



# FM as a Controller

[peter.i.robinson@nasa.gov](mailto: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

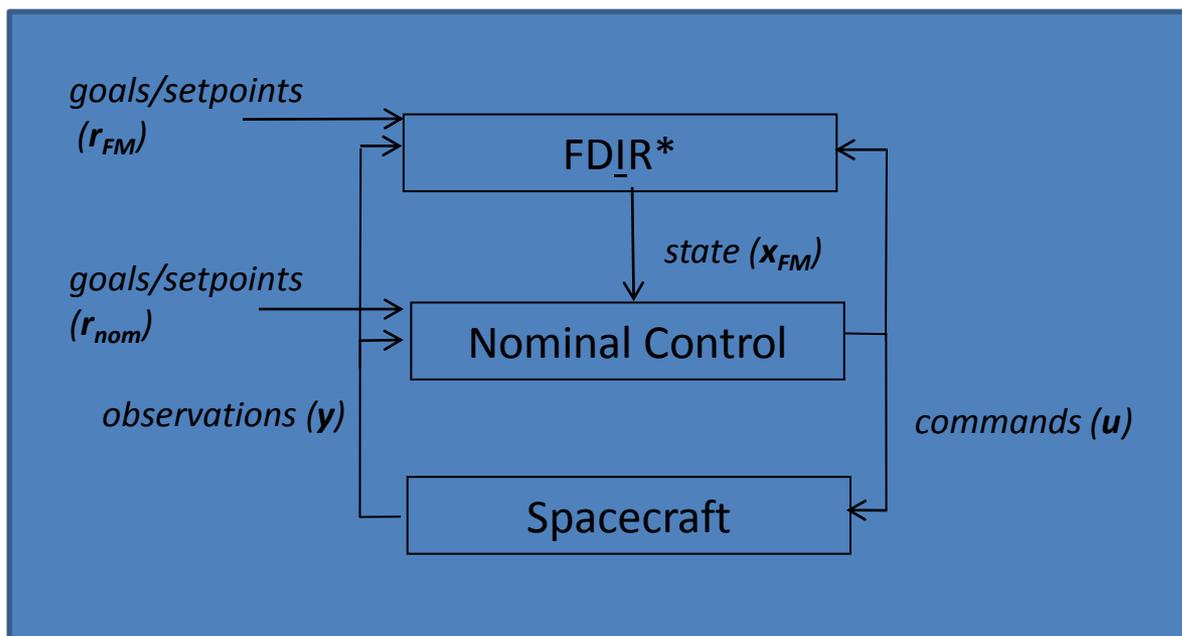


# Introduction

- 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
  - 3<sup>rd</sup> 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
  - 1948 N Wiener – “Cybernetics: or Control and Communication in the Animal and Machine”
- 1957 AD – present – Time Domain Methods – Modern Control Theory
  - 1957 Sputnik
  - [Draper 1960] inertial navigation system (Polaris, and later Apollo AGC)
  - [Kalman 1960] “A New Approach to Linear Filtering and Prediction Problems”
  - [Åström and Wittenmark 1971] “On Self-Tuning Regulators”

# Mechanical Feedback Mechanisms

## [Mayr 1971]

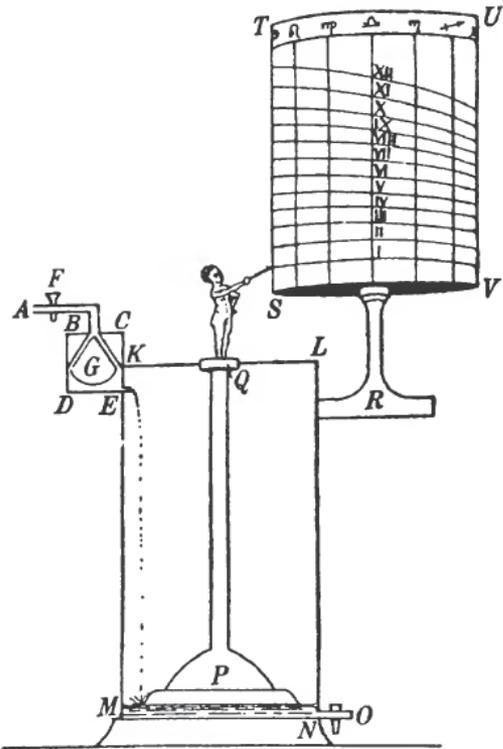


FIGURE 2.—Water clock of Ktesibios (1st half third century B.C.) as reconstructed by Hermann Diels. Reprinted from Hermann Diels, *Antike Technik*, 3rd edition (Leipzig, 1924), fig. 71.

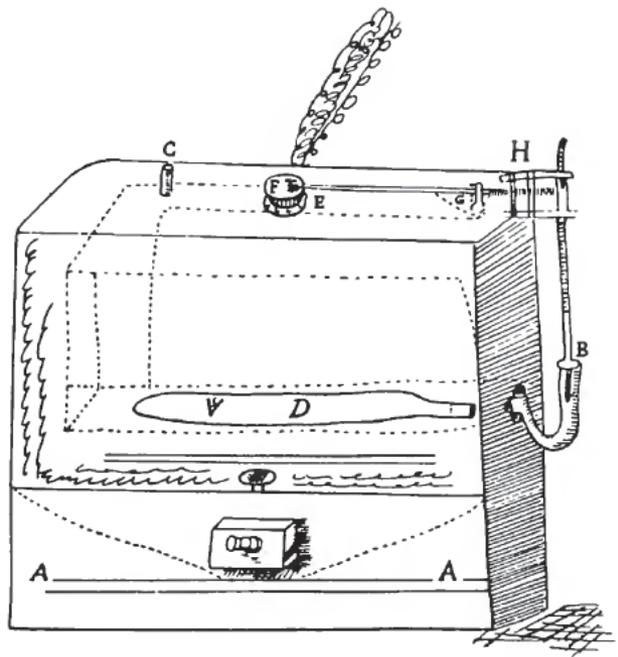


FIGURE 88.—Cornelis Drebbel's chicken incubator with temperature regulation, about 1620. Reprinted with permission of the Cambridge University Library from MS 2206, part 5, fol. 218.

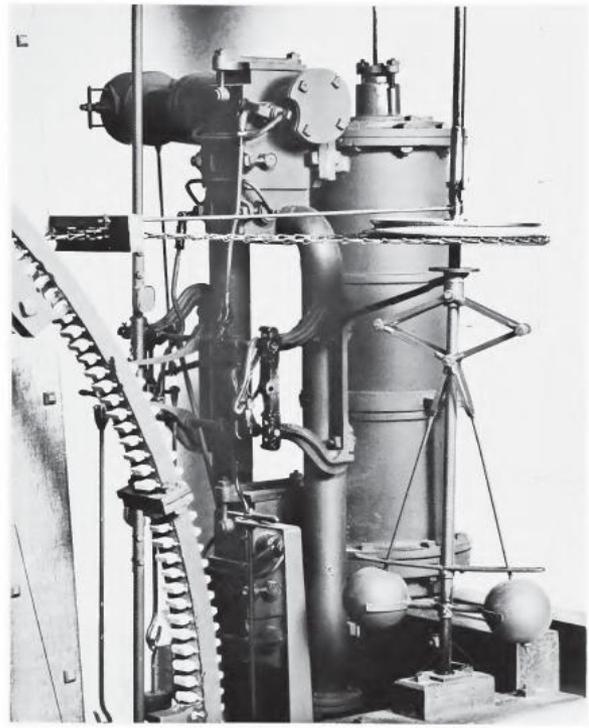
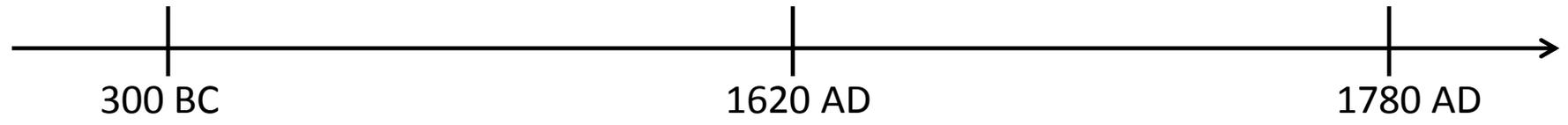


FIGURE 3.—Model of James Watt's "Lap" Engine of 1788. The detail view shows the centrifugal governor with its drive and its connections to the steam valve (top left). (NMHT 323494, Smithsonian photo P-64116.)



