

2021 SYSTEM THEORETIC ACCIDENT MODEL AND PROCESSES (STAMP) WORKSHOP

JUNE 22, 2019

SECURITY POLICY & SYSTEM-THEORETIC PROCESS ANALYSIS FOR SECURITY (STPA-SEC)

William Young, Jr (PhD)

WILLIAM.YOUNG.3@US.AF.MIL ; WYOUNG@MIT.EDU ; WEYOUNG@SYR.EDU

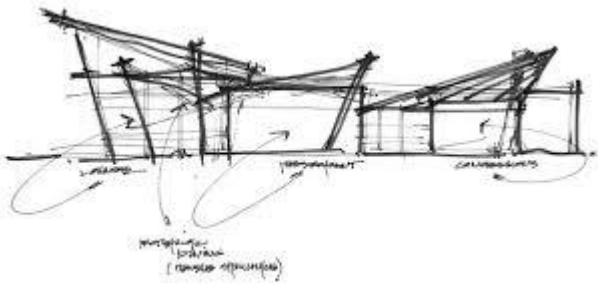
Acknowledgement & Disclaimer

The views expressed in this presentation are those of the presenter and do not reflect the official policy or position the United States Air Force, the United States Department of Defense, or the United States Government

The Following is New Material Representing Insights Gained Applying STPA-Sec on Real-World Projects over the last 12 Months

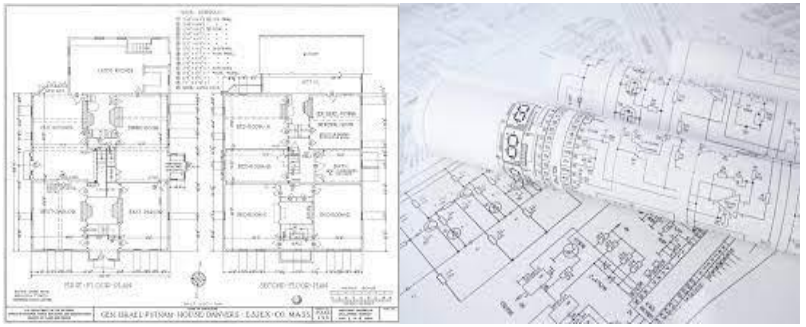
Bottom Line Up Front (BLUF)

- Security architecture is the collection of hardware, software, processes, etc that work together to **protect** something
- Security architectures implement & enforce security policy (rules defining "security" for given ConOps & specifying secure behavior)
- Security architecture will only be as effective (at best) as the security policy it implements (most losses are policy-related)
- STPA-Sec allows stakeholders to find and fix deficiencies in policy **before** adversaries find and exploit them in the architecture



Sketch of Security Policy (STPA-Sec)

Control Plane (Abstraction)



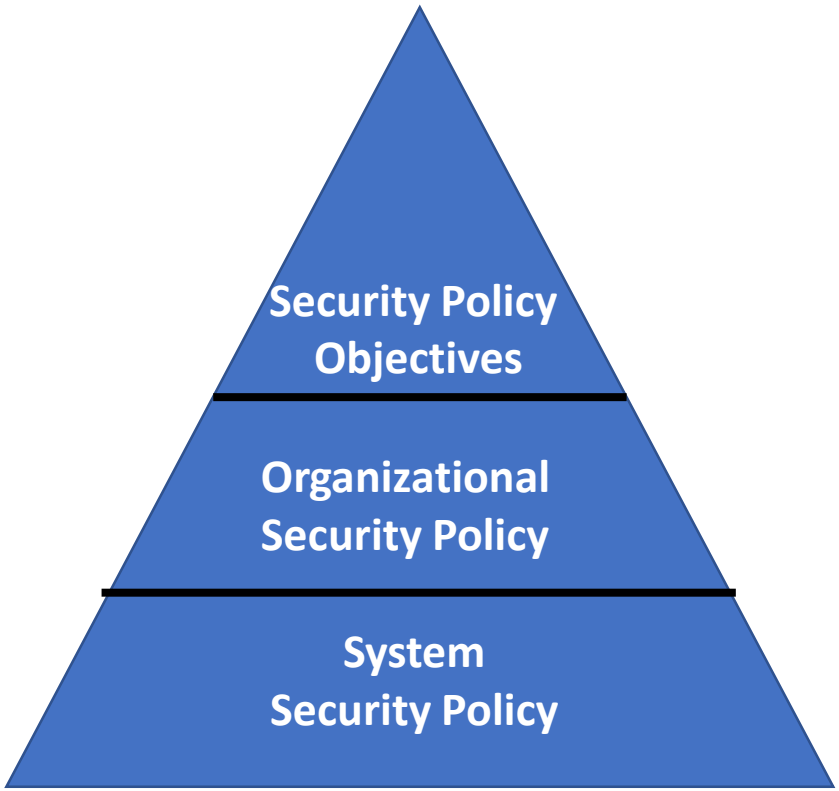
Security Architecture Blueprints (Digital Engineering)

