CyberFMECA
An Adaptation of the FMECA Process to Cyber Effects Criticality Determination

19th Annual NDIA Systems Engineering Conference
24 – 27 October 2016

Roy E. Wilson, CISSP, CEH, Sec+
NAVAIR 4.5.18.3
roy.wilson@navy.mil

Objective

- Build a tool that DOD and industry can use to assess consequences of a cyber attack on a weapon system
- Support risk based decisions for vulnerability remediation
- Repeatable
- Objective
- User friendly
- Provide results as consequence value on risk cube
- Evaluate cyber attack criticality effects on
  - Integrity & Availability (mission impacts)
  - Confidentiality

FMEA/FMECA

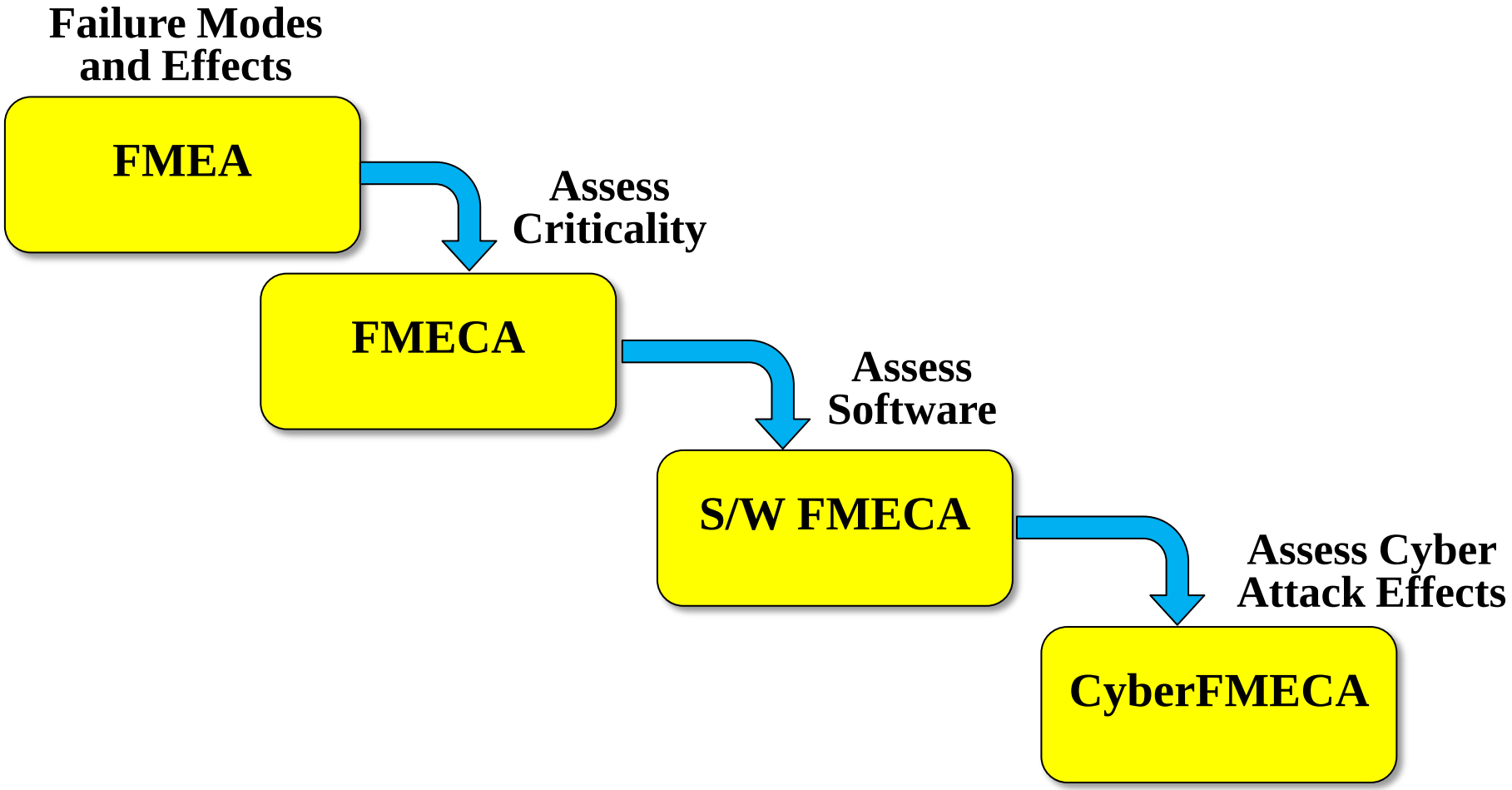
- Analysis of independent single item failures
- Impact on mission success, performance, safety, and maintainability
- Bottom-up analytical method
- Performed at either the functional or piece-part level
- Charts the probability of failure modes against the severity of their consequences
- Highlights failure modes with relatively high probability and severity of consequences
- Typically assumes S/W functions as programmed
- Repeatable
- Objective
- User friendly

