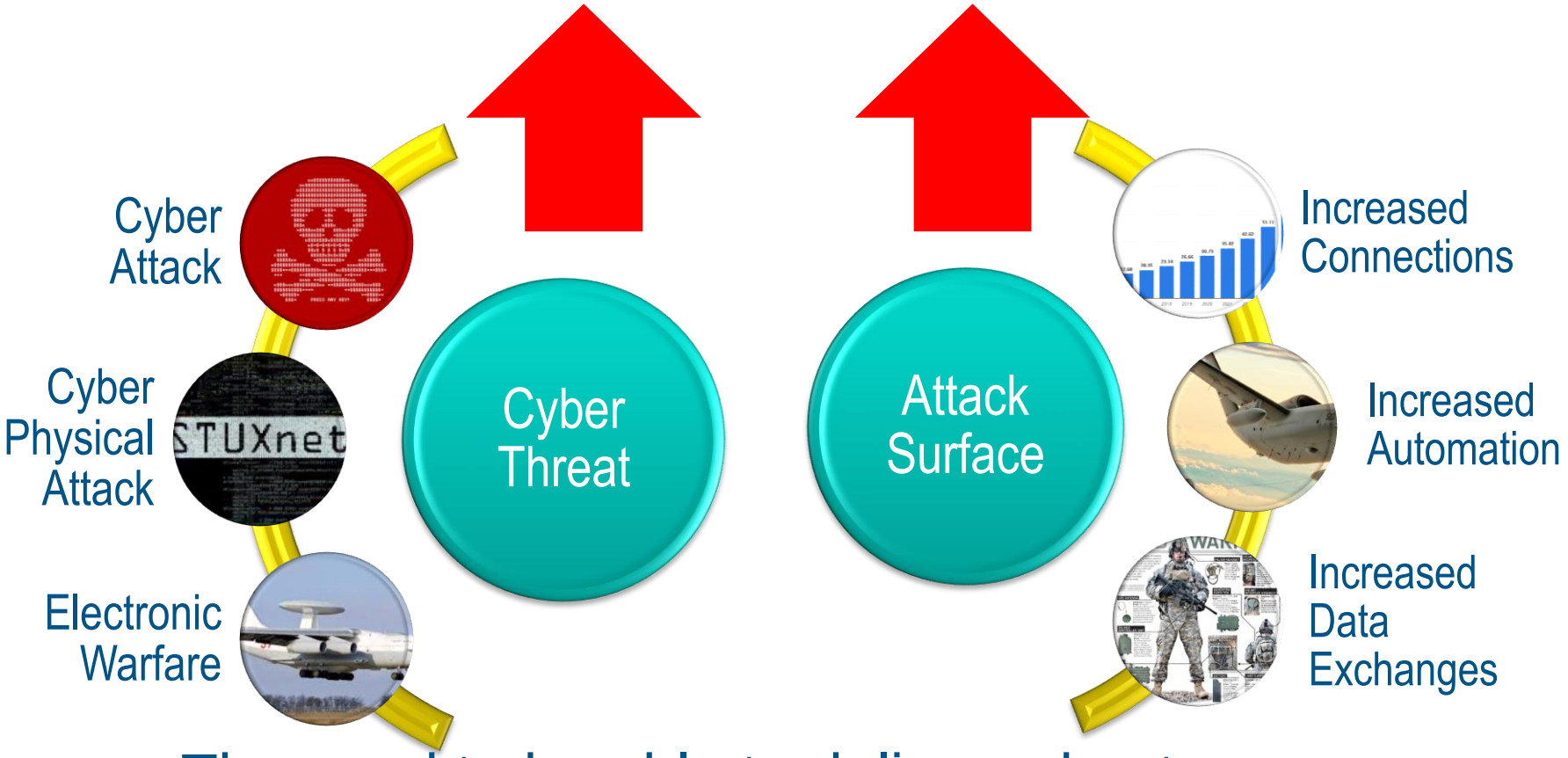
# Integrating Systems Engineering, Cyber Security and Cyber T&E through MBSE

## Applying the Digital Engineering Strategy
## Abstract: 21488


▶Barry L Papke
▶No Magic Inc.
▶Allen, Texas, U.S.
▶bpapke@3ds.com

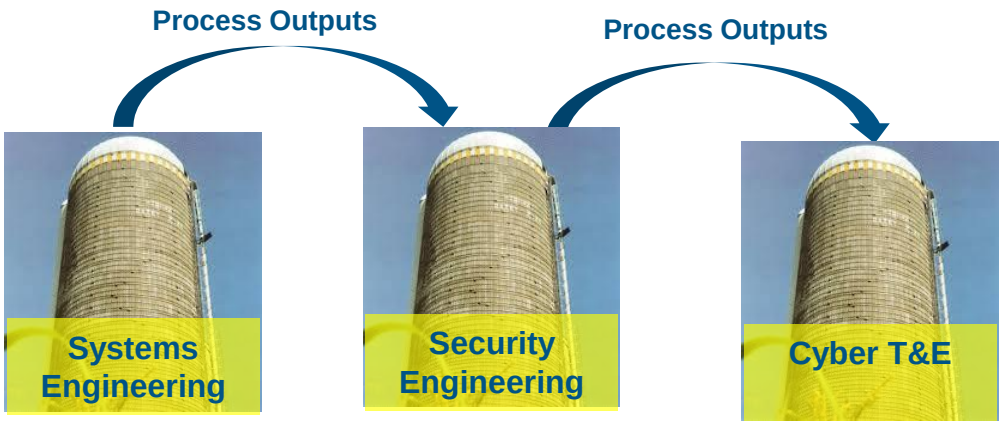
Michael G. Lilienthal Ph.D, CTEP
EWA Government Systems, Inc.
571-238-4532
MLilienthal@ewa.com

# We Should be Motivated - Increasing Cyber Threat with an Increasing Attack Surface




The need to be able to deliver robust, secure systems will only increase.

