Cyber Failure Modes, Effects and Criticality Analysis (CFMECA)

Jess F. Granone

August 16, 2011

Cyber Background

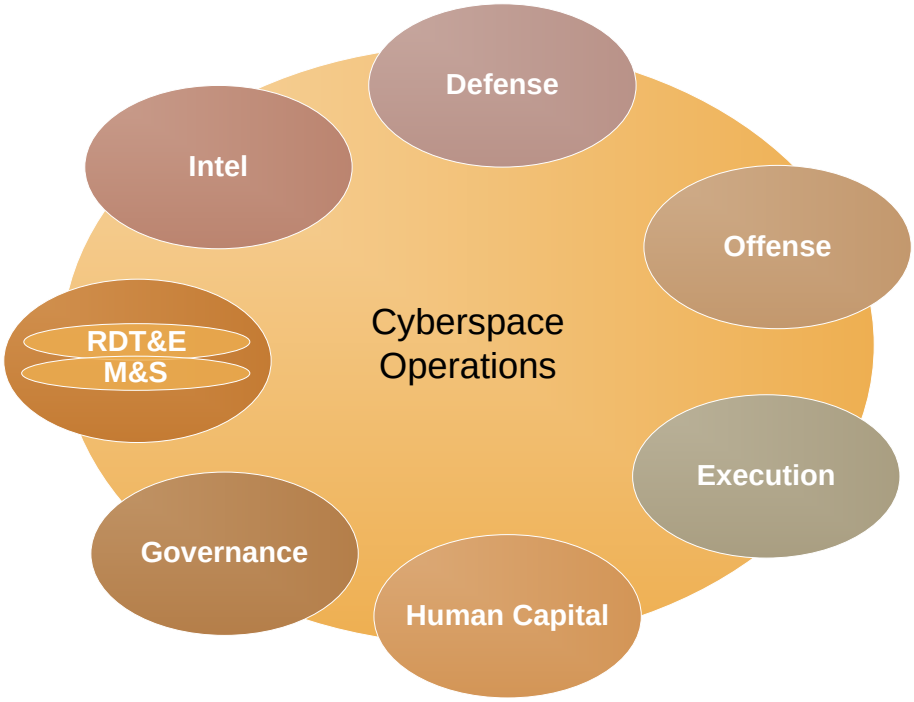
Cyber Crime

- **Computers hijacked per day: 148**
- **Malicious threats in existence at the beginning of 2009: 2.6M**
  - Password stealing ranks at the top
  - 36.2% originated in China (4.4% in the USA)
  - Most target the Windows OS
  - All target the unaware and least sophisticated
- **Mobile malware increased by 46 percent from 2009 to 2010**
- **Internet Crime Complaint Center (IC3)**
  - Recieves average of 25,000 complaints per month
  - Most common Crime types (2010):
  - Age distribution of victims is balanced
  - 91% of complaints from US

