Intelligent-Controller Extensions to STPA

Dan “Mirf” Montes

Disclaimer

The views expressed in this document are those of the author and do not reflect the official position or policies of the United States Air Force, Department of Defense, or Government.

Massachusetts Institute of Technology

DRAPER LABORATORY

88ABW-2015-1004

All images courtesy of Google

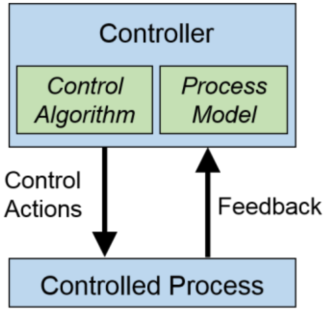
Overview

- Motivation
- Work
- Snapshot

Background

The increase of interacting humans and autonomous components in complex systems necessitates rigorous methods to classify information about the **controllers** in a system.

STPA, although advanced in terms of safety analysis, still oversimplifies the human's role in complex systems.



STPA Gaps

1) Detailed fundamental human-engineering considerations missing from the analysis

2) Controller process-model investigation does not capture higher levels of abstraction used in making robust and flexible decisions

3) No current method in the analysis to summarize the impact of social and organizational influences

Human Requirements

1) Detailed fundamental human-engineering considerations missing from the analysis

MIL-HDBK-1908B – Human Factors Definitions
MIL-STD-1472G – Human Engineering
MIL-STD-46855A – Human Engineering for the Military
MIL-HDBK-87213A – Visual Displays
MIL-STD-1787C – Display Symbology
MIL-STD-411F – Aircrew Alerts
MIL-STD-1797A – Flying Qualities
MIL-STD-1474D – Noise Limits
MIL-HDBK-516C – Airworthiness
Air Force HSI Handbook
Air Force HSI Pocket Guide
NASA HSI Overview

Standards

Guidance

Best Practices

STPA Gaps

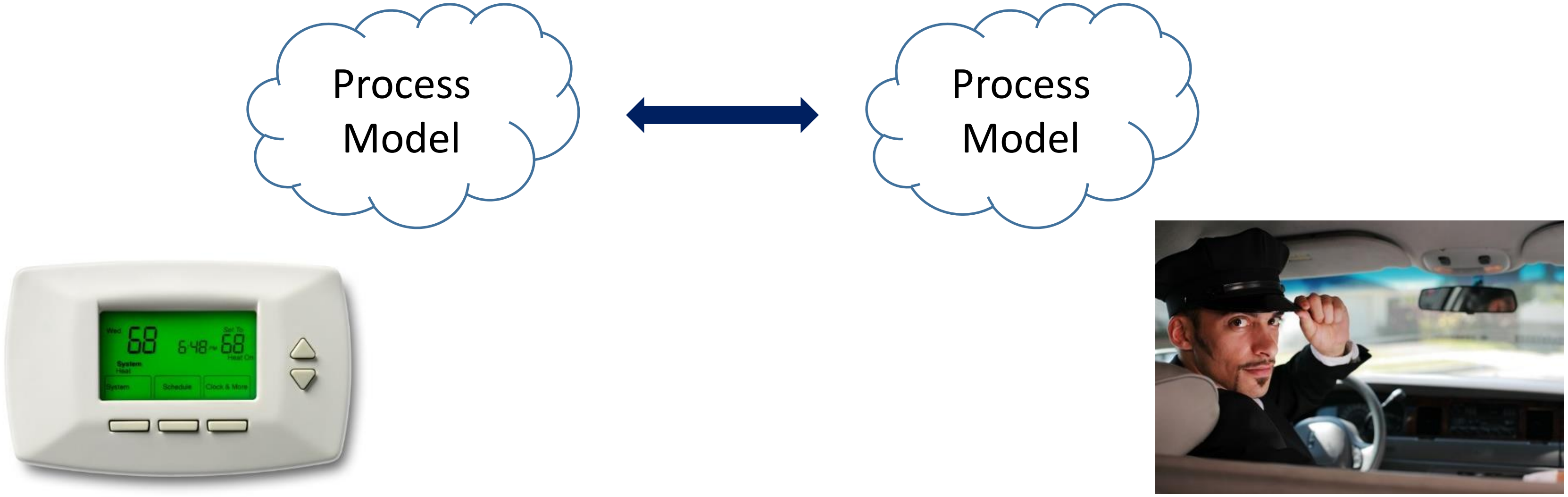
1) Detailed fundamental human-engineering considerations missing from the analysis

2) Controller process-model investigation does not capture higher levels of abstraction used in making robust and flexible decisions

3) No current method in the analysis to summarize the impact of social and organizational influences

More to the process model?

2) Controller process-model investigation does not capture higher levels of abstraction used in making robust and flexible decisions



Process Model

Process Model

Adapting in Systems

Optimized – System can satisfy fixed objectives in a fixed environment

Robust – System can satisfy fixed objectives and adapt to changes or uncertainties in the environment or the system itself

Flexible – System can also adapt to changes or uncertainties in objectives

Saleh et al., 2003

STPA Gaps

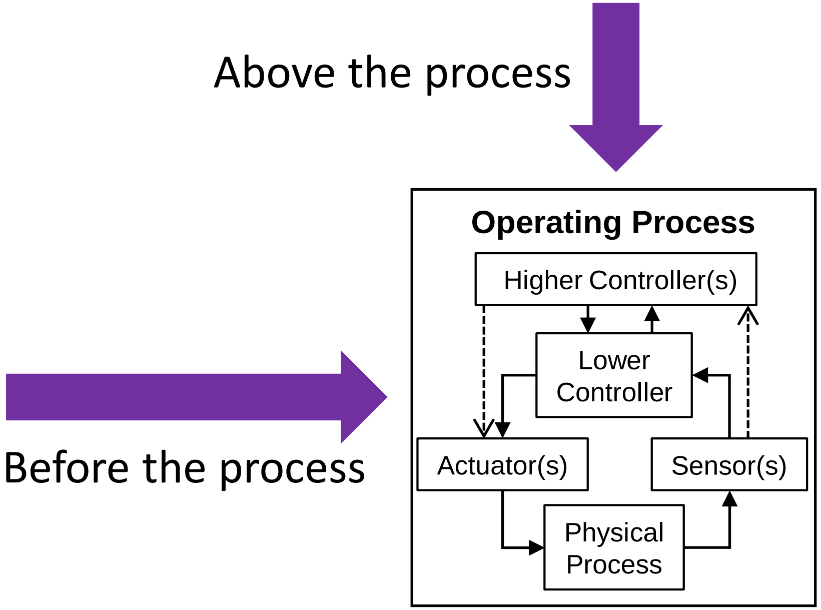
1) Detailed fundamental human-engineering considerations missing from the analysis

2) Controller process-model investigation does not capture higher levels of abstraction used in making robust and flexible decisions

3) No current method in the analysis to summarize the impact of social and organizational influences

