\{ i \in \mathcal{I}_R^- : \tilde{x}_i \in \tilde{S}_i,\ r_i \in R_i^H \right\}$$

- $\mathcal{I}_R$: under recovery sensors

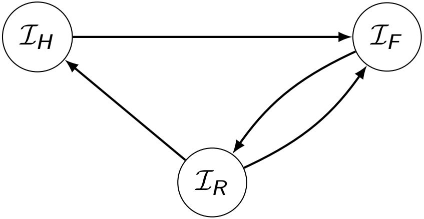
$$\mathcal{I}_F = \left\{ i \in \mathcal{I} : r_i \notin R_i^H \right\}$$

- $\mathcal{I}_F$: faulty sensors

$$\mathcal{I}_R = \mathcal{I} \setminus (\mathcal{I}_H \cup \mathcal{I}_F)$$

Sensor partitioning

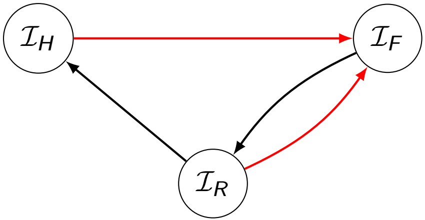
$$I = I_H \cup I_F \cup I_R$$



	$\mathcal{I}_H$	$\mathcal{I}_F$	$\mathcal{I}_R$
$\tilde{x}_i \in \tilde{S}_i$	✓	–	X
$r_i \in R_i^H$	✓	X	✓

Sensor partitioning

$$I = I_H \cup I_F \cup I_R$$

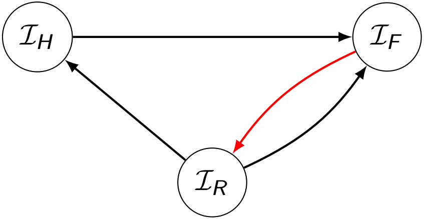


	$\mathcal{I}_H$	$\mathcal{I}_F$	$\mathcal{I}_R$
$\tilde{x}_i \in \tilde{S}_i$	✓	–	X
$r_i \in R_i^H$	✓ ⟶	X	⟵ ✓

$$r_i \in R_i^H \longrightarrow r_i \notin R_i^H$$

Sensor partitioning

$$I = I_H \cup I_F \cup I_R$$

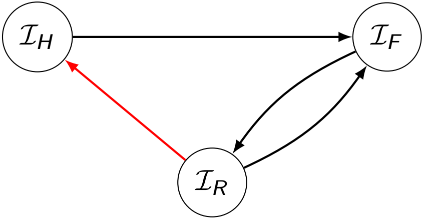


	$\mathcal{I}_H$	$\mathcal{I}_F$	$\mathcal{I}_R$
$\tilde{x}_i \in \tilde{S}_i$	✓	–	X
$r_i \in R_i^H$	✓	X ⟶	✓

$$r_i \notin R_i^H \longrightarrow r_i \in R_i^H$$

Sensor partitioning

$$I = I_H \cup I_F \cup I_R$$



	$\mathcal{I}_H$	$\mathcal{I}_F$	$\mathcal{I}_R$
$\tilde{x}_i \in \tilde{S}_i$	✓	–	X
$r_i \in R_i^H$	✓	X	✓

$$\tilde{x}_i \notin \tilde{S}_i \longrightarrow \tilde{x}_i \in \tilde{S}_i$$

FDI mechanism

We can now recast the FDI elements as follows:

- fault detection and isolation: $\mathcal{I}_H \to \mathcal{I}_F$ we need to test only that

$$r_i \in R_i^H / R_i^F$$

- sensor recovery: $\mathcal{I}_R \to \mathcal{I}_H$

$$\left(\tilde{x}_i \in \tilde{S}_i,\ r_i \in R_i^H\right) \longrightarrow (\mathcal{I}_R \to \mathcal{I}_H)$$

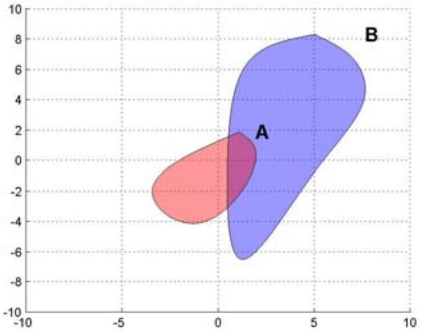
$\tilde{x}_i = x - \hat{x}_i$ is not measurable

Solution: construct a bound $Z^i_{\mathcal{I}_H}$ that contains $\tilde{x}_i$ and use

- necessary conditions
- sufficient conditions

to verify inclusion $\tilde{x}_i \in \tilde{S}_i$.