Some Elements of Cyber

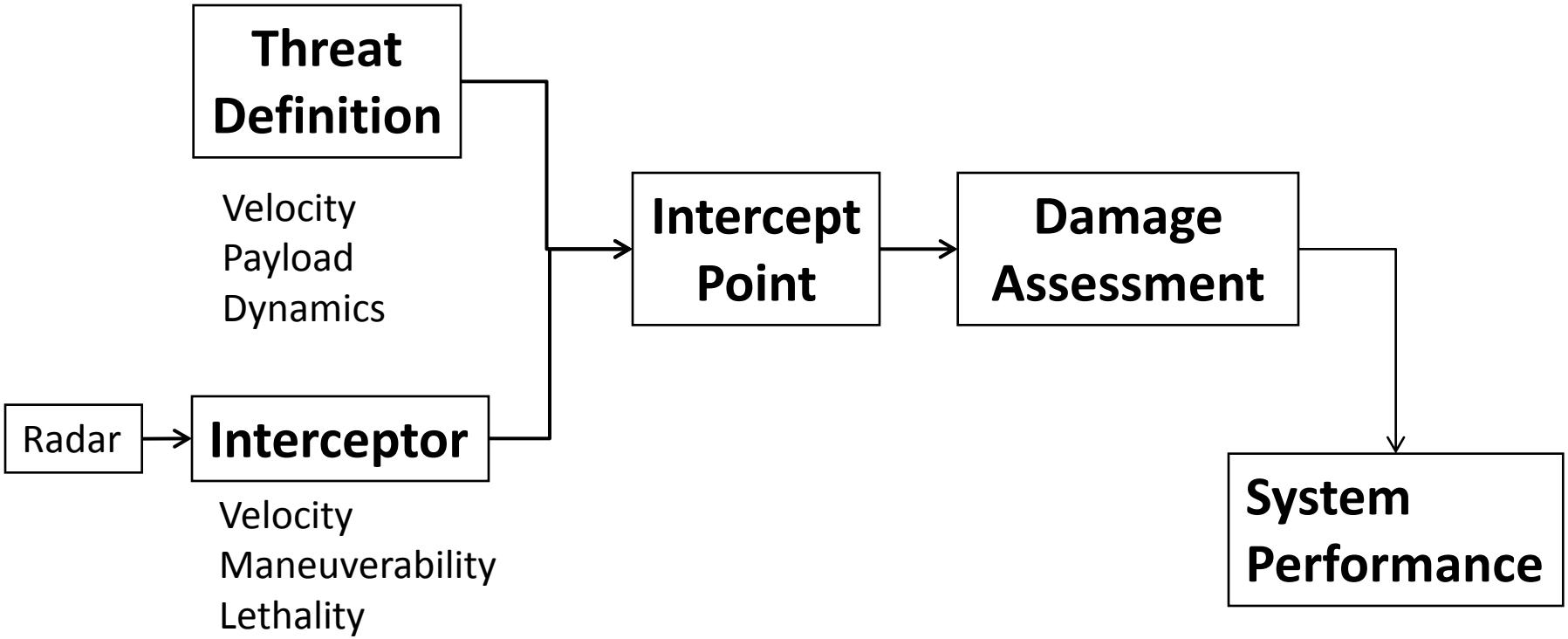
Some Elements of "Cyber"

- **Supply Chain Risk Management**
  - Counterfeit Parts
  - Malicious Software
  - Intelligence Components
- **Network Protection**
  - Where Does The Network Start And Stop?
- **System Protection**
  - What Is A System
    - Bank
    - City
    - Power
    - Military
- **New Start vs Legacy System**