Physical & Data Plane (Real World)

Security Policy Example: Pre-911 Airport Screening

Attackers Most Often Defeat Your Security Policy, Not Your Technology (Security Architecture)

Security Policy is Main Element of the **Concept of Secure Function*** for a Given Business or Mission ConOp



+

3 classes of "rules"

An informal model of how rule enforcement is intended to "work"

Concept of Secure Function Identifies What Things Within the ConOp Must Be Protected and How They Will be Protected

*Definition: A strategy for achievement of secure system function that embodies proactive and reactive protection capability of the system (NIST).

Problem Framework

- Goal / Purpose
- Unacceptable Losses

Analysis / Synthesis

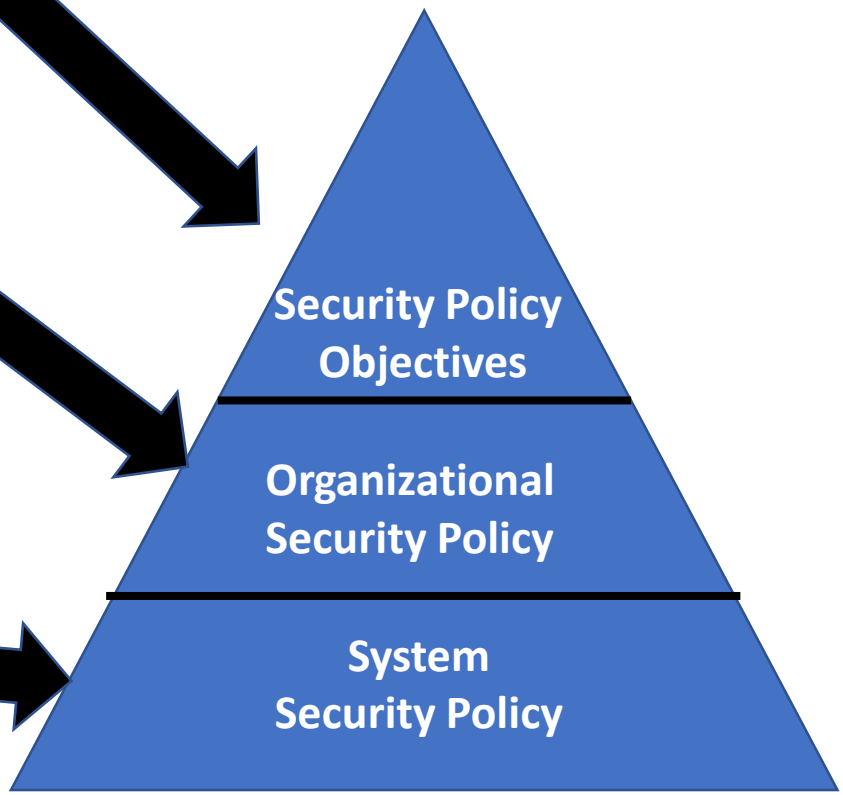
Functional Framework

- Hazards
- Control Structure
- Hazardous Control Actions
- Constraints / Control Requirements