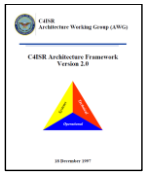
# Security Cylinders of Excellence



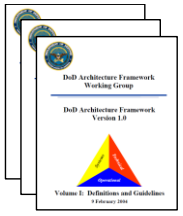

- Today, each discipline:
  - Has well established processes and methods
    - SE - Model Based System Architecture and System Design
    - SecE - NIST Risk Management Framework / ATO process
    - CT&E – Cyber Table Top Exercises and Cyber Test Ranges
  - Is at different levels of Model Based/Digital Engineering maturity
  - Operates differently within each program phase
  - Is experiencing advancements in methods and/or tools

# The Systems Engineering Perspective

- Continuing migration from spreadsheets, Visio and PowerPoint to Model Based Systems Engineering.
- Modeling tools have significantly advanced.
- Processes and methods continue to evolve:
  - Enterprise Architecture Frameworks
  - Modeling Languages
  - Analysis and Synthesis Capabilities

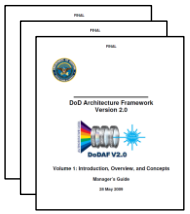


C4ISR AF V1.0 June 1996
C4ISR AF V2.0 December 1997
ISR Data

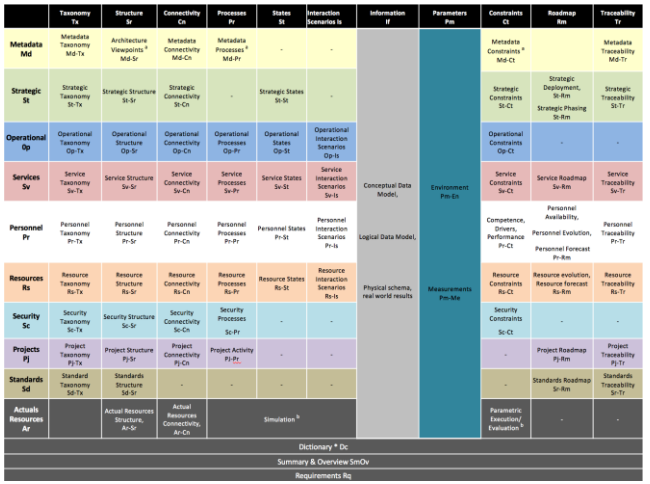


DODAF V 1.0 August 2003
Any Information

DODAF V 1.5 April 2007
Net-Centric Concepts



DODAF V 2.0 May 2009
Any Operational Work Flow




Any Notation

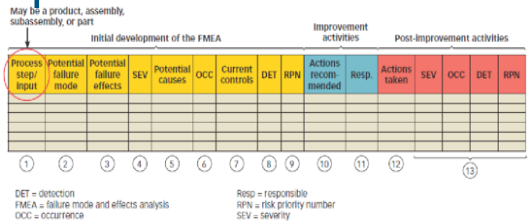


2013

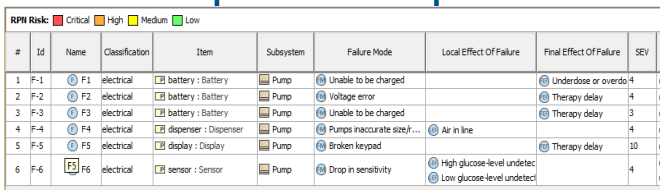

2017

# A Related DES Success Story – R&M and FMEA

## Spreadsheet Based




## Vendor Specific Implementation




**Safety and Reliability for UML Request For Proposal**

OMG Document: ad/2017-03-05

Letters of Intent due: *15 June 2017*
Submissions due: *28 August 2017*

In 2017, a new group consisting of both industry and academia formed at the OMG to define a new standard profile for UML that addresses safety and reliability aspects of a system.

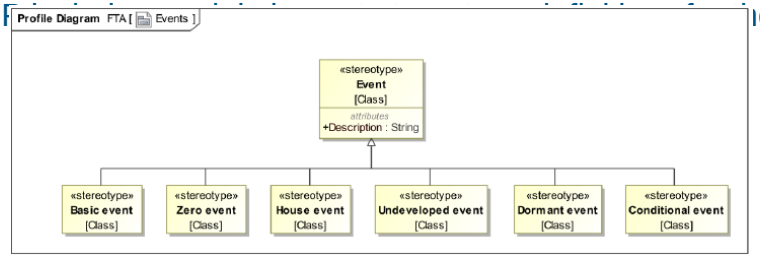
For safety, the RFP calls for support for each of the following domains:

- Aerospace (DO-178C (RTCA 2012a) and DO-331 (RTCA 2012b)),
- Automotive (ISO 26262 (ISO 2011)),
- Medical (IEC 62304, IEC 60601-1, and ISO 14971 (IEC 2015a, 2015b; ISO 2007))
- Railway (EN 50128 (CEN 2012)) domains.