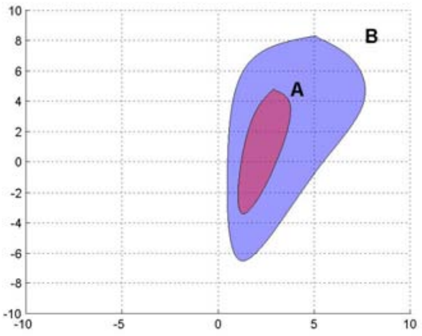
Necessary and sufficient conditions



Let $\mathcal{A}$ and $\mathcal{B}$ be two sets, then

- $\alpha \in \mathcal{A}$, a necessary condition for $\alpha \in \mathcal{B}$ is $\mathcal{A} \cap \mathcal{B} \neq \emptyset$
- $\alpha \in \mathcal{A}$, a sufficient condition for $\alpha \in \mathcal{B}$ is $\mathcal{A} \subseteq \mathcal{B}$

Necessary and sufficient conditions

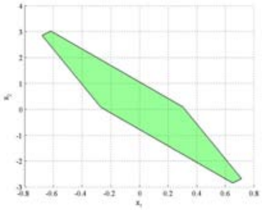


Let $\mathcal{A}$ and $\mathcal{B}$ be two sets, then

- $\alpha \in \mathcal{A}$, a necessary condition for $\alpha \in \mathcal{B}$ is $\mathcal{A} \cap \mathcal{B} \neq \emptyset$
- $\alpha \in \mathcal{A}$, a sufficient condition for $\alpha \in \mathcal{B}$ is $\mathcal{A} \subseteq \mathcal{B}$

Sensor recovery – I

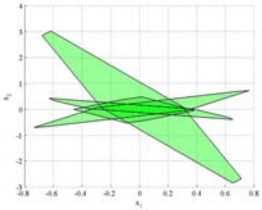
$$z = \underbrace{\hat{z}_l}_{\text{measured value}} + \underbrace{\tilde{x}_l}_{\text{uncertainities}}$$



details are to be found in Olaru et al. [2009]

Sensor recovery – I

$$z = \underbrace{\hat{z}_l}_{\text{measured value}} + \underbrace{\tilde{x}_l}_{\text{uncertainities}}$$



$$z \in \bigcap_{l \in I_H} \left[\left\{ \hat{z}_l \right\} \oplus \tilde{S}_l \right]$$

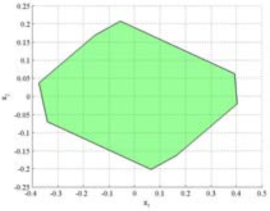
$$\hat{z}_j + \tilde{x}_j \in \bigcap_{l \in I_H} \left[\left\{ \hat{z}_l \right\} \oplus \tilde{S}_l \right]$$

$$\tilde{x}_j \in \underbrace{\left\{ -\hat{z}_j \right\} \oplus \bigcap_{l \in I_H} \left[\left\{ \hat{z}_l \right\} \oplus \tilde{S}_l \right]}_{Z^i_{\mathcal{I}_H}}$$

details are to be found in Olaru et al. [2009]

Sensor recovery – I

$$z = \underbrace{\hat{z}_l}_{\text{measured value}} + \underbrace{\tilde{x}_l}_{\text{uncertainities}}$$



$$z \in \bigcap_{l \in I_H} \left[\{\hat{z}_l\} \oplus \tilde{S}_l \right]$$

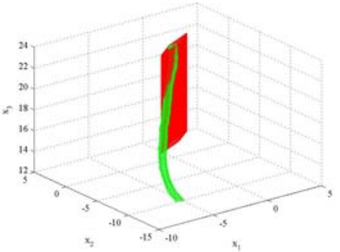
$$\hat{z}_j + \tilde{x}_j \in \bigcap_{l \in I_H} \left[\{\hat{z}_l\} \oplus \tilde{S}_l \right]$$

