Security Architecture in the IoT Age

Stephen L Arnold

Principal Scientist, VCT Labs

Gentoo Linux Developer,

OpenEmbedded and LibreOffice contributor

http://www.vctlabs.com

- Seriously?
  - Stuxnet *
  - Other recent/glaring examples of vulnerabilities being exploited in "enterprise" IT architectures
    (Sony, Anthem, etc)

- Refresher
  - Confidentiality, Integrity, and Availability =>
    - Authentication – users, hosts, nodes
    - Integrity – services, data
    - Non-repudiation – more legal than technical?
    - WRT digital security, the cryptological meaning and application of non-repudiation usually means:
      - proof of both integrity and origin of data
      - high assurance and genuine authentication

- What's *your* risk?

* http://www.pbs.org/newshour/bb/science-july-dec10-computervirus_10-01/

Where do you go for credible cybersecurity information?

- Vendors? Upstream docs? ISC2?
- ACM? IEEE?
- NIST? NSA? DoD?

Previous requirements and implementation guidance was scattered, duplicative, overlapping, conflicting...

Several factors have led to converge in all sectors, ie, federal govt, commercial, open source.

Although relatively recent, current cybersecurity guidance is now much more unified, standards-based, and integrated to fit within a modern risk management framework.

So where do we go?

A great place to get started is the Information Assurance Support Environment site, "your one-stop shop for cybersecurity information":

- https://public.cyber.mil/cyber-training/

Help page, FAQs, acronym list, more, eg:

- https://public.cyber.mil/acronyms/

Contains information and guidance documents, training materials, and guides/tools for everything from requirements to technical implementation to risk management and operations.

Risk Management Framework

Date: Mar 28, 2014 New - *"Cybersecurity Guidance for DoD! - The new cybersecurity overarching guidance for DoD has been published. Included are two new DoD instructions"*:

DoDI 8500.01, "Cybersecurity," replacing previous information assurance (IA) guidance.

- http://www.dtic.mil/whs/directives/corres/pdf/850001_2014.pdf

DoDI 8510.01, "*Risk Management Framework (RMF) for DoD Information Technology (IT),*" replacing the previous DIACAP guidance with an assessment and authorization (A&A) process.

- http://www.dtic.mil/whs/directives/corres/pdf/851001_2014.pdf

RMF Training Video Presentation: Cybersecurity and Risk Management Framework Implementation - Date: May 8, 2014

- http://iasecontent.disa.mil/rmf/rmf_v3.wmv

RMF Training Slide Presentations: Cybersecurity and the Risk Management Framework - Date: April 4, 2014

- http://iase.disa.mil/rmf/Documents/02_RMF_for_DoD_IT_Implementation_v4.pptx

Risk Management Framework Implementation - Date: April 4, 2014

- http://iase.disa.mil/rmf/Documents/01_RMF_for_DoD_IT_v3.pptx

Security Requirements Guides

Security Requirements Guides (SRGs)

- https://public.cyber.mil/stigs/

Security Requirement Guide (SRG) - "*A compilation of Control Correlation Identifiers (CCIs) grouped into more applicable, specific technology areas at various levels of technology and product specificity. An SRG provides DoD specificity to CCI requirements (organizationally defined parameters). An SRG is used by DISA FSO and vendor guide developers to build Security Technical Implementation Guides (STIGs). There are basically two types of SRGs. The first group are the four CORE SRGs which deal with Applications, Networking Devices, Operating Systems, and Policy. The second group are the Technology specific SRGs. A Technology specific SRG is a child of a CORE SRG. For example, the Database SRG was derived from the requirements in the Application SRG.*"

Security Requirements Guides

- Application Server SRG

- Database Security Requirements Guide (SRG)

- Domain Name System (DNS) SRG

- Firewall SRG

- Intrusion Detection and Prevention System SRG

- Mobile Applications SRG

- Mobile Application Store SRG

- Mobile Policy SRG

- Network Device Management SRG (Draft)