For Reliability, the RFP requires support for two analysis techniques:

- Fault Tree Analysis (FTA) (IEC 61025)
- Failure Mode and Effects Analysis (FMEA) (IEC 60812) and FMECA (IEC 2006a)

The RFP[illegible]ie Profile:



# Safety and Reliability Profile

- With the Safety and Reliability Profile, FMEA data is integrated with the system elements within the architecture.
- The failure elements and modes themselves can be analyzed for taxonomy, frequency, etc.
- Mitigation can be tracked and unmitigated failure modes can also be tracked and assessed for cost/risk.

| # | Id | Name | Classification | Item | Subsystem | Failure Mode | Local Effect Of Failure | Final Effect Of Failure | SEV | Cause Of Failure | OCC | Prevention Control | Detection Control |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | F-1 | F1 | electrical | battery : Battery | Pump | Unable to be charged | | Underdose or overdo | 4 | Battery degraded | 1 | Meter designed to I | Charging test 02- |
| 2 | F-2 | F2 | electrical | battery : Battery | Pump | Voltage error | | Therapy delay | 4 | Battery depleted | 4 | Meter designed to I | |
| 3 | F-3 | F3 | electrical | battery : Battery | Pump | Unable to be charged | | Therapy delay | 3 | Battery overcharged | 1 | | |
| 4 | F-4 | F4 | electrical | dispenser : Dispenser | Pump | Pumps inaccurate size/r... | Air in line | | 4 | Failure to release inside air, lc | 2 | | |
| 5 | F-5 | F5 | electrical | display : Display | Pump | Broken keypad | | Therapy delay | 10 | Incorrect operation | 1 | | |
| 6 | F-6 | F6 | electrical | sensor : Sensor | Pump | Drop in sensitivity | High glucose-level undetec<br>Low glucose-level undetect | | 4 | Battery degraded<br>Flawed sensor | 2 | | |

# The Security Engineering Perspective

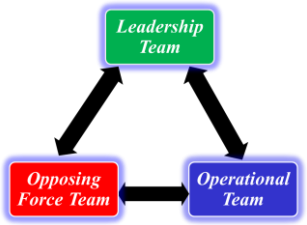
- Security Engineering performs analysis of the system in support of obtaining a Authority to Operate IAW NIST Risk Management Framework:
  - Categorize System
  - Select Controls
  - Implement Controls
  - Assess Controls
  - Authorize System
  - Monitor Controls
- Through the features of SysML, Security Engineers have extended the R&M FMECA profile to support NIST RMF assessment:

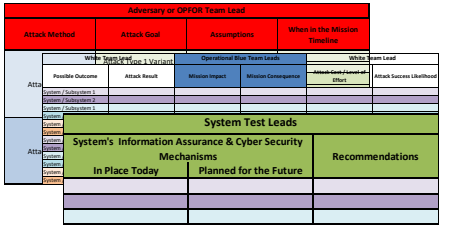
| # | Name | Potential Causeof Failure | OCC | Potential Risk | Risk Impact | Item |
|---|---|---|---|---|---|---|
| 1 | Security TVR Item | Threat | Very High | Potential Risk | Very High | Software Element |

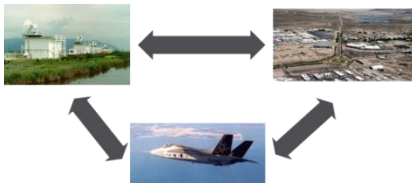
| Causeof Failure | Vul SEV | Mitigation | Detection Design Element | Recommended Person Responsbility | Recommended System Action | DET | Target Completion Date | Action Taken |
|---|---|---|---|---|---|---|---|---|
| Vulnerability | Very High | Resource Mitgation | Detection Design Element | Perform Detection Runs | Execute Detection Softwar | | | |

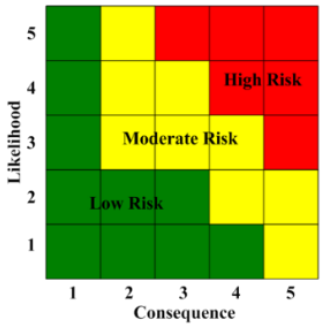
# The Cyber T&E Perspective

- The Cyber T&E community has adopted a process called Cyber Table Top Exercises (CTT) to mitigate risk of failure during Cyber OT&E:
  - 4 phase low cost, intellectually intensive assessment process
  - Introduces and explores mission effects of offensive cyber operations
  - Helps estimate "Mission Risk" to the system, systems of systems or family of systems






Starting point to bake in cyber resiliency with new systems

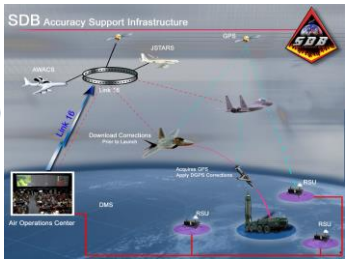
Identify priorities to improve cyber resiliency of legacy systems

