FM as a Controller

peter.i.robinson@nasa.gov

NASA Ames Research Center
## Introduction

- **Acknowledgements**
- Fault Management (FM) as Controller
- Feedback Control Timeline
- AI Methods–Timeline
- Fault Management Timeline
- Assertion
- Modern Control Theory FM DRDs
- Conclusions
- References
Acknowledgements

• FM Conference
  – Lorraine Fesq, John Day

• NASA Ames Line Management
  – Dr. Ann Patterson-Hine, Dr. Eric Barszcz

• NASA Marshall SLS FM
  – Stacy Cook, Jon Patterson, Dr. Stephen Johnson

• NASA ARC/JSC HA/AMO Autonomy/FM
  – Dr. Mark Schwabacher, Dr. Jeremy Frank
Introduction

• Acknowledgements

• Fault Management (FM) as Controller

• Feedback Control Timeline

• AI Methods–Timeline

• Fault Management Timeline

• Assertion

• Modern Control Theory FM DRDs

• Conclusions

• References
Fault Management (FM) as Controller

- Two loops – one nominal, one FDIR (FM).
- View FM as a form of feedback control which complements nominal control.
- Leverage methodology of modern control theory.
Feedback Control - Definitions

• Cybernetics: “The science of communication and control in the animal and in the machine.” [Weiner 48]

• “Feedback control is the basic mechanism by which systems, whether mechanical, electrical, or biological, maintain their equilibrium or homeostasis. “[Lewis 1992]

• “Feedback control may be defined as the use of difference signals, determined by comparing the actual values of system variables to their desired values, as a means of controlling a system. Since the system output is used to regulate its input, such a device is said to be a closed-loop control system.” “[Lewis 1992]
Benefits

• Provides a common language for FM practitioners to communicate with Nominal Control practitioners
• Provides a framework to define FM Requirements and Data Requirement Definitions
• Provides a framework to define formal estimates of FM domain complexity to support model development and accreditation costing. - TBD
• Provides a framework to help determine FM FP/FN requirements through controller properties of stability, observability and stability - TBD
Introduction

• Acknowledgements
• Fault Management (FM) as Controller
  • Feedback Control Timeline
• AI Methods—Timeline
• Fault Management Timeline
• Assertion
• Modern Control Theory FM DRDs
• Conclusions
• References
Feedback Control Timeline

- **300 BC – 1200 AD**
  - 3rd Century BC Ktesibios – Water Clock

- **1600 AD – 1875 AD Industrial Revolution – control of machines**
  - 1620 Cornelius Drebbel – Temperature Regulator
  - 1780 James Watt - Governor – Pressure Regulator
  - Mathematics (Least Squares, DiffEq, Linear Algebra, Optimality)

- **1910 AD – 1945 AD – Frequency Domain Methods - Classic Control Theory**
  - 1922 Minorsky *Proportional-integral-derivative (PID) controller.*
  - 1936 George Philbrick – Analog Computer for Process Control

- **1957 AD – present – Time Domain Methods – Modern Control Theory**
  - 1957 Sputnik
  - [Draper 1960] inertial navigation system (Polaris, and later Apollo AGC)
  - [Åström and Wittenmark 1971] “On Self-Tuning Regulators”

Abstracted from [Lewis 92] + additions
Mechanical Feedback Mechanisms

[Mayr 1971]

Figure 2.—Water clock of Ktesibios (1st half third century B.C.) as reconstructed by Hermann Diels. Reprinted from Hermann Diels, *Antike Technik*, 3rd edition (Leipzig, 1924), fig. 71.

Figure 88.—Cornelis Drebbel’s chicken incubator with temperature regulation, about 1620. Reprinted with permission of the Cambridge University Library from MS 2206, part 5, fol. 218.

300 BC 1620 AD 1780 AD
Period of Classical Control

Cybernetics: “The science of communication and control in the animal and in the machine.”

PID Control Defined

Frequency Domain Approaches
Period of Modern Control I

- [Draper 1960] inertial navigation system (Polaris, and later Apollo AGC)

- Sputnik 1957

- 1960s
Kalman’s Advances:

1. **time-domain approach**
2. **linear algebra and matrices**
3. **the concept of the internal system state**
4. **the notion of optimality in control theory**
An adaptive controller can be thought of as having two loops. One loop is normal feedback with the process [plant] and the controller. The other loop is the parameter adjustment loop. 