# Period of Classical Control

PID Control Defined

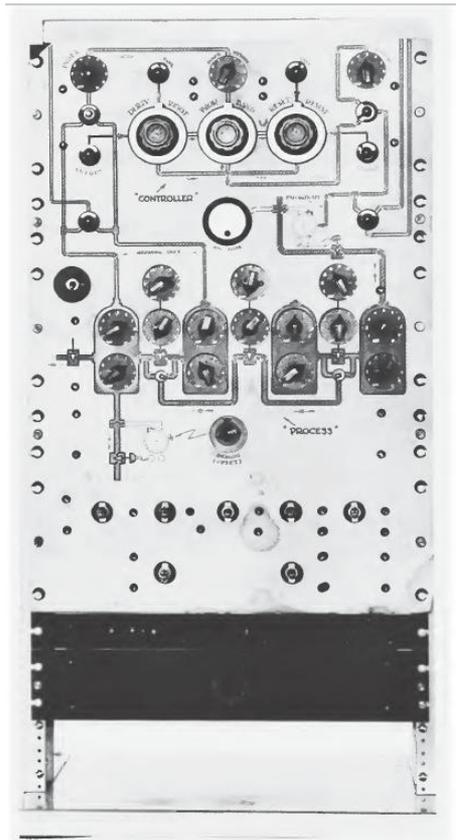
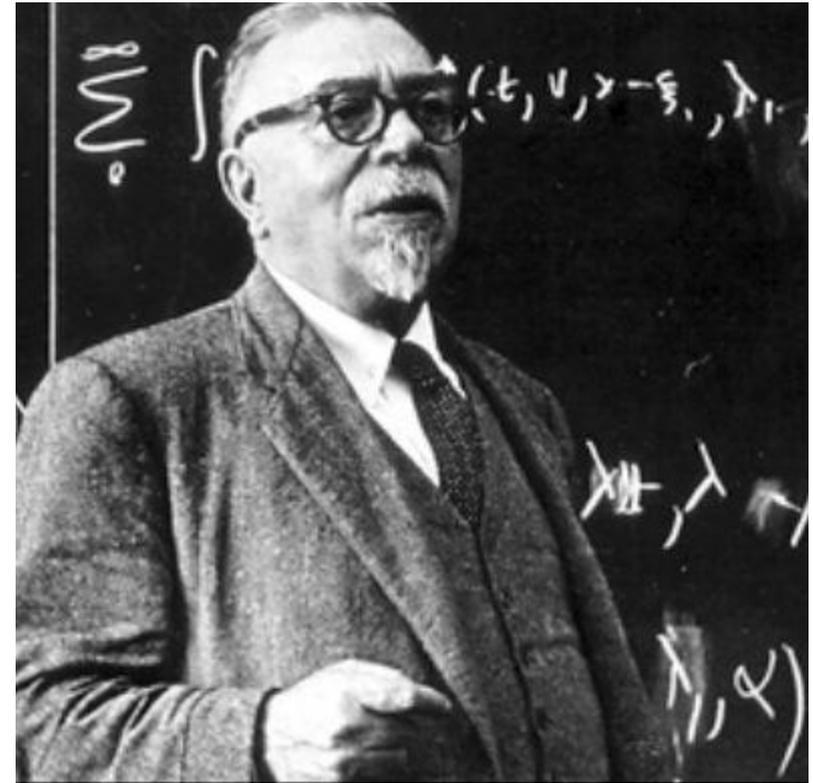
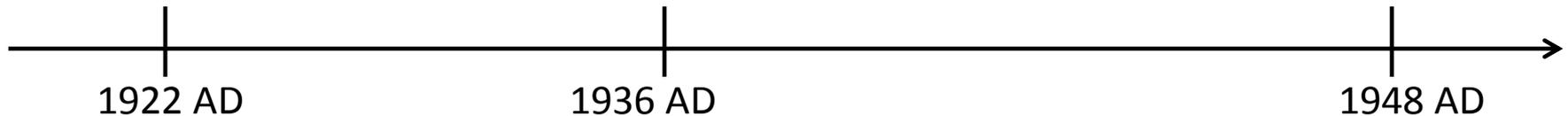


FIGURE 145.—Philbrick electronic analog computer for feedback control system analysis. (NMHT 327546. Smithsonian photo 61757-A.)

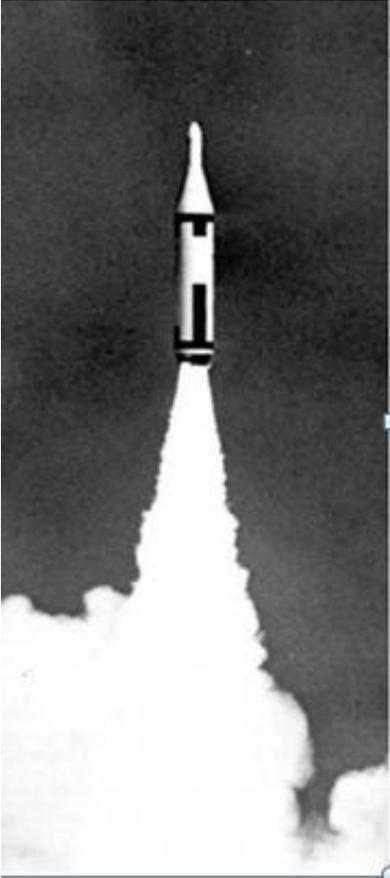


Cybernetics: “The science of communication and control in the animal and in the machine.”

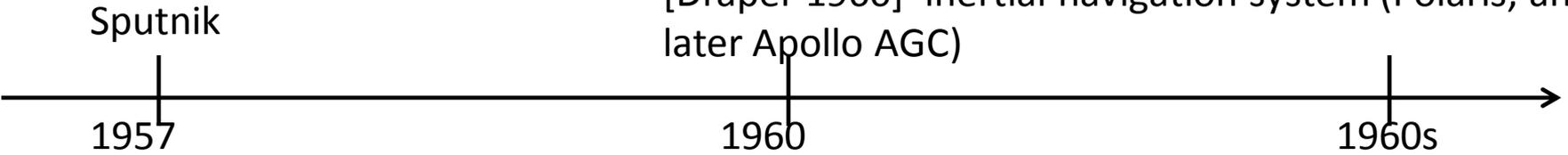




# Period of Modern Control I



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



# Period of Modern Control - II

[Kalman 1960] "A New Approach to Linear Filtering and Prediction Problems"

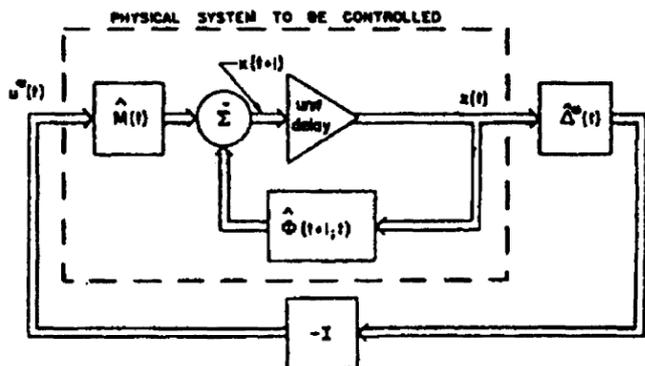


Fig. 4 Matrix block diagram of optimal controller

$$x(t+1) = \hat{\Phi}(t+1; t)x(t) + \hat{M}(t)u(t)$$

$$u^*(t) = -\hat{\Delta}^*(t)x(t)$$

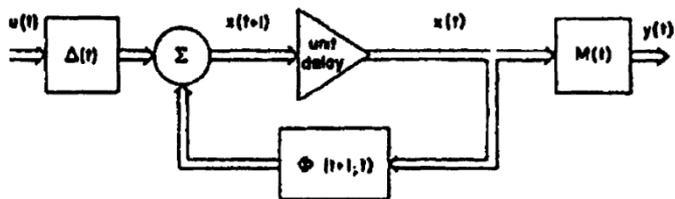


Fig. 2 Matrix block diagram of the general linear, discrete-dynamic system

$$x(t+1) = \Phi(t)x(t) + \Delta(t)u(t); t = 0, 1, \dots$$

$$y(t) = M(t)x(t)$$

Kalman's Advances:

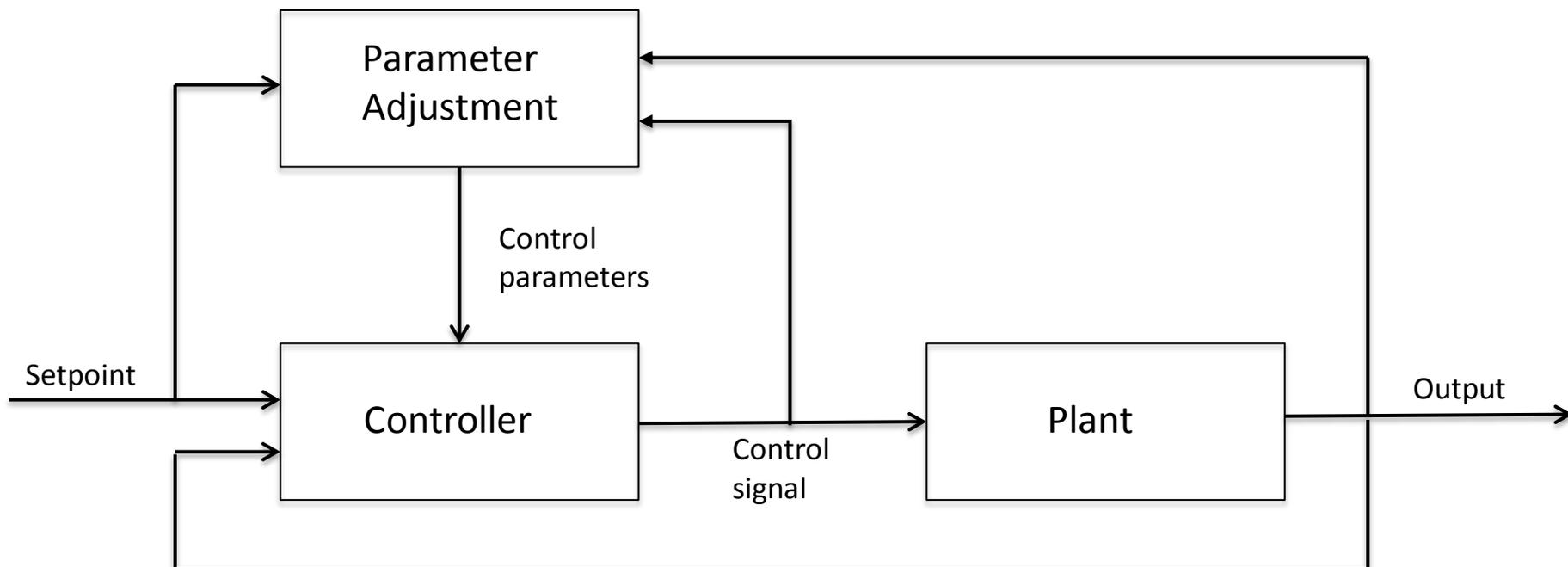
1. *time-domain approach*
2. *linear algebra and matrices*
3. *the concept of the internal system state*
4. *the notion of optimality in control theory*

