United States Air Force Warfare Center

Testing-Tactics - Training-Innovation-Integration

Leveraging Secure Systems Analysis to Generate Testable Cybersecurity Requirements

Col William "$" Young, PhD
Commander, 53d EW Group
8 Mar 2018

This Briefing is:
UNCLASSIFIED

DISCLAIMER:

The views expressed in this presentation are are those of the presenter and do not reflect the official policy or position of the 53d Wing, United States Air Force, Department of Defense, Air Combat Command, MIT Lincoln Laboratory, Syracuse University, or the U.S. Government

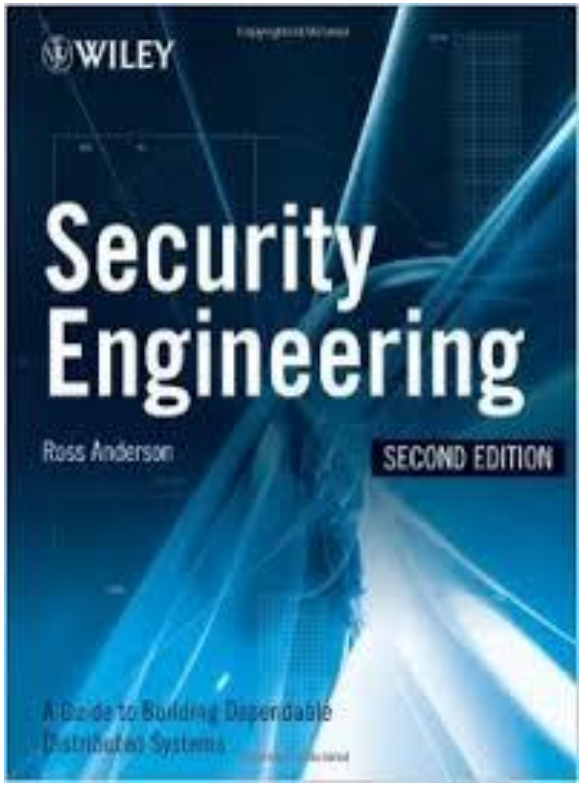
Overview

- **Framework – Establishing a foundation to aid our thinking / reasoning about cybersecurity testing**
- **Model – A useful abstraction capturing the mechanism for losses we want to prevent**
- **Secure Systems Analysis – Using STPA-Sec to generating testable (functional) requirements?**
- **Does it work?**

This Won't Necessarily Replace Anything You Do, but Will Probably Make Everything You Do Better!

Framing the Security Problem Provides the Foundation for Effective Test

- Determining life cycle security concepts
- Defining & specifying security objectives
- Defining & specifying functional security requirements
- Determining measures of success

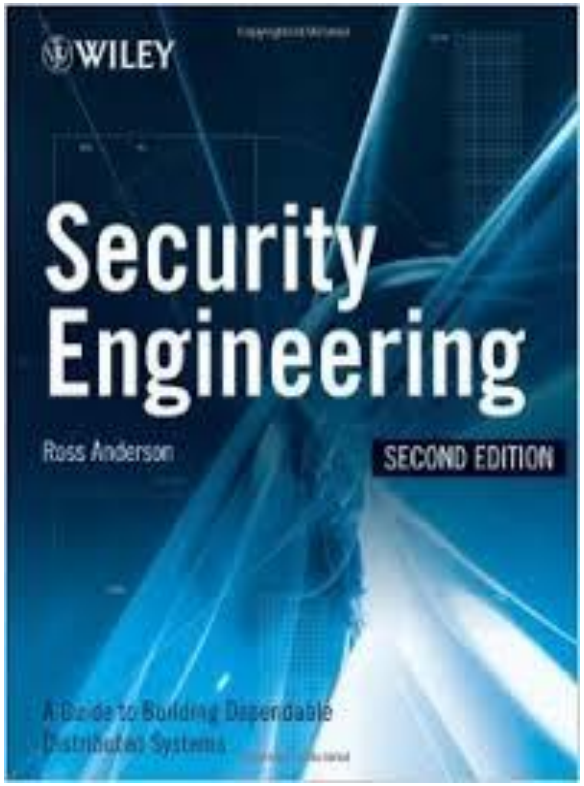


"Many systems fail because their designers protect the wrong things, or protect the right things in the wrong way" – Ross Anderson "Security Engineering"

You Cannot Effectively Test the Solution (Architecture) To A Problem You Do Not Understand

Framing the Security Problem Provides the Foundation for Effective Test

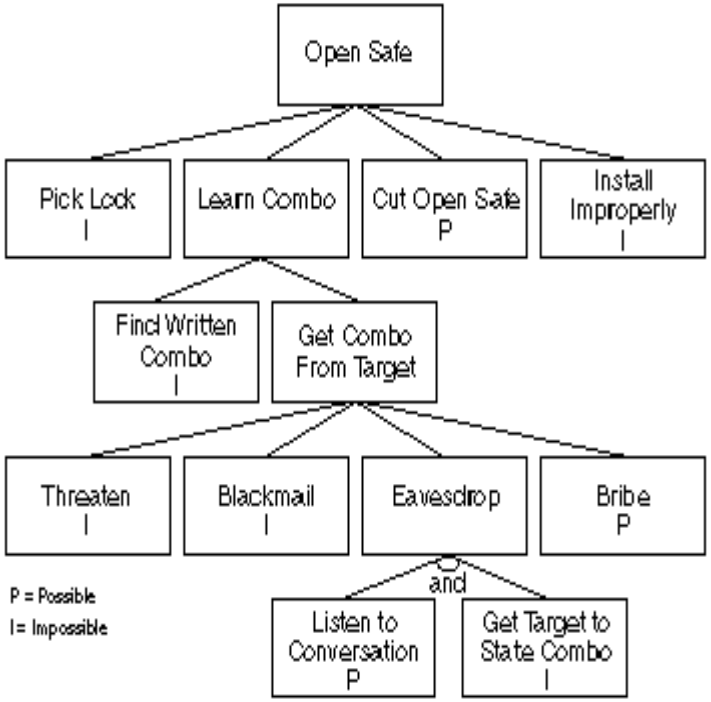
- Determining life cycle security concepts
- Defining & specifying security objectives
- Defining & specifying functional security requirements
- Determining measures of success