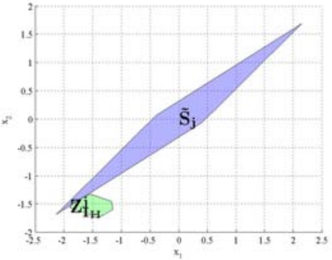
$$\tilde{x}_j \in \underbrace{\{-\hat{z}_j\} \oplus \bigcap_{l \in I_H} \left[\{\hat{z}_l\} \oplus \tilde{S}_l \right]}_{Z^i_{\mathcal{I}_H}}$$

details are to be found in Olaru et al. [2009]

Sensor recovery – II

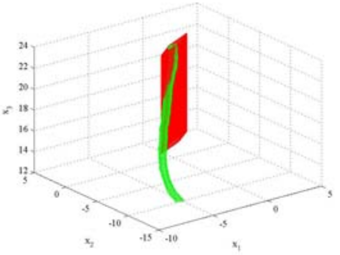
Necessary condition: $\tilde{S}_j \cap Z^i_{\mathcal{I}_H} \neq \emptyset$
Sufficient condition: $\tilde{S}_j \supseteq Z^i_{\mathcal{I}_H}$

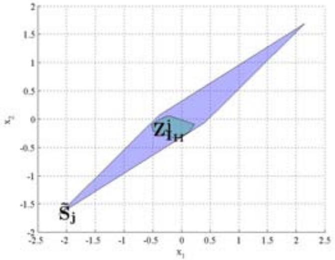




Sensor recovery – II

Necessary condition: $\tilde{S}_j \cap Z^i_{\mathcal{I}_H} \neq \emptyset$
Sufficient condition: $\tilde{S}_j \supseteq Z^i_{\mathcal{I}_H}$





Sensor recovery - III

Obstacles against recovery acknowledgment:

- significant inclusion time (the time it takes for $\tilde{x}_i$ to converge to $\tilde{S}_i$)
  - wait for the convergence to take place
  - change the estimator dynamics (Stoican et al. [2010b])
  - provide an artificial estimation that "keeps" $\tilde{x}_i$ close to $\tilde{S}_i$ (Stoican et al. [2010c])
- validation of inclusion $\tilde{x}_i \in \tilde{S}_i$
  - wait for test $\tilde{S}_j \supseteq Z^i_{\mathcal{I}_H}$ to be validated
  - for a given bound of the estimation error, $Z^i_{\mathcal{I}_H}$, find

$$\tau_j = \min\ \theta$$

$$\text{subj. to}: \begin{cases} S_0 = Z^i_{\mathcal{I}_H}, S_\theta \subseteq \tilde{S}_i, \\ S_k = (A - L_j C_j) S_{k-1} \oplus EW \oplus (-L_j) N_j, \ \forall k > 0 \end{cases}$$

then if healthy functioning ($r_i \in R_i^H$) is true for τ_j time instants, the sensor is recovered (Stoican et al. [2011]).

Outline

Introduction

Multisensor scheme

Fault detection and isolation

Reconfiguration of the control action

Analysis of the FTC scheme

Illustrative example

Conclusions

Reconfiguration of the control action

In our case, as long as $\mathcal{I}_H \neq \emptyset$ we can reformulate the control action as:

$$u^* = u_{ref} - K\hat{z}^*$$

with

$$\hat{z}^* = \arg\min_{\hat{z}} \left\{ J(\hat{z}, v);\ \hat{z} \in \{\hat{z}_i\}_{i \in \mathcal{I}_H}, v \in \mathbb{R}^m \right\}$$

Outline

Introduction

Multisensor scheme

Fault detection and isolation

Reconfiguration of the control action

Analysis of the FTC scheme
- Controlled invariance
- Reference governor

Illustrative example

Conclusions

Analysis of the FTC scheme

Usually the FDI mechanism is designed without looking at the "big picture":

$$\text{FDI condition:} \quad \underbrace{\left(C_i\ S_z\ \oplus N_i\right)}_{R_i^H} \cap \underbrace{\left(-C_i\ X_{ref}\ \oplus N_i^F\right)}_{R_i^F} = \emptyset$$

There are two main components of the scheme that influence the viability of the FTC scheme:

- the design of the control action
- the reference signals

Strategies:

- for a fixed gain control type of law, optimize after matrix K (Stoican et al. [2010a])
- find the feasible domain of references and use it in a reference governor (Stoican et al. [2010d])

Analysis of the FTC scheme

Usually the FDI mechanism is designed without looking at the "big picture":

$$\text{FDI condition:} \quad \underbrace{\left(C_i \, S_z \, \oplus N_i\right)}_{R_i^H} \cap \underbrace{\left(-C_i \, X_{ref} \, \oplus N_i^F\right)}_{R_i^F} = \emptyset$$

