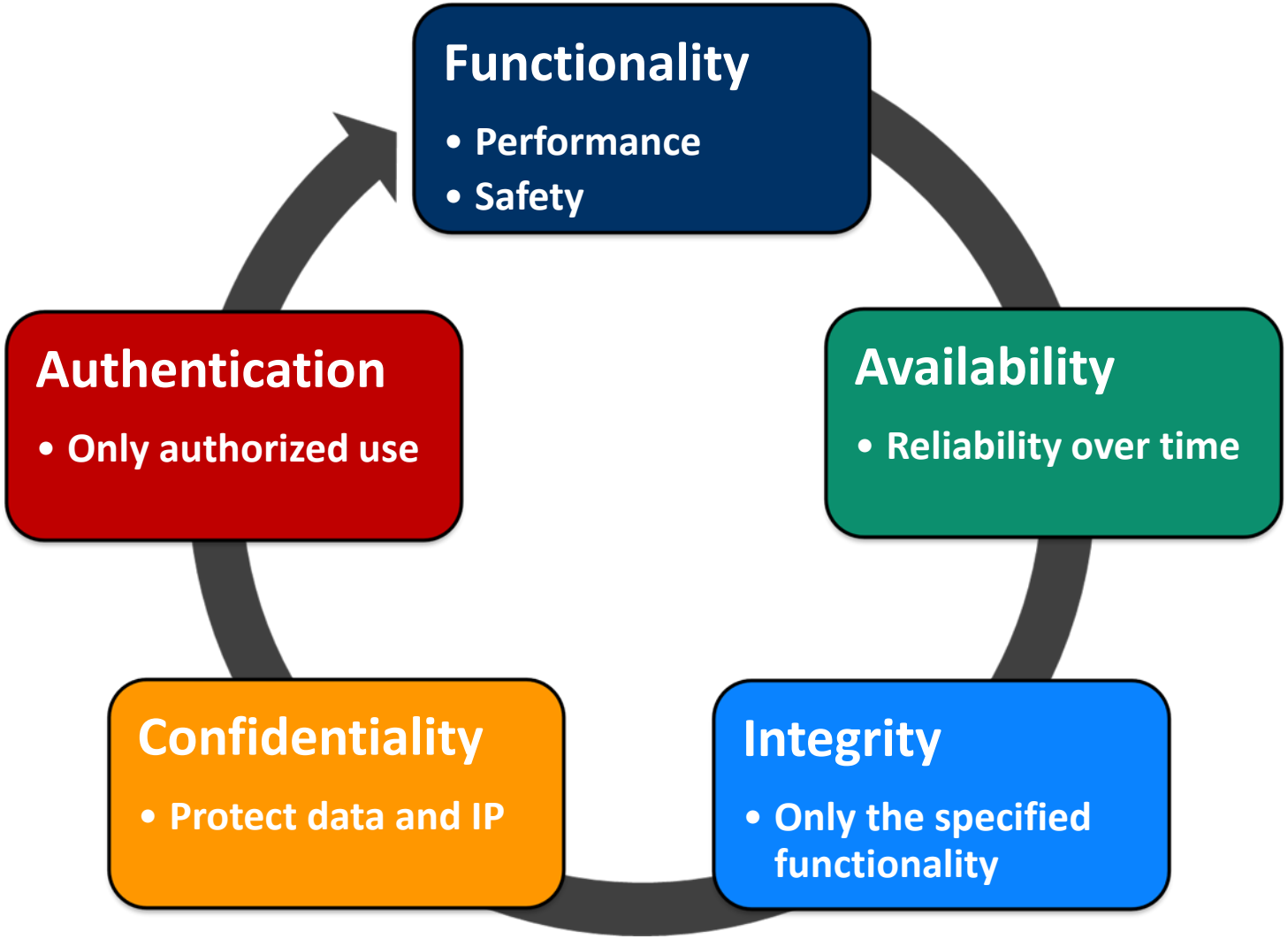
Trusted Computing:
The Convergence of Trusted, Safe, and Secure