"Many systems fail because their designers protect the wrong things, or protect the right things in the wrong way" – Ross Anderson "Security Engineering"

Models (Useful Abstractions) Allow us to Identify and Frame a Complex Problem

Schneier's Attack Tree Model is the Intellectual Foundation of Most Security Testing



"Clearly, what we need is a way to model threats against computer systems. If we can understand all the different ways in which a system can be attacked, we can likely design countermeasures to thwart those attacks…Security is not a product – it's a process. Attack trees form the basis of understanding that process."

Schneier Based His Security Attack Trees on Fault Trees He Saw Used for Safety

Despite Schneier's Warning, We Still Tend to Think of Cybersecurity in Terms of Products

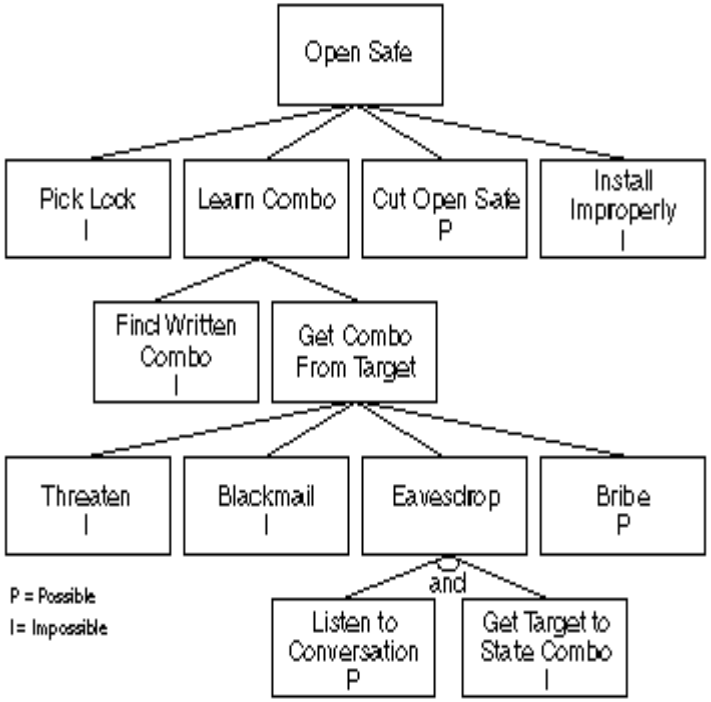
"When you ask an engineer to make your boat go faster, you get the trade-space. You can get a bigger engine but give up some space in the bunk next to the engine room. You can change the hull shape, but that will affect your draw. You can give up some weight, but that will affect your stability. When you ask an engineer to make your system more secure, they pull out a pad and pencil and start making lists of bolt-on technology, then they tell you how much it is going to cost."

Prof Barry Horowitz, UVA

William.Young.3@US.AF.Mil

Ref: Hamilton et al., 2010)

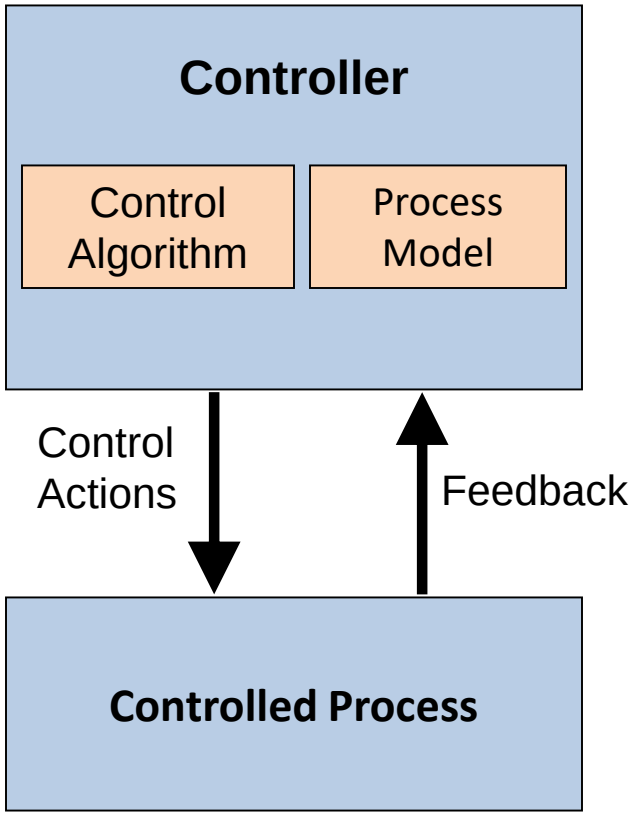
Schneier's Attack Tree Model is the Intellectual Foundation of Most Security Testing



"Clearly, what we need is a way to model threats against computer systems. If we can understand all the different ways in which a system can be attacked, we can likely design countermeasures to thwart those attacks…Security is not a product -- it's a process. Attack trees form the basis of understanding that process."

The Power of This Model Has Decreased, But What if We Thought About Security as a Process?