# Period of Modern Control - II

[Åström and Wittenmark 1971] “On Self-Tuning Regulators”

“ 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. ”

[Åström and Wittenmark 1995 ]



**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
  - [Newell, Simon, Shaw 1958] ““Report of a General Problem-Solving Program”
  - 1972 [Nilsson 1984] “Shakey The Robot”
  - [Brooks, 1986] Brooks, R.A., "A robust layered control system for a mobile robot
  - [Williams, Nayak 1996] – NASA Deep Space 1
    - Remote Agent Experiment
  - [Dvorak et al 2000] Mission Data Systems

# AI Methods I

[Newell, Simon, Shaw 1958] “Report of a General Problem-Solving Program”

[Nilsson 1984] “Shakey The Robot”

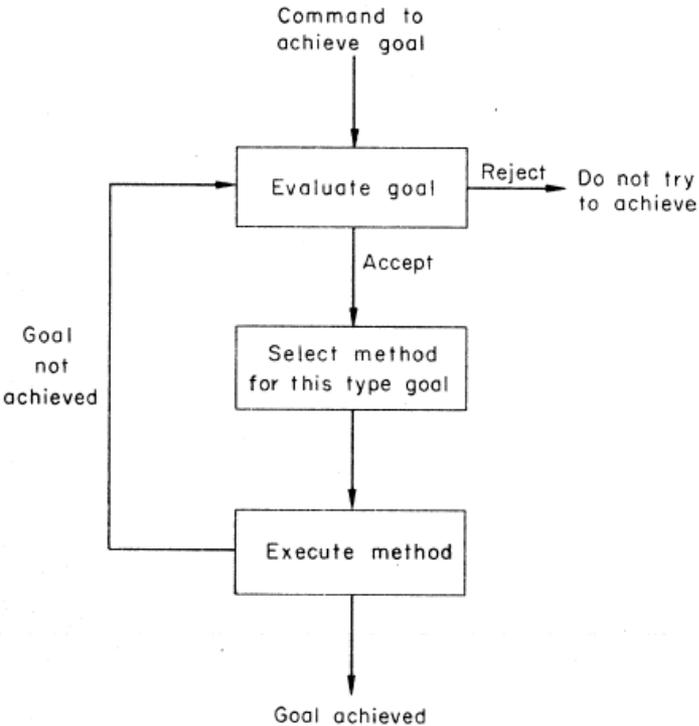
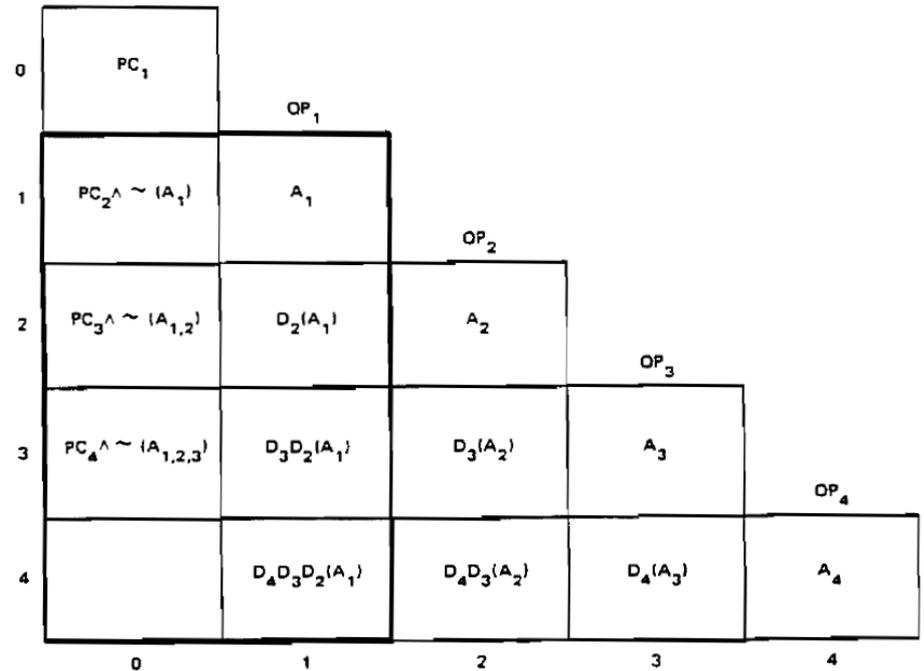
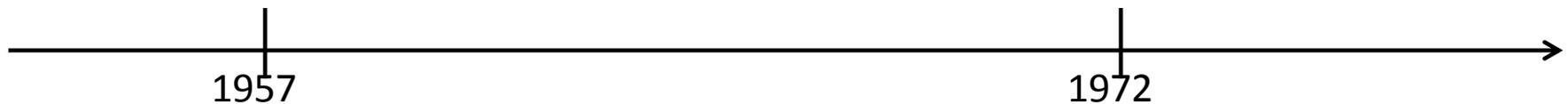


Fig. 1—Executive organization of GPS



TA-8973-12

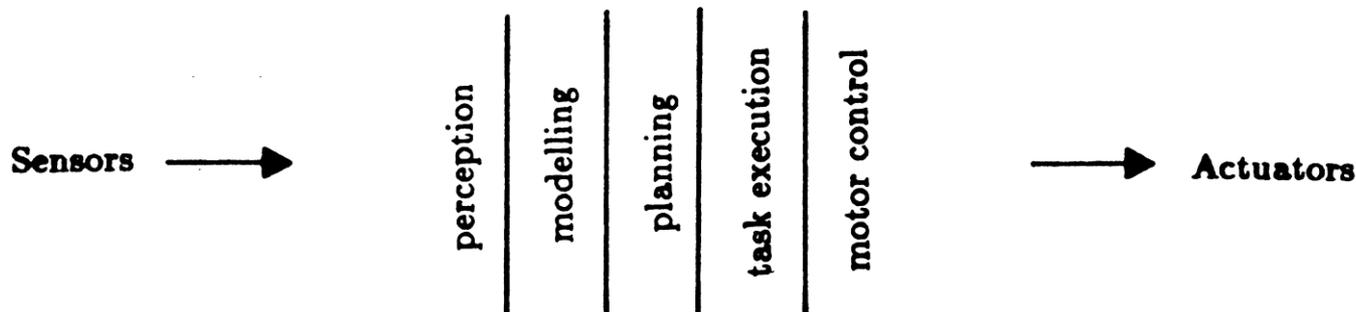
Figure 10: TYPICAL MACROP



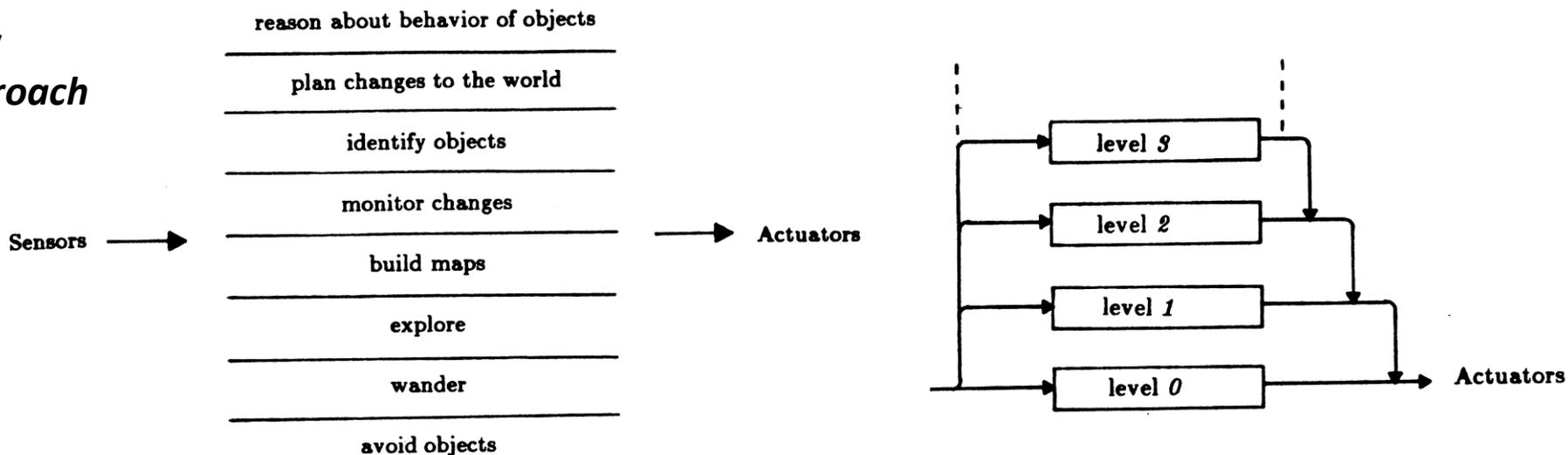
# AI Methods II

- [Brooks, 1986] Brooks, R.A., "A robust layered control system for a mobile robot"
- Moved away from traditional AI approaches to layers of feedback loops.