Figure 1.1 Block diagram of an adaptive system. [Åström and Wittenmark 1995 ]
Introduction

• Acknowledgements
• Fault Management (FM) as Controller
• Feedback Control Timeline
  • AI Methods–Timeline
• Fault Management Timeline
• Assertion
• Modern Control Theory FM DRDs
• Conclusions
• References
AI Methods–Timeline

• 1957 - present
    – Remote Agent Experiment
AI Methods I


[Nilsson 1984] "Shakey The Robot"

Fig. 1 — Executive organization of GPS

Figure 10: TYPICAL MACROP
AI Methods II

- Moved away from traditional AI approaches to layers of feedback loops.

**Old Approach**

- Sensors → perception → modelling → planning → task execution → motor control → Actuators

**New Approach**

- Sensors → reason about behavior of objects → plan changes to the world → identify objects → monitor changes → build maps → explore → wander → avoid objects → Actuators
AI Methods III

- [Williams, Nayak 1996] – NASA Deep Space 1 Remote Agent Experiment (RAX)
- MI – Mode Identification, MR – Mode Recovery
- MI, MR – Model-Based (schematic network, each with FSM)

Figure 2: Model-based configuration management
AI Methods IV

- [Dvorak et al 2000] Mission Data Systems
- Model-Based

Figure 3. This diagram emphasizes several architectural themes: the central role of state knowledge and models, goal-directed operation, separation of state determination from control, and closed-loop control.
Introduction

• Acknowledgements
• Fault Management (FM) as Controller
• Feedback Control Timeline
• AI Methods–Timeline
• Fault Management Timeline

• Assertion
• Modern Control Theory FM DRDs
• Conclusions
• References
Fault Management Timeline

• 1990 – Present
  – [NPR-8705.2B] NASA Human-Rating Requirements for Space Systems
Fault Management - I

• [Johnson 1994] “VHM Generic Architecture” Dr. Stephen Johnson – personal communication
Fault Management - II


Dulac, Owens, Leveson (PI),

Chapter 7. Foundations of System Safety

![Diagram of a control loop]

**FIGURE 7.2**
A standard control loop.

Figure 1. The general form of a model of socio-technical safety control.
Fault Management III

- [Robinson et al. 2003] “Applying Model-Based Reasoning to the FDIR of the Command & Data Handling Subsystem of the International Space Station”
Fault Management IV

• [NPR-8705.2B] NASA Human-Rating Requirements for Space Systems

• 3.2.8 The space system shall provide the capability to detect and annunciate faults that affect critical systems, subsystems, and/or crew health (Requirement 58569).

• 3.2.9 The space system shall provide the capability to isolate and/or recover from faults identified during system development that would result in a catastrophic event (Requirement 58572).
Introduction

- Acknowledgements
- Fault Management (FM) as Controller
- Feedback Control Timeline
- AI Methods—Timeline
- Fault Management Timeline
- Assertion
  - Modern Control Theory FM DRDs
- Conclusions
- References
Assertion
Fault Management can be formally modeled as a feedback control process using concepts from modern control theory.
Evidence

- [Dean, Wellman 1991] “Planning & Control”
- First formal attempt to bridge the gap between AI symbolic methods and traditional control.
- AI Methods Identify Three Types of Goals:
  - Achievement
  - Maintenance
  - Prevention.
- What do they both have in common with FM?
  - The concept of state – however AI methods tend to blur state vs. observations
  - The ability to measure a difference between the objective and the current state.
  - Use of the difference to drive the next action.
  - Goals of Maintenance
Formal Modeling of Feedback Loops

- [Robinson 1997a] “Feedback to Basics” (AAAI) Fall Symposium Model-Directed Autonomous Systems
- [Robinson 2003] “Applying Model-Based Reasoning to the FDIR of the Command & Data Handling Subsystem of the International Space Station”, Robinson et. al. -SAIRAS 2003
Modern Control Theory

• Kalman’s Key Points
  – time-domain approach
  – linear algebra and matrices
  – internal system state
  – the notion of optimality

"Unfortunately, no one can be told what the Matrix is. You have to see it for yourself."
Morpheus, *The Matrix*
MCT Definition [Kalman 60]

State equation: \( x' = Ax + Bu \)
Observation equation: \( y = Cx \)
Gain Equation: \( u(t) = -Kx \)
Introduction

• Acknowledgements
• Fault Management (FM) as Controller
• Feedback Control Timeline
• AI Methods—Timeline
• Fault Management Timeline
• Assertion