Richard Jaenicke

Director, Strategic Marketing and Alliances

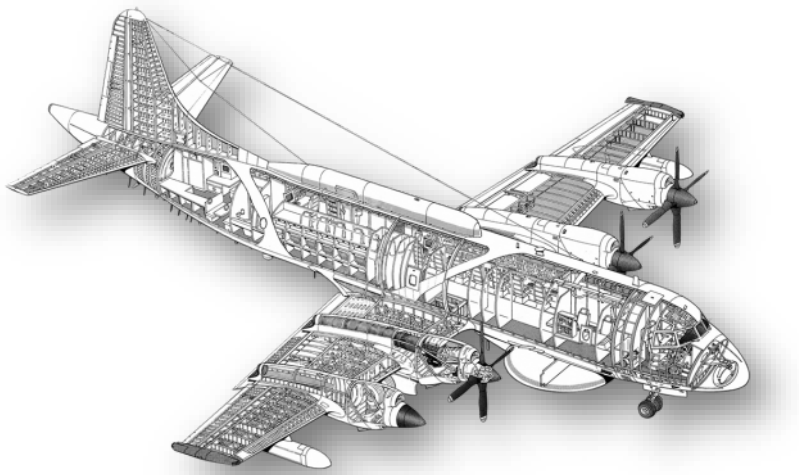
Richard Jaenicke@mrcy.com

Goals of Trusted Computing



Components of Trusted Computing

Trusted Design & Manufacturing

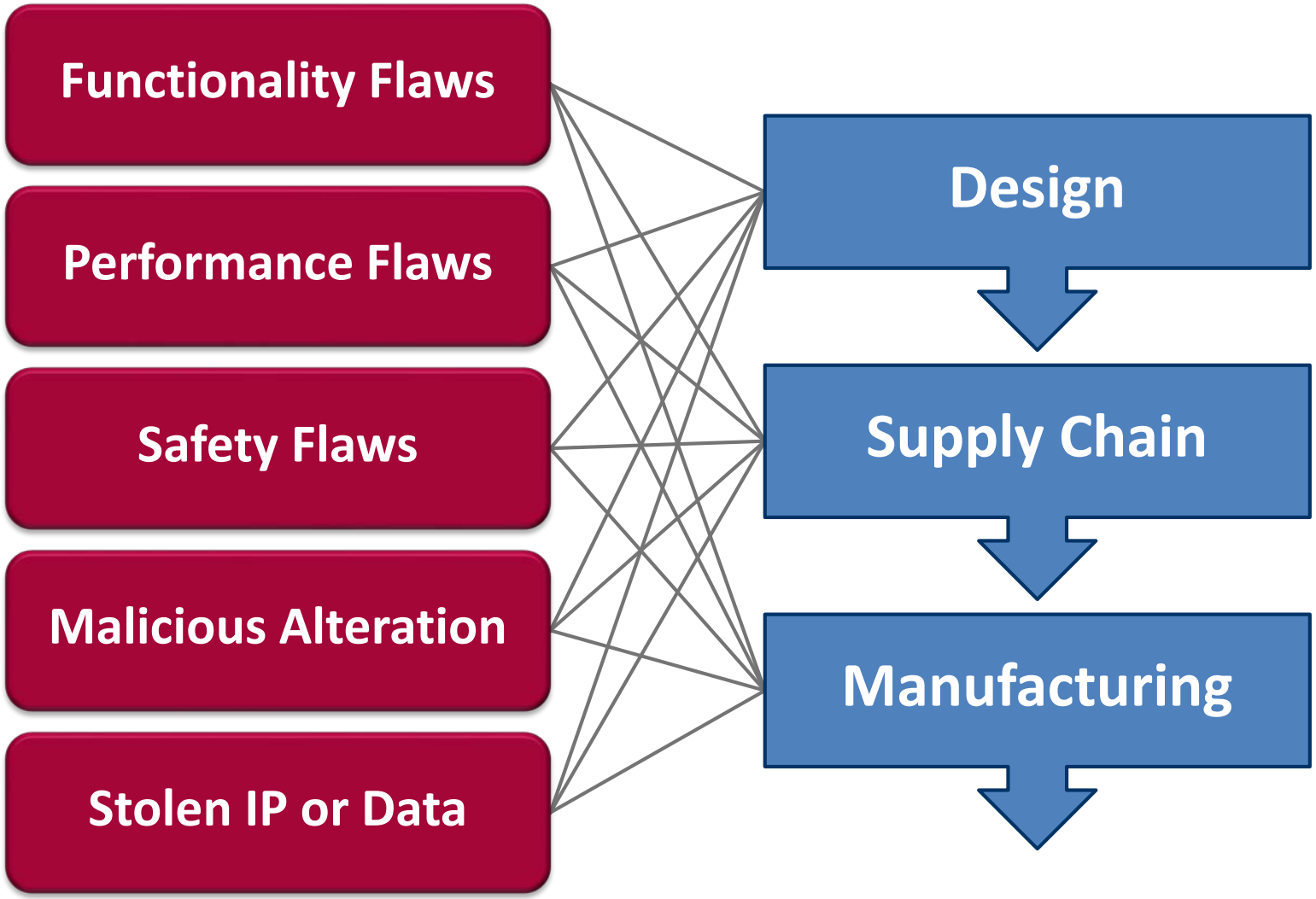


Protecting the Trusted System

Trusted Design & Manufacturing

- Functionality Flaws
- Performance Flaws
- Safety Flaws
- Malicious Alteration
- Stolen IP or Data

Trusted Design & Manufacturing



JSF Supply Chain Compromised

"Secret F-35, P-8, C-130, JDAM data stolen in Australian defense contractor hack"
October 11, 2017

Assurance of Trusted Design & Manufacturing

Issue	Assurance
Performance Flaws	AS9100
Reliability Flaws	VITA 47
Safety Flaws	DO-254 DO-178C
Malicious Alteration	US Persons & US Owned
Stolen Data or IP design data: deployed data:	DFARS Compliant; FIPS 140-2

DFARS clause 252.204-7012, including NIST 800-171

Assurance of Trusted Design & Manufacturing

Issue	Basic	Best
Performance Flaws	AS9100	
Reliability Flaws	VITA 47	Double the Cycles
Safety Flaws	DO-254 DO-178C	DAL-A with in-house certs
Malicious Alteration	US Persons & US Owned	DMEA Certified
Stolen Data or IP design data: deployed data:	DFARS Compliant; FIPS 140-2	James Cogswell Award from DSS; CSfC*

***NSA's Commercial Solutions for Classified**
https://www.nsa.gov/resources/everyone/csfc/components-list/#hw-fde

Protecting Deployed Systems

Cyber

- Disabling or Denying Functionality
- Stealing Data or IP
- Taking control

Reverse Engineering

- Stealing Data or IP
- Redeploying
- Cloning

Commercial Protection Technology Examples

Intel

- **Protected Boot/Boot Guard**
- **Trusted Execution Technology (TXT/TPM)** *SW Root of Trust*
- **Enhanced Privacy ID (EPID)** *HW Root of Trust*
- **Platform Trust Technology (PTT)**
- **Software Guard Extensions (SGX)**

Xilinx

- **Key storage**
- **Bitstream decryption and authentication**