Leveson's System-Theoretic Accident Model



- Treat safety (and security) as emergent, system-level properties
- Leverage Systems Theory to provide alternative (more powerful) explanation for losses in complex, software intensive systems
- Losses involve a complex, dynamic "process"
  - Not simply chains of failure events
  - Arise in interactions among humans, machines and the environment
- Identify and focus on stakeholder defined unacceptable losses and the associated adverse functionality (hazards)
- Develop, implement, & monitor a sociotechnical security architecture to enforce constraints on system function

Ref: (Leveson, 2011; Thomas 2012)

Systems Analysis

"A systematic examination of a problem of choice in which each step of the analysis is made explicit wherever possible."

Malcom W. Hoag, "An Introduction to Systems Analysis" RAND Research Memorandum, RM-1678, 18 April 1956

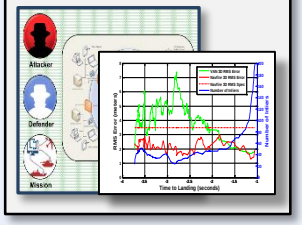
Pose Problem

- Understand mission
- Identify stakeholders
- Determine threats
- Limitations of current work

Characterize System*

- Understand environment
- Identify key factors
- Assess objectives
- Identify requirements

Develop and Analyze Model



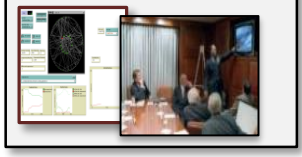
Reevaluate Problem

Analysis Cycle

Present Recommendation

- Summarize results
- Identify driving factors/trades
- Layout alternatives

Assess Implementation



- Persuade community
- Develop performance measures
- Understand impact

STPA-Sec Allows the Systems Analysis Framework to be Applied to Security

Systems Analysis– Pose Problem

Pose Problem

- **Understand mission**
- **Identify stakeholders**
- **Determine threats**
- **Limitations of current work**

ID	Goals
G1	Autonomous engagement
G2	Automated mission planning
G3	Minimize collateral damage
G4	Strike from distance
G5	Reduce logistic footprints

Mission Goals Explicitly Stated

ID	Unacceptable Loss
L1	Loss or damage to the aircraft or equipment
L2	Serious injury or fatality to personnel
L3	Inability to complete mission

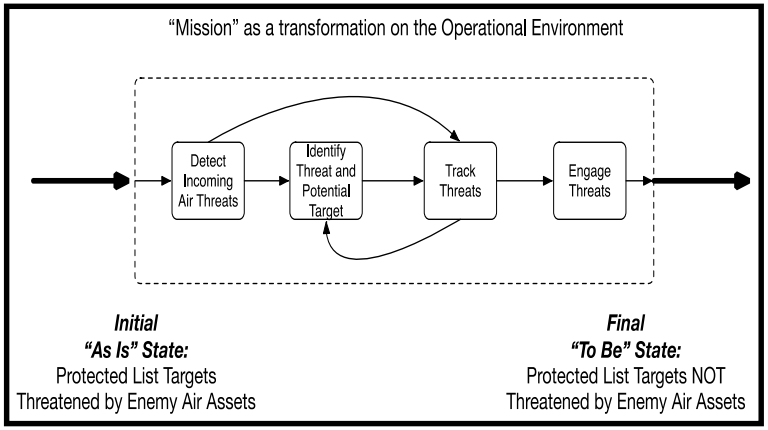
Mission Unacceptable Losses Clearly Identified

A system to safely and timely purchase the correct products...

by means of an cost-effective relationship with our supplier and their transport...

in order to contribute to the company's bottom line and reputation

Mission Problem and Operational Approach Stated*



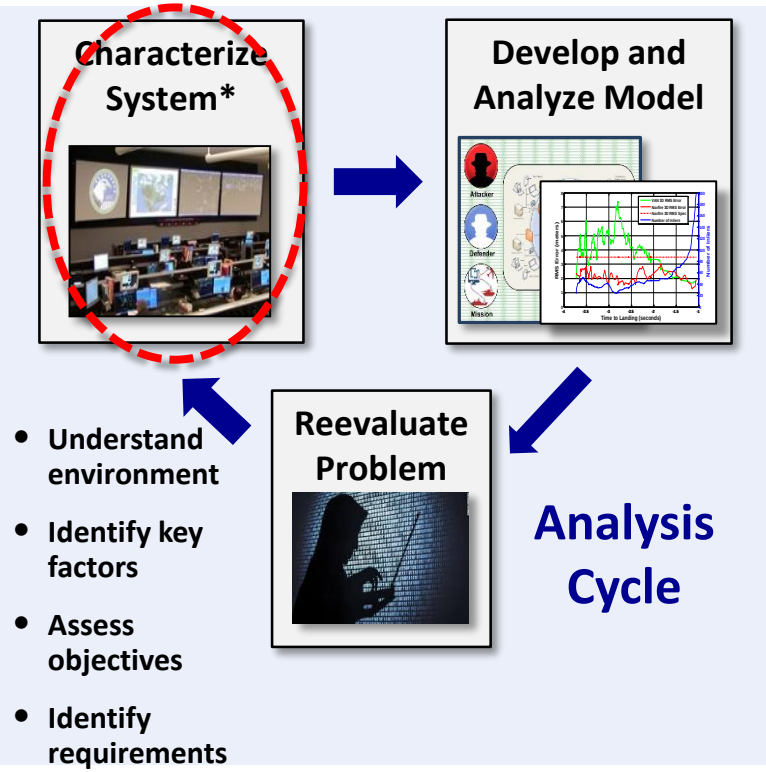
Abstract Mission Activity System Developed