*Old Approach*

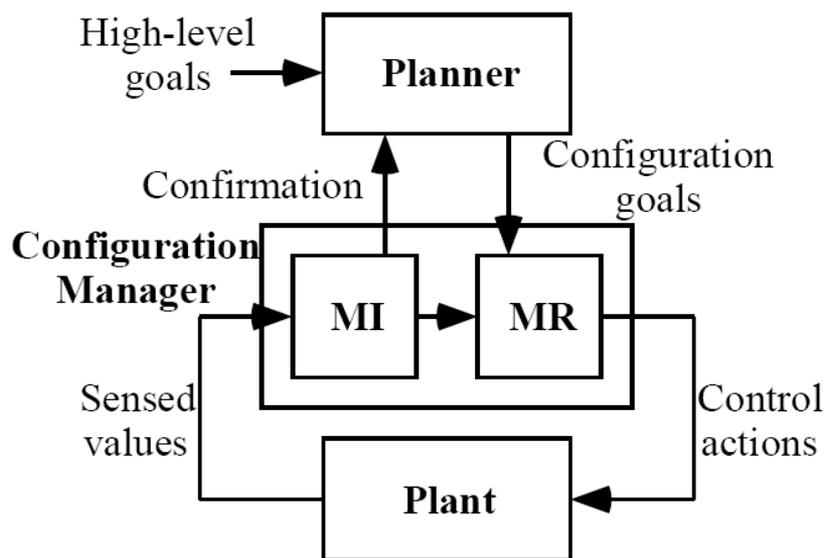


*New Approach*



# 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)

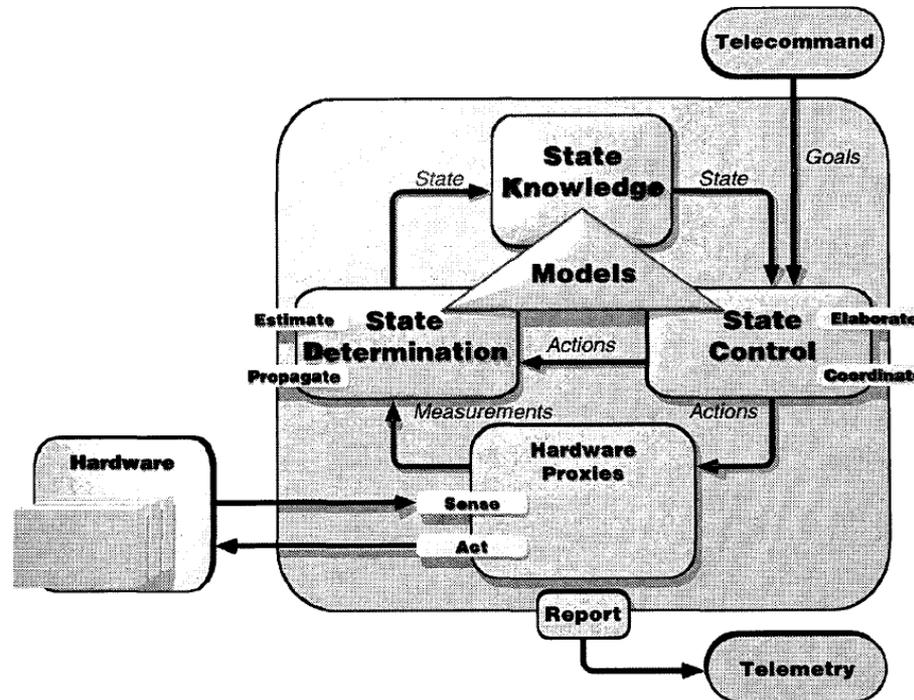


<Picture of DS1>

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

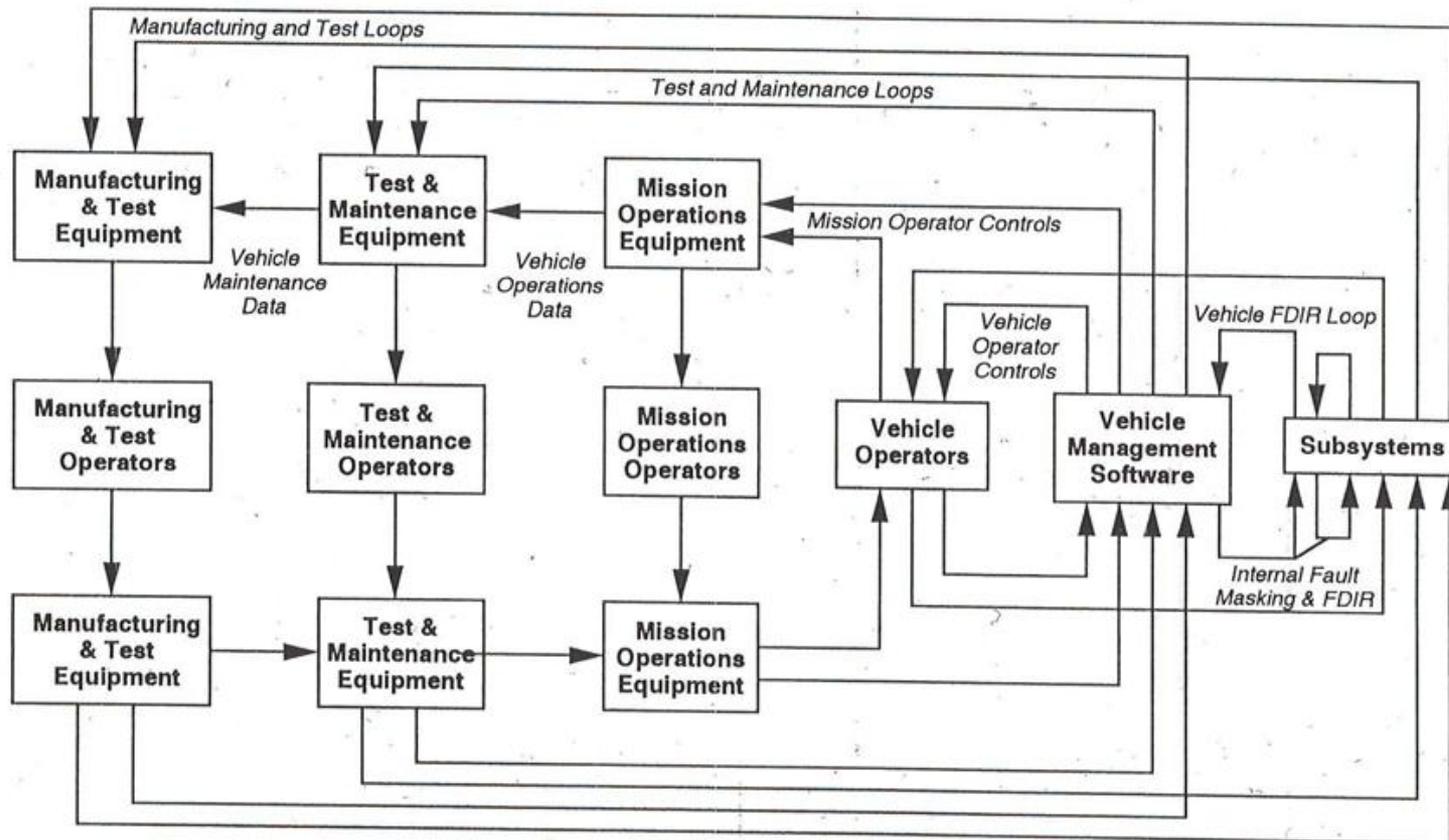


# Fault Management Timeline

- 1990 – Present
  - [Johnson 1994] – “VHM Generic Architecture”
  - [Leveson 1995] – “Safeware – System Safety and Computers”
  - [Robinson 2003] – “Applying Model-Based Reasoning to the FDIR of the Command & Data Handling Subsystem of the International Space Station”
  - [Dulac et al. 2007] “Demonstration of a New Dynamic Approach to Risk Analysis for NASA’s Constellation Program”  
Leveson (PI)
  - [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

1. Leveson 1995] “Safeware – System Safety and Computers”
2. [Dulac et al. 2007] “Demonstration of a New Dynamic Approach to Risk Analysis for NASA’s Constellation Program  
Dulac, Owens, Leveson (PI),

Chapter 7. Foundations of System Safety

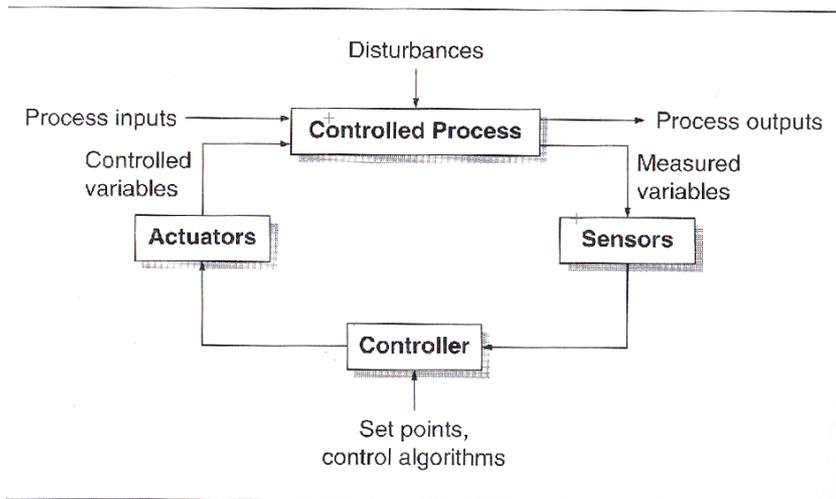


FIGURE 7.2  
A standard control loop.