# Wargame Flow: Focus on Threat Mission

Operational Team: Mission Planning

Develop Mission Plan

Operational Team: Brief mission execution




Combined Team: OPFOR Mission Order #1 - #N

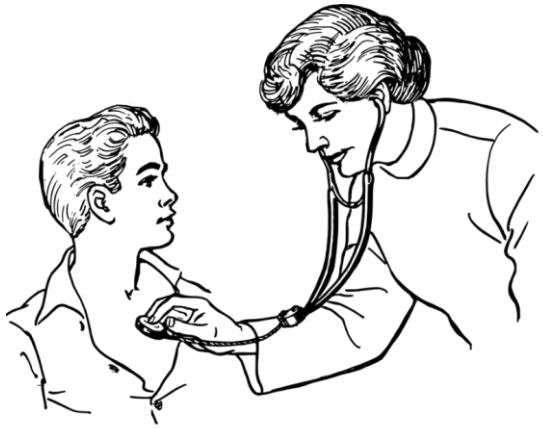

OPFOR Team: Review Reconnaissance Data & attack surface

Assess potential attack surfaces

OPFOR Team: Brief Cyber Kill Chain opportunities

## AT&L Risk Management Framework (RMF) Process

- Get Authority to Operate (ATO) certification



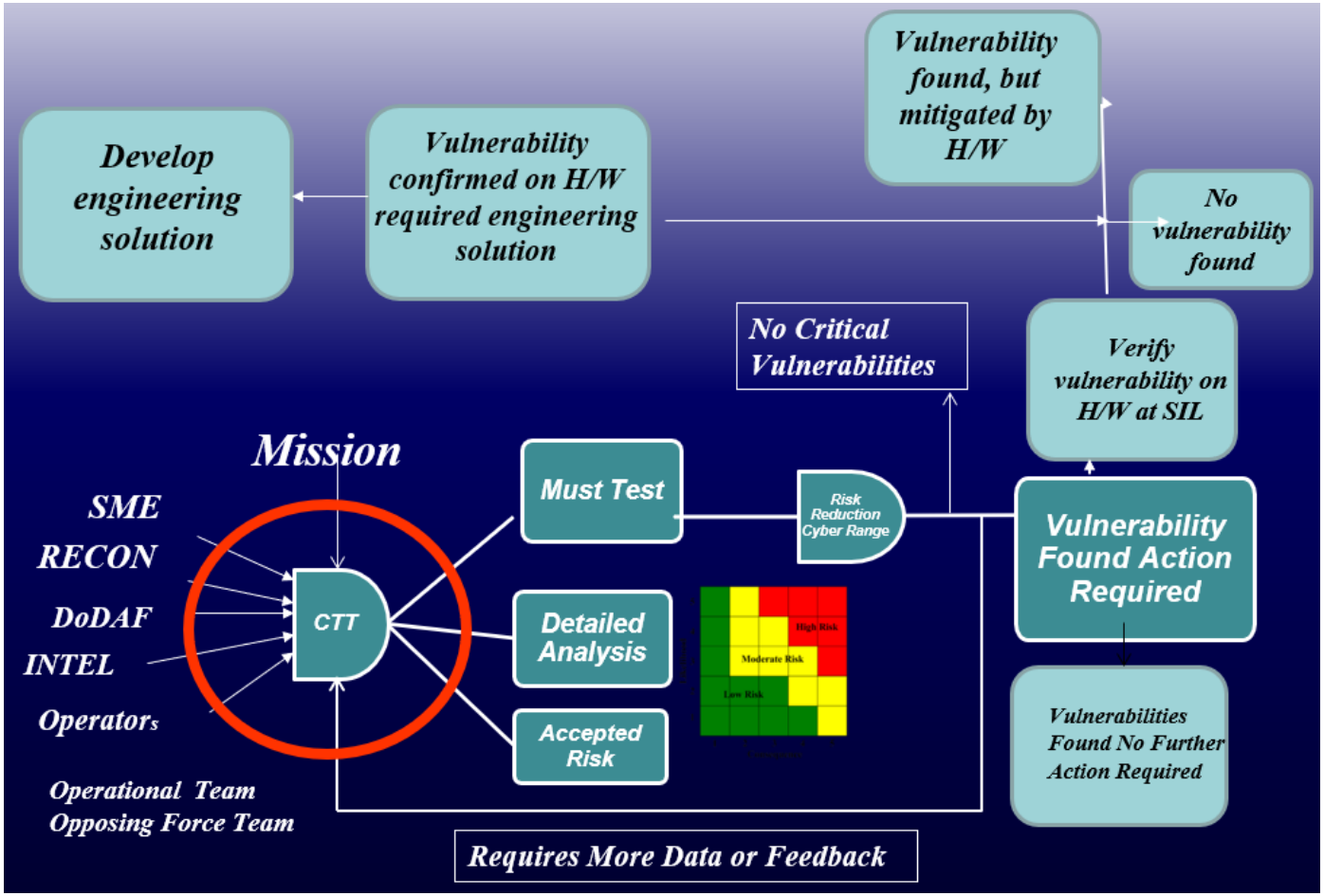
Is my blood work normal?

## DOT&E Cybersecurity T&E Process

- Assess how the mission can be degraded or disrupted by exploiting system vulnerabilities

How many ways can I break in and kill your mission?