Influences to the Controller

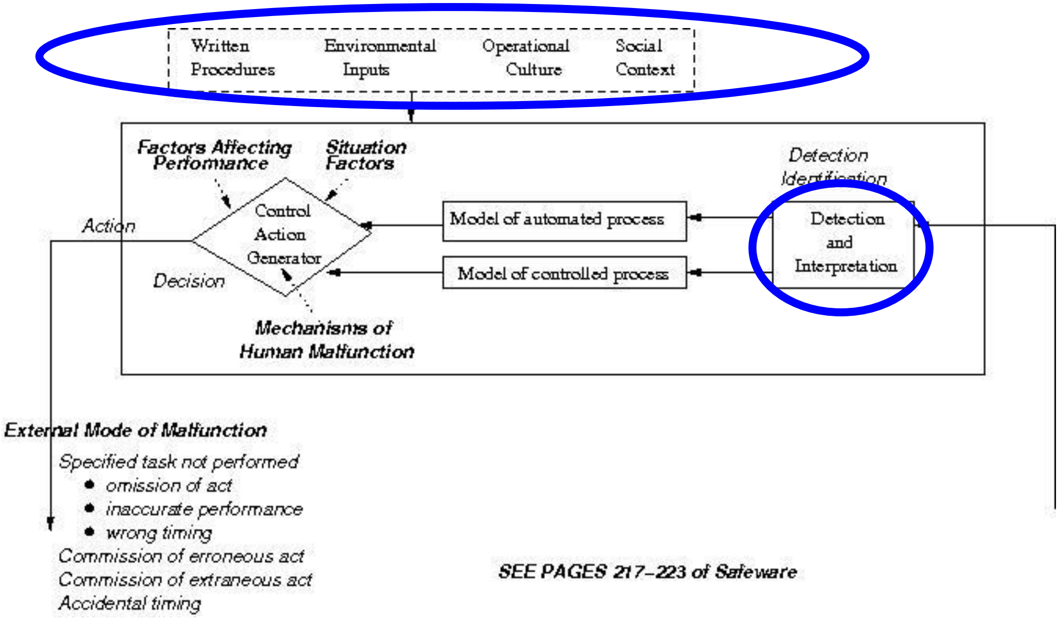
3) No current method in the analysis to summarize the impact of social and organizational influences from *outside* the operating process

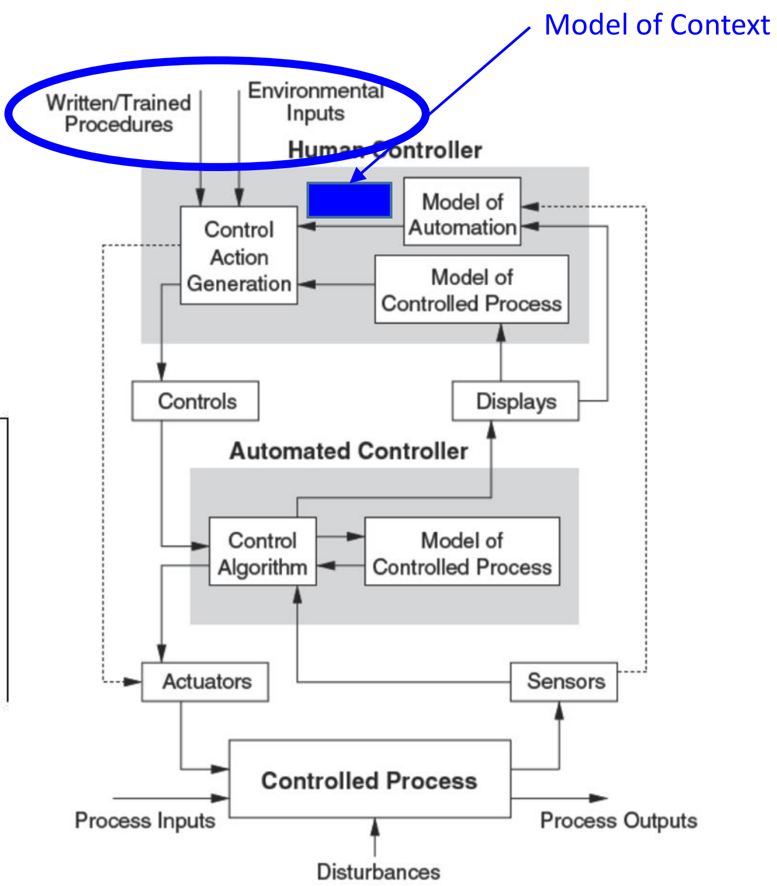


Objectives

- Recognize existing STPA human models & analyses
- Extend analysis to address STPA gaps
- Stay general to any controller

Previous Human Models

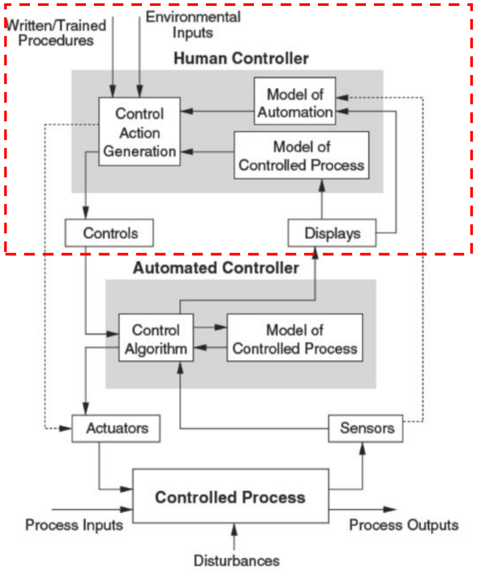

Written Procedures
Environmental Inputs
Operational Culture
Social Context
Factors Affecting Performance
Situation Factors
Control Action Generator
Action
Decision
Model of automated process
Model of controlled process
Detection Identification
Detection and Interpretation
Mechanisms of Human Malfunction
External Mode of Malfunction
Specified task not performed
omission of act
inaccurate performance
wrong timing
Commission of erroneous act
Commission of extraneous act
Accidental timing
SEE PAGES 217–223 of Safeware