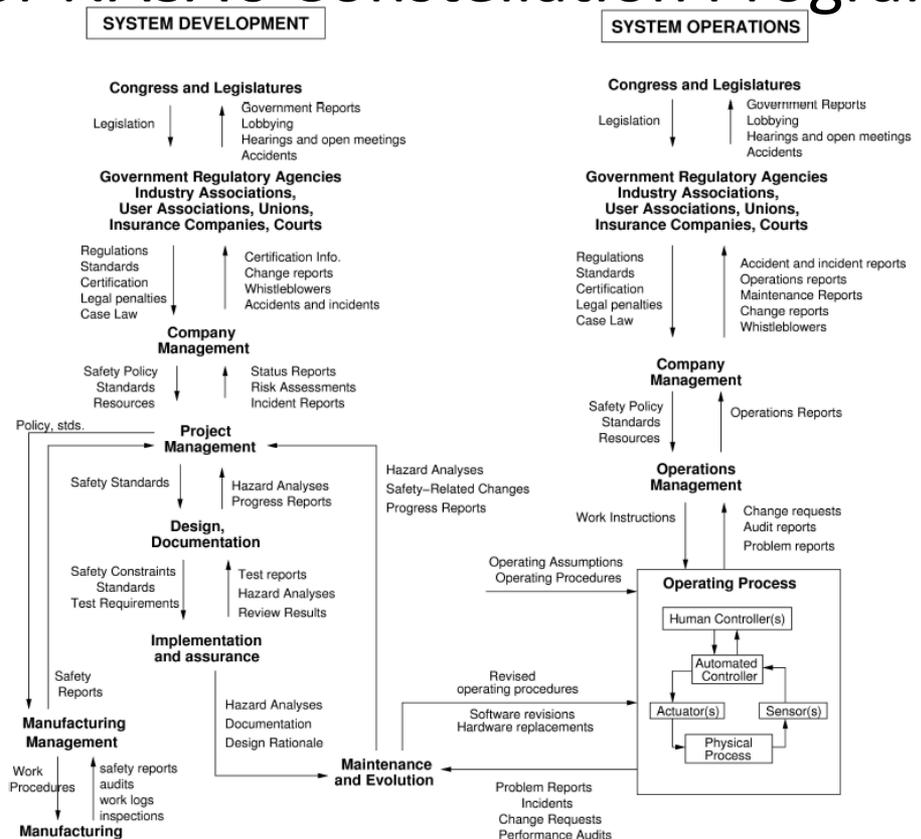
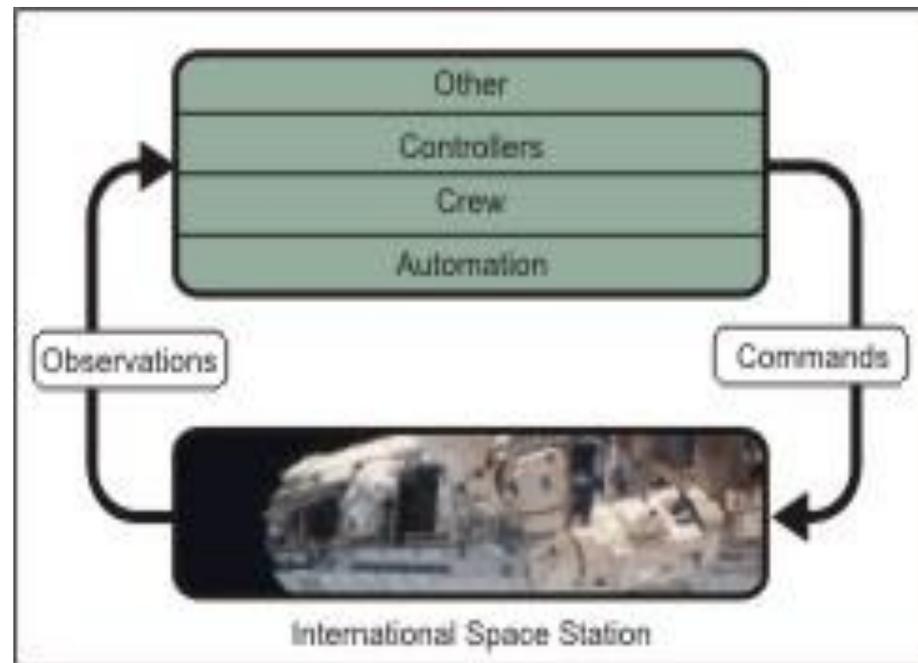
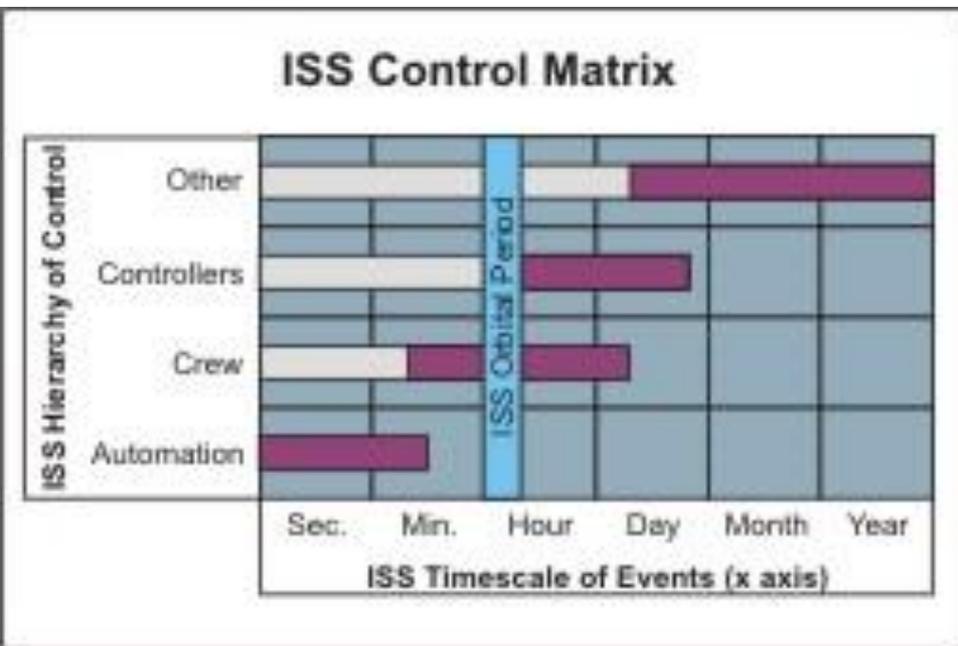


Figure 1. The general form of a model of socio-technical safety control.

# 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

Table of Contents

- Change History
- Preface
- Chapter 1. Human Rating Certification Process
- Chapter 2. Human Rating Certification Requirements
- Chapter 3. Technical Requirements For Human Rating
- Appendix A. Definitions
- Appendix B. Acronyms
- Appendix C. References
- Appendix D. Human Rating Certification Package

- [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).

