Secure SW Engineering developments in ESA + OPS-SAT security experiment

CCSDS Spring 2021

M.Wallum – European Space Agency

CCSDS Spring 2021

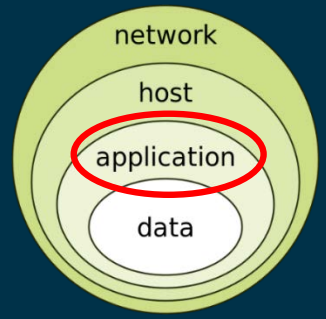
18/05/2021

Security gaps in ECSS

- Space System and Software Engineering follow ECSS (E10, E70C, E40C)

- Security is not an explicit consideration in the ECSS SDLC

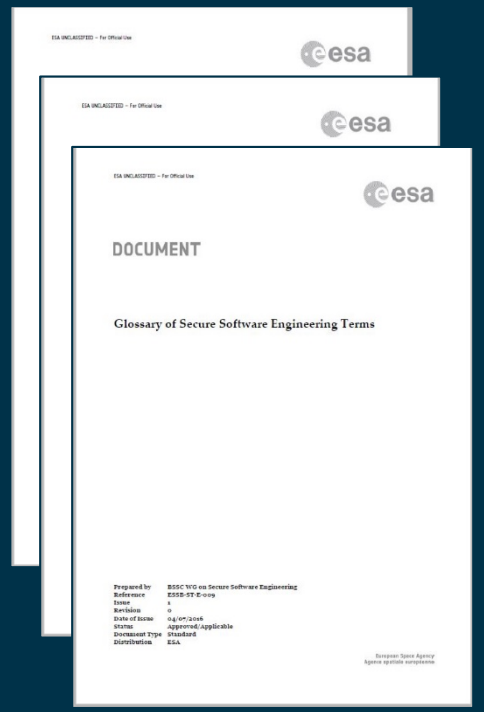
- Critical software systems need appropriate protection as an essential layer of the defence-in-depth model