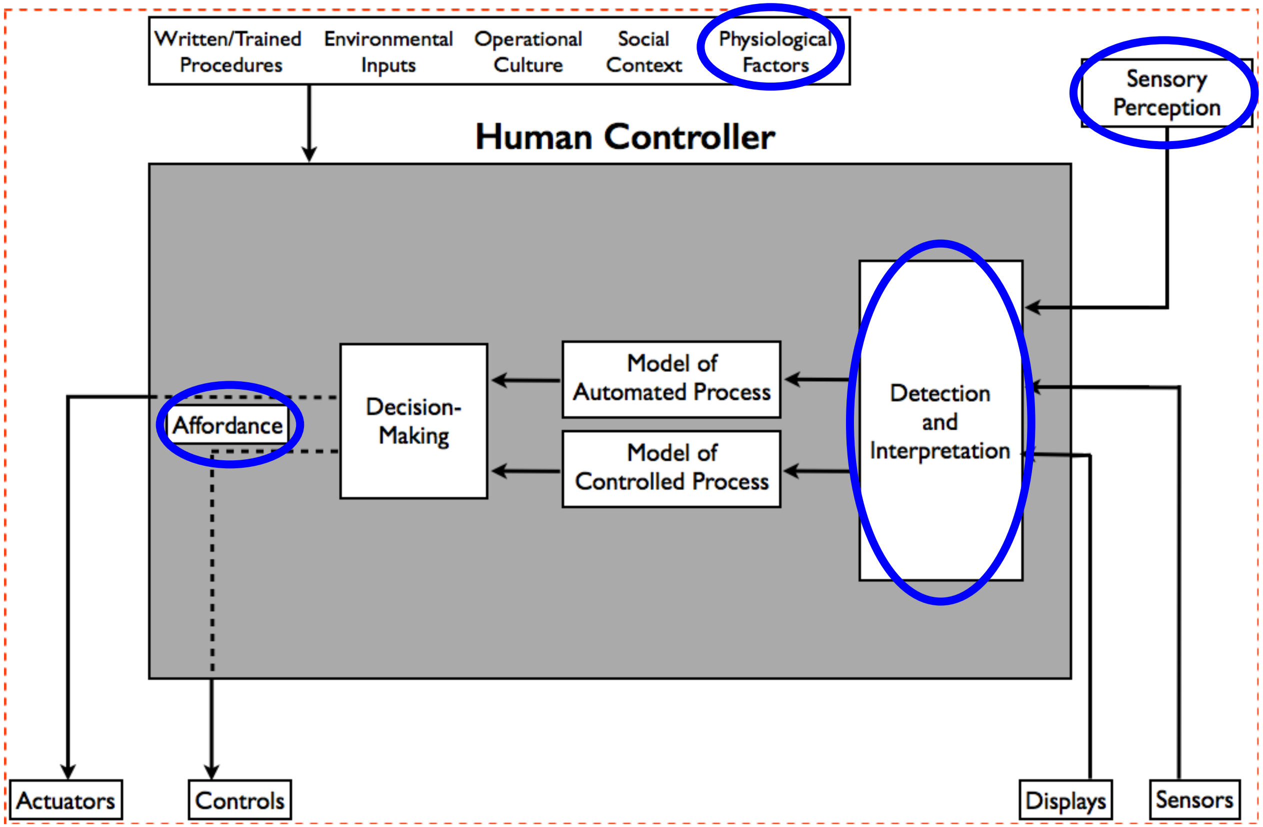


Leveson, Engineering a Safer World

Most Recent Model

Work

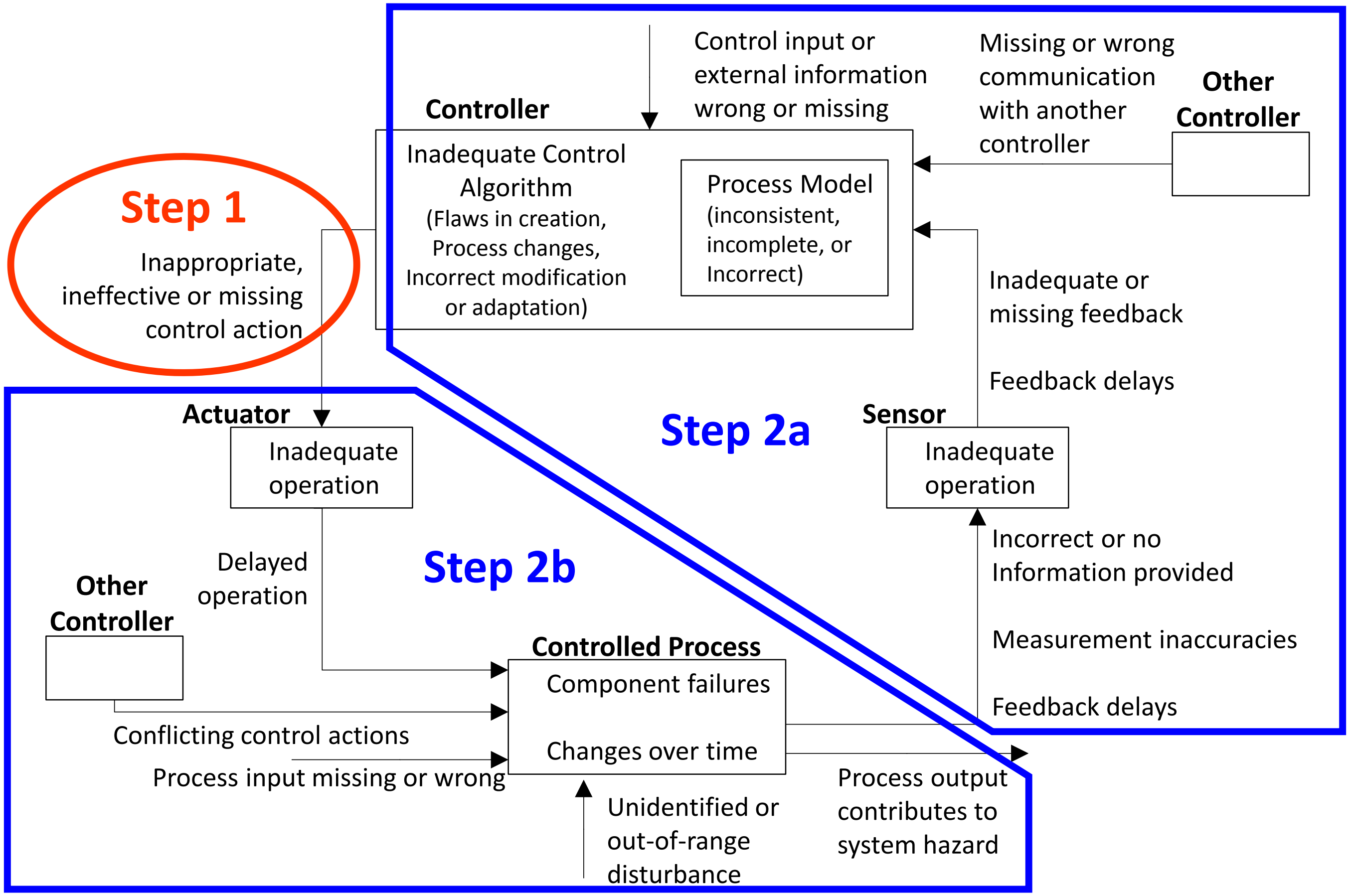




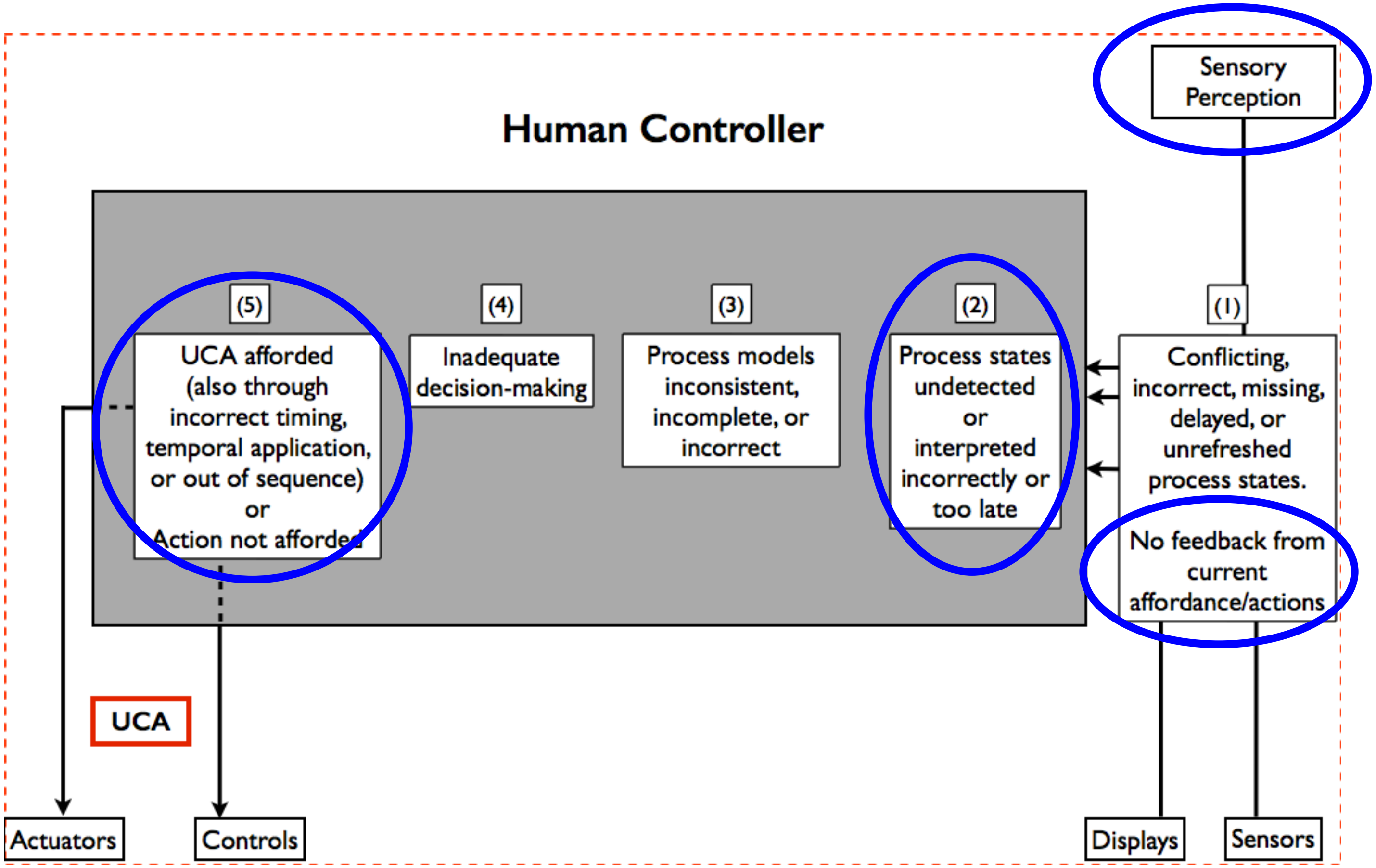
Thornberry, 2014

Human Analysis

Work


Step 1
Inappropriate, ineffective or missing control action
Controller
Control input or external information wrong or missing
Missing or wrong communication with another controller
Other Controller
Inadequate Control Algorithm
(Flaws in creation, Process changes, Incorrect modification or adaptation)
Process Model
(inconsistent, incomplete, or Incorrect)
Inadequate or missing feedback
Feedback delays
Step 2a
Actuator
Inadequate operation
Sensor
Inadequate operation
Incorrect or no Information provided
Measurement inaccuracies
Feedback delays