Early Concept Documents Parsed to Support Stakeholder Security-Related Discourse

William.Young.3@US.AF.Mil

* **Example from** Sepulveda, 2017 "**The use of STPA for Understanding Cyber Risks in a Physical Supply Chain**"

Systems Analysis– Characterize Complex Socio-Technical System



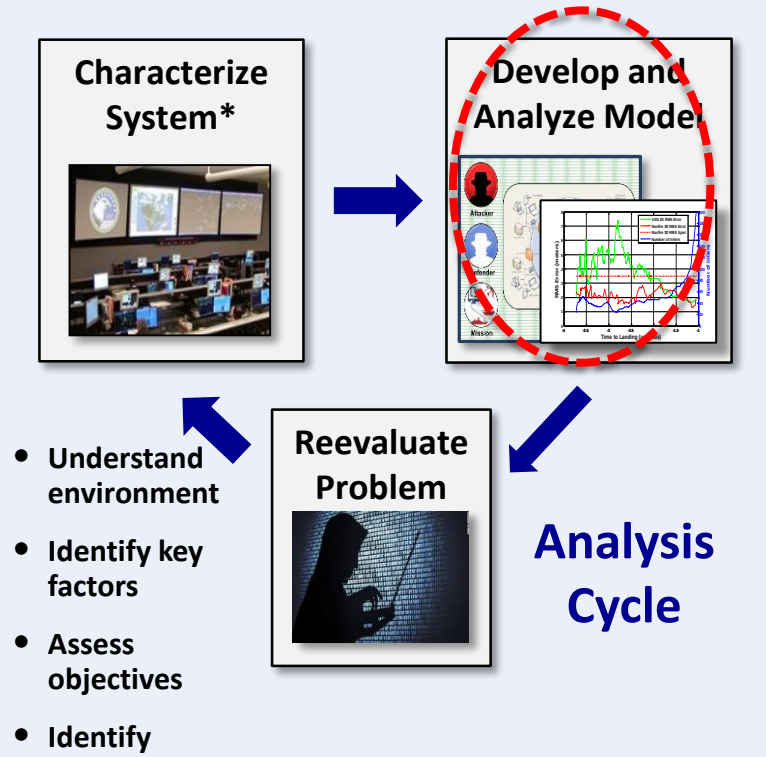
ID	Hazard	Required High-Level Functional Constraint	Loss
H1	Unacceptable collateral damage	Weapon must not inflict damage that is not authorized	L1, L2
H2	Loss of Blue asset	Weapon must not damage blue personnel or material from stockpile to employment	L2
H3	Weapon fail to achieve desired effect	Proper number of weapons must hit and function on the designated DMPI	L1
H4	CPI exposed (implied)	Identified CPI must not be exposed under unplanned or unauthorized conditions	L3

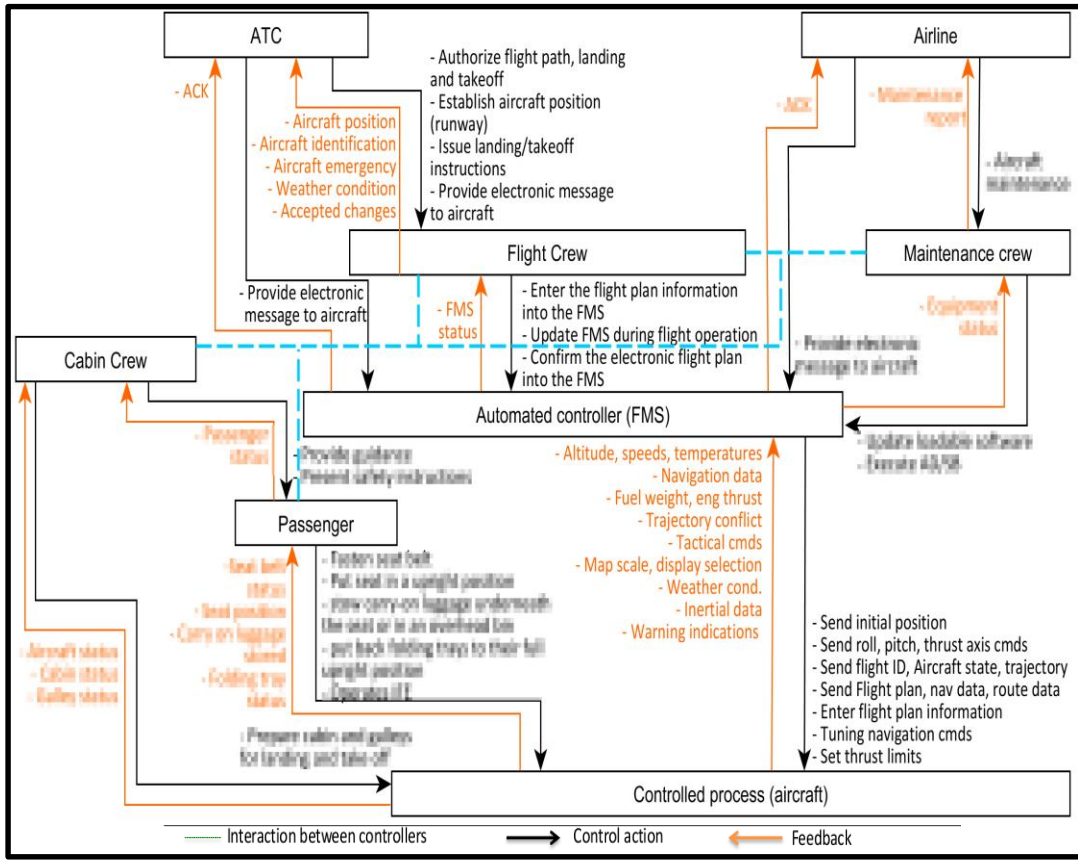
Hazards Capture and Specify Necessary System Conditions Preceding Unacceptable Losses