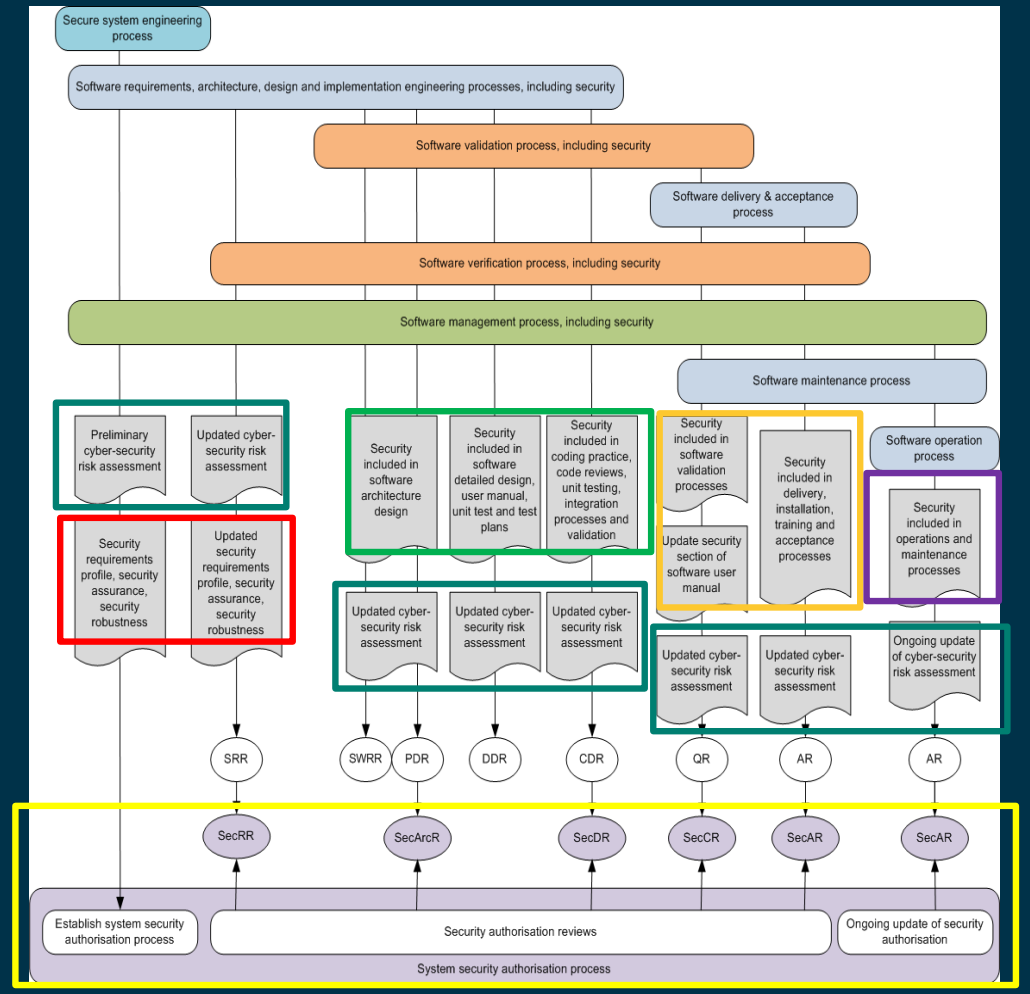
Security gaps in ECSS

- Gap analysis performed and subsequent definition of an ESA-internal Secure Software Engineering (SSE) standard (released 2016).

- Requirements subsequently addressed in 2020/21 as ECSS Security CR resulting in proposed changes to E40 and Q80 standards as well as those proposed for a new system level standard



Key processes



- Cyber-security risk assessment
- Security requirements engineering
- Secure design and implementation
- Security verification and validation
- Secure operations, maintenance and disposal
- Security authorisation (including accreditation & certification processes)
- Supporting methodologies and tools, aimed at simplifying implementation:

-> Security risk management (**SEST**)

-> Security requirements engineering (**GASF**)

-> Automated penetration testing (**PenBox**)