Step 2b
Delayed operation
Other Controller
Controlled Process
Component failures
Changes over time
Conflicting control actions
Process input missing or wrong
Unidentified or out-of-range disturbance
Process output contributes to system hazard

Most Recent Analysis

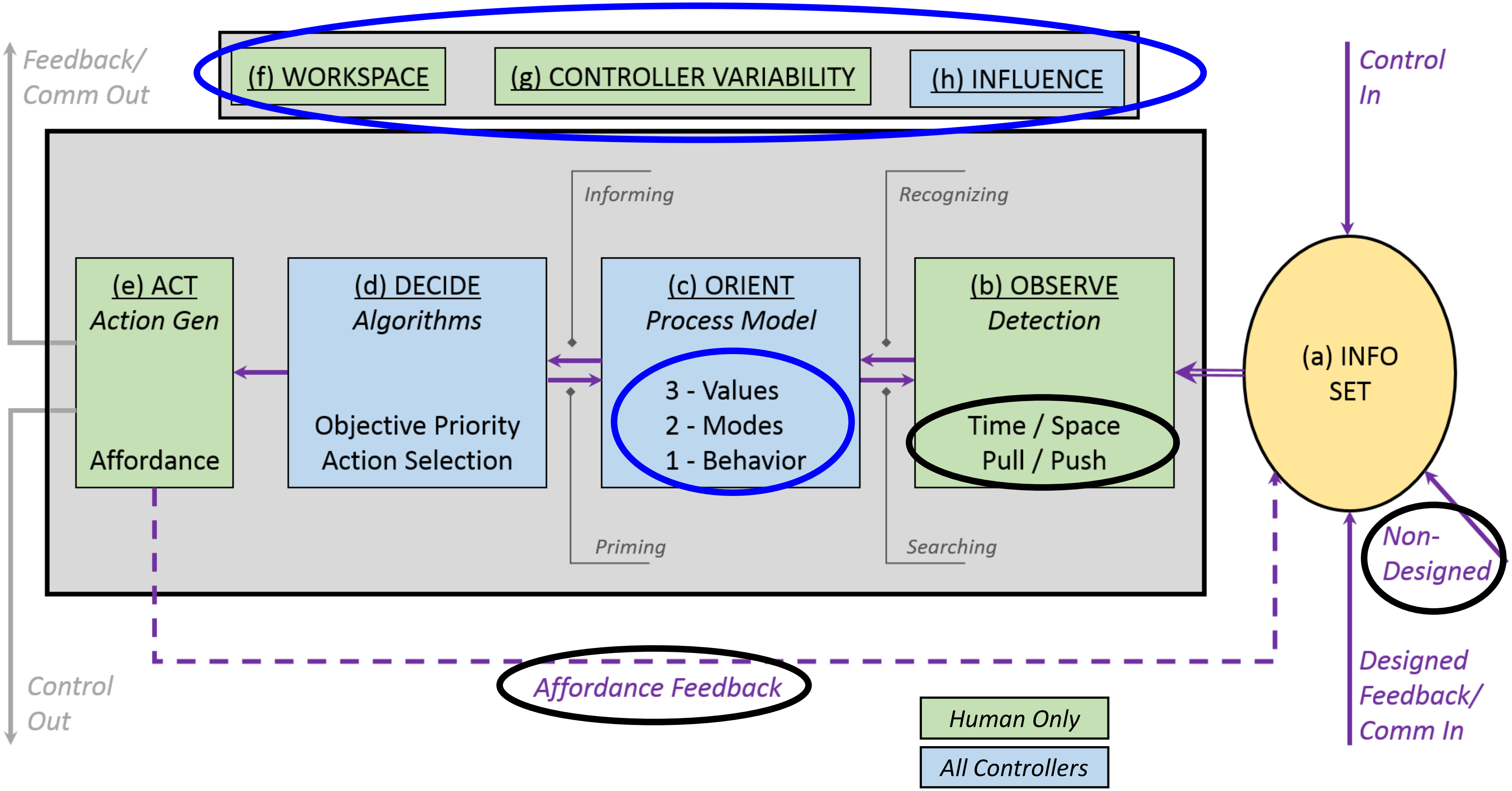

Sensory Perception
Human Controller
(5)
UCA afforded (also through incorrect timing, temporal application, or out of sequence) or Action not afforded
(4)
Inadequate decision-making
(3)
Process models inconsistent, incomplete, or incorrect
(2)
Process states undetected or interpreted incorrectly or too late
(1)
Conflicting, incorrect, missing, delayed, or unrefreshed process states.
No feedback from current affordance/actions
UCA
Actuators
Controls
Displays
Sensors