# CTT Inputs and Outputs Map to the SE and RMF Processes



# Post Wargame Analysis

- The output of the CTT is a Cyber FMEA.
- However:
  - The Cyber Test Community is not integrated into the Digital Engineering Environment
  - Their products are spreadsheets tossed over the fence to “systems engineering.”
  - No traceability to the rest of the system architecture.

| Opposing Force Team Lead | | | |
|---|---|---|---|
| Attack Method | Attack Goal | Assumptions | When in the Mission Timeline |
| Attack Type 1 | Attack Type 1 Variant 1 | | |
| | Attack Type 1 Variant 2 | | |
| | Attack Type 1 Variant 3 | | |
| Attack Type 2 | Attack Type 2 Variant 1 | | |
| | Attack Type 2 Variant 2 | | |
| | Attack Type 2 Variant 3 | | |

| Leadership Team Lead | | Operational Team Leads | |
|---|---|---|---|
| Possible Outcome | Attack Result | Mission Impact | Mission Consequence |
| System / Subsystem 1 | | | |
| System / Subsystem 2 | | | |
| System / Subsystem 1 | | | |
| System / Subsystem 3 | | | |
| System / Subsystem 2 | | | |
| System / Subsystem 3 | | | |
| System / Subsystem 1 | | | |
| System / Subsystem 2 | | | |
| System / Subsystem 1 | | | |
| System / Subsystem 3 | | | |
| System / Subsystem 2 | | | |
| System / Subsystem 3 | | | |

| Leadership Team Lead | | System Test Leads | | |
|---|---|---|---|---|
| Attack Cost / Level of Effort | Attack Success Likelihood | System's Information Assurance & Cyber Security Mechanisms | | Recommendations |
| | | In Place Today | Planned for the Future | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

# Digital Engineering Strategy Goals

**Formalize the development, integration, and use of models to inform enterprise and program decision making**

- Plan and use

**Provide an enduring, authoritative source of truth**

- Digital Technical Baseline Controlled over the System Lifecycle

**Incorporate technological innovation to improve the engineering practice**

- End-to-End Digital Enterprise

**Establish a supporting infrastructure and environments to perform activities, collaborate, and communicate across stakeholders**