• Modern Control Theory FM DRDs

• Conclusions
• References
Modern Control Theory FM DRDs

• DRD 1 – Define variables and values
• DRD 2 – Define matrices which relate variables
• DRD 3 – Define control law equations from matrices and variables – TBD
• DRD 4 – Define properties of controller - TBD
Data Requirements Definition 1

- Define vector variables $r, y, x, u, e$ for the domain(s)

<table>
<thead>
<tr>
<th>Controller Parameter</th>
<th>Variable Name</th>
<th>Vector Size</th>
<th>Possible Values (each element)</th>
</tr>
</thead>
<tbody>
<tr>
<td>setpoints</td>
<td>$r$</td>
<td>$l \times 1$</td>
<td>reals, integers, discretes</td>
</tr>
<tr>
<td>observations</td>
<td>$y$</td>
<td>$m \times 1$</td>
<td>reals, integers, discretes</td>
</tr>
<tr>
<td>state variables</td>
<td>$x$</td>
<td>$n \times 1$</td>
<td>reals, integers, discretes</td>
</tr>
<tr>
<td>loads</td>
<td>$u$</td>
<td>$r \times 1$</td>
<td>reals, integers, discretes</td>
</tr>
<tr>
<td>error</td>
<td>$e$</td>
<td>$l \times 1$</td>
<td>reals, integers, discretes</td>
</tr>
</tbody>
</table>
Variable Mapping: Spacecraft Products -> Control Theory

- CW event (off-nominal state) \((e)\)
- nominal event (sensors, state) \((y,x)\)
- flight procedures/software \((u)\)
- flight rules \((x)\)
- spacecraft schematics \((x)\)
- nominal spacecraft state space \((x)\)
- total spacecraft state space \((x)\)
Each element of the \( r \) vector defines a setpoint for the system

\[
\begin{bmatrix}
r_1 \\
r_2 \\
r_3 \\
\vdots \\
r_i \\
\end{bmatrix}
\begin{bmatrix}
cabin\_temp \\
cabin\_pressure \\
cabin\_CO_2\_level \\
\vdots \\
cabin\_NO_2\_level \\
\end{bmatrix}
= \begin{bmatrix}
20 °C \\
1 \text{ atm} \\
25 \text{ ppm} \\
\vdots \\
250 \text{ ppm} \\
\end{bmatrix}
\]

Different \( r \) vector for nominal control vs FM control.

\[
\begin{bmatrix}
r_1 \\
r_2 \\
r_3 \\
\vdots \\
r_i \\
\end{bmatrix}
\begin{bmatrix}
fuelpump\_state \\
cooler\_state \\
TVC\_state \\
\vdots \\
SW_1\_state \\
\end{bmatrix}
= \begin{bmatrix}
\text{working} \\
\text{working} \\
\text{working} \\
\vdots \\
\text{Mode}_1 \\
\end{bmatrix}
\]
y – observation vector \((m \times 1)\)

- Each element of the \(y\) vector defines an observation for the system.
- Different \(y\) vector for nominal control vs FM control.

\[
\begin{align*}
\bar{y}_{\text{nom}} &= \begin{bmatrix} y_1 \\ y_2 \\ y_3 \\ \vdots \\ y_l \end{bmatrix} = \begin{bmatrix} \text{cabin\_temp} \\ \text{cabin\_pressure} \\ \text{cabin\_CO2\_level} \\ \vdots \\ \text{cabin\_NO2\_level} \end{bmatrix} = \begin{bmatrix} 15\, ^\circ\text{C} \\ .8\, \text{atm} \\ 20\, \text{ppm} \\ \vdots \\ 200\, \text{ppm} \end{bmatrix} \\
y_{FM} &= \begin{bmatrix} y_1 \\ y_2 \\ y_3 \\ \vdots \\ y_l \end{bmatrix} = \begin{bmatrix} \text{fuelpump\_rpm} \\ \text{cooler\_current} \\ \text{TVC\_presure} \\ \vdots \\ \text{SW\_heartbeat} \end{bmatrix} = \begin{bmatrix} 1000\, \text{rpm} \\ 50\, \text{amp} \\ 2000\, \text{psi} \\ \vdots \\ \text{present} \end{bmatrix}
\end{align*}
\]
\( \mathbf{x} \) – state vector \((n \times 1)\)