Thornberry, 2014

Extending the Analysis

- Address STPA gaps
- Add refinement to the controller investigation
- Maintain exhaustiveness

Analysis Extension



Process Model Investigation

Behavior

How the controlled process interacts with the environment

Model of Controlled Process

Mode

Mutually exclusive set of system behaviors

Model of Automation/Context

Value

Higher-level goals that are driving the local (safety) constraints

Means-Ends Relationships

Mode – Three Parts

Supervisory Structure	**The control relationships and communication links in the system hierarchy.**
	Which controllers currently have or share priority over each controlled component?
	Which controlled components may apply authority limits and under what circumstances? Can those limits be overridden? How will conflicts be decided (i.e., who should have the final authority?)
Component Operating Mode	**The set of algorithms that components under my control can use to exert control over their process(es).**
	What are the physical or logical assumptions and constraints associated with the component's current operating mode?
	What data in the information set is the controlled component using to inform its model?
	What input/and output format am I using with my controlled component(s)?
Mission Phase	**The specified set of related behaviors of the controlled system representing its operational state.**
	What mission phase is the system in (e.g., takeoff, cruise, etc.)
	Do all controllers know the current mission phase?
	Does a change in mission phase mode cause a change in supervisory structure and/or component operating modes (including input/output formats)?

Leveson, 1997

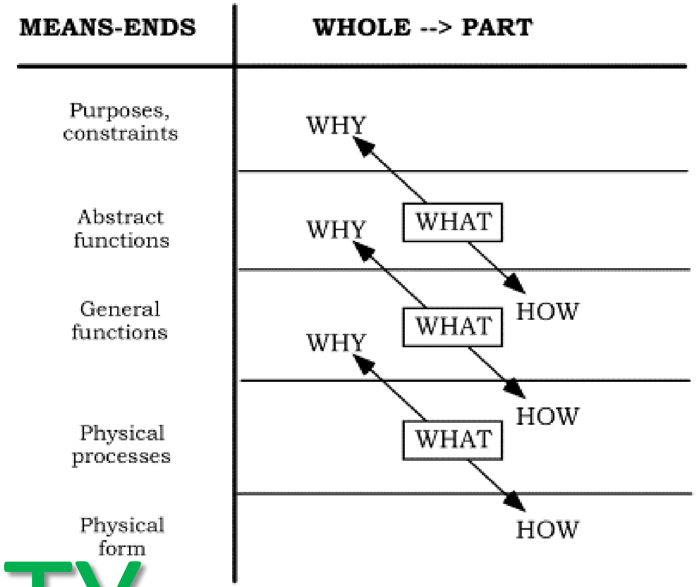
ROBUSTNESS

Values

What is the controller's understanding of how values at higher levels of the means-ends hierarchy map to objectives at the controller's level?

Are there any values the controller personally maintains that originate outside the system?

Example: "get-there-itis"



FLEXIBILITY

Rasmussen, 1994

Too Much Flexibility?

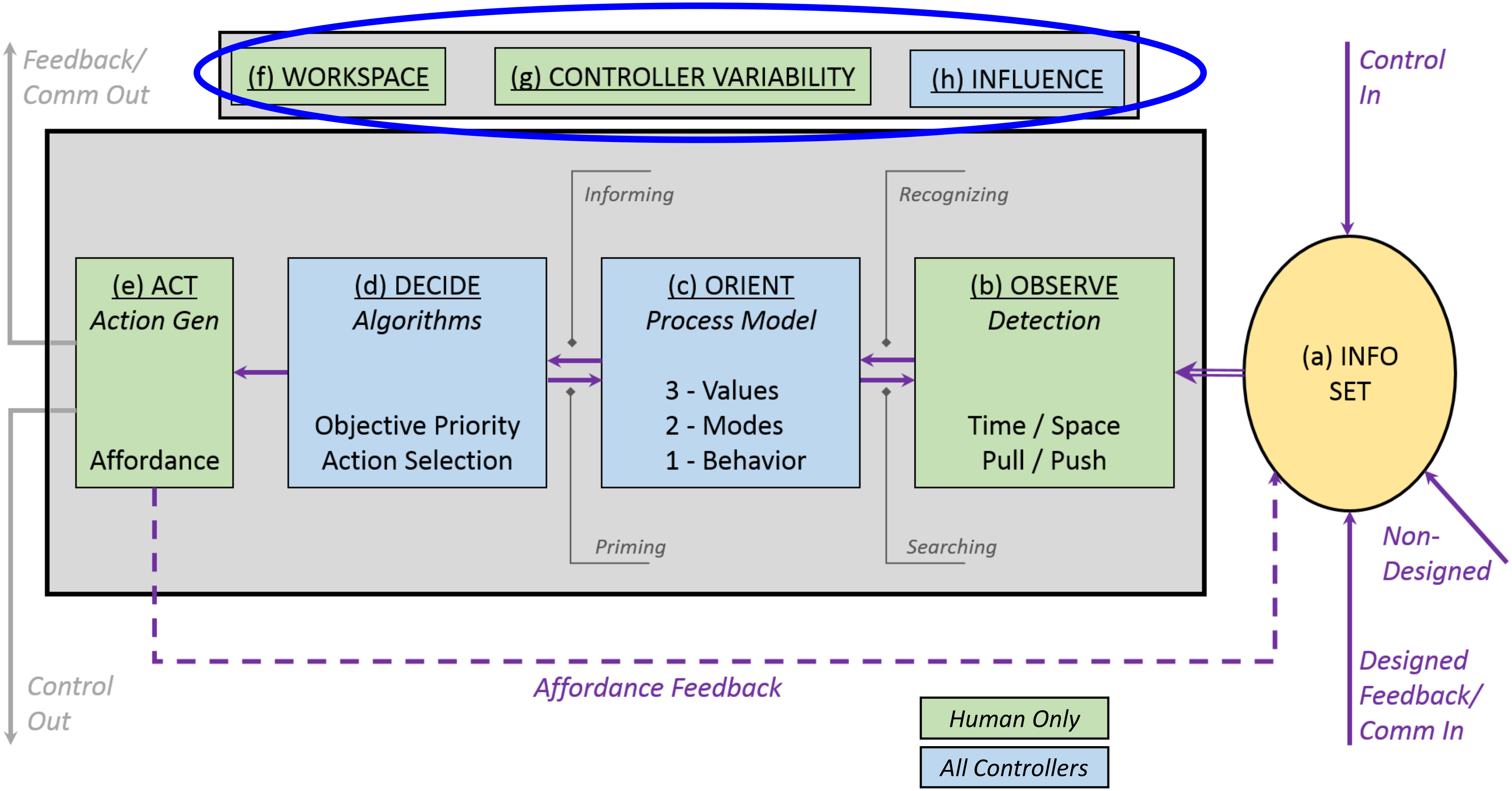
Exploratory behavior!

Normalization of deviance!