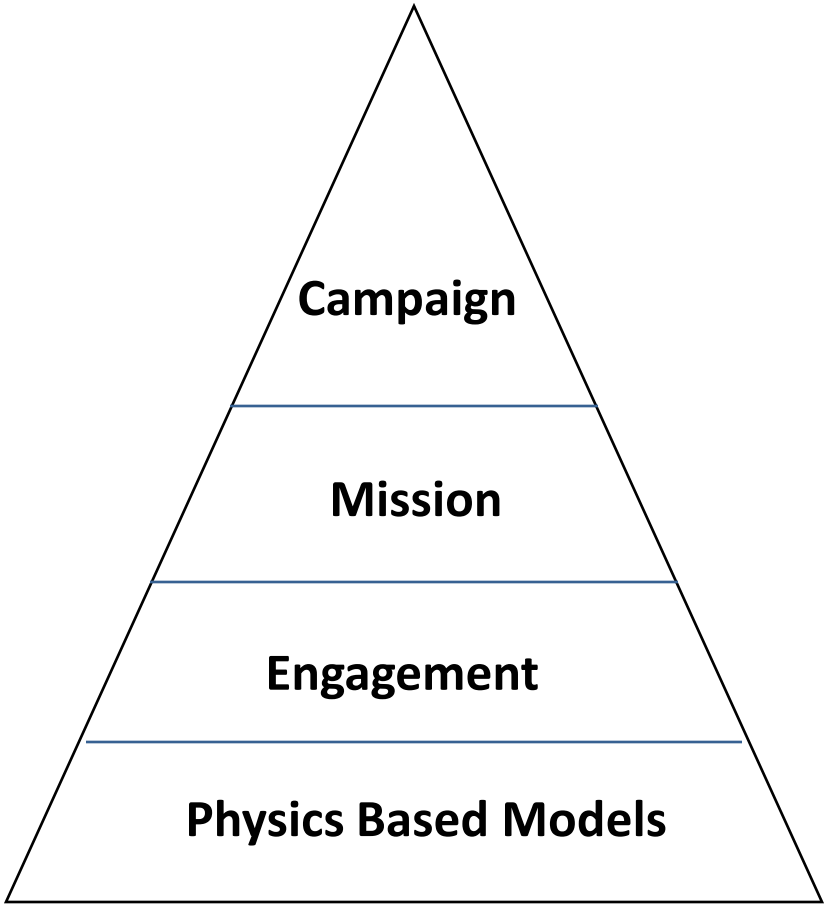


Traditional System Evaluation

Modeling System Performance

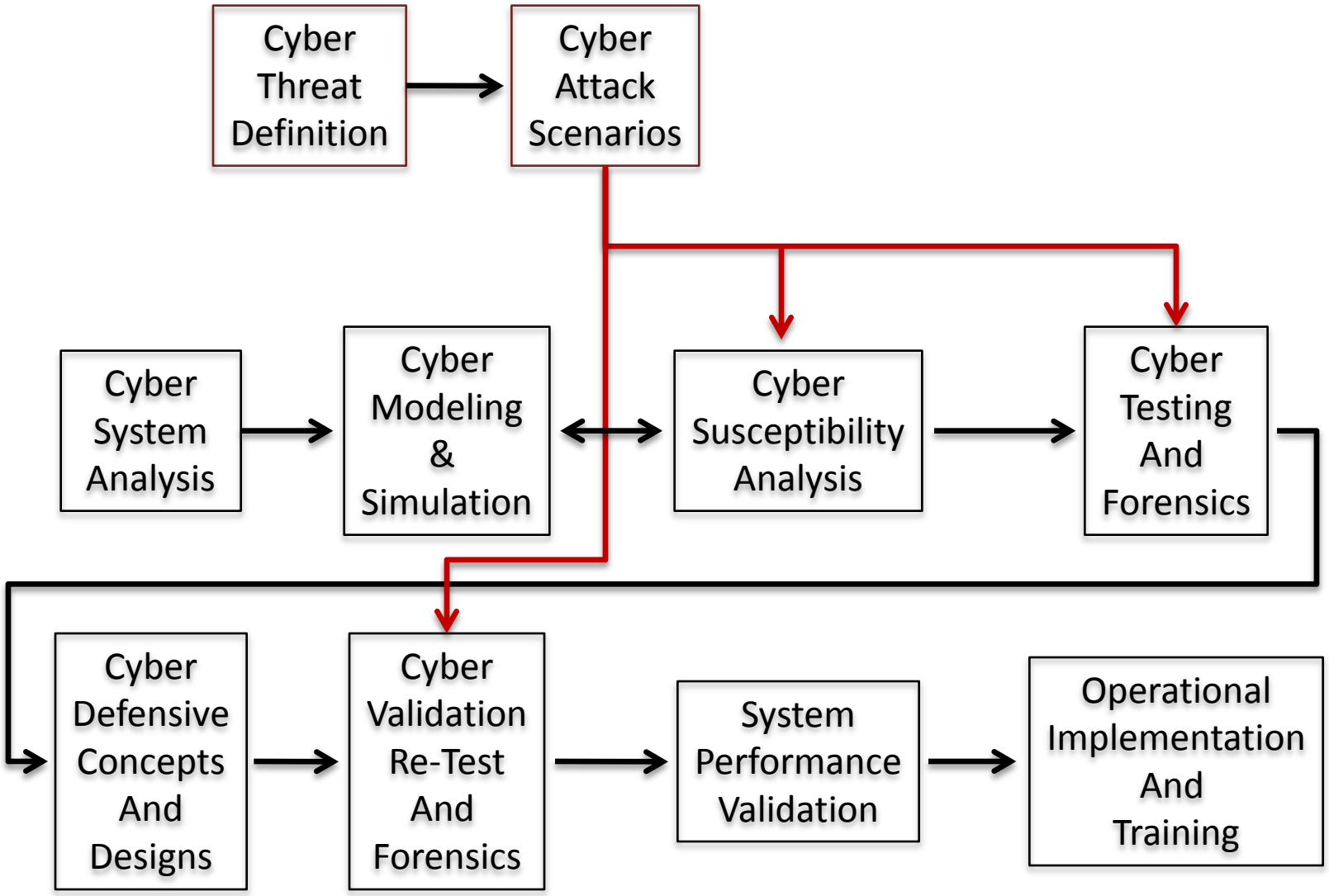


Traditional Modeling and Simulation

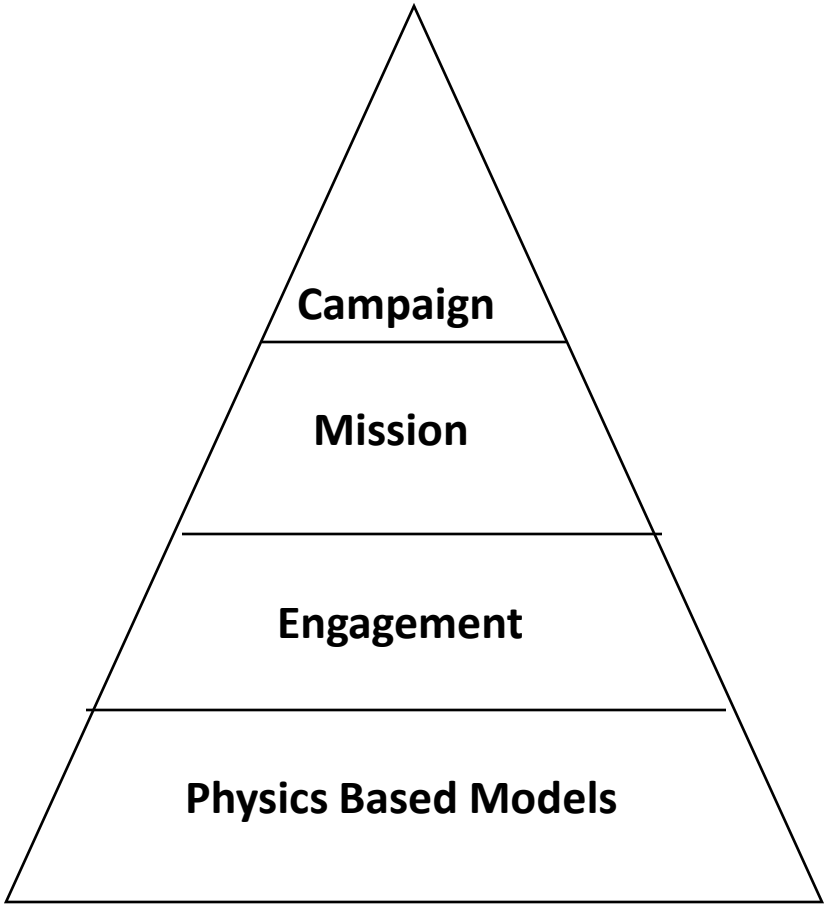


Cyber System Evaluation

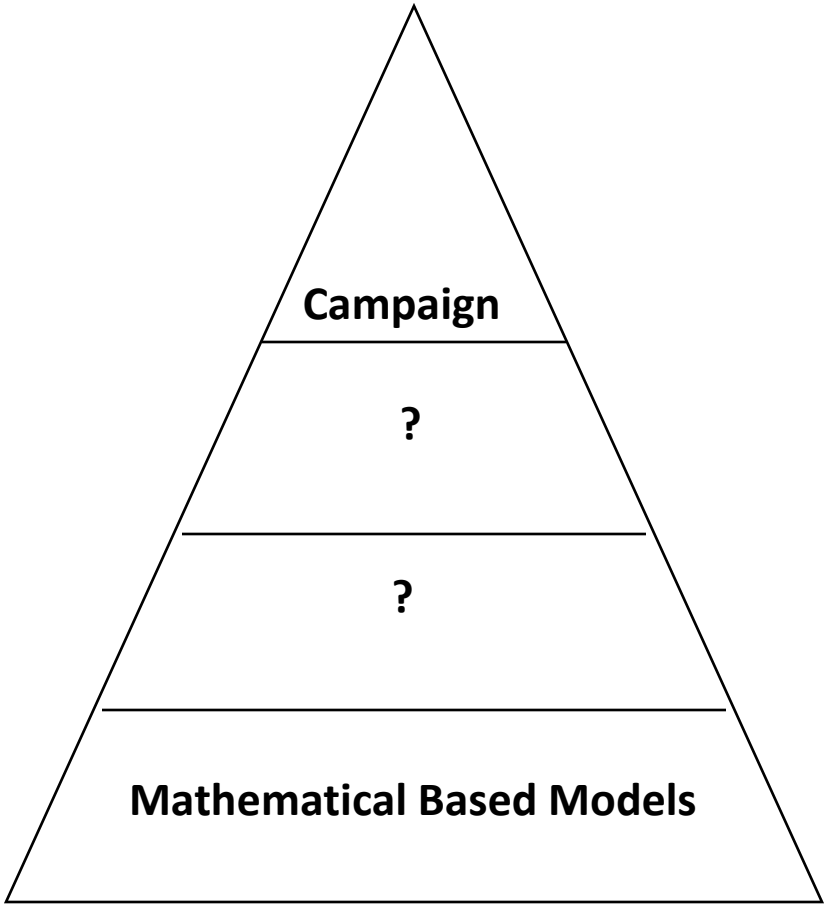
Cyber Systems Evaluation



Modeling and Simulation