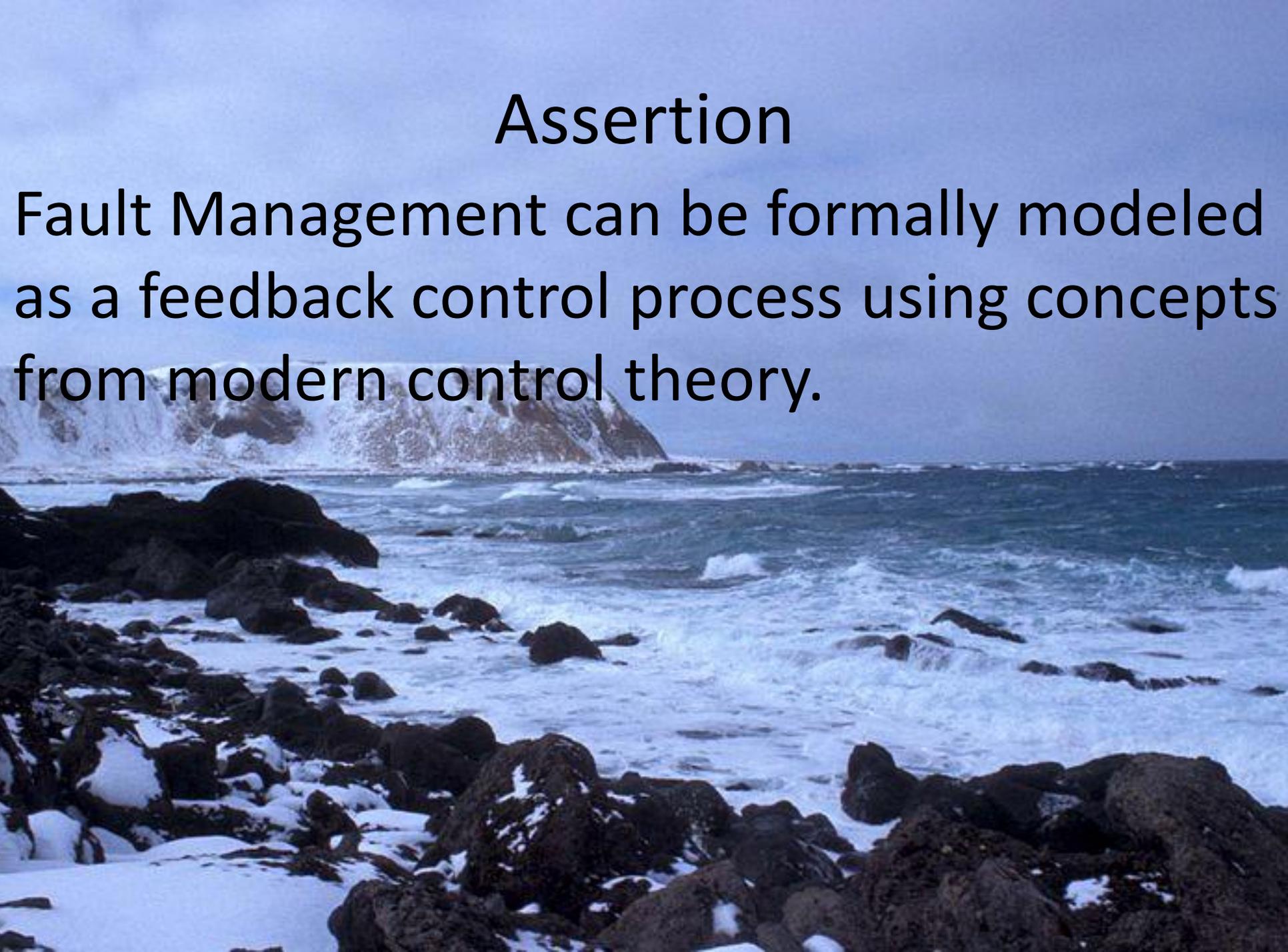


# Introduction

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

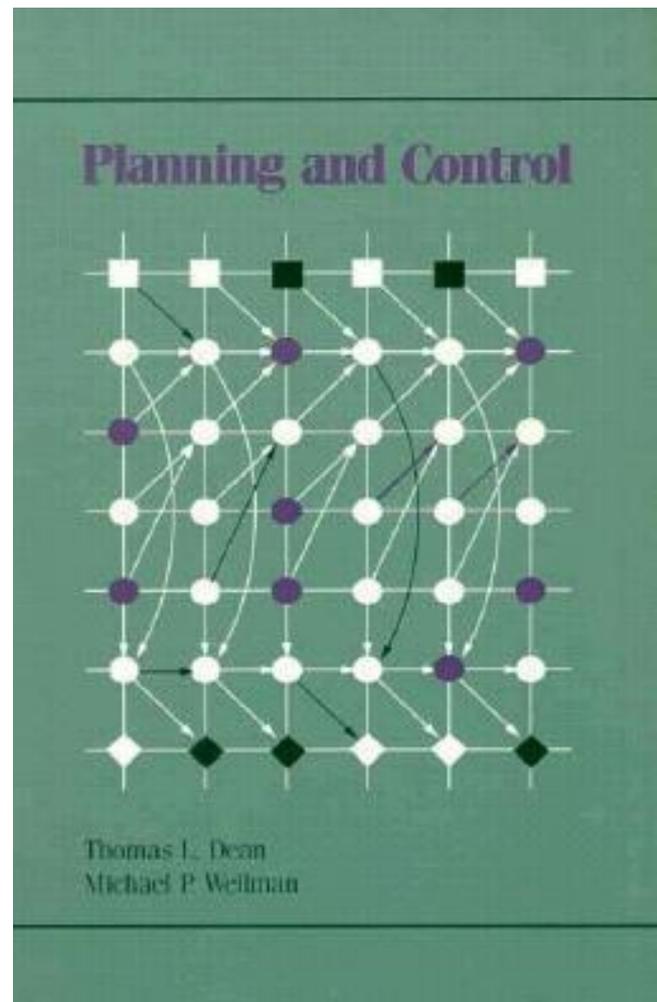
# Assertion

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 1997b] “Autonomous design and execution of process controllers for untended scientific instruments”, AGENTS '97 Proceedings of the first international conference on Autonomous agents, ACM
- [Robinson 2001] “Automatic Overset Grid Generation with Heuristic Feedback Control” NASA/TM-2001-210931 November 2001.
- [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
- [Robinson 2005] “A Three Level Autonomous Software System for Increased Science Return” Robinson et. Al., American Geophysical Union, Fall Meeting 2005



# 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]

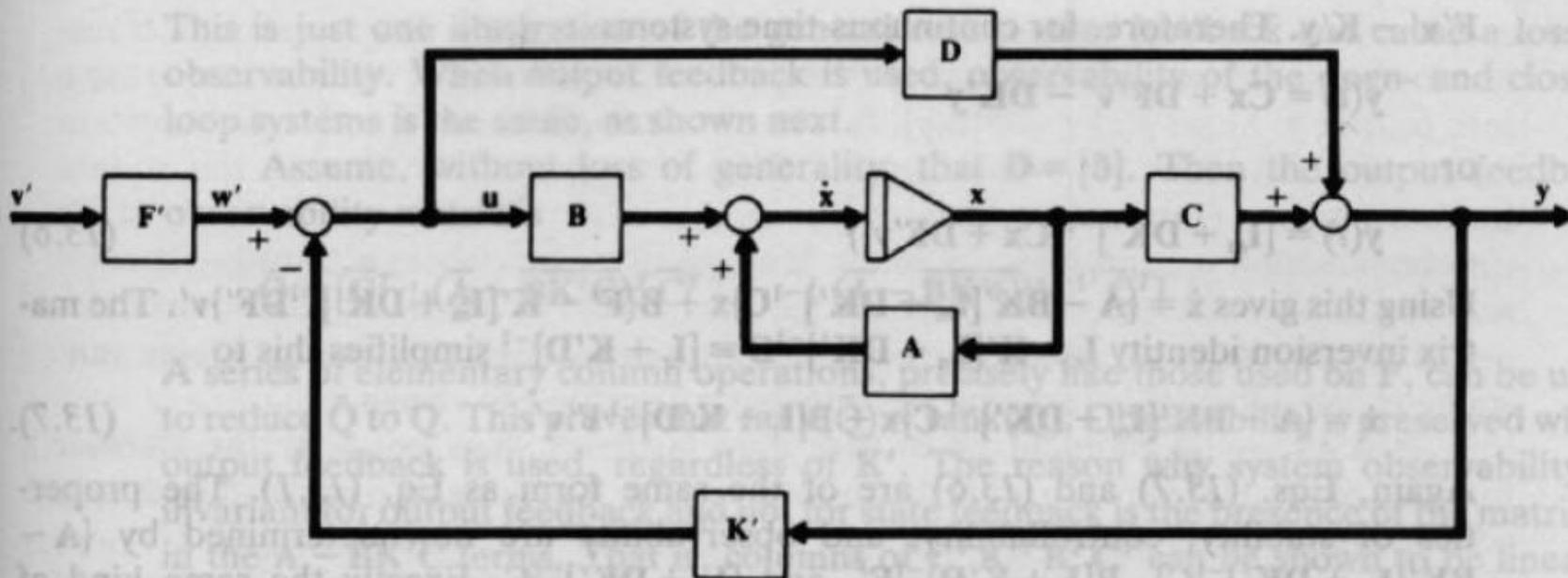


Figure 13.2 Output feedback system.

[Brogan 1982]

State equation:  $\mathbf{x}' = \mathbf{Ax} + \mathbf{Bu}$

Observation equation:  $\mathbf{y} = \mathbf{Cx}$

Gain Equation:  $\mathbf{u}(t) = -\mathbf{Kx}$



# 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

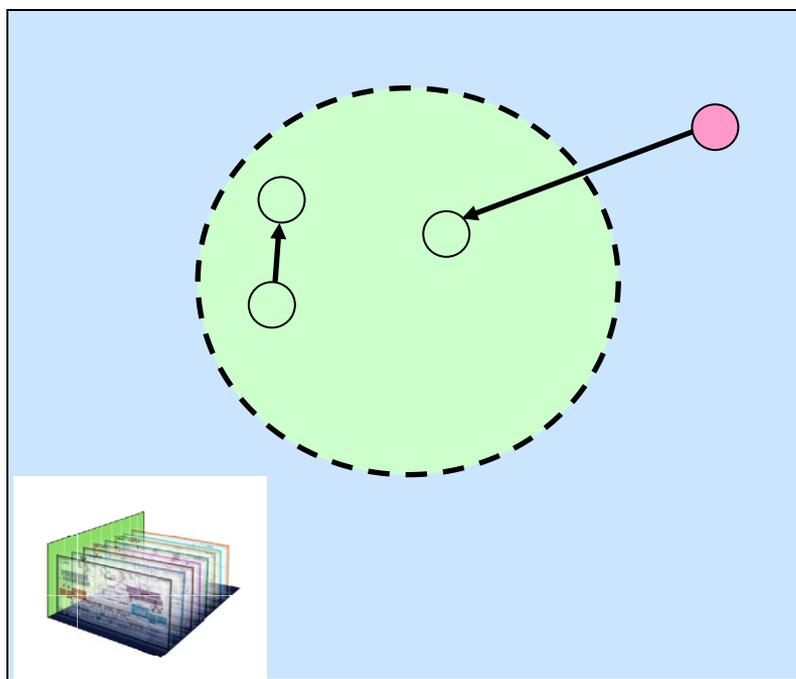


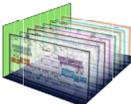
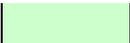
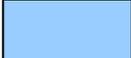
# Data Requirements Definition 1

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

Controller Parameter	Variable Name	Vector Size	Possible Values (each element)
setpoints	<b>r</b>	$l \times 1$	reals, integers, discretets
observations	<b>y</b>	$m \times 1$	reals, integers, discretets
state variables	<b>x</b>	$n \times 1$	reals, integers, discretets
loads	<b>u</b>	$r \times 1$	reals, integers, discretets
error	<b>e</b>	$l \times 1$	reals, integers, discretets

# 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 ( $x$ )



# $\mathbf{r}$ – setpoint vector ( $1 \times 1$ )

- Each element of the  $\mathbf{r}$  vector defines a setpoint for the system
- Different  $\mathbf{r}$  vector for nominal control vs FM control.

$$\vec{r}_{nom} = \begin{bmatrix} r_1 \\ r_2 \\ r_3 \\ \vdots \\ r_l \end{bmatrix} = \begin{bmatrix} cabin\_temp \\ cabin\_pressure \\ cabin\_CO_2\_level \\ \vdots \\ cabin\_NO_2\_level \end{bmatrix} = \begin{bmatrix} 20^\circ C \\ 1\ atm \\ 25\ ppm \\ \vdots \\ 250\ ppm \end{bmatrix}$$

$$\vec{r}_{FM} = \begin{bmatrix} r_1 \\ r_2 \\ r_3 \\ \vdots \\ r_l \end{bmatrix} = \begin{bmatrix} fuelpump\_state \\ cooler\_state \\ TVC\_state \\ \vdots \\ SW_1\_state \end{bmatrix} = \begin{bmatrix} working \\ working \\ working \\ \vdots \\ Mode_1 \end{bmatrix}$$