STPA-Sec Provides Early, Threat-Agnostic, Structured Inquiry into Mission Risk

William.Young.3@US.AF.Mil

Systems Analysis– Develop and Analyze Model* (1/2)





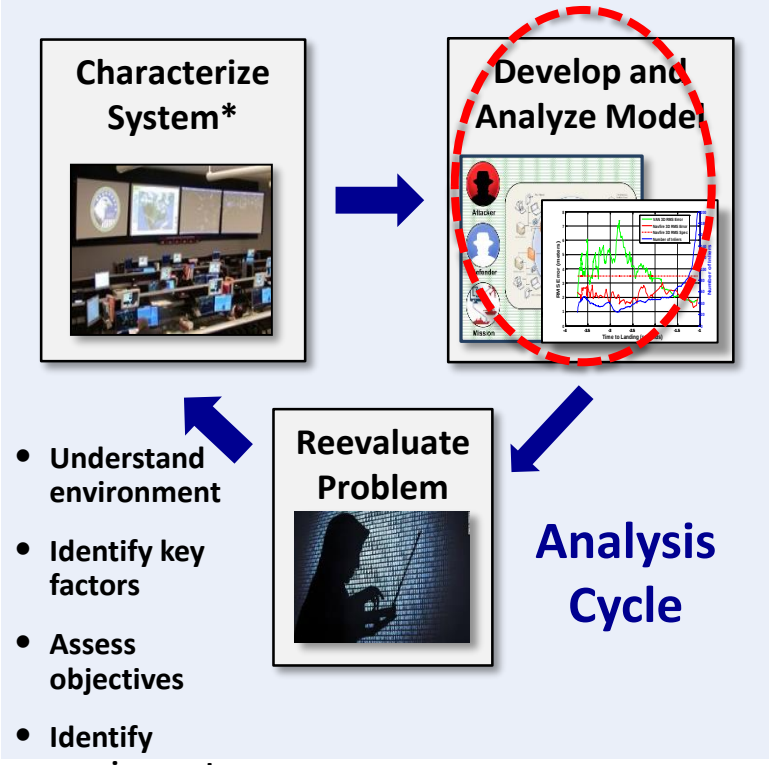
Functional Control Structure Model Informs Development of Requirements and Architecture

Control Structure is Iteratively Developed, Mission-Centric Abstraction

William.Young.3@US.AF.Mil

*** Example Diagram from Pereira, Hirata, Pagliares, Lemos 2017. "STPA-Sec: System-Theoretic Process Analysis for Security - Flight Management System"**

Systems Analysis– Develop and Analyze Model (2/2)*



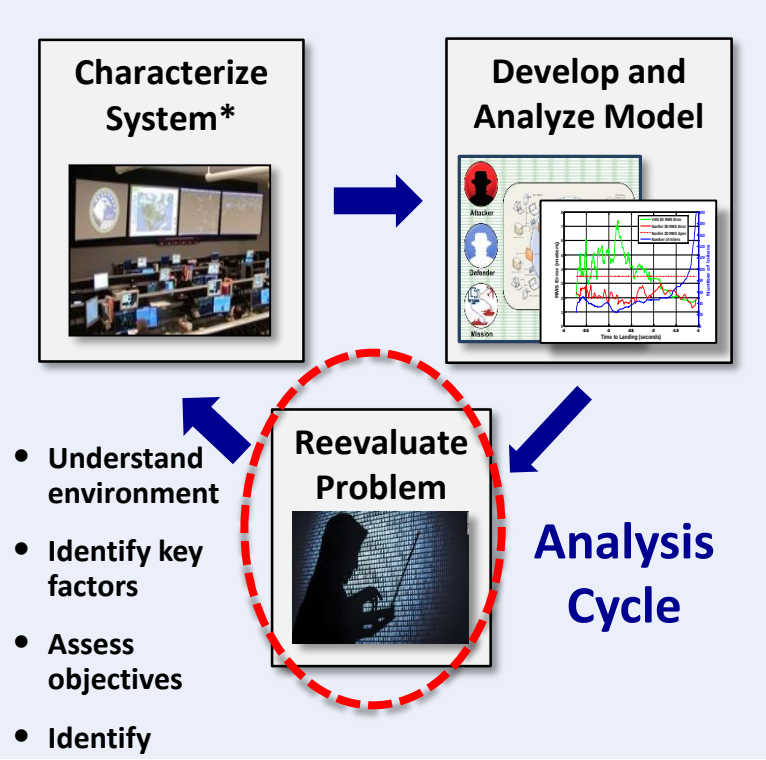
1. Describing hazardous, functional, and required behavior
   - HP(h ∈ H, ca ∈ CA, c ∈ C)
     - True iff providing command ca in context c will cause hazard h
   - HNP(h ∈ H, ca ∈ CA, c ∈ C)
     - True iff not providing command ca in context c will cause hazard h
   - FP(f ∈ F, ca ∈ CA, c ∈ C)
     - True iff providing command ca in context c is necessary to achieve function f
   - R(ca ∈ CA, c ∈ C)
     - True iff command CA is required to be provided in context c
2. Consistency checks
   - ∀h1 ∈ H,h2 ∈ H ¬ ∃ ca ∈ CA, c ∈ C : HP(h1, ca, c) ^ HNP(h2, ca, c)
     - For every potential context, it must be possible to avoid hazardous control actions/inactions. In other words, if it is hazardous to provide CA then it should be non-hazardous to not provide CA
   - ∀ h ∈ H, f ∈ F ¬ ∃ ca ∈ CA, c ∈ C : HP(h, ca, c) ^ F(f, ca, c)
     - For every potential context, if it is necessary to provide a command to fulfill a function then it must not be hazardous to provide the command in that context
3. Requirements generation (SpecTRM-RL tables)
   - Compute R(ca ∈ CA, c ∈ C) to satisfy the following:
   - ∀h,ca,c: h ∈ H ^ ca ∈ CA ^ c ∈ C → [HP(h, ca, c) → ¬ R(ca, c)]
   - ∀h,ca,c: h ∈ H ^ ca ∈ CA ^ c ∈ C → [R(ca, c) → HNP(h, ca, c)]
   - ∀f,ca,c: f ∈ F ^ ca ∈ CA ^ c ∈ C → [FP(f, ca, c) → R(ca, c)]