There are two main components of the scheme that influence the viability of the FTC scheme:

- the design of the control action
- the reference signals

Strategies:

- for a fixed gain control type of law, optimize after matrix K (Stoican et al. [2010a])
- find the feasible domain of references and use it in a reference governor (Stoican et al. [2010d])

Analysis of the FTC scheme

Usually the FDI mechanism is designed without looking at the "big picture":

$$\text{FDI condition:} \quad \underbrace{\left(C_i\ S_z\ \oplus N_i\right)}_{R_i^H} \cap \underbrace{\left(-C_i\ X_{ref}\ \oplus N_i^F\right)}_{R_i^F} = \emptyset$$

There are two main components of the scheme that influence the viability of the FTC scheme:

- the design of the control action
- the reference signals

Strategies:

- for a fixed gain control type of law, optimize after matrix K (Stoican et al. [2010a])
- find the feasible domain of references and use it in a reference governor (Stoican et al. [2010d])

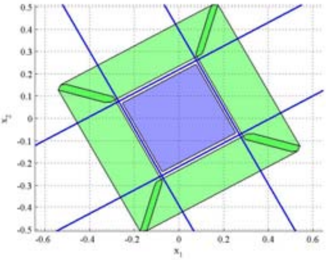
Controlled invariance

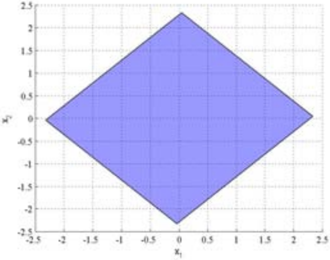
If FDI condition

$$R_i^H \cap R_i^F = \emptyset$$

holds, then there exists a separating hyperplane (c_i^T, p_i) such that:

$$c_i^T(C_i z + \eta_i) < p_i < c_i^T(-C_i x_{ref} + \eta_i^F)$$





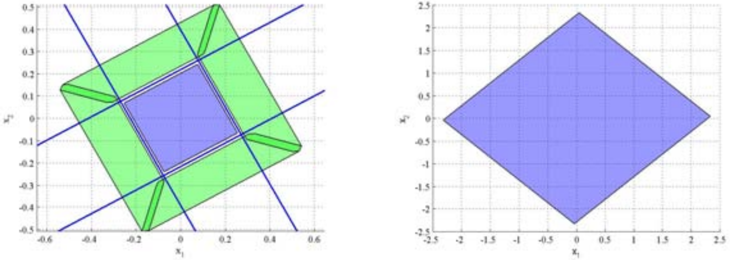
Controlled invariance

If FDI condition

$$R_i^H \cap R_i^F = \emptyset$$

holds, then there exists a separating hyperplane (c_i^T, p_i) such that:

$$c_i^T C_i z < p_i - \max_{\eta_i \in N_i} c_i^T \eta_i$$



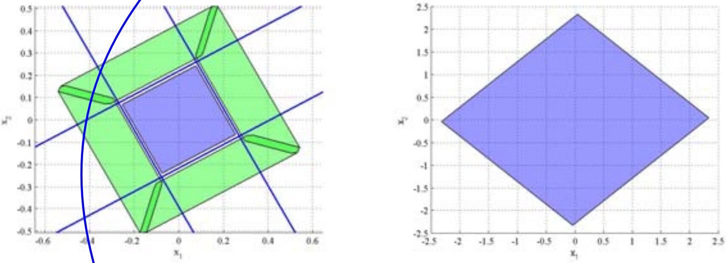
Controlled invariance

If FDI condition

$$R_i^H \cap R_i^F = \emptyset$$

holds, then there exists a separating hyperplane (c_i^T, p_i) such that:

$$c_i^T C_i z < p_i - \max_{\eta_i \in N_i} c_i^T \eta_i$$



$$S_z = \left\{ z : c_i^T C_i z < p_i - \max_{\eta_i \in N_i} c_i^T \eta_i, \quad i \in \mathcal{I} \right\}$$

Testing the invariance of a set

We recall here a result first presented in Bitsoris [1988]:

The set

$$R(F,\theta) = \{x \in \mathbb{R}^n : Fx \leq \theta\}$$

with $F \in \mathbb{R}^{s\times n}$ and $\theta \in \mathbb{R}^s$ is a *positively invariant* set for system

$$x^+ = Ax$$

if and only if there exists a elementwise positive matrix $H \in \mathbb{R}^{s\times s}$ and an $0 \leq \epsilon \leq 1$ such that

$$\begin{aligned} HF &= FA \\ H\theta &\leq \epsilon\theta \end{aligned}$$

If $\epsilon \leq 1$ in the previous results we say that the set is *invariant*.