People might tradeoff performance of one behavior for another (or use modes in ways not intended by the designer)

This may inadvertently violate higher-level constraints that should not be violated

Extrinsic Factors



Just for Humans…

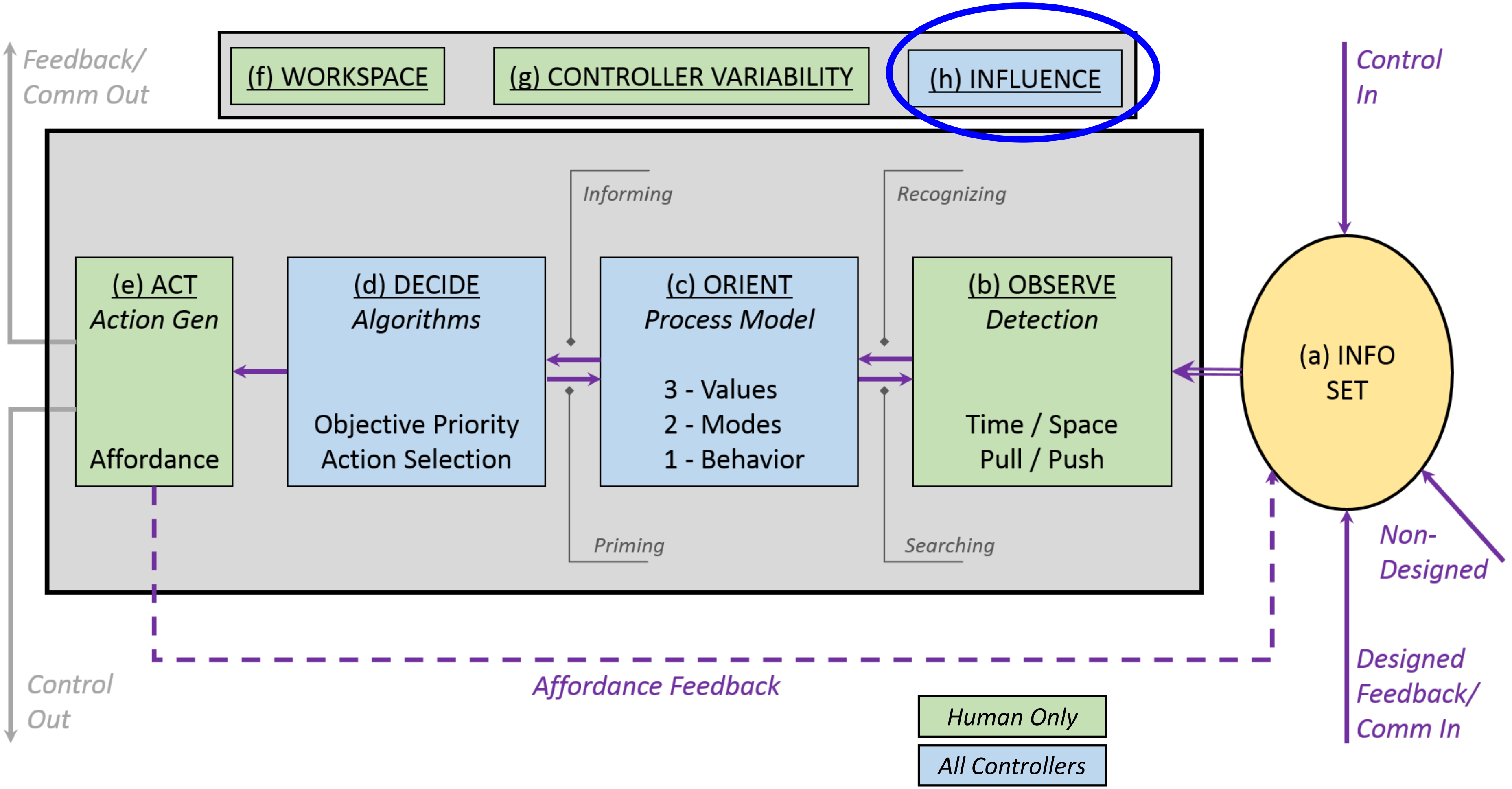
Workspace

- Climate (light, temp, noise)
- Physiology (inertial, vibrations)
- Anthropometry / ergonomics
- Task workload

Variability

- Age
- Perceptual acuity
- Natural attention capability
- Disposition
- Health, injury, disability, disease
- Psychological / emotional
- Fatigue, physical stress, sleep
- Drugs, medications

What is this?