STPA-Sec Models Can Be Analyzed Through Formal Methods (CSBD)

William.Young.3@US.AF.Mil

*Ref: Thomas, 2013. "EXTENDING AND AUTOMATING A SYSTEMS-THEORETIC HAZARD ANALYSIS FOR REQUIREMENTS GENERATION AND ANALYSIS"

Systems Analysis– Reevaluate Problem



Hazardous Control Actions	Required System Constraint
UCA-CO-1: *LAUNCH Command Not Provided* when a valid enemy target should be engaged	SC-CO-1: LAUNCH Command must be for valid engagements (Functional Req)
UCA-CO-2: *Providing LAUNCH Command* when the engagement is not valid	SC-CO-2 : LAUNCH Command must only be provided for valid engagements
UCA-CO-3: *Providing LAUNCH Command* when the engagement may become invalid during the flight-time of the engagement (from release to impact)	SC-CO-3: LAUNCH Command must only be provided if the engagement will remain valid during the entire ordinance Time of Flight
UCA-CO-4: *Continuing Providing LAUNCH Command* (*too long*), *after* DISENGAGE Command received	SC-CO-4: LAUNCH Command must be discontinued after a DISENGAGE Command is issued
UCA-CO-5: *Providing LAUNCH Command (early)* before CONSENT command	SC-CO-5: LAUNCH Command must be issued and received after CONSENT command
UCA-CO-6: *Providing LAUNCH Command (late)* After DISENGAGE Command	SC-CO-6: LAUNCH Command must not be issued or received after the DISENGAGE Command has been issued

Models Generate Insights and Establish Mission-Traceable Security Requirements

William.Young.3@US.AF.Mil

Systems Analysis– Present Recommendations*

Present Recommendations

- **Summarize results**
- **Identify driving factors/trades**
- **Layout alternatives**

Component	Comparison
Lead PIC Process Model	Architecture 1 (A1) involves the PIC more and thus their process model is more likely to be updated if the formation changes. Requiring the PIC to choose the shape invests them more in the tethering activity, likely increasing situational awareness. (SA)
Tethered A/C Process Models	Both architectures should have the same general process model for the tethered A/C. It is possible that requiring the tethered A/C to make piloting decisions would result in a more robust sensor system and process model as design plays out.
Lead PIC Workload	A2 would not require the lead PIC to perform as many tasks but the number of tasks assigned is not necessarily the cause of high workload. Experiments should be done to compare workload between the architectures.
Hardware	The hardware should be the same. As stated above, requiring tethered A/C to perform processing tasks could affect the hardware choices.
Software Design	Certifying tethered A/C to make piloting decisions would require more stringent software development. As seen in the analysis, A1 would still require the tethered A/C to make individual piloting decisions in case of an emergency.
Airspace Certification	Agencies such as the FAA should be consulted to determine if there would be differences in the certification processes for A1 and A2.

Analysis Allows Inclusion of Mission-Specific Security Concerns in Early Trades

William.Young.3@US.AF.Mil

*Ref: Horney, 2017. "Using STPA for a Safety Trades Study"

Systems Analysis—Assess Implementation

SCENARIO 4: During a congested, denied, or operationally restrictive communications environment, Aircrew does not issue ABORT command when required.

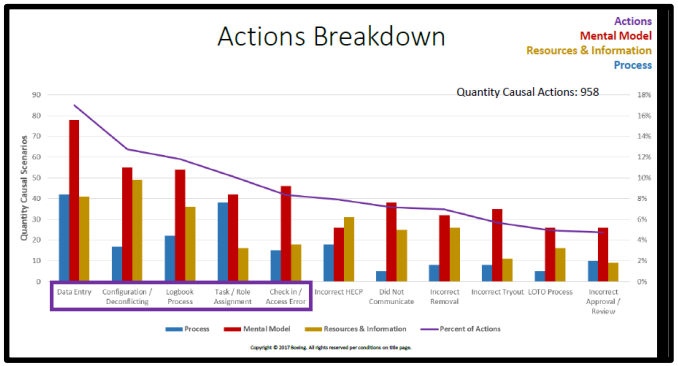
Possible CAUSE: There is a potential conflict between the JTAC and the aircrew mental models in a reduced communications environment (perhaps due to enemy communications jamming). The adequacy of current guidance for large-scale employment of networked weapons in a degraded mode is inadequate or non-existent in doctrine.

The scenario does not involve a component failure, but illustrates potential conflicts between expanded weapon capabilities, existing doctrine and procedures, and aircrew mental models. Current doctrine applicable for older weapons might actually result in negative transfer for aircrew employing Network-enabled Weapons. The aircrew's mental models are represented by the controller process model.