Search over K – robust invariance

Instead of computing the set invariant for a given dynamics we try to determine the dynamics that make a given set invariant:

$$S_z = \left\{ z : \; c_i^T C_i z < p_i - \max_{\eta_i \in N_i} c_i^T \eta_i, \quad i \in \mathcal{I} \right\}$$

$$z^+ = (A - B\ K\ )z + \begin{bmatrix} E & B\ K \end{bmatrix} \begin{bmatrix} w \\ \tilde{x}_l \end{bmatrix}$$

$$\epsilon^* = \max_{l} \min_{\substack{K,H,\epsilon \\ \epsilon \geq 0 \\ HF_z = F_z(A-BK) \\ H\theta_z + F_z B_{z,l}\delta_{z,l} \leq \epsilon\theta_z \\ \delta_{z,l} \in \Delta_{z,l}}} \epsilon$$

if $\epsilon^* \leq 1$ the solution is feasible

Search over K – robust invariance

Instead of computing the set invariant for a given dynamics we try to determine the dynamics that make a given set invariant:

$$S_z = \left\{ z : \; c_i^T C_i z < p_i - \max_{\eta_i \in N_i} c_i^T \eta_i, \quad i \in \mathcal{I} \right\}$$

$$z^+ = (A - B\, K\,)z + \begin{bmatrix} E & B\, K \end{bmatrix} \begin{bmatrix} w \\ \tilde{x}_l \end{bmatrix}$$

$$\epsilon^* = \max_{l} \min_{\substack{K,H,\epsilon \\ \epsilon \geq 0 \\ HF_z = F_z(A-BK) \\ H\theta_z + F_z B_{z,l}\delta_{z,l} \leq \epsilon\theta_z \\ \delta_{z,l} \in \Delta_{z,l}}} \epsilon$$

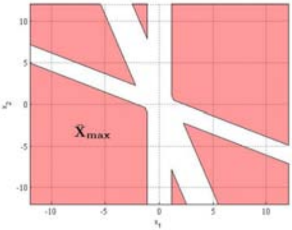
if $\epsilon^* \leq 1$ the solution is feasible

Reference governor

$$X_{ref} = \left\{ x_{ref} : \ R_i^H \cap R_i^F = \emptyset, \ i \in \mathcal{I} \right\}$$

Reminder:

$$\begin{cases} R_i^H = C_i S_z \oplus N_i \\ R_i^F = -C_i X_{ref} \oplus N_i^F \end{cases}$$



Reference governor

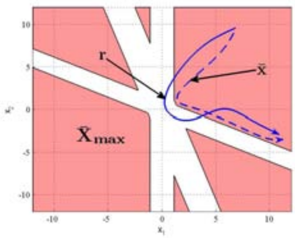
$$X_{ref} = \left\{ x_{ref} : \ R_i^H \cap R_i^F = \emptyset, \ i \in \mathcal{I} \right\}$$

Reference governor

$$(x_{ref}^*, u_{ref}^*) = \arg\min \sum \left(\left\| r - x_{ref} \right\|_Q + \left\| u_{ref} \right\|_R \right)$$

subject to

$$\begin{aligned} x_{ref} &\in X_{ref} \\ x_{ref}^+ &= Ax_{ref} + Bu_{ref} \end{aligned}$$



Reference governor

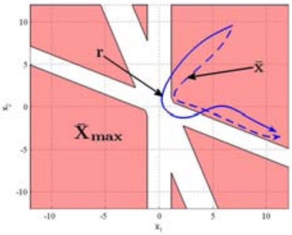
$$X_{ref} = \left\{ x_{ref} : \; R_i^H \cap R_i^F = \emptyset, \; i \in \mathcal{I} \right\}$$

Reference governor

$$(x^*_{ref}, u^*_{ref}) = \arg\min \sum \left(\left\| r - x_{ref} \right\|_Q + \left\| u_{ref} \right\|_R \right)$$

subject to

$$\begin{aligned} x_{ref} &\in X_{ref} \\ x^+_{ref} &= Ax_{ref} + Bu_{ref} \end{aligned}$$