Analysis / Synthesis

Enterprise Architecture

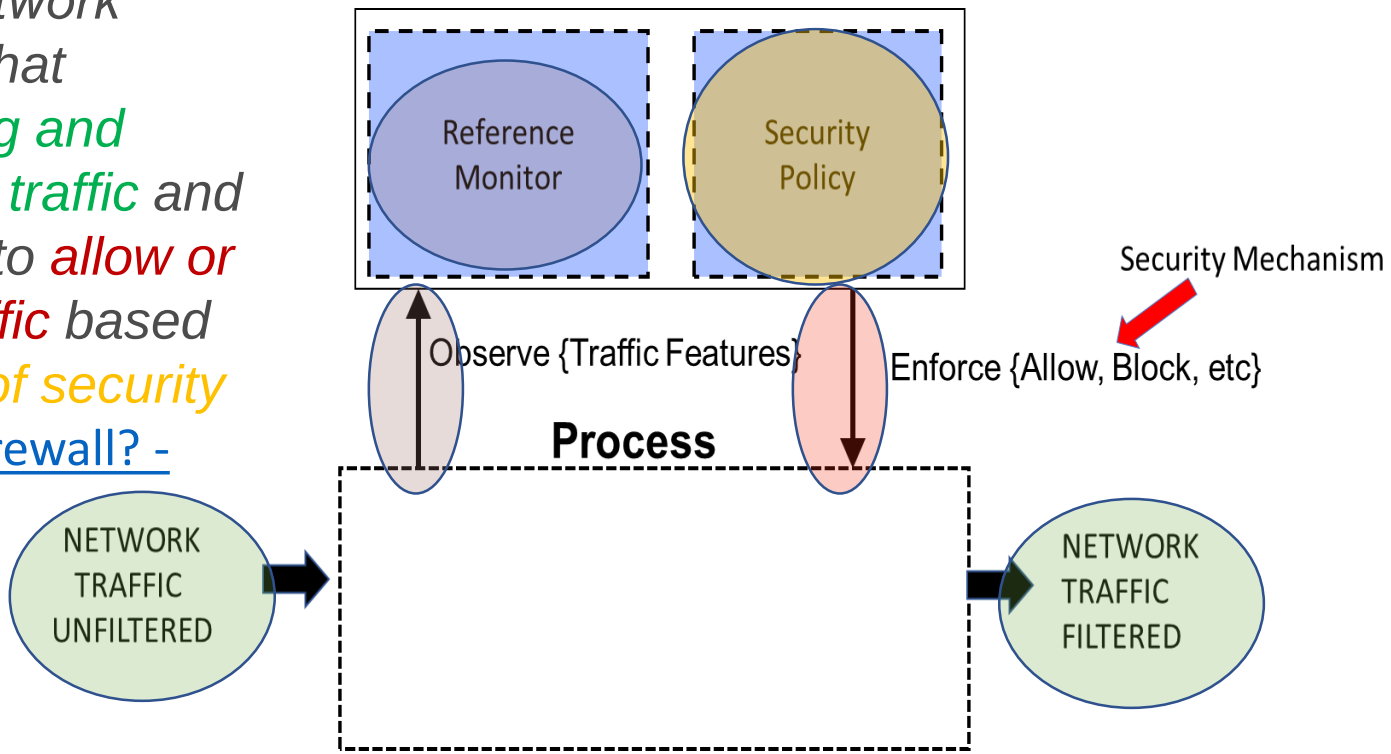
- Components, Connections, Flows
- Disruption Scenarios (Adversary, Accident, Nature)
- Initial Control Set
- Wargame
- Refine



STPA-Sec Maps to the 3 Classes of Policy

Modelling a Firewall As Part of A Network's Policy Enforcement Architecture

"A firewall is a network ***security*** *device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules"* What Is a Firewall? - Cisco