# $\mathbf{y}$ – observation vector ( $m \times 1$ )

- Each element of the  $\mathbf{y}$  vector defines an observation for the system
- Different  $\mathbf{y}$  vector for nominal control vs FM control.

$$\vec{y}_{nom} = \begin{bmatrix} y_1 \\ y_2 \\ y_3 \\ \vdots \\ y_l \end{bmatrix} = \begin{bmatrix} cabin\_temp \\ cabin\_pressure \\ cabin\_CO2\_level \\ \vdots \\ cabin\_NO2\_level \end{bmatrix} = \begin{bmatrix} 15^\circ C \\ .8 atm \\ 20 ppm \\ \vdots \\ 200 ppm \end{bmatrix}$$

$$y_{FM} = \begin{bmatrix} y_1 \\ y_2 \\ y_3 \\ \vdots \\ y_l \end{bmatrix} = \begin{bmatrix} fuelpump\_rpm \\ cooler\_current \\ TVC\_pressure \\ \vdots \\ SW_1\_heartbeat \end{bmatrix} = \begin{bmatrix} 1000 rpm \\ 50 amp \\ 2000 psi \\ \vdots \\ present \end{bmatrix}$$



# $\mathbf{x}$ – state vector ( $n \times 1$ )

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

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

$$\mathbf{x}_{FM} = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} pump\_state \\ cooler\_state \\ TVC\_state \\ \vdots \\ SW_1\_state \end{bmatrix} = \begin{bmatrix} working \\ failed \\ working \\ \vdots \\ Standby \end{bmatrix}$$



# $\mathbf{u}$ – load vector ( $r \times 1$ )

- Each element of  $\mathbf{u}$  defines a loads/commands for the system
- Different  $\mathbf{u}$  vector for nominal control vs FM control.

$$\mathbf{u}_{nom} = \begin{bmatrix} u_1 \\ u_2 \\ u_3 \\ \vdots \\ u_r \end{bmatrix} = \begin{bmatrix} \text{apply\_thrust\_in\_z\_direction} \\ \text{circulate\_air\_in\_cabin} \\ \text{gimbal\_nozzle} \\ \vdots \\ \text{scrub\_CO}_2 \end{bmatrix} = \begin{bmatrix} \text{turn on/off valve} \\ \text{turn on/off pump} \\ \text{extend/retractvc} \\ \vdots \\ \text{turn on/off scrubber} \end{bmatrix}$$

$$\mathbf{u}_{FM} = \begin{bmatrix} u_1 \\ u_2 \\ u_3 \\ \vdots \\ u_r \end{bmatrix} = \begin{bmatrix} \text{fuel\_pump} \\ \text{cooler} \\ \text{HW component}_i \\ \vdots \\ \text{SW component}_j \end{bmatrix} = \begin{bmatrix} \text{turn on/off} \\ \text{turn on/off} \\ \text{turn on/off} \\ \vdots \\ \text{turn on/off} \end{bmatrix}$$



# 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)

$$\vec{e}_{nom} = \begin{bmatrix} e_1 \\ e_2 \\ e_3 \\ \vdots \\ e_m \end{bmatrix} = \begin{bmatrix} \Delta cabin\_temp \\ \Delta cabin\_pressure \\ \Delta cabin\_CO2\_level \\ \vdots \\ \Delta cabin\_NO2\_level \end{bmatrix} = \left( \begin{bmatrix} y_1 \\ y_2 \\ y_3 \\ \vdots \\ y_m \end{bmatrix} - \begin{bmatrix} r_1 \\ r_2 \\ r_3 \\ \vdots \\ r_m \end{bmatrix} \right) = \left( \begin{bmatrix} 15^\circ C \\ .8 atm \\ 20 ppm \\ \vdots \\ 200 ppm \end{bmatrix} - \begin{bmatrix} 20^\circ C \\ 1 atm \\ 25 ppm \\ \vdots \\ 250 ppm \end{bmatrix} \right) = \begin{bmatrix} -5 \\ -.2 \\ -5 \\ \vdots \\ -50 \end{bmatrix}$$

$$\vec{e}_{FM} = \begin{bmatrix} e_1 \\ e_2 \\ e_3 \\ \vdots \\ e_n \end{bmatrix} = \begin{bmatrix} \Delta pump\_state \\ \Delta cooler\_state \\ \Delta TVC\_state \\ \vdots \\ \Delta SW_1\_state \end{bmatrix} = \left( \begin{bmatrix} working \\ failed \\ working \\ \vdots \\ Standby \end{bmatrix} - \begin{bmatrix} working \\ working \\ working \\ \vdots \\ Mode_1 \end{bmatrix} \right) = \begin{bmatrix} - \\ failed - working \\ - \\ \vdots \\ Standby - Mode_1 \end{bmatrix}$$

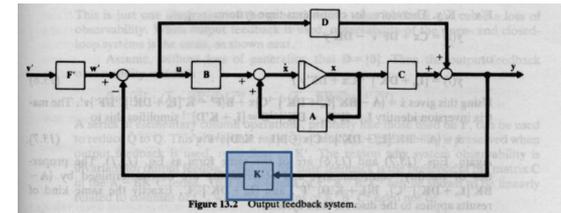
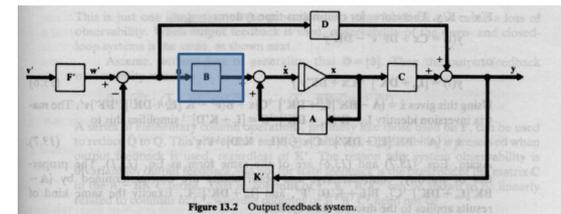
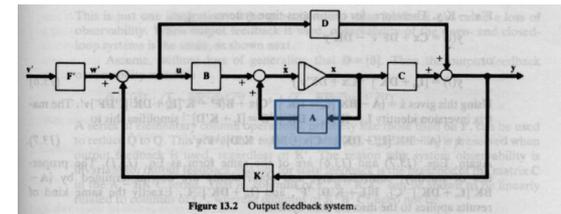
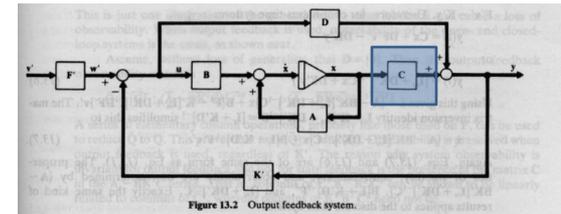


# Modern Control Theory FM DRDs

- 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  $\mathbf{y}, \mathbf{x}, \mathbf{u}$
- Definitions for the matrices forces modelers to be systematic.
- $\mathbf{y} = \underline{\mathbf{C}}\mathbf{x}$ 
  - What is the state  $\mathbf{x}$  wrt to the sensors  $\mathbf{y}$ ?
- $\mathbf{x}' = \underline{\mathbf{A}}\mathbf{x} + \mathbf{B}\mathbf{u}$ 
  - How does the state  $\mathbf{x}$  affect the change of the state  $\mathbf{x}$ ?
- $\mathbf{x}' = \mathbf{A}\mathbf{x} + \underline{\mathbf{B}}\mathbf{u}$ :
  - How does next loads/actions  $\mathbf{u}$  affect the change of state  $\mathbf{x}'$ .
- $\mathbf{u} = -\underline{\mathbf{K}}\mathbf{x}$ :
  - What should the next action  $\mathbf{u}$  be given the current state  $\mathbf{x}$ ?





# Observation Matrix: $\mathbf{C}$

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

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

$$C_{nom} = \begin{bmatrix} f(O_2\_volume, cabin\_temp) & \cdots & f(hydrazine\_volume, cabin\_temp) \\ \vdots & \ddots & \vdots \\ f(O_2\_volume, cabin\_N_2\_temp) & \cdots & f(hydrazine\_volume, cabin\_N_2\_temp) \end{bmatrix}$$

$$C_{FM} = \begin{bmatrix} f(fuelpump\_state, fuelpump\_rpm) & \cdots & f(GNC\_software\_state, fuelpump\_rpm) \\ \vdots & \ddots & \vdots \\ f(fuelpump\_state, SW_1\_heartbeat) & \cdots & f(GNC\_software\_state, cabin\_N_2\_temp) \end{bmatrix}$$