Generic Application Security Framework

ESA Unclassified - For Official Use

DOCUMENT

Generic Application Security Framework

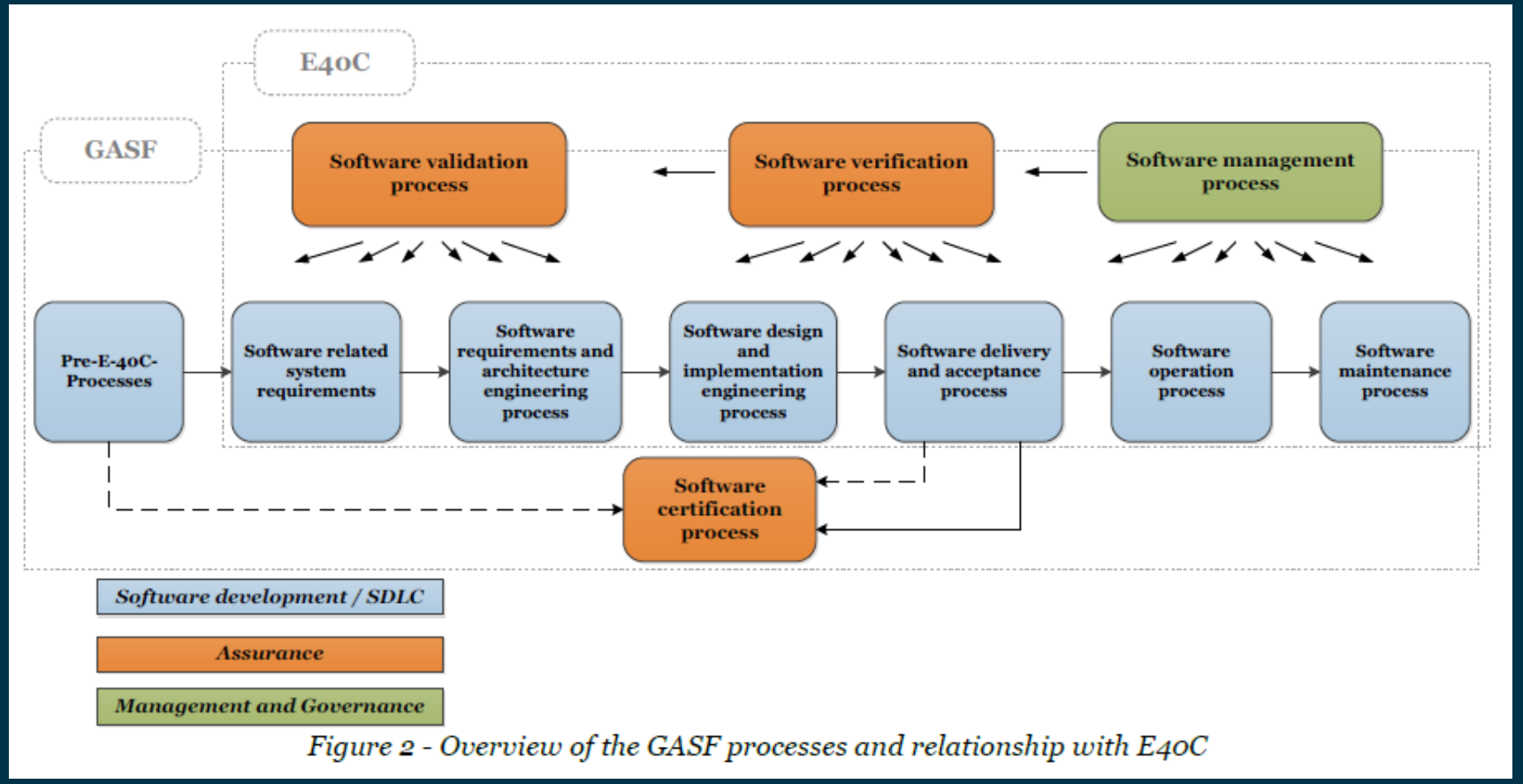
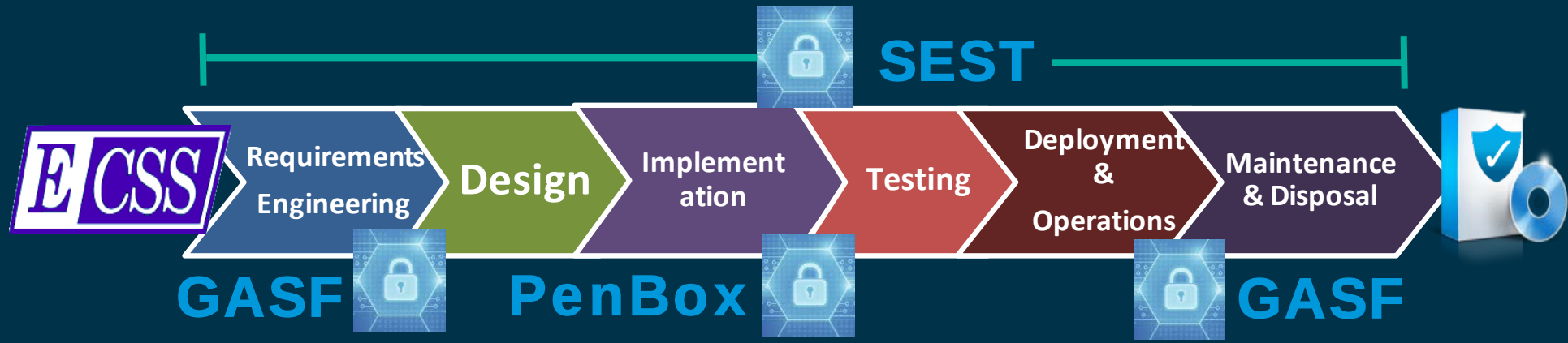
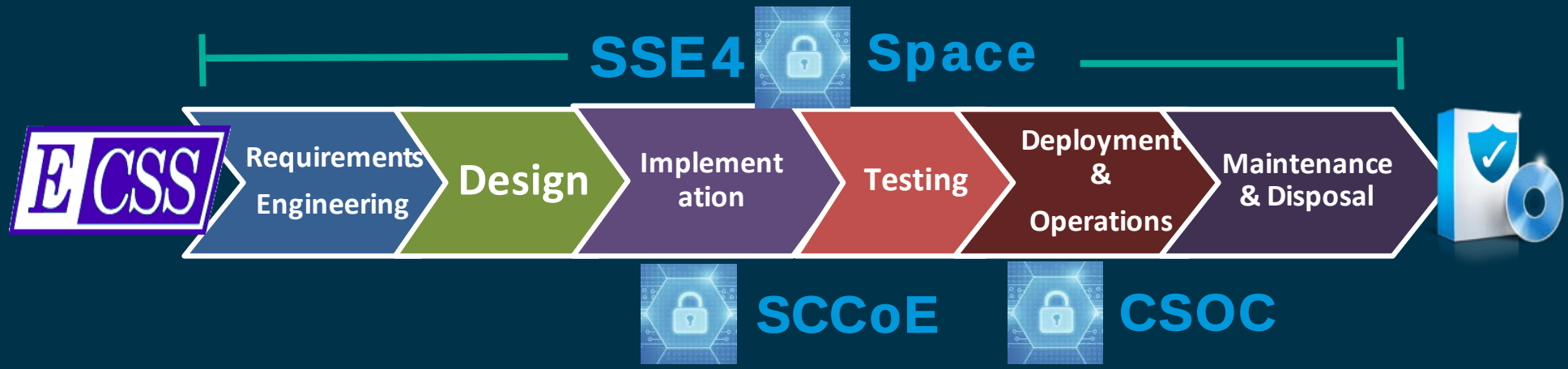