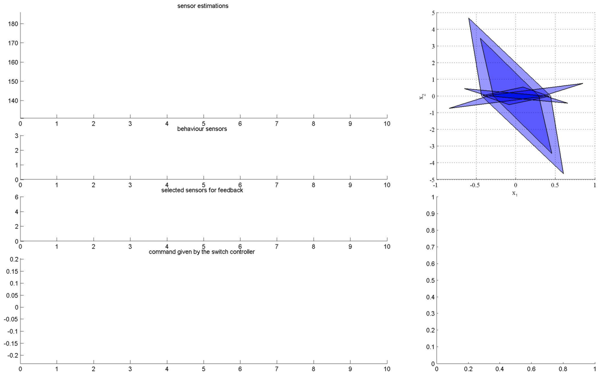


As in Olaru et al. [2009]an evaluation $z \in Z_{\mathcal{H}}$ of the current tracking error is computed. This permits to write

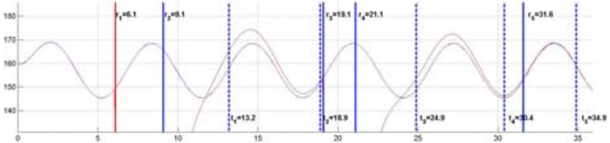
$$C_i \left(\oplus S_z \cap Z_{\mathcal{H},pred} \right) \oplus N_i \cap -C_i \{ x_{ref} \} \oplus N_i^F = \emptyset, \; \forall i \in I$$