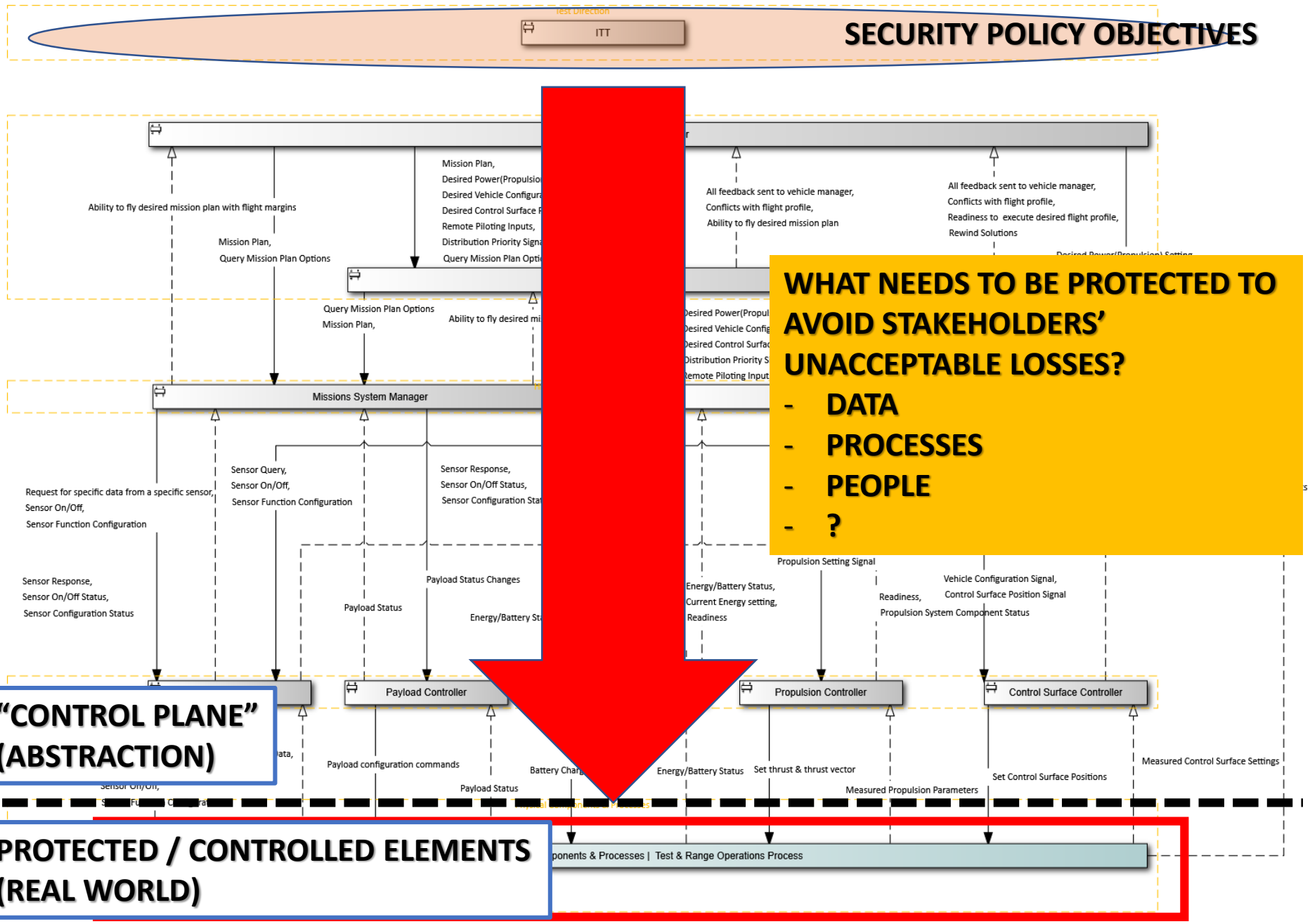


Control Structure Can Be Used to Model Security Policy Enforcement (and Required Security Architecture Behavior)