Traditional



Cyber

Forensics

- **Traditional Missile Defense**
  - Damage Physics Models (PEELS)
  - Computational Fluid Dynamics Models
    - Predict Damage With Higher Fidelity
  - Visible Effects

- **Cyber**
  - Damage At The Computational Element
  - Changes In The Mathematical Processes
  - Second And Third Order Effects

Measuring and Metrics

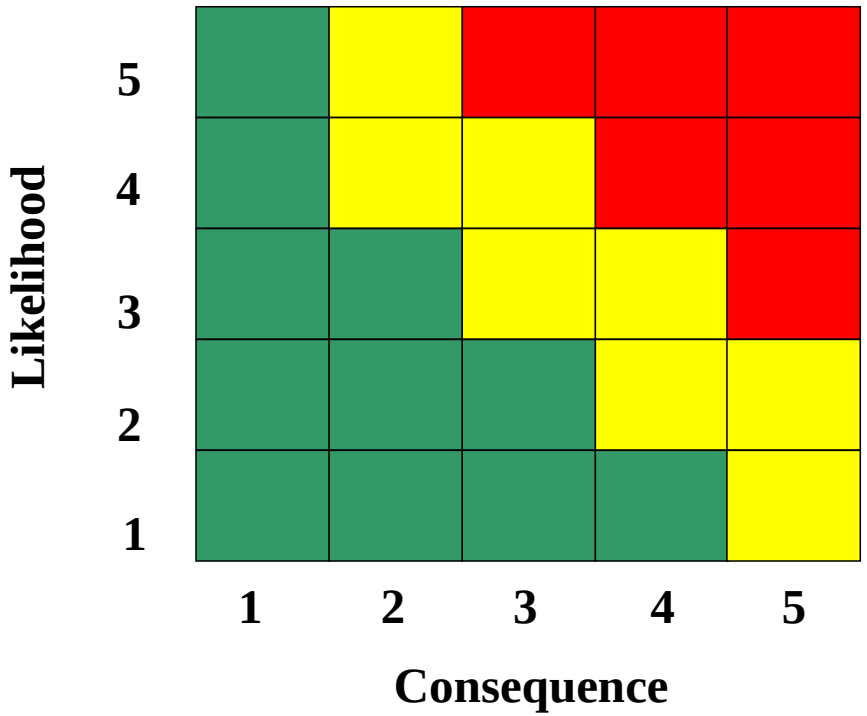
- **Failure Modes, Effects and Criticality Analysis (FMECA)**
  - Widespread Use Today
  - Identifies Risks
  - Determines Severity and Probability
- **Cyber Failure Modes, Effects and Criticality Analysis (CFMECA)**
  - Possible Metric For Cyber Risk Analysis