- **Readback disabling**
- **JTAG disable**
- **Environmental monitors**
- **Device DNA**
- **Internal memory clear**

These are some of the best commercial technologies

Commercial Protection is Not Sufficient

"Intel fixes security flaw that plagued its processors for years"
May 2, 2017

- Critical flaw in Active Management Technology (AMT)
- Allows system to be taken over by a remote hacker
- Affects 7 generations of processors over 9 years of production

"Intel Admits Security Flaws Contained in Most PC Chips It Sold for Years"
November 21, 2017

- Researchers uncover critical flaw in Management Engine (ME), Server Platform Services (SPS), and Trusted Execution Engine (TXT)
- Covers 10 different CVEs, including executing arbitrary code with escalation of privilege
- Affects 8 product families over 3 generations

"Meltdown and Spectre Vulnerabilities Affect Nearly Every Computer"
January 3, 2018

- Applications, malware, and JavaScript running in web browsers and other users processes can access kernel memory and memory of other users
- Covers 3 different CVEs, that allow a rogue user to collect secret information such as passwords and authentication keys
- Affects multiple chip suppliers, including 24 Intel product families over 9 generations

Mercury's System Security Engineering

BuiltSECURE™

- Suite of proven, seamlessly integrated software, firmware and hardware for robust system integrity
- Mercury is investing heavily in security IP
  - 30 person security solutions team with decades of expertise
- 4th Generation suite of proven System Security Engineering (SSE) IP
  - Baseline is built-in for Mercury Ensemble Series products
- IP can be applied at chip level, board level, and system level
  - Prevent unauthorized debugging
  - Ensure clock integrity
  - Boot securely
  - Respond to unauthorized access attempts
  - Prevent reverse engineering
  - Secure hypervisor