- Router SRG (Draft)

- UNIX OS SRG

- Web Server SRG

Control Correlation Identifier (CCI)

- https://public.cyber.mil/stigs/cci/

"*The Control Correlation Identifier (CCI) provides a standard identifier and description for each of the singular, actionable statements that comprise an IA control or IA best practice. CCI bridges the gap between high-level policy expressions and low-level technical implementations. CCI allows a security requirement that is expressed in a high-level policy framework to be decomposed and explicitly associated with the low-level security setting(s) that must be assessed to determine compliance with the objectives of that specific security control. This ability to trace security requirements from their origin (e.g., regulations, IA frameworks) to their low-level implementation allows organizations to readily demonstrate compliance to multiple IA compliance frameworks. CCI also provides a means to objectively rollup and compare related compliance assessment results across disparate technologies.*"

CCI List (draft)

A draft version of the CCI List conforming to the CCI version 2 has been available since last year, containing CCIs derived from NIST SP 800-53.

- http://iasecontent.disa.mil/stigs/zip/u_cci_list.zip

- http://iasecontent.disa.mil/stigs/pdf/u_cci_process_v1r0.1.pdf

- http://iasecontent.disa.mil/stigs/zip/u_draft_cci_specification_v2r0.2.zip

- http://iasecontent.disa.mil/stigs/xls/u_cci_comment_matrix.xls

Security Technical Implementation Guides

- https://public.cyber.mil/stigs/

"The Security Technical Implementation Guides (STIGs) and the NSA Guides are the configuration standards for DoD IA and IA-enabled devices/systems. Since 1998, DISA Field Security Operations (FSO) has played a critical role enhancing the security posture of DoD's security systems by providing the Security Technical Implementation Guides (STIGs). The STIGs contain technical guidance to "lock down" information systems/software that might otherwise be vulnerable to a malicious computer attack."

STIG Documents

STIG Viewing Guide Quick Ref

- http://iase.disa.mil/stigs/downloads/pdf/u_stig_viewer_quick_reference_guide_v1.0.1.pdf

STIGs Master List (A to Z)

- http://iase.disa.mil/stigs/Pages/a-z.aspx

Automate everything:

Security Content Automation Protocol (SCAP) Content and Tools. Various SCAP benchmarks are available, but specific SCAP content is *PKI only

- http://iase.disa.mil/stigs/scap/Pages/index.aspx

- ## DoD / NATO / MOD, NASA, NIST

  - http://en.wikipedia.org/wiki/Department_of_Defense_Architecture_Framework
  - DoDAF, MODAF, other derivatives

- ## OpenGroup

  - http://en.wikipedia.org/wiki/The_Open_Group_Architecture_Framework
  - TOGAF, ADML
  - Model Driven Architecture

- ## Archie

  - http://archi.cetis.ac.uk/
  - ArchieMate

- ## CMM, EA, other guidance

  - eg, http://www.sei.cmu.edu/architecture/
  - http://www.enterprise-architecture.info/index.htm

- Open Source Tools
    - Essential Project
    - Archie
    - Eclipse
        - EPF, EMF, GMT
        - Polarsys, Capella, Kitalpha
    - ArgoUML
        - Supports DoDAF notation
- Other tools
    - IBM System Architect
    - SEI Tools page