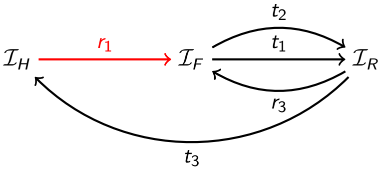
Outline

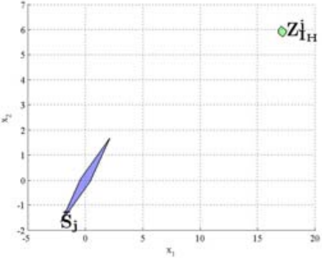
Example – FTC simulation



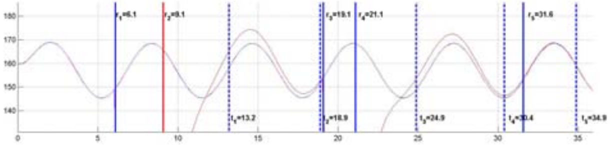
Example – Sensor recovery

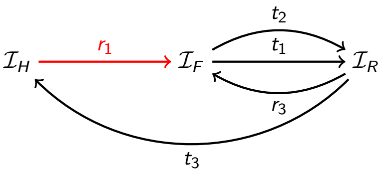


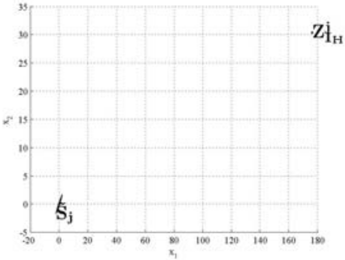




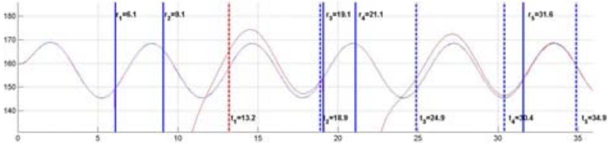
Example – Sensor recovery

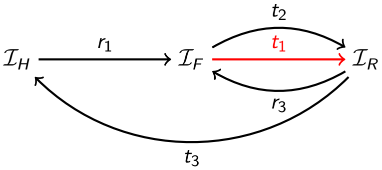


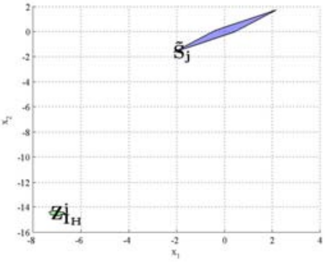




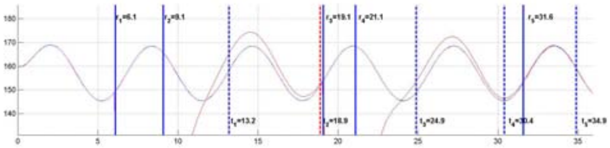
Example – Sensor recovery

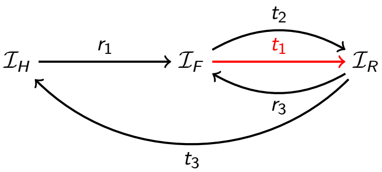


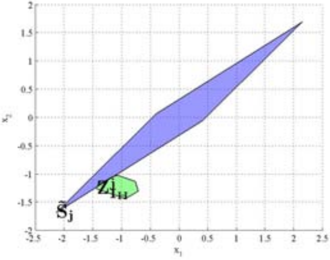




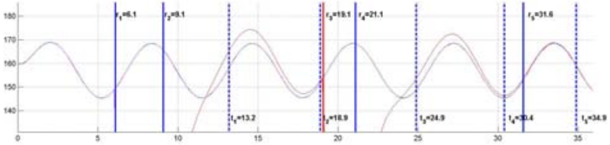
Example – Sensor recovery

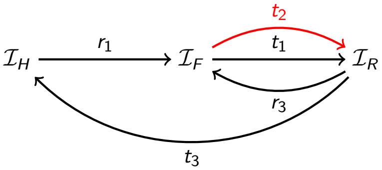


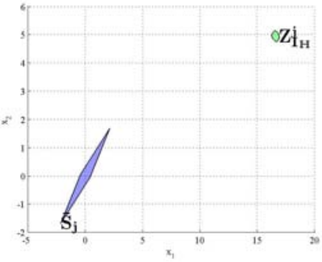




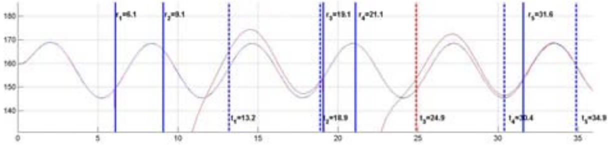
Example – Sensor recovery

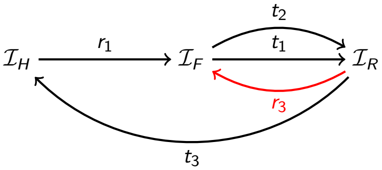


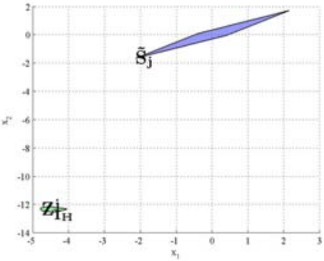




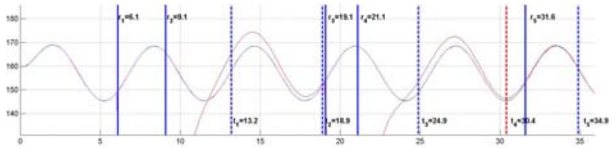
Example – Sensor recovery

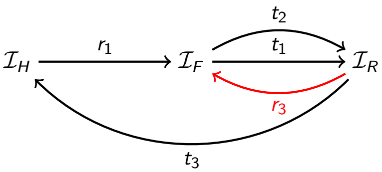


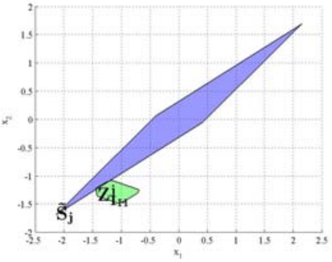




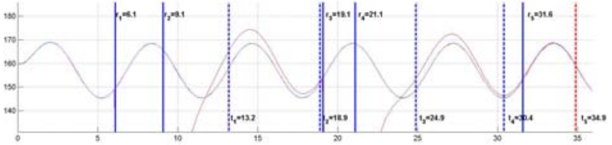
Example – Sensor recovery

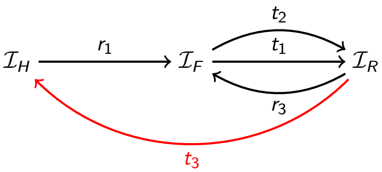


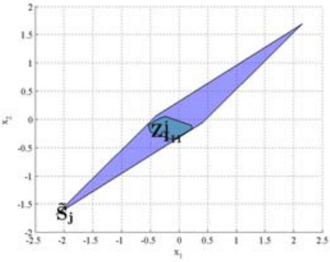




Example – Sensor recovery



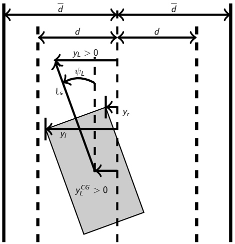




Practical applications

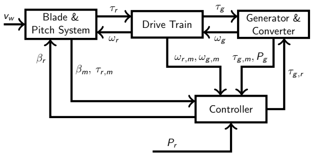
vehicle lane dynamics (Minoiu Enache et al.)