- Each element of \( \mathbf{x} \) defines a state variable for the system.
- Different \( \mathbf{x} \) vector for nominal control vs FM control.

\[
\mathbf{x}_{\text{nom}} = \begin{bmatrix}
    x_1 \\
    x_2 \\
    x_3 \\
    \vdots \\
    x_n \\
\end{bmatrix} = \begin{bmatrix}
    O_2\_volume \\
    \text{thermal\_capacitance} \\
    \text{hydraulic\_volume} \\
    \vdots \\
    \text{hydrazine\_volume} \\
\end{bmatrix} = \begin{bmatrix}
    20\text{liters} \\
    50\text{C} \\
    5\text{liters} \\
    \vdots \\
    2\text{liters} \\
\end{bmatrix}
\]

\[
\mathbf{x}_{\text{FM}} = \begin{bmatrix}
    x_1 \\
    x_2 \\
    x_3 \\
    \vdots \\
    x_n \\
\end{bmatrix} = \begin{bmatrix}
    \text{pump\_state} \\
    \text{cooler\_state} \\
    \text{TVC\_state} \\
    \vdots \\
    \text{SW}_1\_state \\
\end{bmatrix} = \begin{bmatrix}
    \text{working} \\
    \text{failed} \\
    \text{working} \\
    \vdots \\
    \text{Standby} \\
\end{bmatrix}
\]
**u – load vector (r x 1)**

- Each element of \( u \) defines a loads/commands for the system.
- Different \( u \) vector for nominal control vs FM control.

\[
\begin{align*}
\mathbf{u}_{\text{nom}} &= \begin{bmatrix} u_1 \\ u_2 \\ \vdots \\ u_r \end{bmatrix} = \begin{bmatrix} \text{apply\_thrust\_in\_z\_direction} \\ \text{circulate\_air\_in\_cabin} \\ \text{gimbal\_nozzle} \\ \text{scrub\_CO}_2 \end{bmatrix} = \begin{bmatrix} \text{turnon/off valve} \\ \text{turnon/off pump} \\ \text{extend/retract tvc} \\ \text{turnon/off scrubber} \end{bmatrix} \\
\mathbf{u}_{\text{FM}} &= \begin{bmatrix} u_1 \\ u_2 \\ \vdots \\ u_r \end{bmatrix} = \begin{bmatrix} \text{fuel\_pump} \\ \text{cooler} \\ \text{HW component} \\ \text{SW component} \end{bmatrix} = \begin{bmatrix} \text{turnon/off} \\ \text{turnon/off} \\ \text{turnon/off} \\ \text{turnon/off} \end{bmatrix}
\end{align*}
\]
e – error vector

- Two types of error, observation vs. state error.
- What does symbolic difference mean? (points to transition between two states of an FSM)

\[
\begin{bmatrix}
  e_1 \\
  e_2 \\
  e_3 \\
  \vdots \\
  e_m
\end{bmatrix}
\begin{bmatrix}
  \Delta \text{cabin\_temp} \\
  \Delta \text{cabin\_pressure} \\
  \Delta \text{cabin\_CO2\_level} \\
  \vdots \\
  \Delta \text{cabin\_NO2\_level}
\end{bmatrix}
= 
\begin{bmatrix}
  y_1 \\
  y_2 \\
  y_3 \\
  \vdots \\
  y_m
\end{bmatrix}
- 
\begin{bmatrix}
  r_1 \\
  r_2 \\
  r_3 \\
  \vdots \\
  r_m
\end{bmatrix}
= 
\begin{bmatrix}
  15 \degree \text{C} \\
  .8 \text{ atm} \\
  20 \text{ ppm} \\
  \vdots \\
  200 \text{ ppm}
\end{bmatrix}
- 
\begin{bmatrix}
  20 \degree \text{C} \\
  1 \text{ atm} \\
  25 \text{ ppm} \\
  \vdots \\
  250 \text{ ppm}
\end{bmatrix}
= 
\begin{bmatrix}
  -5 \\
  -2 \\
  -5 \\
  \vdots \\
  -50
\end{bmatrix}
\]

\[
\begin{bmatrix}
  e_1 \\
  e_2 \\
  e_3 \\
  \vdots \\
  e_n
\end{bmatrix}
\begin{bmatrix}
  \Delta \text{pump\_state} \\
  \Delta \text{cooler\_state} \\
  \Delta \text{TVC\_state} \\
  \vdots \\
  \Delta \text{SW}_{1\_state}
\end{bmatrix}
= 
\begin{bmatrix}
  \text{working} \\
  \text{failed} \\
  \text{working} \\
  \vdots \\
  \text{Standby}
\end{bmatrix}
- 
\begin{bmatrix}
  \text{working} \\
  \text{working} \\
  \text{working} \\
  \vdots \\
  \text{Mode}_1
\end{bmatrix}
= 
\begin{bmatrix}
  \text{failed} - \text{working} \\
  \text{ failed} - \text{working} \\
  \vdots \\
  \text{ Standby} - \text{Mode}_1
\end{bmatrix}
\]
Modern Control Theory FM DRDs