- Tools and Processes

**Transform the culture and workforce to adopt and support digital engineering across the lifecycle**

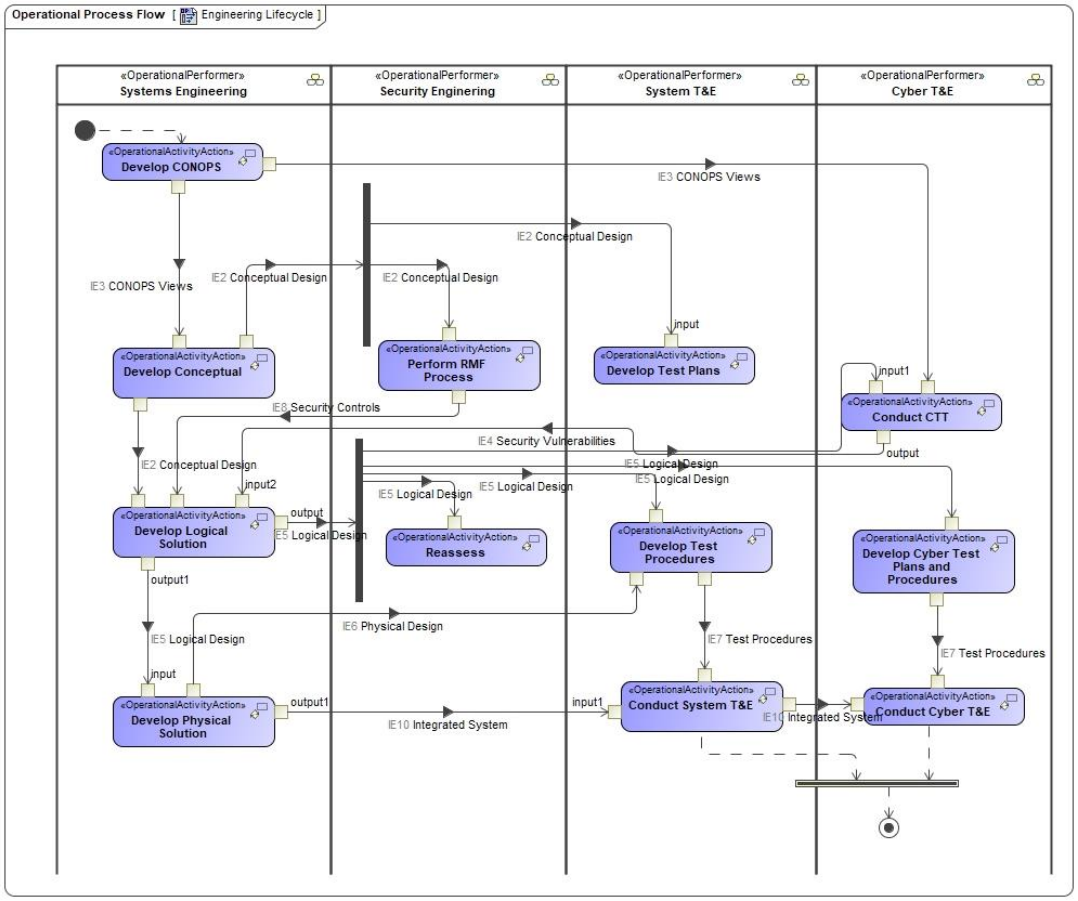
- Culture Change and Training

# Goal 1 - Plan for Modeling and Exchange of Data

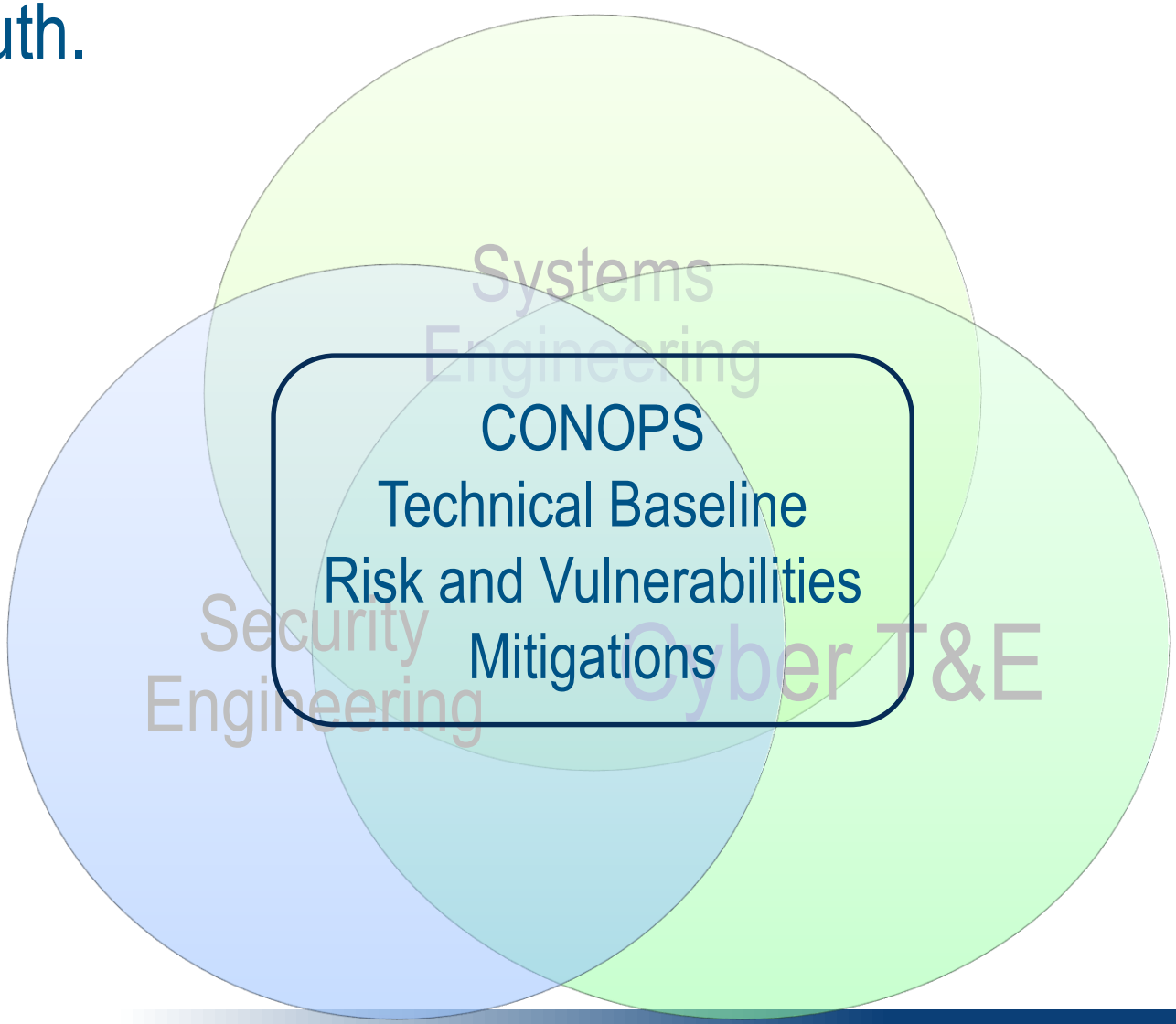
What data is shared across organizational and process boundaries?

What form will it take?

Who will produce it?