Feedback/ Comm Out

(f) WORKSPACE

(g) CONTROLLER VARIABILITY

(h) INFLUENCE

Control In

Informing

Recognizing

(e) ACT
Action Gen
Affordance

(d) DECIDE
Algorithms
Objective Priority
Action Selection

(c) ORIENT
Process Model
3 - Values
2 - Modes
1 - Behavior

(b) OBSERVE
Detection
Time / Space
Pull / Push

(a) INFO SET

Priming

Searching

Non-Designed

Control Out

Affordance Feedback

Designed Feedback/ Comm In

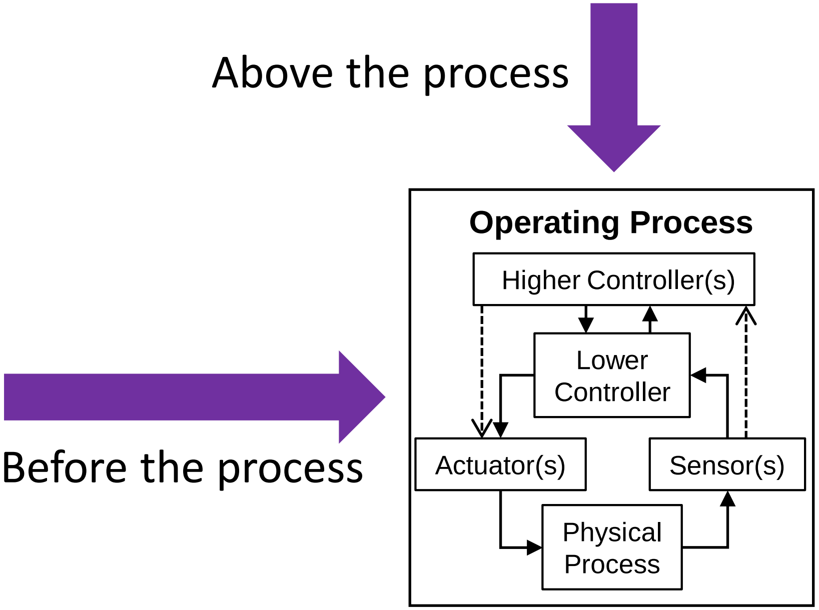
🟩 *Human Only*

🟦 *All Controllers*

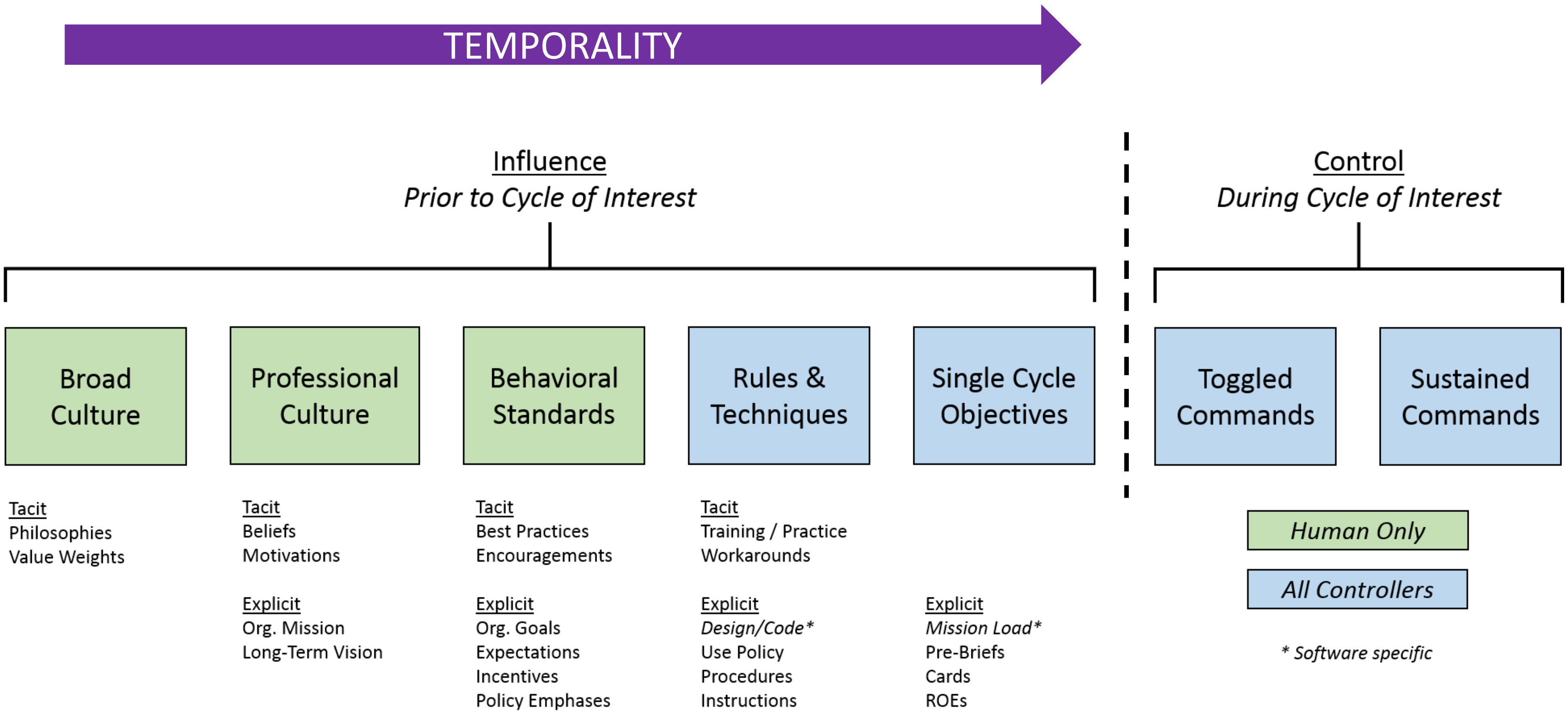
Influence

Above the process

Before the process



Influence



TEMPORALITY

Influence
Prior to Cycle of Interest

Control
During Cycle of Interest

Broad Culture

Professional Culture

Behavioral Standards

Rules & Techniques

Single Cycle Objectives

Toggled Commands

Sustained Commands

Broad Culture

Tacit
Philosophies
Value Weights

Professional Culture

Tacit
Beliefs
Motivations

Explicit
Org. Mission
Long-Term Vision

Behavioral Standards

Tacit
Best Practices
Encouragements

Explicit
Org. Goals
Expectations
Incentives
Policy Emphases

Rules & Techniques

Tacit
Training / Practice
Workarounds

Explicit
*Design/Code**
Use Policy
Procedures
Instructions

Single Cycle Objectives

Explicit
*Mission Load**
Pre-Briefs
Cards
ROEs

🟩 *Human Only*

🟦 *All Controllers*

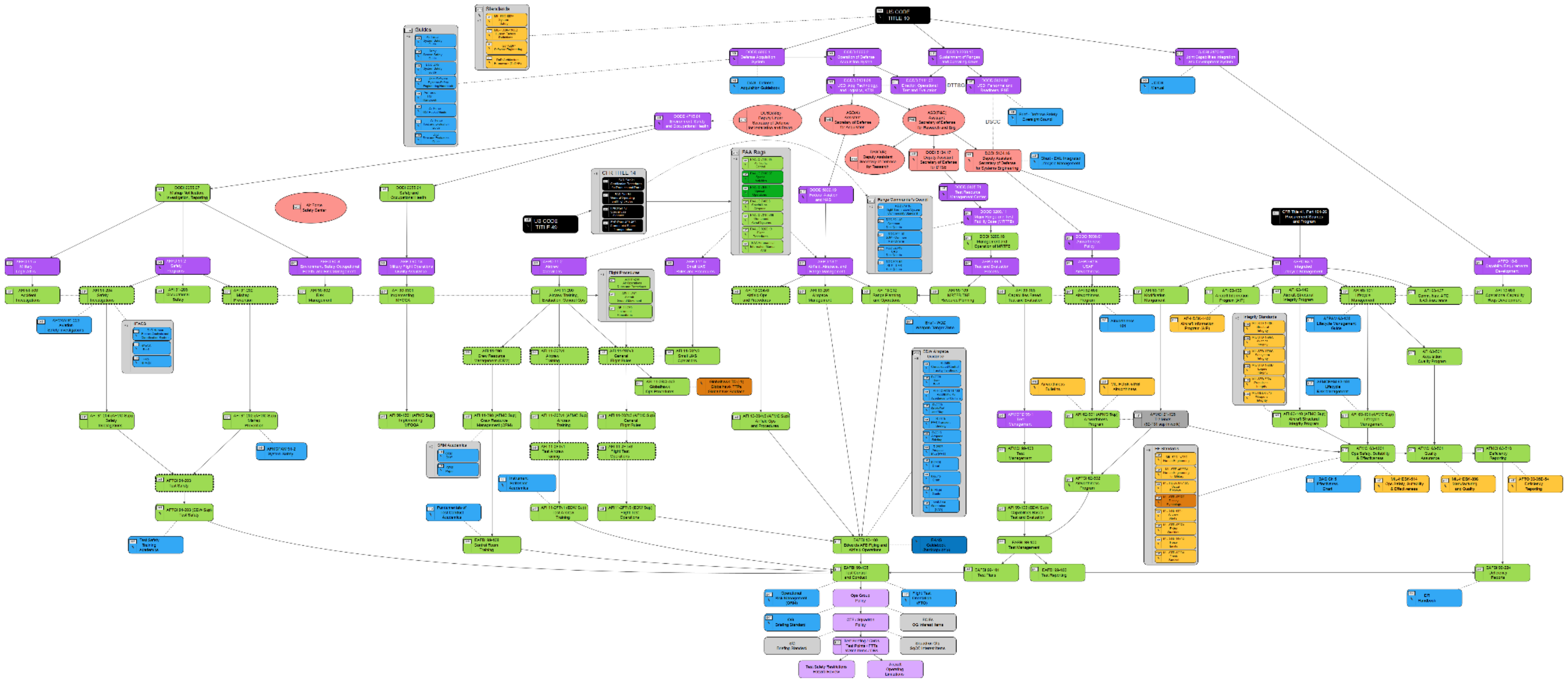
** Software specific*

AF HSI Handbook (2009)

- Personnel
  - Selection, attributes (e.g., acuity, cognition), background, skills
- Training – tactics, decision-making
- Human Factors
  - Workload, workspace, displays, anthro/ergo, automation
- Habitability
  - Living conditions, sleep, stress
- Environment/OSHA/Safety
  - HAZMAT, noise, moving parts, wiring