• DRD 1 – Define variables and values
• DRD 2 – Define matrices which relate variables
• DRD 3 – Define control law equations from matrices and variables –TBD
• DRD 4 – Define properties of controller - TBD
Data Requirements Definition 2

• Matrices which relate $y,x,u$
• Definitions for the matrices forces modelers to be systematic.

$y=Cx$
  – What is the state $x$ wrt to the sensors $y$?

$x'=Ax+Bu$
  – How does the state $x$ affect the change of the state $x$?

$x'=Ax+Bu$:
  – How does next loads/actions $u$ affect the change of state $x'$.

$u=-Kx$:
  – What should the next action $u$ be given the current state $x$?
**Observation Matrix: C**

- \( y = Cx \)
- \( C \) is an \( n \times m \) matrix.
- \( C_{ij} \): the contribution of state variable \( x_i \) on observation \( y_j \).

\[
C(t) = \begin{bmatrix}
C_{11} & \cdots & C_{1m} \\
\vdots & \ddots & \vdots \\
C_{n1} & \cdots & C_{nm}
\end{bmatrix}
\]

\[
C_{nom} = \begin{bmatrix}
f(O_2\_volume, cabin\_temp) & \cdots & f(hydrazine\_volume, cabin\_temp) \\
\vdots & \ddots & \vdots \\
f(O_2\_volume, cabin\_N2\_temp) & \cdots & f(hydrazine\_volume, cabin\_N2\_temp)
\end{bmatrix}
\]

\[
C_{FM} = \begin{bmatrix}
f(fuelpump\_state, fuelpump\_rpm) & \cdots & f(GNC\_software\_state, fuelpump\_rpm) \\
\vdots & \ddots & \vdots \\
f(fuelpump\_state, SW1\_heartbeat) & \cdots & f(GNC\_software\_state, cabin\_N2\_temp)
\end{bmatrix}
\]
\[ x = C^+ y \]

- Note: pseudo inverse (or true inverse) of the observation equation is diagnosis.
- For diagnosis, the inverse is not unique – due to the fact that there are significantly less sensors than state variables.
- A selling point for FM methods, as many traditional control methods will fail due to non-unique inverse.
Livingstone Example: Support for non-unique inverse [Robinson 2003]

**State vector**

- State vector element failed
- State vector element working

*Non-unique Inverse*
State Transition Matrix: \( A \)

- \( x' = Ax + Bu \)
- \( A \) is an \( n \times n \) matrix.
- \( A_{ij} \): the contribution of state variable \( x_i \) on the change of state variable \( x_j \).

State Transition
- Numeric systems: Derivative
- Symbolic systems: Finite State Transition

\[
A(t) = \begin{bmatrix}
a_{11} & \cdots & a_{1n} \\
\vdots & \ddots & \vdots \\
a_{n1} & \cdots & a_{nn}
\end{bmatrix}
\]
Nominal and FM A Matrix

\[ A_{\text{nom}} = \begin{bmatrix}
    f(\Delta O_2 \text{ volume}, O_2 \text{ volume}) & \cdots & f(\Delta \text{hydrazine volume}, O_2 \text{ volume}) \\
    \vdots & \ddots & \vdots \\
    f(\Delta O_2 \text{ volume}, \text{hydrazine volume}) & \cdots & f(\Delta \text{hydrazine volume}, \text{hydrazine volume})
\end{bmatrix} \]

\[ A_{\text{FM}} = \begin{bmatrix}
    f(\Delta \text{pump state}, \text{pump state}) & \cdots & f(\Delta W_1 \text{ state}, \text{pump state}) \\
    \vdots & \ddots & \vdots \\
    f(\Delta \text{pump state}, W_1 \text{ state}) & \cdots & f(\Delta W_1 \text{ state}, W_1 \text{ state})
\end{bmatrix} \]
Loads Matrix: B

- $x' = Ax + Bu$
- B is an $n \times r$ matrix.
- $B_{ij}$: the contribution of load/command $u_i$ on the change of state variable $x_j$.