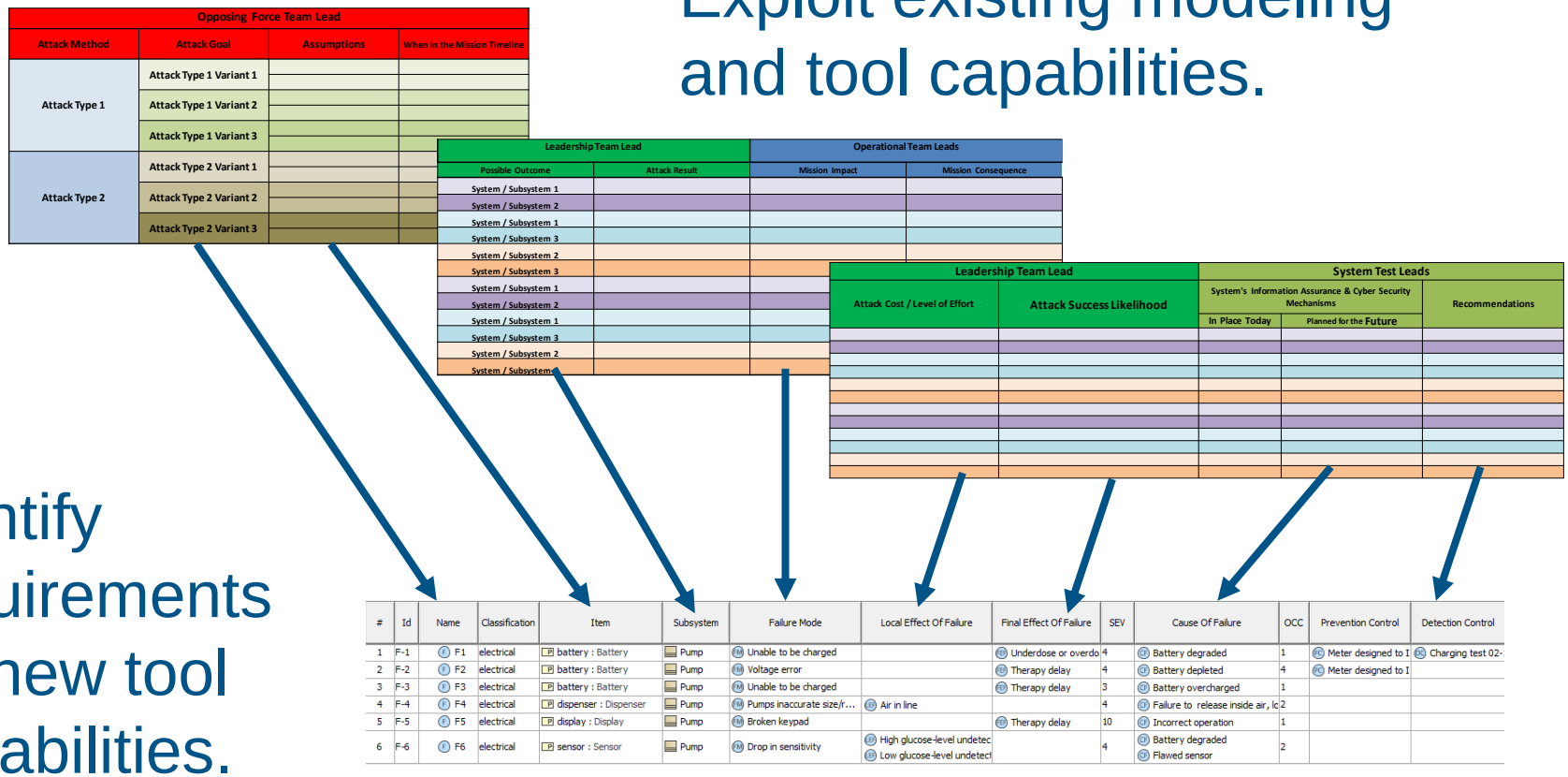


# Goal 2 – Provide the enduring, authoritative source of truth.



# 3. Incorporate technological innovation to improve the engineering practice

Exploit existing modeling and tool capabilities.



| Opposing Force Team Lead | | | |
|---|---|---|---|
| Attack Method | Attack Goal | Assumptions | When in the Mission Timeline |
| Attack Type 1 | Attack Type 1 Variant 1 | | |
| | Attack Type 1 Variant 2 | | |
| | Attack Type 1 Variant 3 | | |
| Attack Type 2 | Attack Type 2 Variant 1 | | |
| | Attack Type 2 Variant 2 | | |
| | Attack Type 2 Variant 3 | | |

| Leadership Team Lead | | Operational Team Leads | |
|---|---|---|---|
| Possible Outcome | Attack Result | Mission Impact | Mission Consequence |
| System / Subsystem 1 | | | |
| System / Subsystem 2 | | | |
| System / Subsystem 1 | | | |
| System / Subsystem 3 | | | |
| System / Subsystem 2 | | | |
| System / Subsystem 3 | | | |
| System / Subsystem 1 | | | |
| System / Subsystem 2 | | | |
| System / Subsystem 1 | | | |
| System / Subsystem 3 | | | |
| System / Subsystem 2 | | | |
| System / Subsystem | | | |

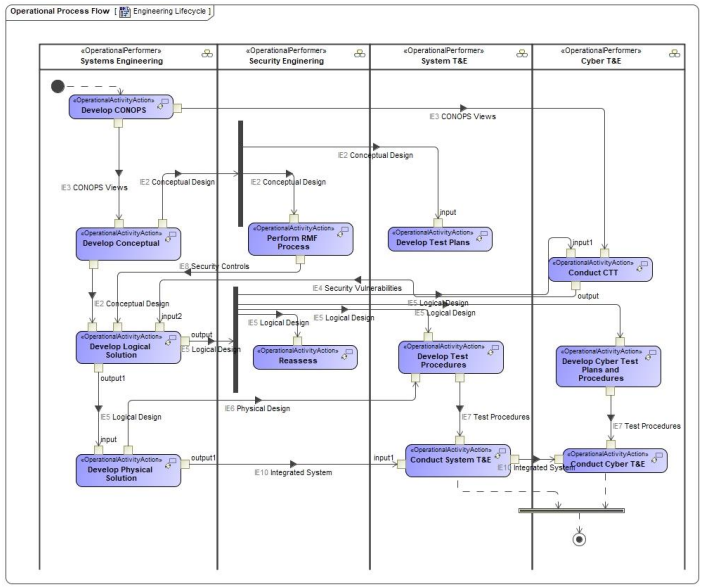
| Leadership Team Lead | | System Test Leads | | |
|---|---|---|---|---|
| Attack Cost / Level of Effort | Attack Success Likelihood | System's Information Assurance & Cyber Security Mechanisms | | Recommendations |
| | | In Place Today | Planned for the Future | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