# NASA "All" Viewpoint
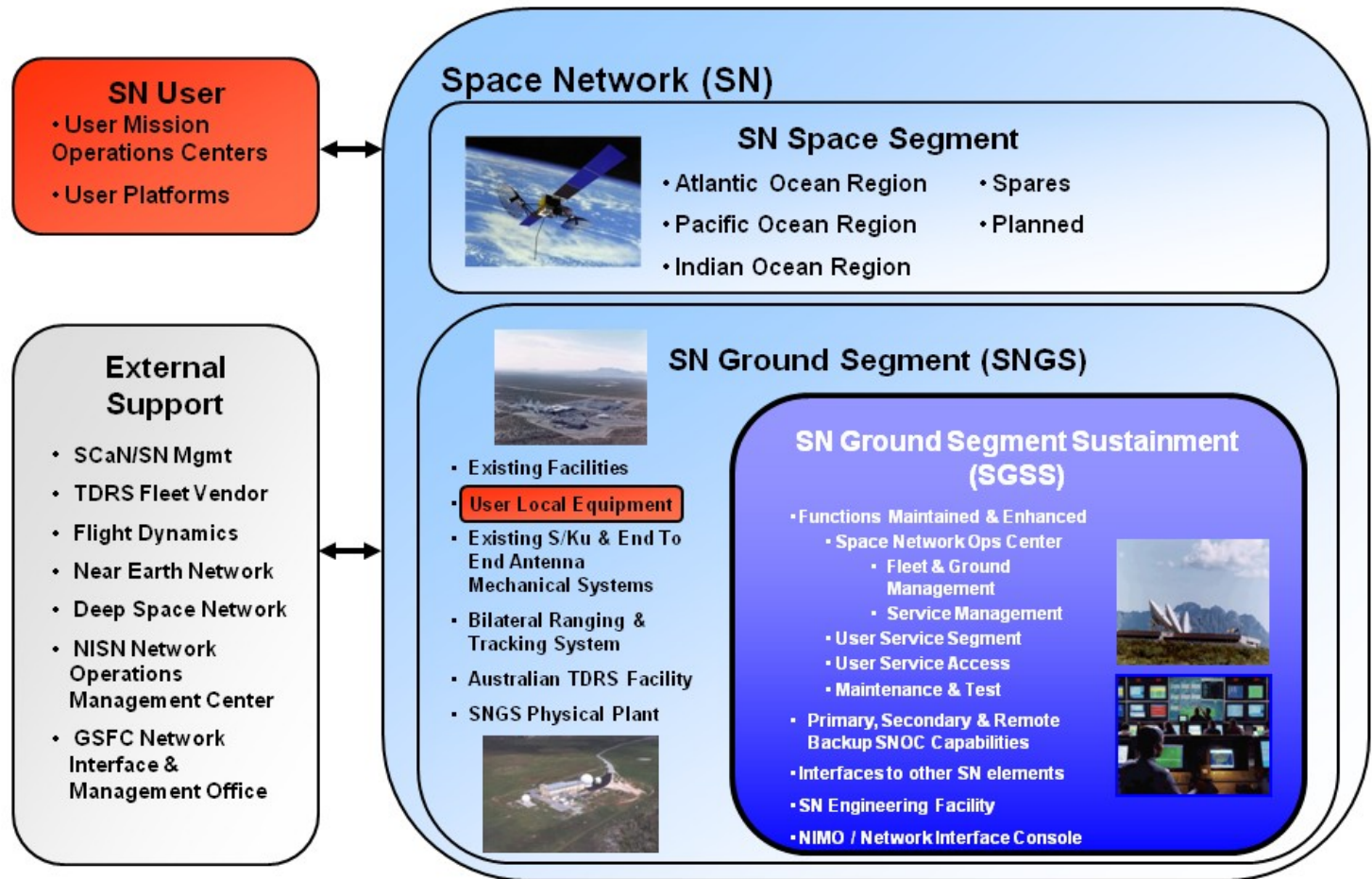
SGSS Context Diagram, Scoping SGSS Within SN & SNGS
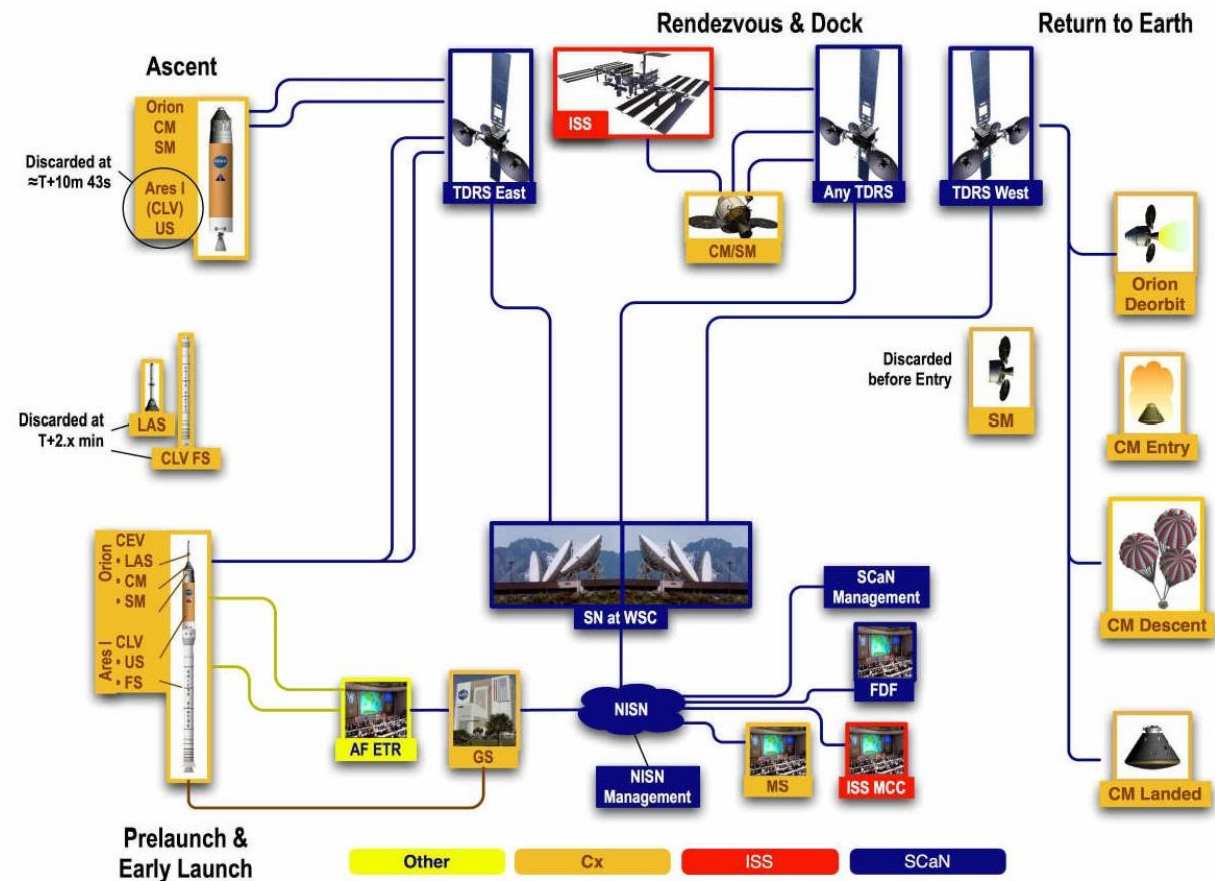
Figure 2 – Overview of the Concept of Operations for the CEV-ISS mission represented using the OV-1
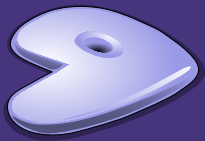