State Transition
- Numeric Systems: load are forces on system
- Symbolic Systems: loads are the commands

\[
B(t) = \begin{bmatrix}
b_{11} & \cdots & b_{1r} \\
\vdots & \ddots & \vdots \\
b_{n1} & \cdots & b_{nr}
\end{bmatrix}
\]
Nominal and FM B Matrix

\[
B_{\text{nom}} = \begin{bmatrix}
  f(\Delta O_2\_\text{volume, turnon/ off _ valve}) & \cdots & f(\Delta \text{hydrazine }\_\text{volume, turnon/ off _ valve}) \\
  \vdots & \ddots & \vdots \\
  f(\Delta O_2\_\text{volume, turnon/ off _ scrubber}) & \cdots & f(\Delta \text{hydrazine }\_\text{volume, turnon/ off _ scrubber})
\end{bmatrix}
\]

\[
B_{\text{FM}} = \begin{bmatrix}
  f(\Delta\text{pump }\_\text{state, turnon/ off _ fuelpump}) & \cdots & f(\Delta SW_1\_\text{state, turnon/ off _ fuelpump}) \\
  \vdots & \ddots & \vdots \\
  f(\Delta\text{pump }\_\text{state, turnon/ off _ SW}_1) & \cdots & f(\Delta SW_1\_\text{state, turnon/ off _ SW}_1)
\end{bmatrix}
\]
Gain Matrix: $K$

- $u = -Kx$
- $K$ is an $n \times r$ matrix.
- $K_{ij}$: the contribution of the state variable $x_i$ on the next load $u_j$.

$$K(t) = \begin{bmatrix} k_{11} & \cdots & k_{1r} \\ & \ddots & \vdots \\ k_{n1} & \cdots & k_{nr} \end{bmatrix}$$
Nominal and FM $K$ Matrix

$$K_{\text{nom}} = \begin{bmatrix} f(O2 \_ \text{volume}, \text{turnon} / \text{off} \_ \text{valve}) & \cdots & f(\text{hydrazine} \_ \text{volume}, \text{turnon} / \text{off} \_ \text{valve}) \\ \vdots & \ddots & \vdots \\ f(O2 \_ \text{volume}, \text{turnon} / \text{off} \_ \text{scrubber}) & \cdots & f(\text{hydrazine} \_ \text{volume}, \text{turnon} / \text{off} \_ \text{scrubber}) \end{bmatrix}$$

$$K_{\text{FM}} = \begin{bmatrix} f(\text{pump} \_ \text{state}, \text{turnon} / \text{off} \_ \text{fuelpump}) & \cdots & f(SW1 \_ \text{state}, \text{turnon} / \text{off} \_ \text{fuelpump}) \\ \vdots & \ddots & \vdots \\ f(\text{pump} \_ \text{state}, \text{turnon} / \text{off} \_ \text{SW1}) & \cdots & f(SW1 \_ \text{state}, \text{turnon} / \text{off} \_ \text{SW1}) \end{bmatrix}$$
Modern Control Theory FM DRDs

- DRD 1 – Define variables and values
- DRD 2 – Define matrices which relate variables
- DRD 3 – Define control law equations from matrices and variables – TBD
- DRD 4 – Define properties of controller - TBD
DRD 3 Control Law Equations - TBD

State equation: \( \mathbf{x}' = \mathbf{A}\mathbf{x} + \mathbf{B}\mathbf{u} \)

\[
\begin{bmatrix}
    x_1' \\
    
    \\
    x_n'
\end{bmatrix} =
\begin{bmatrix}
    a_{11} & \cdots & a_{1n} \\
    \vdots & \ddots & \vdots \\
    a_{n1} & \cdots & a_{nn}
\end{bmatrix}
\begin{bmatrix}
    x_1 \\
    
    \\
    x_n
\end{bmatrix} +
\begin{bmatrix}
    b_{11} & \cdots & b_{1r} \\
    \vdots & \ddots & \vdots \\
    b_{n1} & \cdots & b_{nr}
\end{bmatrix}
\begin{bmatrix}
    u_1 \\
    
    \\
    u_r
\end{bmatrix}
\]