| # | Id | Name | Classification | Item | Subsystem | Failure Mode | Local Effect Of Failure | Final Effect Of Failure | SEV | Cause Of Failure | OCC | Prevention Control | Detection Control |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | F-1 | F1 | electrical | battery : Battery | Pump | Unable to be charged | | Underdose or overdo | 4 | Battery degraded | 1 | Meter designed to I | Charging test 02- |
| 2 | F-2 | F2 | electrical | battery : Battery | Pump | Voltage error | | Therapy delay | 4 | Battery depleted | 4 | Meter designed to I | |
| 3 | F-3 | F3 | electrical | battery : Battery | Pump | Unable to be charged | | Therapy delay | 3 | Battery overcharged | 1 | | |
| 4 | F-4 | F4 | electrical | dispenser : Dispenser | Pump | Pumps inaccurate size/r... | Air in line | | 4 | Failure to release inside air, lc | 2 | | |
| 5 | F-5 | F5 | electrical | display : Display | Pump | Broken keypad | | Therapy delay | 10 | Incorrect operation | 1 | | |
| 6 | F-6 | F6 | electrical | sensor : Sensor | Pump | Drop in sensitivity | High glucose-level undetec<br>Low glucose-level undetect | | 4 | Battery degraded<br>Flawed sensor | 2 | | |

Identify requirements for new tool capabilities.

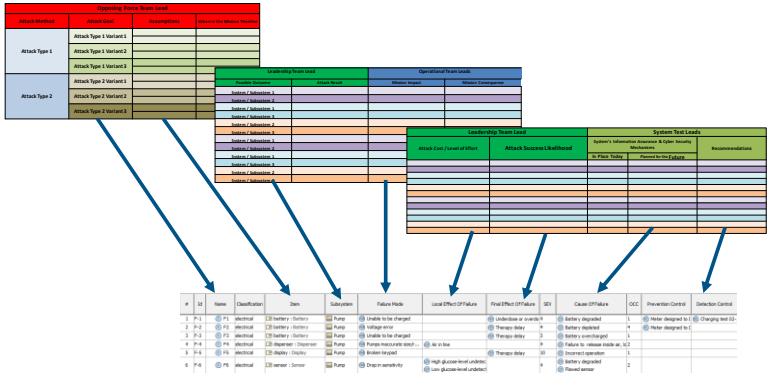
# Goal 4 - Establish a supporting infrastructure and environments to perform activities, collaborate, and communicate across stakeholders.

- Understand the workflow and the format and content of each engineering data exchange.
- Maximize digital access by the end user.
- Exploit custom reporting features and export capabilities to bridge the gap to non-model users.



# Goal 5 - Transform the culture and workforce to adopt and support digital engineering across the lifecycle

- Identify non-digital engineering processes and integrate into the digital environment:
  - Add or modify tool features to support new processes
  - Adjust new processes to match existing tool capabilities



# An Integrated Engineering CONOPS for Cyber Critical Systems

**System Engineering**

- Recognition of Enterprise Architecture as the a fundamental element of Cyber Critical System Design
- Application of established patterns and frameworks or Cyber Protection and Cyber Resilience
- Development of views and viewpoints to support and integrate Security Engineering and Cyber T&E into the SE lifecycle.
- Inclusion of security features as part of core system functionality

**Security Engineering**

- Adoption of Model Based Engineering practices
- Application of Security/Cyber FMEA methods for definition and analysis of RMF controls and mitigations
- Participation in the Architecture Development process
- Support definition of Integrated Security Functionality

**Cyber T&E**

- Participation in SE Planning to ensure Cyber T&E activities are included.
- Integration into the Digital Engineering Environment for access to data and integration of results back into the digital baseline.

# Conclusions

- Successful implementation of the Digital Engineering Strategy will require application of Enterprise Architecture and Model Based Systems Engineering to development of the Digital Enterprise (Systems Engineering will play a critical role):
  - Defining and Understanding the Capability Baseline of the current Digital Engineering Environment
  - Identifying Capability Gaps that require new material solutions
  - Defining and understanding the CONOPS for program execution:
    - What processes will be required?
    - What data will be exchanged (how and when and in what form)?
    - Who are the producers and consumers?
  - Defining and understanding the current Digital Engineering Baseline:
    - What disciplines and processes are integrated and performing digitally?
    - Which disciplines and processes are ready to become integrated?
    - Barriers to those disciplines and processes that are not ready?

# About the Author

**Barry Papke**
bpapke@nomagic.com

Director of Professional Services for No Magic, (US) responsible for training and consulting services. Performs training and project consulting for SysML and UPDM (DoDAF) projects.

30 years experience in Systems Engineering and Project Management on DoD and NASA programs with companies including: LTV Aerospace, Lockheed Martin, Raytheon, L-3 Communications

BS Mechanical Engineering (Texas A&M)
MS Systems Engineering (Steven's Institute of Technology)
OMG Certified SysML Professional

# Additional Information on CTT

CTT Tutorial 25 March 2019

International Test and Evaluation Association (ITEA) sponsored workshop

5th Cybersecurity: Challenges Facing Test and Evaluation

Tutorials:  25 March 2019

Workshop: 26-29 March 2019

**Water's Edge Event Center**
4687 Millennium Drive
Belcamp, MD 21017

www.itea.org