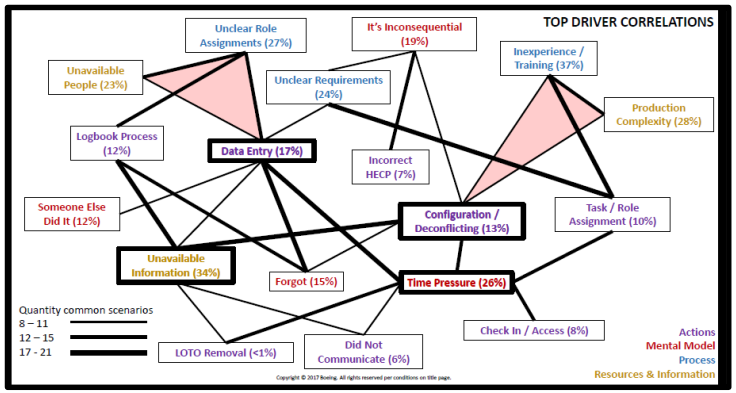
Assess Implementation

- **Persuade community**
- **Develop performance measures**
- **Understand impact**

Scenarios Provide Relevant Context at a Particular Level of Abstraction Allowing for Technical, Operational, Managerial Constraint Development



Key Drivers Identified*



Visualized Interactions Support Prioritization*

Models Generate Insights and Establish Mission-Traceable Security Requirements

William.Young.3@US.AF.Mil

*Ref: Belvin, 2017. "Using STPA Trend Analysis To Determine Key Systems Drivers"

Akamai

President and CEO Tom Leighton's advice in Whitehouse meeting of Tech CEOs on improving Federal Cybersecurity

"Cybersecurity is a growing area of Akamai's business, one where IT organizations seek expert help repeatedly. Solutions that work for private companies can also work for federal agencies, specifically:…

- Protecting federal data through role and policy-based access controls
- Encouraging "security by design" through systems analysis methodologies like STPA-SEC

William.Young.3@US.AF.Mil

Ref: https://www.linkedin.com/pulse/technology-ceos-share-best-practices-us-government-cios-tom-leighton-1/

IT Alliance for Public Sector Cybersecurity

- Key Recommendation: Institutionalize "security by design" for federal IT modernization and development.
  - Included within a DevSecOps approach needs to be a "security by design" process, such as a System- Theoretic Process Analysis for Security (STPA-Sec) for all future development. Security is not an add-on, it needs to be a fundamental part of all IT design, from start to finish. (p.37-38)

William.Young.3@US.AF.Mil

*Ref: IT Alliance for Public Sector, "Tech Industry's Recommendations for Federal IT Modernization"

Embraer

- Conclusions from Embraer's STPA-Sec pilot study
  - "The application of STPA-Sec, in the aerospace area (FMS),was a good example of its potential to identify design recommendations
  - STPA Sec shows to be an alternative method to current ED-203/DO-356 implementations
    - Identification of security environment and security perimeter is addressed during elaboration of the functional control structure
    - Security Risk Assessment activity is covered during Step1 and Step2 of STPA-Sec
  - Embraer has proposed STPA-Sec as an alternative means of compliance to ED-202A/DO-326A (in progress)"

*Ref: Pereira, Hirata, Pagliares, de Lemos " STPA-Sec: System-Theoretic Process Analysis for Security – Flight Management System"

Summary and Conclusion

- Good test requirements are the developed through solid analysis
- Generating testable cybersecurity requirements strains existing models and associated analysis
  - Complexity associated with modern, software intensive systems drives a need for a more complete underlying model
  - The system-theoretic model unlocks the key for using new and more powerful analysis methods to generate and validate testable requirements for cybersecurity testing
- Several organizations are already benefitting from using STPA-Sec to inform cybersecurity testing efforts