Failure Modes, Effects and Criticality Analysis (FMECA)

Failure Modes, Effects and Criticality Analysis (FMECA)

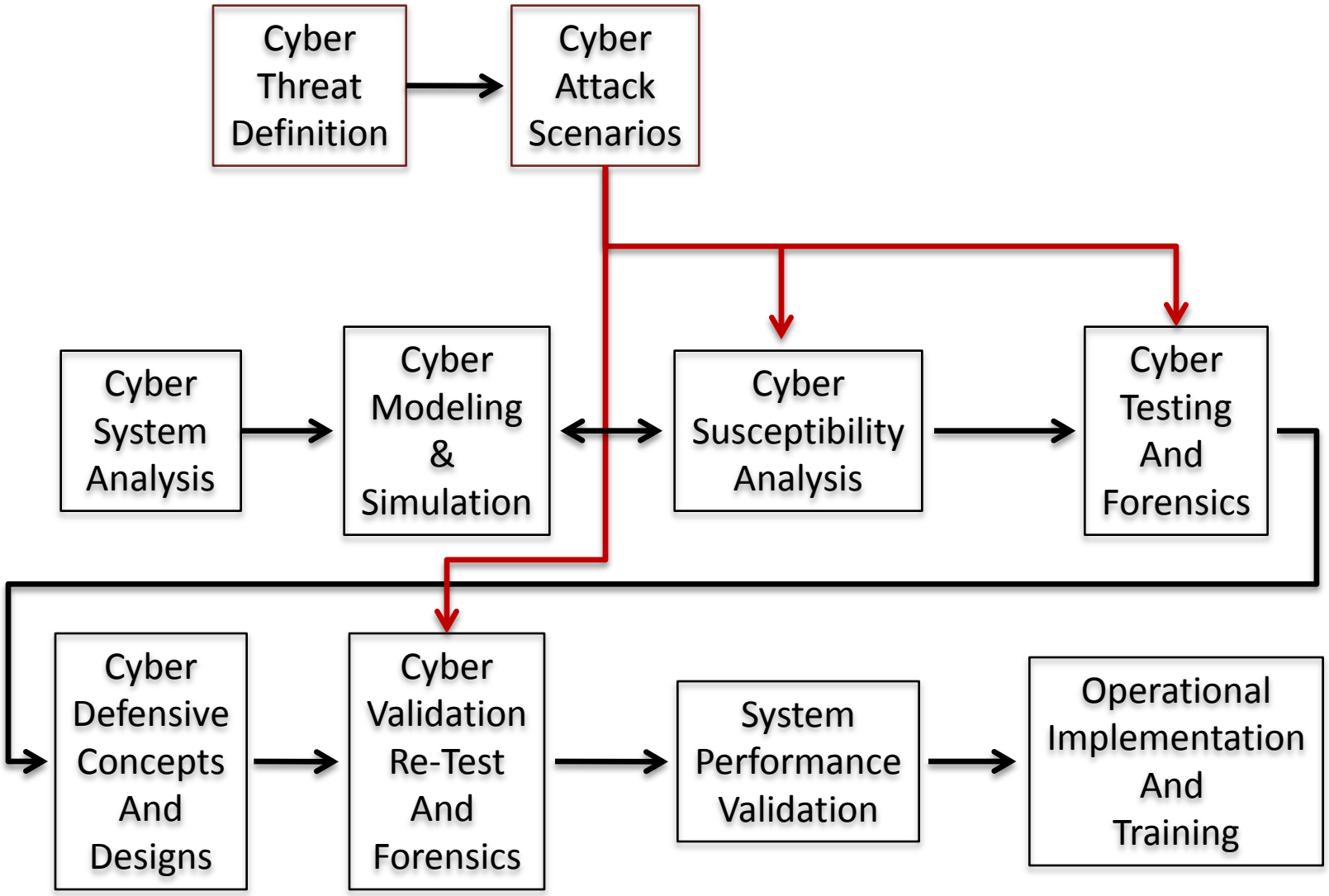
- Methodologies to identify potential failure modes
- Assess the risk associated with failure modes
- Rank issues in terms of importance
- Identify and carry out corrective actions for most serious concerns
- MIL STD – 1629a
- Developed by US Military, published 1949