FMEA/FMECA Report Format

FMEA																
Identification Number	Item/Functional Identification Nomenclature	Function Number	Function	Functional Failure Letter	Functional Failure Description	Failure Mode & Causes	Mission Phase/ Operational Mode	Failure Effects			Failure Detection Method	Isolation	Compensating Provisions (Design/ Operator)	Severity Classification	Basic Maintenance Actions	Remarks
								Local Effects	Next Higher Effect	End Effect						

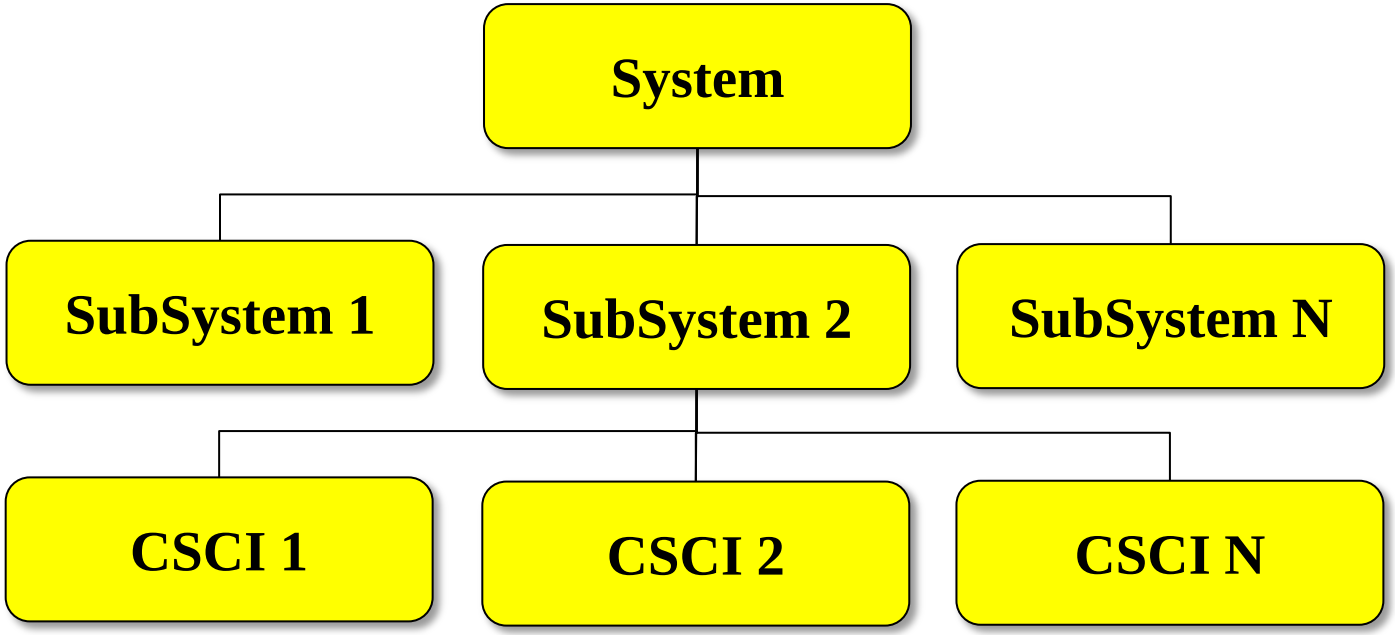
Criticality Analysis													
Identification Number	Item/Functional Identification Nomenclature	Function	Failure Mode & Causes	Mission Phase/ Operational Mode	Severity Classification	Failure Probability OR Failure Rate Data Source	Failure Effect Probability	Failure Mode Ratio	Failure Rate	Operating Time	Failure Mode Criticality #	Item Criticality #	Remarks

CyberFMECA Genesis



CyberFMECA Process

System Decomposition



CyberFMECA Table

ID #	CSCI ID	Function	Malfunction Means	Malfunction Mode	Local Effect	Next Level Effect	System Effect	Criticality Level	Mitigation
1	CSCI 1								
2	CSCI 2								
N	CSCI N								