For More Help

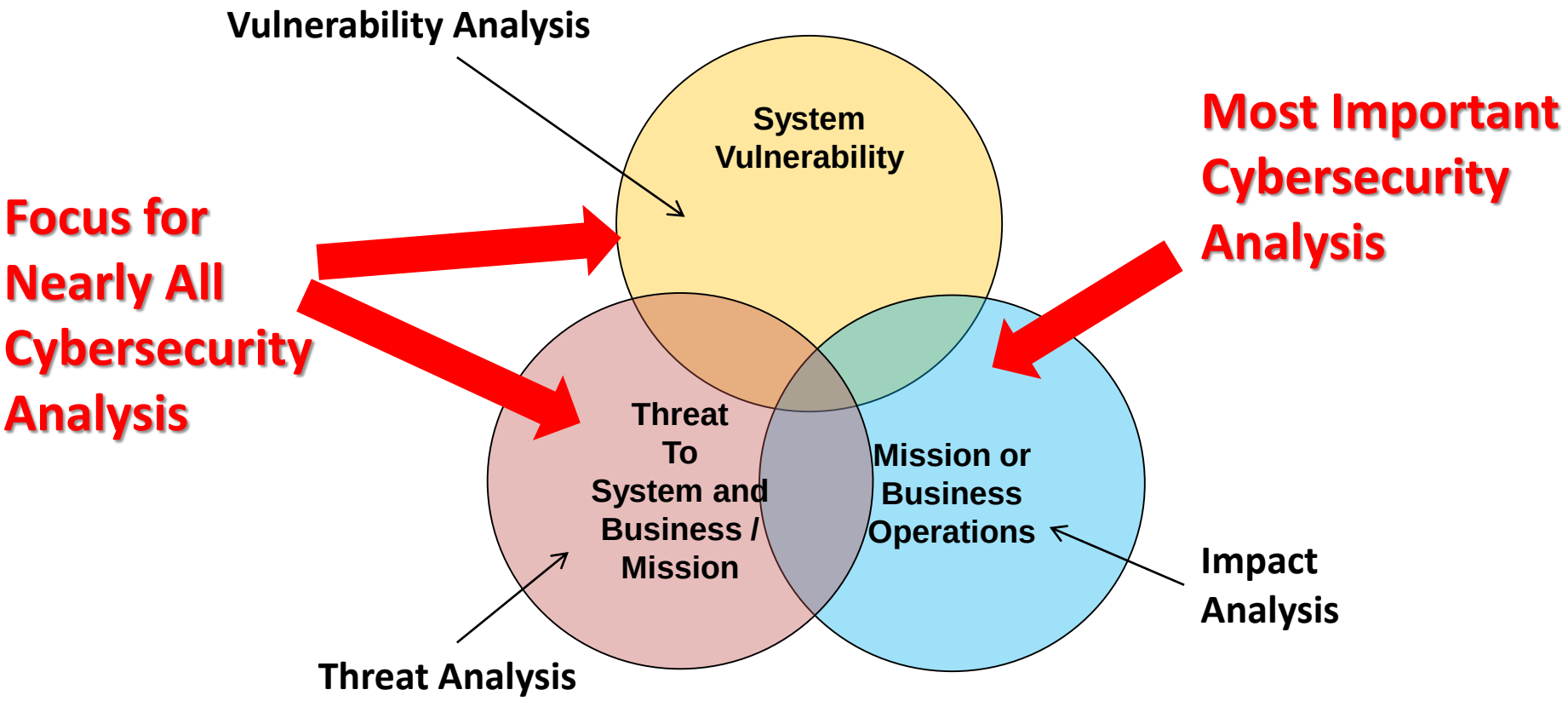
- 2018 STAMP (System-Theoretic Accident Model & Processes) Workshop
  - Great opportunity to see the model applied across a variety of industries (and it's free)
  - Mar 26-29, '18 at MIT, Cambridge, MA
  - http://psas.scripts.mit.edu/home/stamp-workshop-2018/
- USAF Cyber College
  - Teach Functional Mission Analysis Course
  - http://www.airuniversity.af.mil/CyberCollege.aspx
- My Contact Information
  - William.Young.3@US.AF.Mil

Questions

William.Young.3@US.AF.Mil

BACKUPS

Three Types of Cybersecurity Analysis

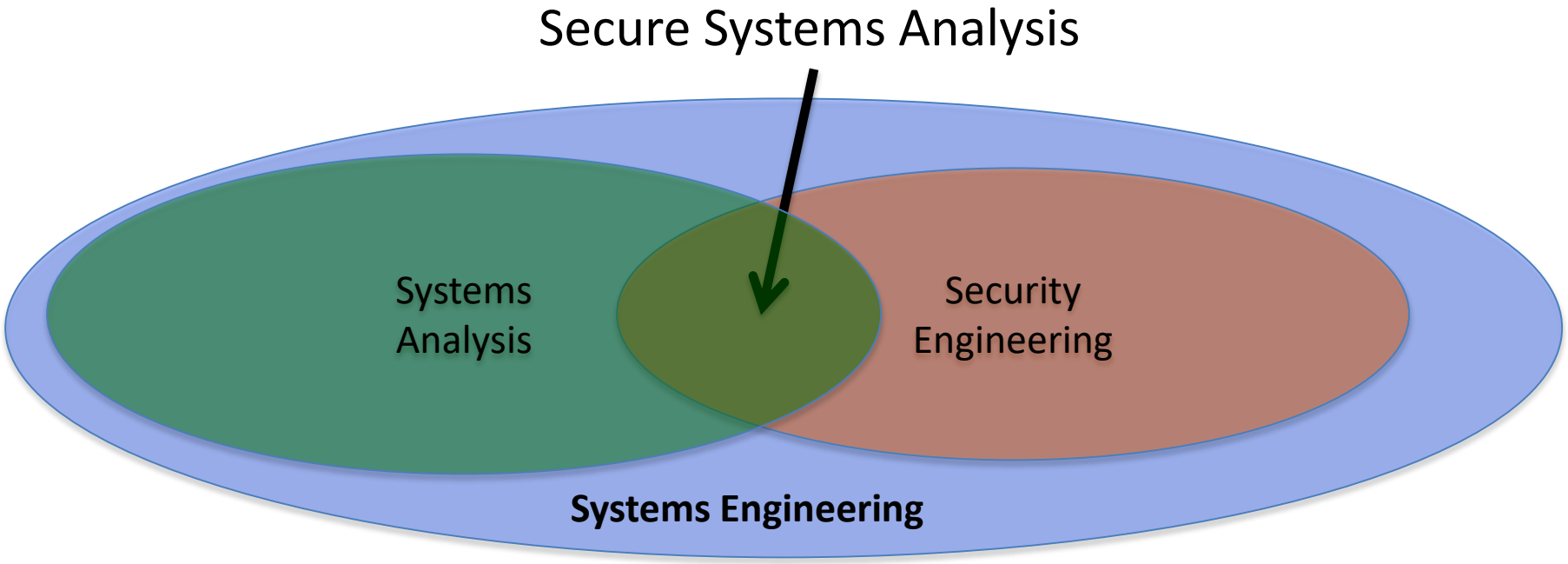


Secure Systems Analysis Should Identify Security Problem as Part of ISO/IEC/IEEE 15288 Business/Mission Analysis (BMA) Technical Process

From Systems Analysis to Secure Systems Analysis

"A systematic examination of a problem of choice in which each step of the analysis is made explicit wherever possible."

Malcom W. Hoag, "An Introduction to Systems Analysis" RAND Research Memorandum, RM-1678, 18 April 1956



Secure Systems Analysis is Based on Models