Ref: www. cisco.com/c/en/us/products/security/firewalls/

Let’s Look at a Real World Example: eVTOL Aircraft Design

SECURITY POLICY OBJECTIVES

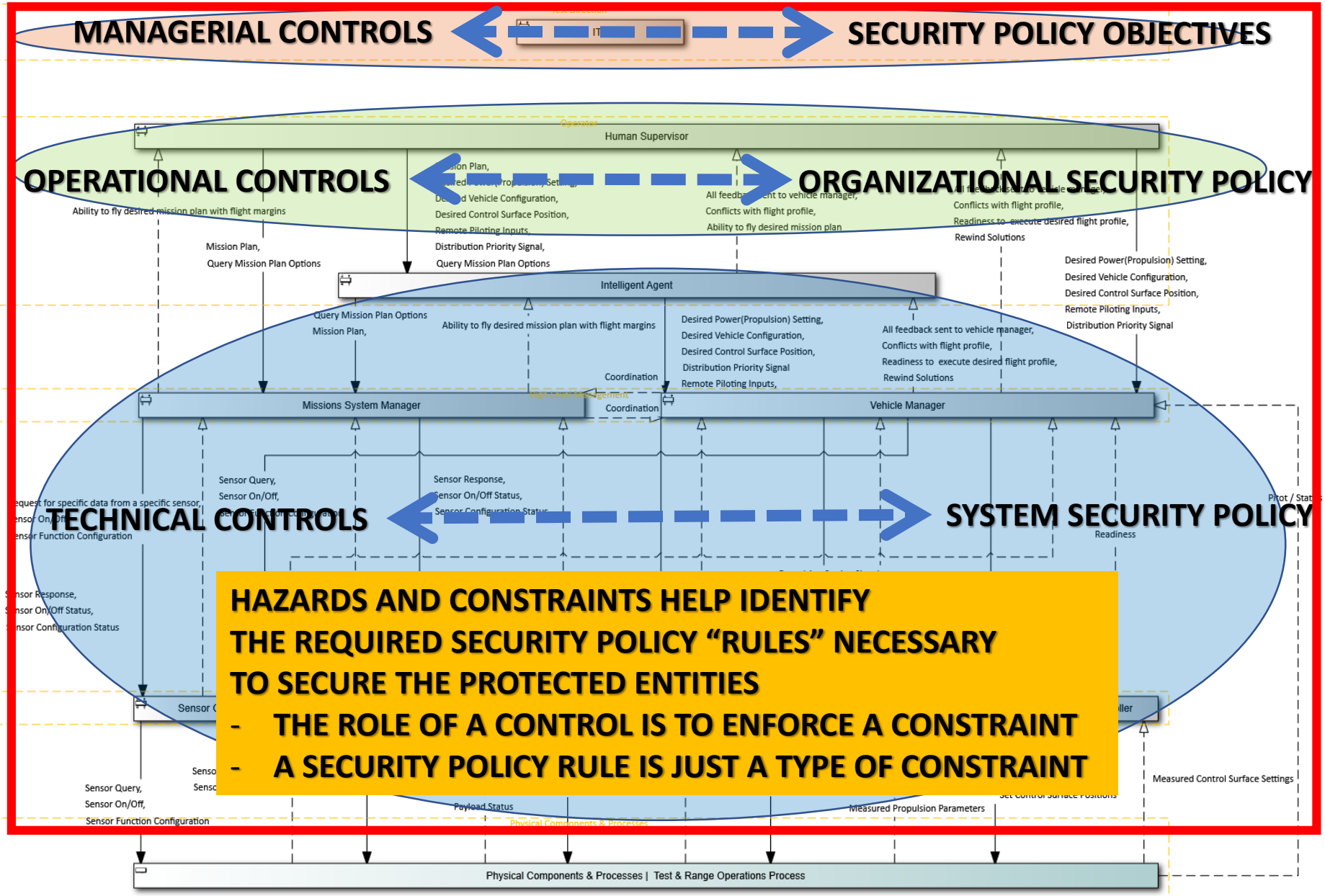


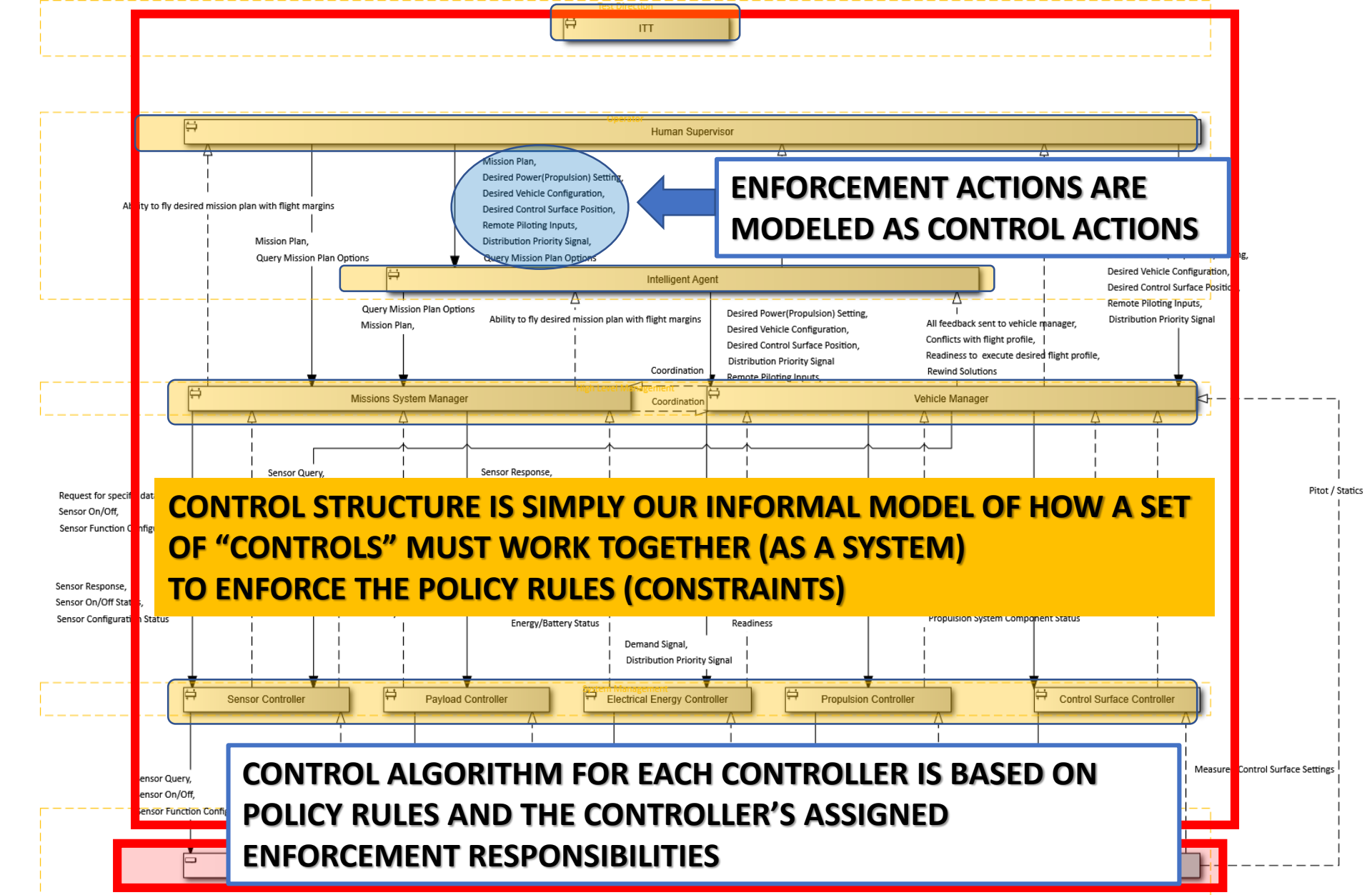
WHAT NEEDS TO BE PROTECTED TO AVOID STAKEHOLDERS' UNACCEPTABLE LOSSES?