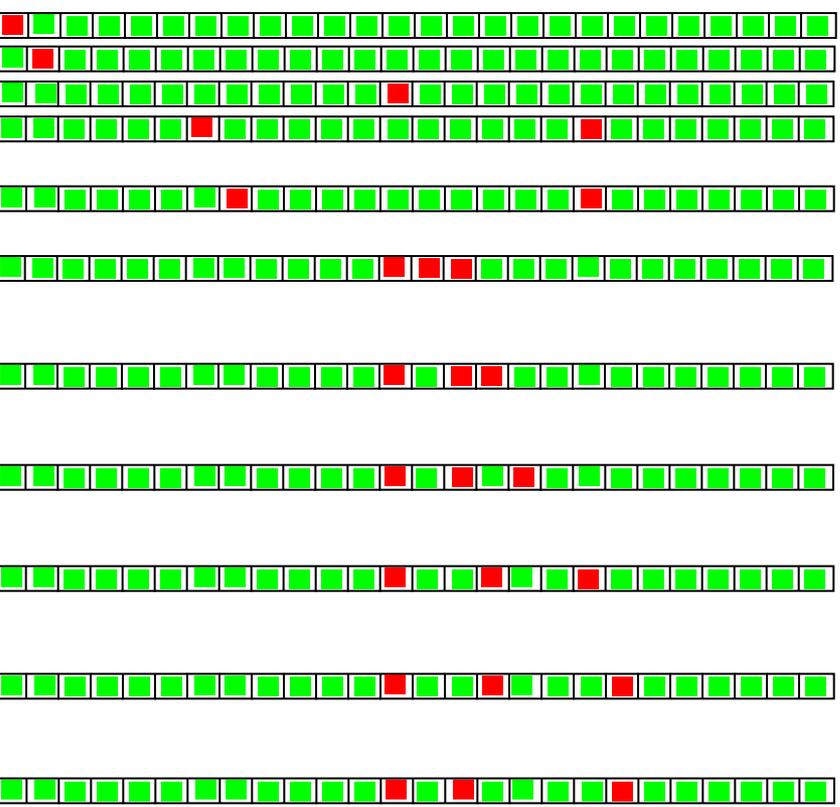
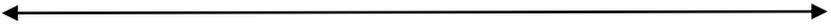


$$x=C^{\dagger}y$$

- 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*

Candidate Manager

---

Classes
Candidates
Assignments

Num	Rank	Time	Failures
0	1	1	n12.spdcard5=unknownFault
1	1	1	n12.sxbackpanel=unknownFault
2	2	2	cb_bia_23=unknownFault
3	2	1	n12.BIA1=unknownFault
		1	n12.spdcard0=unknownFault
4	2	1	n12.IOCU1=unknownFault
		1	n12.spdcard0=unknownFault
5	3	1	cc1.BIA1=unknownFault
		1	cc3.sxbackpanel=unknownFault
		1	cc2.BIA1=unknownFault
6	3	1	cc1.BIA1=unknownFault
		1	cc3.BIA1=unknownFault
		1	cc2.BIA1=unknownFault
7	3	1	cc1.BIA1=unknownFault
		1	cc3.BIA1=unknownFault
		1	cc2.IOCU1=unknownFault
8	3	1	cc1.BIA1=unknownFault
		1	cc3.IOCU1=unknownFault
		1	cc2.BIA1=unknownFault
9	3	1	cc1.BIA1=unknownFault
		1	cc3.IOCU1=unknownFault
		1	cc2.sxbackpanel=unknownFault
10	3	1	cc1.BIA1=unknownFault
		1	cc3.sxbackpanel=unknownFault
		1	cc2.sxbackpanel=unknownFault
11	3	1	cc1.sxbackpanel=unknownFault
		1	cc3.sxbackpanel=unknownFault

**Discrepant Commands and Observations**

```
test.cb_bia_23.port1 = B :0
test.n12.spdcard5.channel1 = C :0
```

CBFS: search found 20 candidate(s), more possible (searched 611)



# State Transition Matrix: A

- $\mathbf{x}' = \underline{\mathbf{A}}\mathbf{x} + \mathbf{B}\mathbf{u}$
- 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

$$A_{nom} = \begin{bmatrix} f(\Delta O2\_volume, O2\_volume) & \cdots & f(\Delta hydrazine\_volume, O2\_volume) \\ \vdots & \ddots & \vdots \\ f(\Delta O2\_volume, hydrazine\_volume) & \cdots & f(\Delta hydrazine\_volume, hydrazine\_volume) \end{bmatrix}$$

$$A_{FM} = \begin{bmatrix} f(\Delta pump\_state, pump\_state) & \cdots & f(\Delta SW_1\_state, pump\_state) \\ \vdots & \ddots & \vdots \\ f(\Delta pump\_state, SW_1\_state) & \cdots & f(\Delta SW_1\_state, SW_1\_state) \end{bmatrix}$$



# Loads Matrix: B

- $\mathbf{x}' = \mathbf{Ax} + \mathbf{Bu}$
- 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

$$B_{nom} = \begin{bmatrix} f(\Delta O2\_volume, turnon/off\_valve) & \cdots & f(\Delta hydrazine\_volume, turnon/off\_valve) \\ \vdots & \ddots & \vdots \\ f(\Delta O2\_volume, turnon/off\_scrubber) & \cdots & f(\Delta hydrazine\_volume, turnon/off\_scrubber) \end{bmatrix}$$

$$B_{FM} = \begin{bmatrix} f(\Delta pump\_state, turnon/off\_fuelpump) & \cdots & f(\Delta SW_1\_state, turnon/off\_fuelpump) \\ \vdots & \ddots & \vdots \\ f(\Delta pump\_state, turnon/off\_SW_1) & \cdots & f(\Delta SW_1\_state, turnon/off\_SW_1) \end{bmatrix}$$



# Gain Matrix: $\mathbf{K}$

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

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



# Nominal and FM K Matrix

$$K_{nom} = \begin{bmatrix} f(O2\_volume, turnon/off\_valve) & \cdots & f(hydrazine\_volume, turnon/off\_valve) \\ \vdots & \ddots & \vdots \\ f(O2\_volume, turnon/off\_scrubber) & \cdots & f(hydrazine\_volume, turnon/off\_scrubber) \end{bmatrix}$$

$$K_{FM} = \begin{bmatrix} f(pump\_state, turnon/off\_fuelpump) & \cdots & f(SW1\_state, turnon/off\_fuelpump) \\ \vdots & \ddots & \vdots \\ f(pump\_state, turnon/off\_SW1) & \cdots & f(SW1\_state, turnon/off\_SW1) \end{bmatrix}$$



# 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:  $\mathbf{x}' = \mathbf{Ax} + \mathbf{Bu}$

$$\begin{bmatrix} x'_1 \\ \vdots \\ x'_n \end{bmatrix} = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{bmatrix} \times \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} + \begin{bmatrix} b_{11} & \cdots & b_{1r} \\ \vdots & \ddots & \vdots \\ b_{n1} & \cdots & b_{nr} \end{bmatrix} \times \begin{bmatrix} u_1 \\ \vdots \\ u_r \end{bmatrix}$$

Observation equation:  $\mathbf{y} = \mathbf{Cx}$

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

Gain Equation:  $\mathbf{u}(\mathbf{t}) = -\mathbf{Kx}$

$$\begin{bmatrix} u_1 \\ \vdots \\ u_r \end{bmatrix} = - \begin{bmatrix} k_{11} & \cdots & k_{1r} \\ \vdots & \ddots & \vdots \\ k_{n1} & \cdots & k_{nr} \end{bmatrix} \times \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$$



# 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



# DRD 4 Controller Properties - 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

Property	Nominal Control	FM Control
Function Definition	Domain, Range in Reals	Finite State Machines/Table Lookup
Derivative of Function	Function Derivative or Difference	Finite State Transition
Integration of Function	Summation of Derivative	State Transition Path from Initial to Final State.
Modeling Primitive	Equation	Generalized Constraint (components)
System of Equations	System of Equations, Linear Algebra operations	Hierarchical Network of HW/SW components, modified Linear Algebra operations (symbolic inner-product methods).
Matrix Inverse Capabilities ( $x=C^{-1}y$ )	Fails – due to under /over constrained system	No failure! – part of FM architecture to handle.
Linearity Assumption: (scalability, superposition properties)	Foundation of MCT	Reflected into fault signatures/ responses which are independent. (i.e. multiple fault signatures are additive)
Solving for K (control policy).	Gradient descent search for minima or maxima	Search through parallel FSMs, enforcing temporal constraints



# 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

- [Weiner 1948] "Cybernetics: or Communication in the Animal and the Machine" – MIT Press
- [Kalman 1960] "A New Approach to Linear Filtering and Prediction Problems," Kalman, R.E., *ASME J. Basic Eng.*, vol. 82, pp.34-45, 1960.
- [Newell,Shaw,Simon 1958] "Report of a General Problem-Solving Program" The RAND Corporation, Carnegie Institute of Technology
- [Newell 1969] "Heuristic Programming: Ill-Structured Problems"
- [Sorenson 1970] "Least-squares estimation: from Gauss to Kalman" Sorenson, H. *IEEE Spectrum*, vol. 7, pp. 63-68, July 1970.
- [Mayr 1970] "Origins of Feedback Control" Otto Mayr 1970 MIT Press
- [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" 5<sup>th</sup> IFAC Conference
- [Lewis 1992] "A Brief History of Feedback Control", Chapter 1: Introduction to Modern Control Theory, F.L.Lewis, Prentice Hall 1992, <http://arri.uta.edu/acs/history.htm>
- [Johnson 1994] "VHM Generic Architecture" Dr. Stephen Johnson – personal communication
- [Leveson 1995] "Safeware – System Safety and Computers"
- [Åström and Wittenmark 1995] "Adaptive Control" 2<sup>nd</sup> Edition, Åström and Wittenmark 1995 Addison-Wesley Publishing Company
- [Williams, Nayak 1996] "A Model-based Approach to Reactive Self-Configuring Systems" AAI-96
- [Robinson 1997a] "Feedback to Basics" (AAAI) Fall Symposium Model-Directed Autonomous Systems
- [Robinson 1997b] "Autonomous design and execution of process controllers for untended scientific instruments", AGENTS '97 Proceedings of the first international conference on Autonomous agents, ACM
- [Dvorak et. al 2000] "Software Architecture Themes in JPL's Mission Data System" Dvorak, Rasmussen, Reeves, Sacks, IEEE Aerospace 2000 conference March 2000



# References II

- [Robinson 2001] “Automatic Overset Grid Generation with Heuristic Feedback Control” NASA/TM-2001-210931 November 2001.
- [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),
- [Brooks, 1986] Brooks, R.A., "A robust layered control system for a mobile robot", IEEE Journal of Robotics and Automation, Volume 2(1), 1986.
- [INM] “Sextant, Apollo Guidance and Navigation System” The Institute of Navigation – Navigation Museum” <cite http>
- [Nilsson 1984] Nilsson, Nils, “Shakey The Robot” SRI International Tech Report 1984
- [NPR-8705.2B] NASA Human-Rating Requirements for Space Systems