Present SCaN Architecture
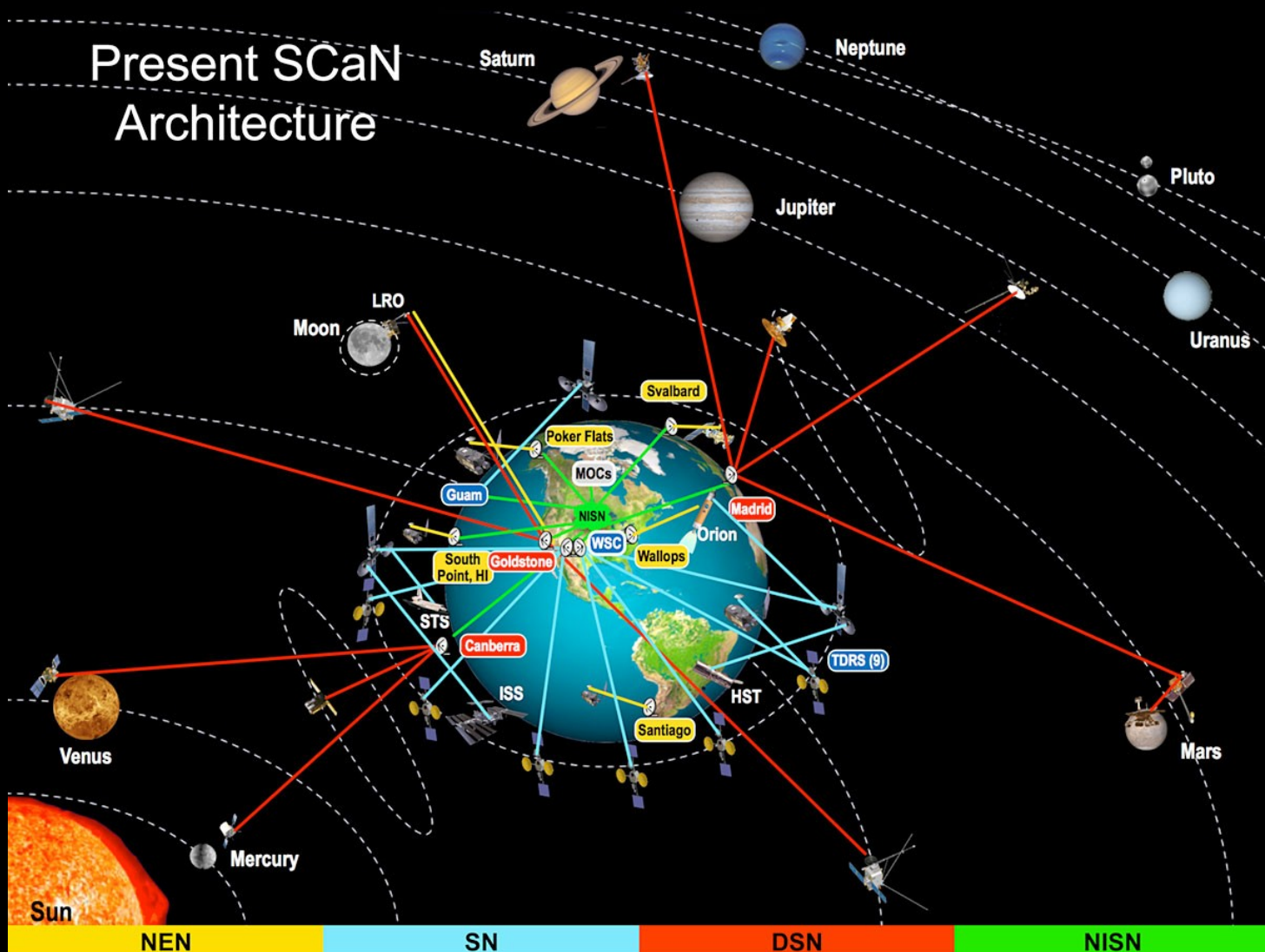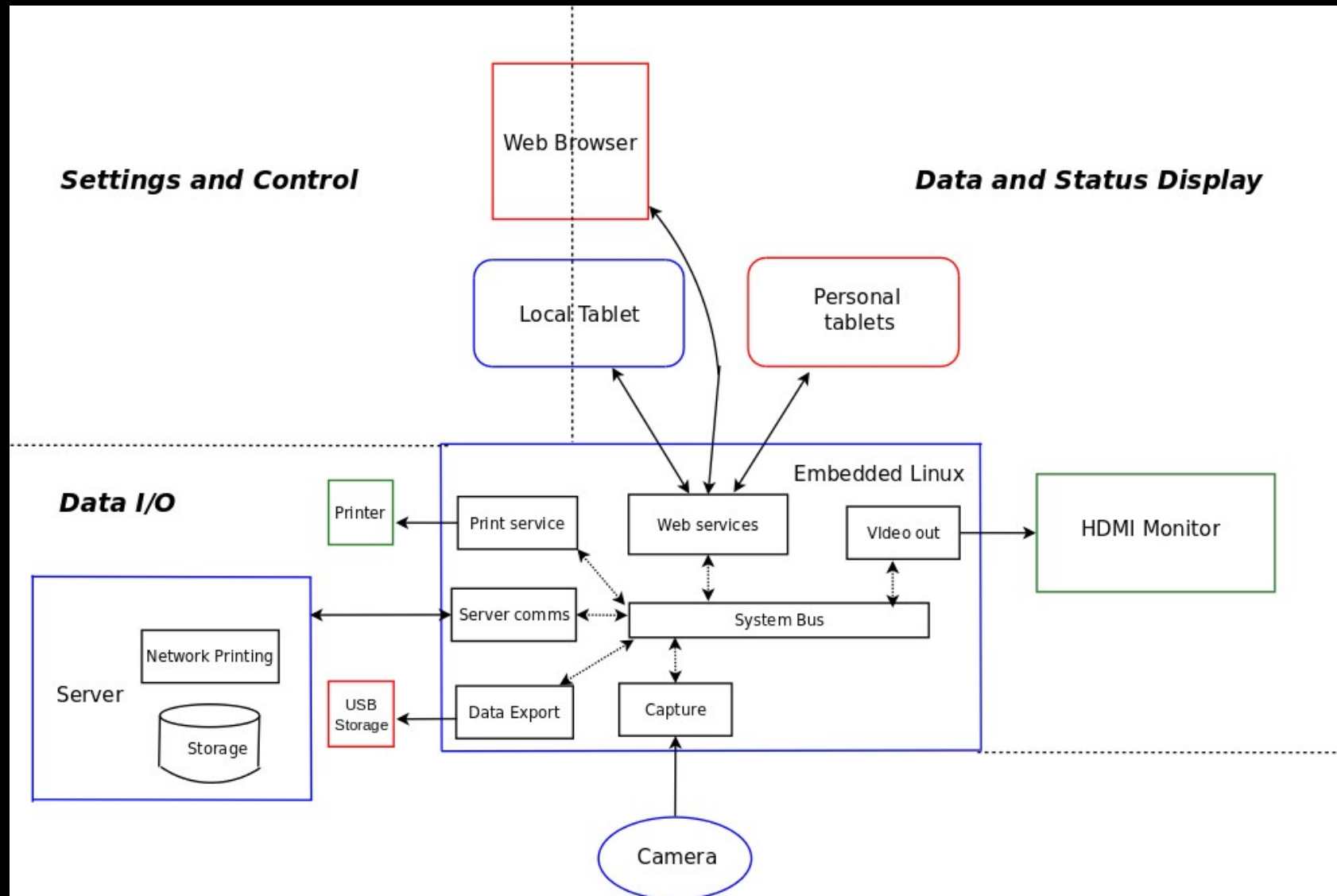
# What are the take-aways?

- Architecture tools and the RMF are pretty much architecture-independent

- Modern embedded and IoT products aren't just opaque devices, but more likely to be a complex system-of-systems

- Modern engineering projects are hard, but you can't just throw up your hands and wave it away

Where next?

- Assess your project
- Defining and understanding your architecture is key
  - *Classify* business/mission-critical systems
  - *Categorize* data sensitivity
  - *Define* your operational environment
  - *Map* requirements to controls
  - *Implement, Test, Verify*
  - *Monitor* operations, *Collect* & *Analyze* data
  - *Feedback* lessons learned, *Reassess* risk

  Communicate

- Integrate RMF with procurement / project management guidance and operations