- DATA
- PROCESSES
- PEOPLE
- ?

"CONTROL PLANE" (ABSTRACTION)

PROTECTED / CONTROLLED ELEMENTS (REAL WORLD)


MANAGERIAL CONTROLS
SECURITY POLICY OBJECTIVES
OPERATIONAL CONTROLS
ORGANIZATIONAL SECURITY POLICY
TECHNICAL CONTROLS
SYSTEM SECURITY POLICY
Human Supervisor
Intelligent Agent
Missions System Manager
Vehicle Manager
Coordination
Ability to fly desired mission plan with flight margins
Mission Plan,
Query Mission Plan Options
Desired Power(Propulsion) Setting,
Desired Vehicle Configuration,
Desired Control Surface Position,
Remote Piloting Inputs,
Distribution Priority Signal
All feedback sent to vehicle manager,
Conflicts with flight profile,
Readiness to execute desired flight profile,
Rewind Solutions
Sensor Query,
Sensor On/Off,
Sensor Function Configuration
Sensor Response,
Sensor On/Off Status,
Sensor Configuration Status
Payload Status
Measured Propulsion Parameters
Measured Control Surface Settings
Physical Components & Processes | Test & Range Operations Process
HAZARDS AND CONSTRAINTS HELP IDENTIFY
THE REQUIRED SECURITY POLICY “RULES” NECESSARY
TO SECURE THE PROTECTED ENTITIES
- THE ROLE OF A CONTROL IS TO ENFORCE A CONSTRAINT
- A SECURITY POLICY RULE IS JUST A TYPE OF CONSTRAINT



Control Structure is a Way to Model Our Security Policy…Before We Implement it in a Security Architecture

Summary

- Most losses are actually policy problems, NOT technology problems
- Losses occur due to incomplete, conflicting, flawed, and/or ineffective security policy
- Security architecture implements (enforces) security policy
- STPA-Sec provides a way to bring security engineering into the concept stage of the engineering lifecycle (through development and analysis of the Concept of Secure Function)
- STPA-Sec allows stakeholders to model and improve their security policy before attempting to build the security architecture

Applying STPA-Sec to Security Policy Development and Analysis Provides a Strategy Perspective to Complement Existing Tactics

Questions?

- My Contact Information
  - Gov't: William.Young.3@US.AF.Mil
  - Academic / Industry: WYOUNG@MIT.edu or WEYoung@Syr.edu