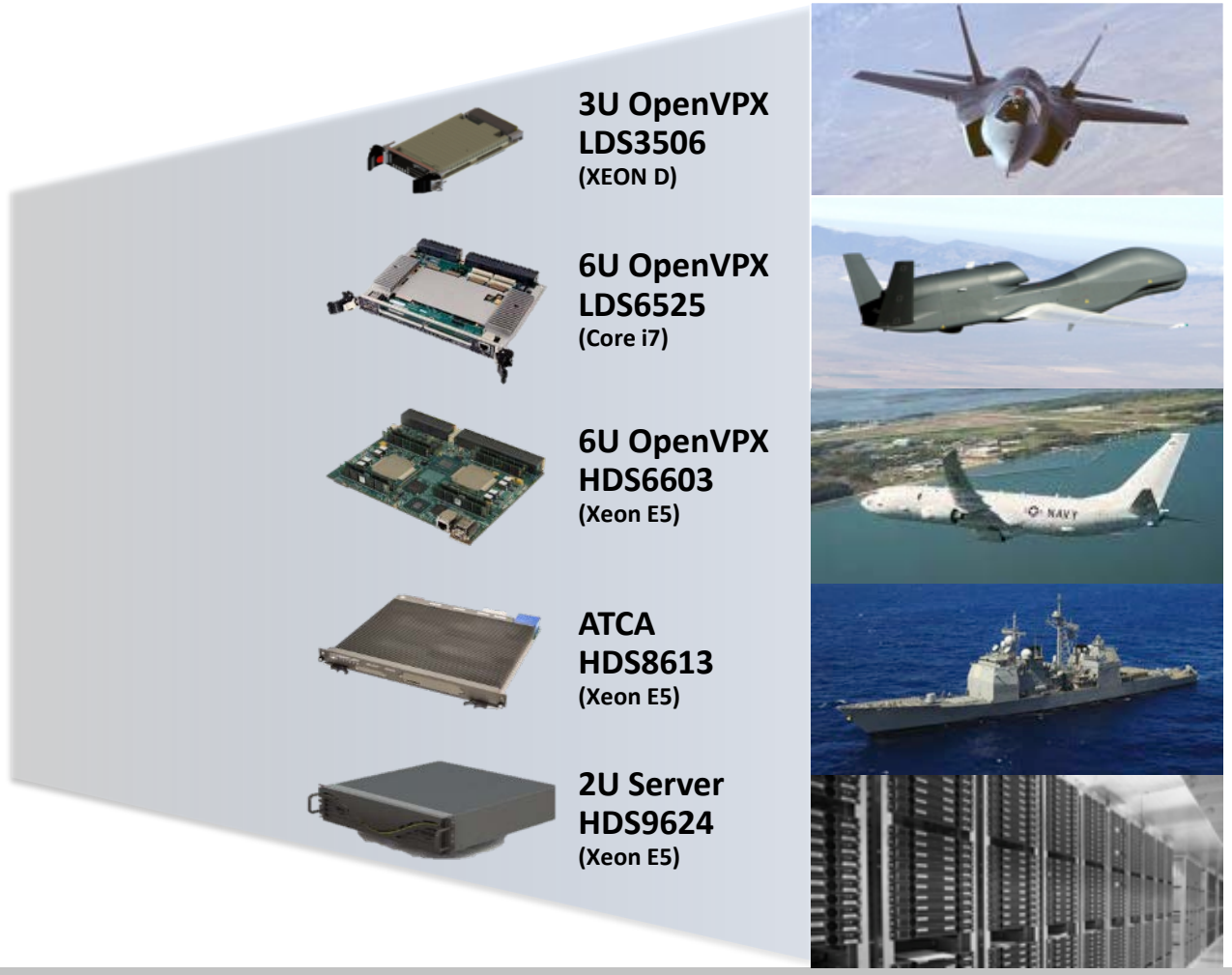
Trusted Product Architecture

mercury systems™

BuiltSECURE™

Trust and Security architectural elements

- Common elements built-in across products lines
  - 3U VPX, 6U VPX, 6U VME, ATCA, ATX
- Extensible architecture may host 3rd party, CFE, and GFE IP, SW, FW and HW



One investment leveraged across multiple missions

For More Information

BuiltSECURE™

www.mrcy.com/BuiltSECURE