Figure 2 - Overview of the GASF processes and relationship with E40C

Secure Systems Engineering for Space Missions



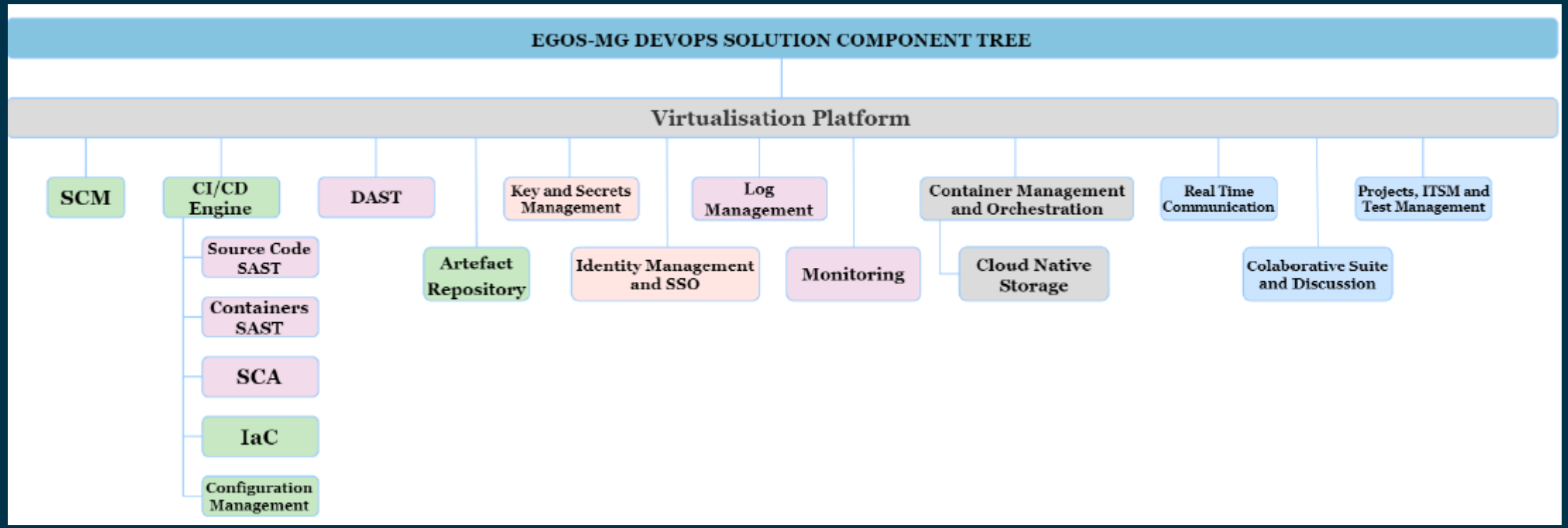
Secure Systems Engineering for Space Missions



- Raising the concept to the system level: address standardisation gaps and integrate all building blocks to develop a framework, including re-usable security data sets based on mission tailoring for E2E secure systems engineering
- Integrate with CSOC and SCCoE development e.g. interchange between threat intelligence, system security risk analysis, security testing