Explicit-Influence Map

Snapshot

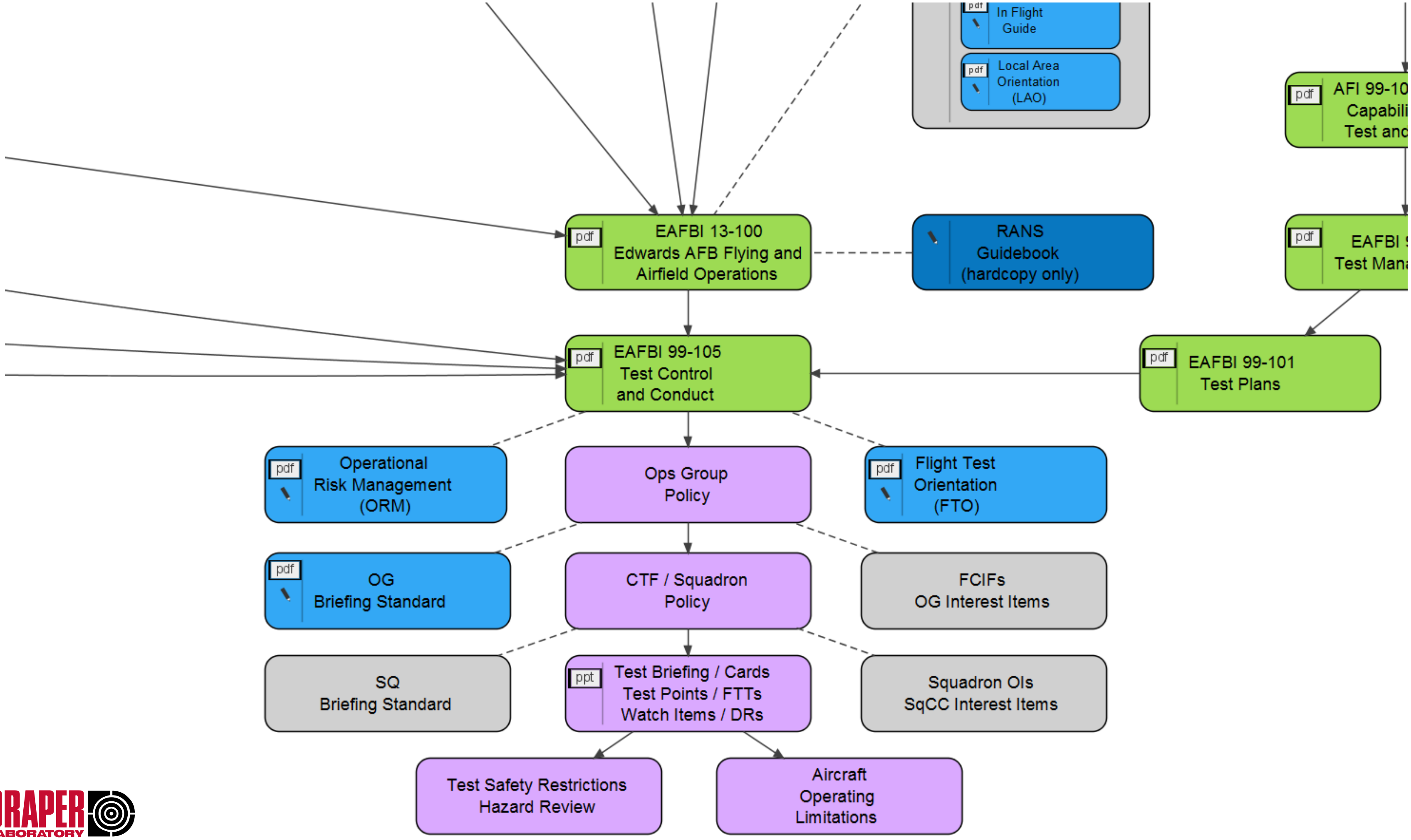


Standards
Guides
US CODE TITLE 10
DODD 5000.01 Defense Acquisition System
DODI 5000.02 Operation of Defense Acquisition System
Sustainment of Ranges and Operating Areas
Defense Acquisition Guidebook
USD Acq, Technology and Logistics, AT&L
Director, Operational Test and Evaluation
DTTSG
USD Personnel and Readiness, P&R
Deputy Under Secretary of Defense for Installation and Environment
ASD(A) Assistant Secretary of Defense for Acquisition
ASD(R&E) Assistant Secretary of Defense for Research and Eng
DSOC
Defense Safety Oversight Council
Deputy Assistant Secretary of Defense for Research
DODI 5134.17 Deputy Assistant Secretary of Defense for DT&E
DODI 5134.16 Deputy Assistant Secretary of Defense for Systems Engineering
DAU Integrated Program Management
FAA Regs
DODD 5030.19 Federal Aviation and NAS
Range Commander's Council
Test Resource Management Center
Major Range and Test Facility Base (MRTFB)
CFR TITLE 14
US CODE TITLE 49
CFR Title 41, Part 101-26
Flight Procedures
DODI 6055.07 Mishap Notification, Investigation, Reporting
Air Force Safety Center
DODI 6055.04 Safety and Occupational Health
Military
Safety Programs
Environment, Safety Occupational Health and Risk Management
Military Flight Operations Quality Assurance
AFI 51-503 Accident Investigations
AFI 91-204 Safety Investigations
AFI 91-202 Occupational Safety
AFI 91-202 Mishap Prevention
AFI 90-802 Risk Management
AFI 90-1301 Implementing MFOQA
Aviation Safety Investigations
IFACG
Integrity Standards
EAFBI 13-100 Edwards AFB Flying and Airfield Operations
RANS Guidebook
EAFBI 99-105 Test Control and Conduct
EAFBI 99-101 Test Plans
Operational Risk Management (ORM)
Ops Group Policy
Flight Test Orientation (FTO)
OG Briefing Standard
CTF / Squadron Policy
OG Interest Items
SQ Briefing Standard
Test Points / FTTs
Squadron CC SqCC Interest Items
Test Safety Restrictions
Aircraft Operating Limitations

© drm

Where it meets the road...

Snapshot



In Flight Guide

Local Area Orientation (LAO)

AFI 99-10
Capabili
Test anc

EAFBI 13-100
Edwards AFB Flying and
Airfield Operations

RANS
Guidebook
(hardcopy only)

EAFBI 9
Test Man

EAFBI 99-105
Test Control
and Conduct

EAFBI 99-101
Test Plans

Operational
Risk Management
(ORM)

Ops Group
Policy

Flight Test
Orientation
(FTO)

OG
Briefing Standard

CTF / Squadron
Policy

FCIFs
OG Interest Items

SQ
Briefing Standard

Test Briefing / Cards
Test Points / FTTs
Watch Items / DRs

Squadron OIs
SqCC Interest Items

Test Safety Restrictions
Hazard Review

Aircraft
Operating
Limitations

Conclusion

- Gaps addressed
  - ✓ Human-engineering considerations
  - ✓ Process model
  - ✓ Socio-organizational and pre-cycle influences

- Any good SE management system can identify, document, and maintain the information elicited with the extended analysis

Special thanks to

Dr. Cody Fleming

Ms. Aubrey Samost

Mr. Dajiang Suo

Mr. Adam Williams