Observation equation: \( \mathbf{y} = \mathbf{C}\mathbf{x} \)

\[
\begin{bmatrix}
    y_1 \\
    
    \\
    y_m
\end{bmatrix} =
\begin{bmatrix}
    c_{11} & \cdots & c_{1m} \\
    \vdots & \ddots & \vdots \\
    c_{n1} & \cdots & c_{nm}
\end{bmatrix}
\begin{bmatrix}
    x_1 \\
    
    \\
    x_n
\end{bmatrix}
\]

Gain Equation: \( \mathbf{u}(t) = -\mathbf{K}\mathbf{x} \)

\[
\begin{bmatrix}
    u_1 \\
    
    \\
    u_r
\end{bmatrix} =
-\begin{bmatrix}
    k_{11} & \cdots & k_{1r} \\
    \vdots & \ddots & \vdots \\
    k_{n1} & \cdots & k_{nr}
\end{bmatrix}
\begin{bmatrix}
    x_1 \\
    
    \\
    x_n
\end{bmatrix}
\]
Modern Control Theory FM DRDs

• DRD 1 – Define variables and values
• DRD 2 – Define matrices which relate variables
• DRD 3 – Define control law equations from matrices and variables – TBD

• DRD 4 – Define properties of controller - TBD
Modern Control Theory provides methods to prove properties for controllability, observability and stability.

How do these methods translate to symbolic reasoning domains?
## Comparison of Modeling Primitives

<table>
<thead>
<tr>
<th>Property</th>
<th>Nominal Control</th>
<th>FM Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Function Definition</td>
<td>Domain, Range in Reals</td>
<td>Finite State Machines/Table Lookup</td>
</tr>
<tr>
<td>Derivative of Function</td>
<td>Function Derivative or Difference</td>
<td>Finite State Transition</td>
</tr>
<tr>
<td>Integration of Function</td>
<td>Summation of Derivative</td>
<td>State Transition Path from Initial to Final State.</td>
</tr>
<tr>
<td>Modeling Primitive</td>
<td>Equation</td>
<td>Generalized Constraint (components)</td>
</tr>
<tr>
<td>Matrix Inverse Capabilities (x=C⁻¹y)</td>
<td>Fails – due to under /over constrained system</td>
<td>No failure! – part of FM architecture to handle.</td>
</tr>
<tr>
<td>Linearity Assumption: (scalability, super-position properties)</td>
<td>Foundation of MCT</td>
<td>Reflected into fault signatures/ responses which are independent. (i.e. multiple fault signatures are additive)</td>
</tr>
<tr>
<td>Solving for K (control policy).</td>
<td>Gradient descent search for minima or maxima</td>
<td>Search through parallel FSMs, enforcing temporal constraints</td>
</tr>
</tbody>
</table>
Introduction

• Acknowledgements
• Fault Management (FM) as Controller
• Feedback Control Timeline
• AI Methods—Timeline
• Fault Management Timeline
• Assertion
• Modern Control Theory FM DRDs

• Conclusions
• References
Conclusions

• Use of generalized linear algebra formalism:
  – provides a common language for FM practitioners to communicate with Nominal Control practitioners
  – Provides a methodology to systematically explore the complexity of the domain.
  – Provides a methodology which supports scalability for extremely large systems (e.g. 50K failure modes, 50K tests).

• However .... Matrix methods will break down and where they do innovations should be implemented to interface with generalized linear algebra methods.
Introduction

- Acknowledgements
- Fault Management (FM) as Controller
- Feedback Control Timeline
- AI Methods—Timeline
- Fault Management Timeline
- Assertion
- Modern Control Theory FM DRDs
- Conclusions

- References
References I

- [Mayr 1971] “Feedback Mechanisms In the Historical Collections of the National Museum of History and Technology” Smithsonian Institution Press 1971
- [Åström and Wittenmark 1972] “On Self-Tuning Regulators” 5th IFAC Conference
- [Robinson 1997a] “Feedback to Basics” (AAAI) Fall Symposium Model-Directed Autonomous Systems
References II

• [Robinson et. al 2003] “Applying Model-Based Reasoning to the FDIR of the Command & Data Handling Subsystem of the International Space Station”, Robinson et. al. -SAIRAS 2003
• [Dulac et al. 2007] “Demonstration of a New Dynamic Approach to Risk Analysis for NASA’s Constellation Program” Dulac, Owens, Leveson (PI),
• [NPR-8705.2B] NASA Human-Rating Requirements for Space Systems