CyberFMECA Criticality Level

Mission Criticality Level

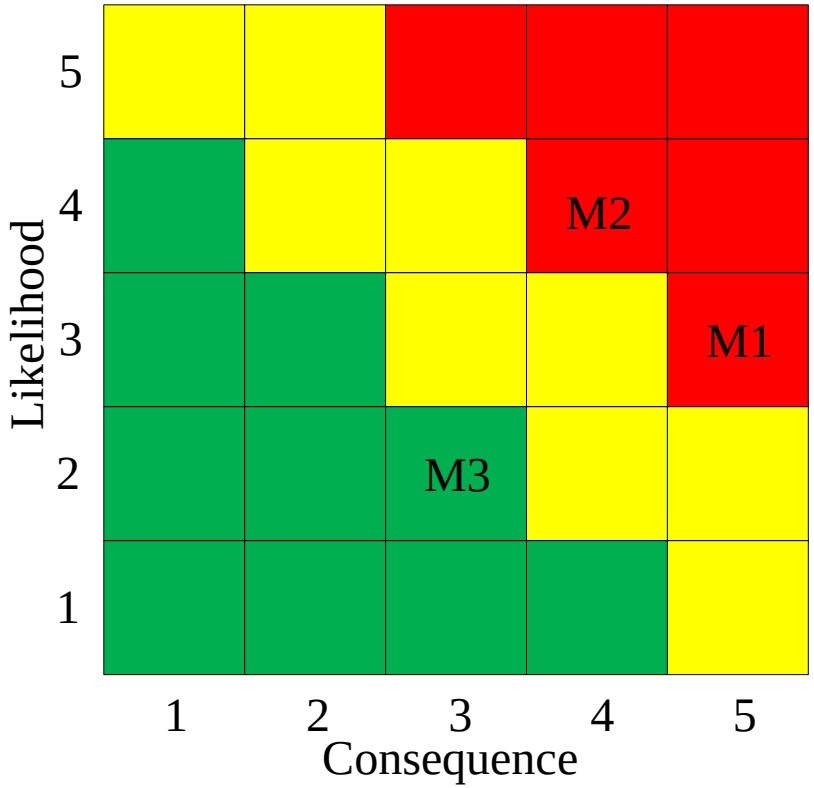
Criticality Level	Description
5	Loss of life or aircraft
4	Loss of full mission capability
3	Loss of partial mission capability
2	Minimal loss of capability
1	No impact

Confidentiality Criticality Level

Criticality Level	Description
5	Exfiltration of TS/SAP or TS/SCI information
4	Exfiltration of TS information
3	Exfiltration of Secret information
2	Exfiltration of Confidential information
1	Exfiltration of CUI/FOUO/SBU information

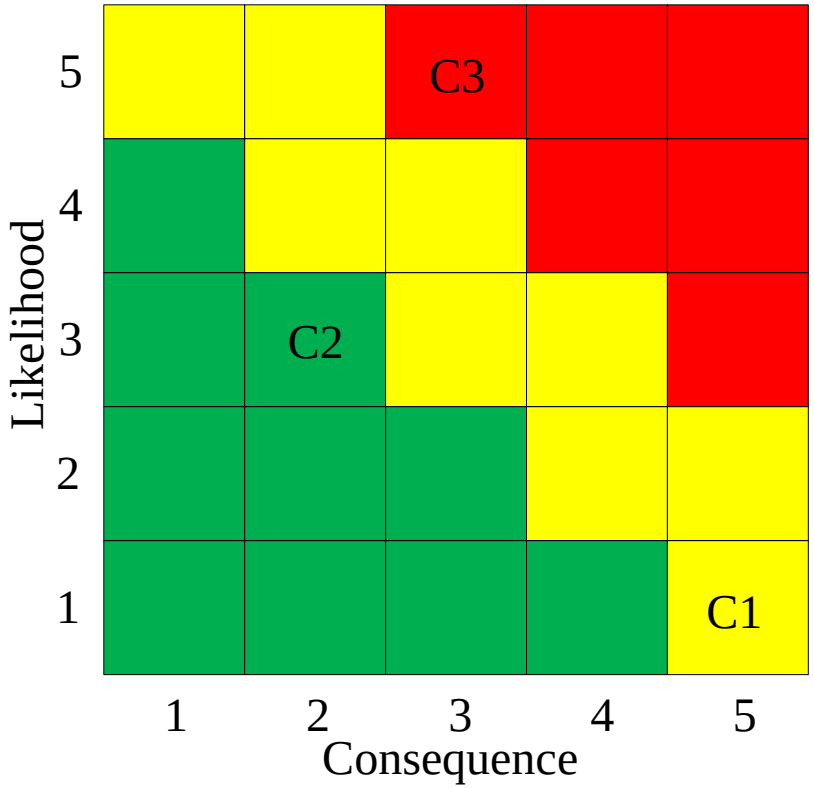
Mission Risk

M1 – Loss of aircraft due to cyber attack on CSCI #4
M2 - Total mission failure due to cyber attack on CSCI #25
M3 – Partial mission failure due to cyber attack on CSCI #14



Confidentiality Risk

C1 – Exfiltration of TS/SAR data due to cyber attack on CSCI #15
C2 - Exfiltration of Confidential data due to cyber attack on CSCI #20
C3 – Exfiltration of Secret data due to cyber attack on CSCI #11



CyberFMECA Summary

- Based upon proven FMEA and FMECA processes
- Repeatable, objective, and user friendly
- Output supports risk based vulnerability mitigation
- Addresses consequences in terms of mission and confidentiality
- Process supports
  - Risk Management Framework system A&A, CYBERSAFE Certification, PPP Criticality Analysis, Cyber Survivability KPP compliance

CyberFMECA Status

- Successfully beta tested by government team on CMBRE
- Under assessment by the CITAG
  - Joint Industry, USAF, & USN aviation systems cybersecurity forum
- Currently required on NAVAIR contracts with
  - Boeing
  - GA
  - LMCO
  - NGC
- Data Item Description developed

Questions?

Think like a hacker!!!