Risk Reporting Matrix

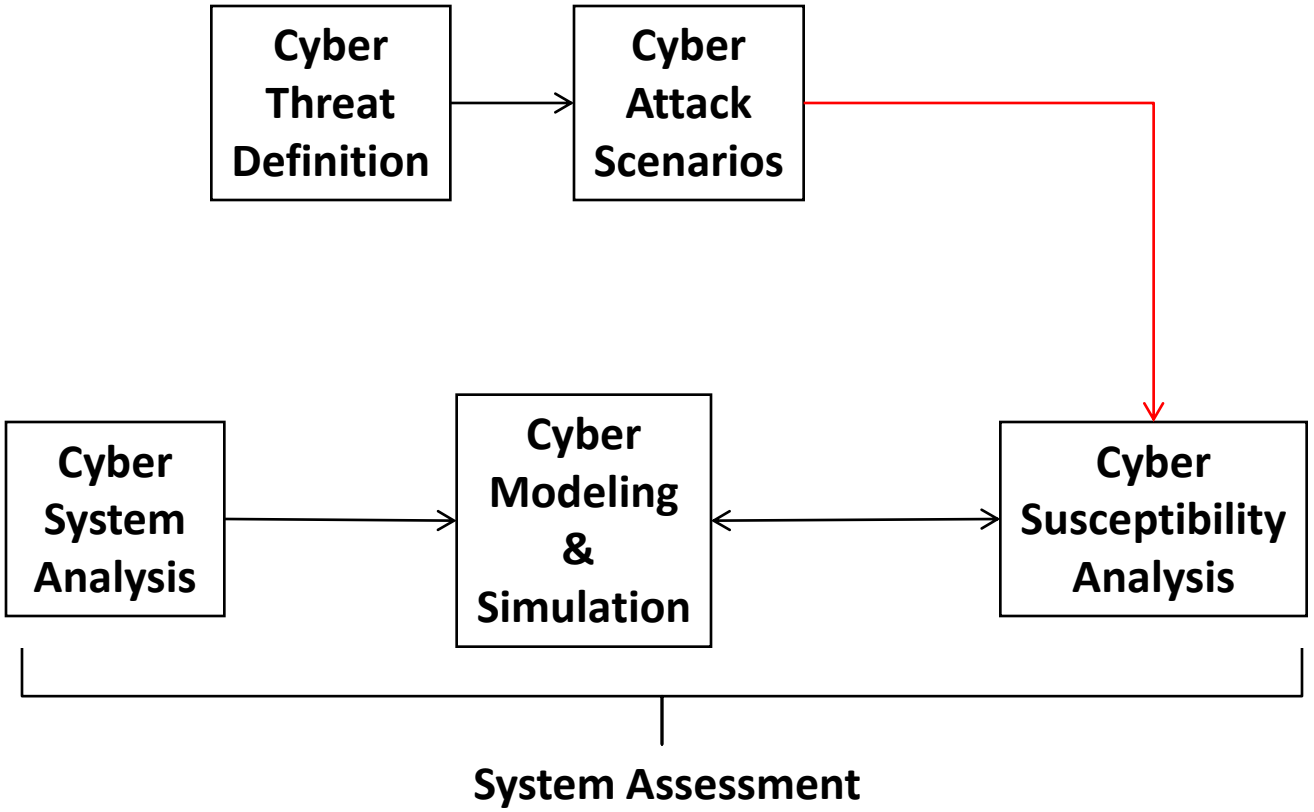


Cyber FMECA (CFMECA)

Cyber Systems Evaluation



CFMECA FLOW DIAGRAM



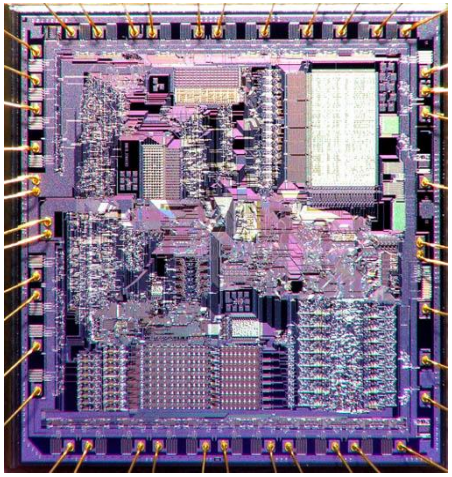
Cyber System Analysis

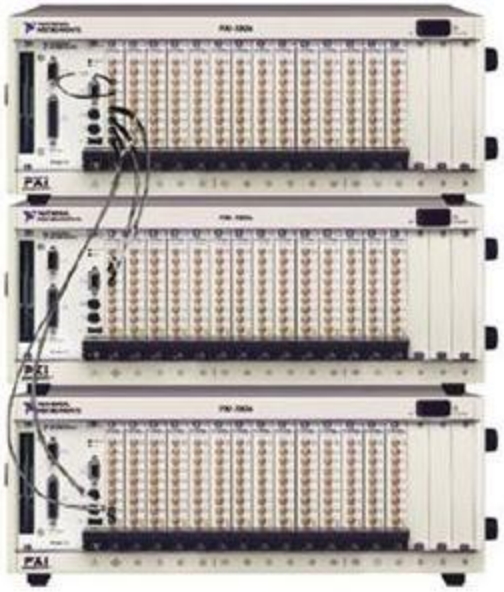
- **Define the system to be analyzed**
  - System boundaries
  - Main system missions and functions
  - Operational and environmental conditions to be considered
- **Collect available information that describes the system to be analyzed**
  - Drawings
  - Specifications
  - Schematics
  - Component lists
  - Interfaces
- **Focus on the Computational Components in the system**

Software Testing

- **Software Penetration Test**
  - Method of evaluating the security of a computer, system or network
- **Simulated Attack from a Malicious Source**
- **Production Environment**
  - Directed at Operational and Configuration Issues
- **Currently Most Common Mechanism Used to "Inject" Security**
- **Tool Driven**

Modeling The Functionality Of The Boolean Mathematics





Model The Mathematical Functionality Of A Single Chip

Model the Mathematical Functionality Of Several Chassis

Model the Mathematical Functionality Of A System

Summary Questions

- How can each part conceivably fail?
- What attack vectors might produce these modes of failure?
- What could the effects be if the failures did occur?
- How is the failure detected?
- What inherent provisions are provided in the design to compensate for the failure?