- corrective mechanism
- faults in sensors
  - vision algorithms
  - GPS RTK



windturbine benchmark (Odgaard et al. [2009])

- strongly nonlinear
- faults in all components



Outline

Conclusions

- invariant sets offer a robust approach
- sensor fault scenario can be arbitrary chosen
- a global view in considering the effects of the FDI mechanism
- extensions to MPC

References I

*Bibliography

George Bitsoris. On the positive invariance of polyhedral sets for discrete-time systems. *Systems & Control Letters*, 11(3):243–248, 1988.

M. Blanke, M. Kinnaert, J. Lunze, and M. Staroswiecki. *Diagnosis and fault-tolerant control*. Springer, 2006.

Ernesto Kofman, Hernan Haimovich, and María M. Seron. A systematic method to obtain ultimate bounds for perturbed systems. *International Journal of Control*, 80(2):167–178, 2007.

Nicoleta Minoiu Enache, Said Mammar, Sebastien Glaser, and Benoit Lusetti. Driver assistance system for lane departure avoidance by steering and differential braking. In *6th IFAC Symposium Advances in Automotive Control, 12 - 14 July, Munich, Germany, 2010*.

P.F. Odgaard, J. Stoustrup, and M. Kinnaert. Fault Tolerant Control of Wind Turbines–a benchmark model. In *Proc. of the 7th IFAC Symp. on Fault Detection, Supervision and Safety of Technical Processes*, pages 155–160, Barcelona, Spain, 30 June-3 July 2009.

Sorin Olaru, Florin Stoican, José A. De Doná, and María M. Seron. Necessary and sufficient conditions for sensor recovery in a multisensor control scheme. In *Proc. of the 7th IFAC Symp. on Fault Detection, Supervision and Safety of Technical Processes*, pages 977–982, Barcelona, Spain, 30 June-3 July 2009.

Sorin Olaru, José A. De Doná, María M. Seron, and Florin Stoican. Positive invariant sets for fault tolerant multisensor control schemes. *International Journal of Control*, 83(12):2622–2640, 2010.

P. Planchon and J. Lunze. Diagnosis of linear systems with structured uncertainties based on guaranteed state observation. *International Journal of Control Automation and Systems*, 6(3):306–319, June 2008.

Sasa V. Raković, Eric C. Kerrigan, Koustas I. Kouramas, and David Q. Mayne. Invariant approximations of the minimal robust positively invariant set. *IEEE Transactions on Automatic Control*, 50(3): 406–410, 2005.

María M. Seron, Xiang W. Zhuo, José A. De Doná, and J.J. Martinez. Multisensor switching control strategy with fault tolerance guarantees. *Automatica*, 44(1):88–97, 2008. ISSN 0005-1098.

References II

Florin Stoican, Sorin Olaru, and George Bitsoris. A fault detection scheme based on controlled invariant sets for multisensor systems. In *Proceedings of the 2010 Conference on Control and Fault Tolerant Systems*, pages 468–473, Nice, France, 6-8 October 2010a.

Florin Stoican, Sorin Olaru, José A. De Doná, and María M. Seron. Improvements in the sensor recovery mechanism for a multisensor control scheme. In *Proceedings of the 29th American Control Conference*, pages 4052–4057, Baltimore, Maryland, USA, 30 June-2 July 2010b.

Florin Stoican, Sorin Olaru, María M. Seron, and José A. De Doná. A fault tolerant control scheme based on sensor switching and dwell time. In *Proceedings of the 49th IEEE Conference on Decision and Control*, Atlanta, Georgia, USA, 15-17 December 2010c.

Florin Stoican, Sorin Olaru, María M. Seron, and José A. De Doná. Reference governor for tracking with fault detection capabilities. In *Proceedings of the 2010 Conference on Control and Fault Tolerant Systems*, pages 546–551, Nice, France, 6-8 October 2010d.

Florin Stoican, Sorin Olaru, María M. Seron, and José A. De Doná. Recovery techniques. available upon request, 2011.

Thank you!

Questions ?