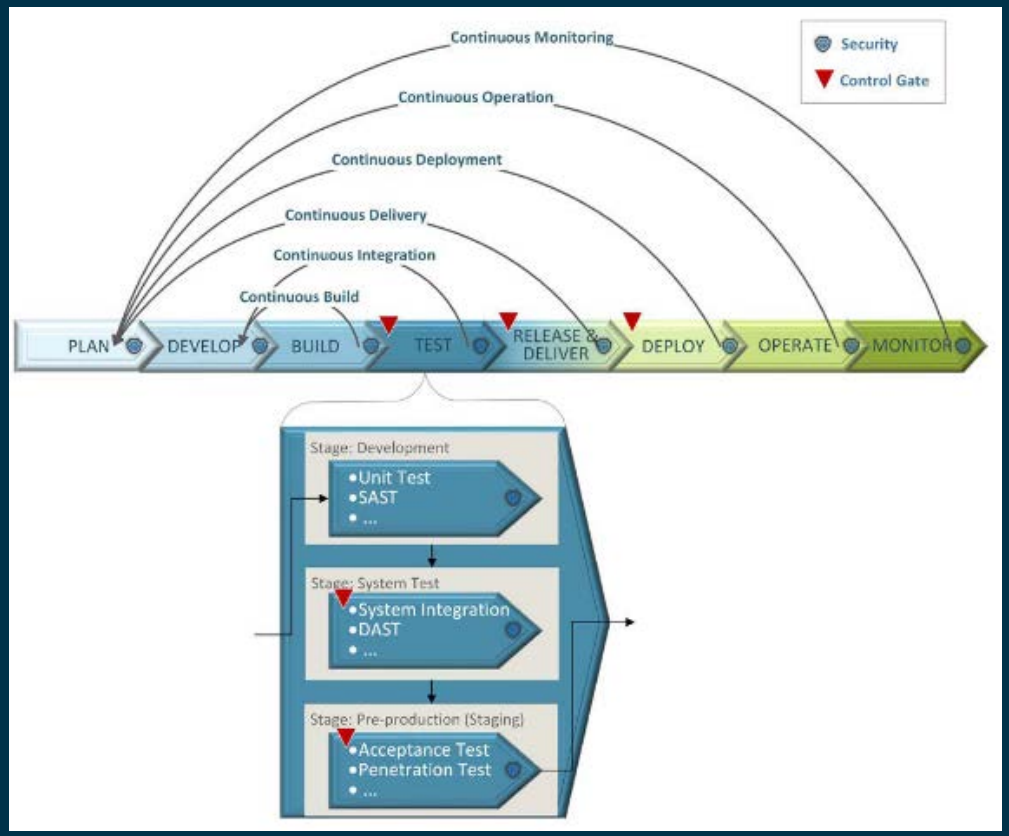
DevSecOps

- Next generation of (multi-mission) ground segment infrastructure will adopt a common dev environment and CI/CD tools – several security challenges



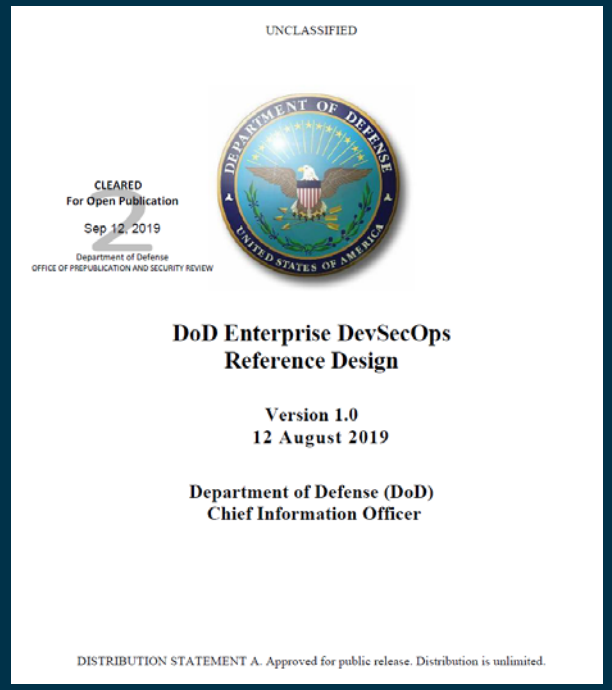
DevSecOps

- Next generation of (multi-mission) ground segment infrastructure will adopt a common dev environment and CI/CD tools – several security challenges



DevSecOps – cloud, containers, k8s, IaC, ..

- Some “recent” useful resources


UNCLASSIFIED

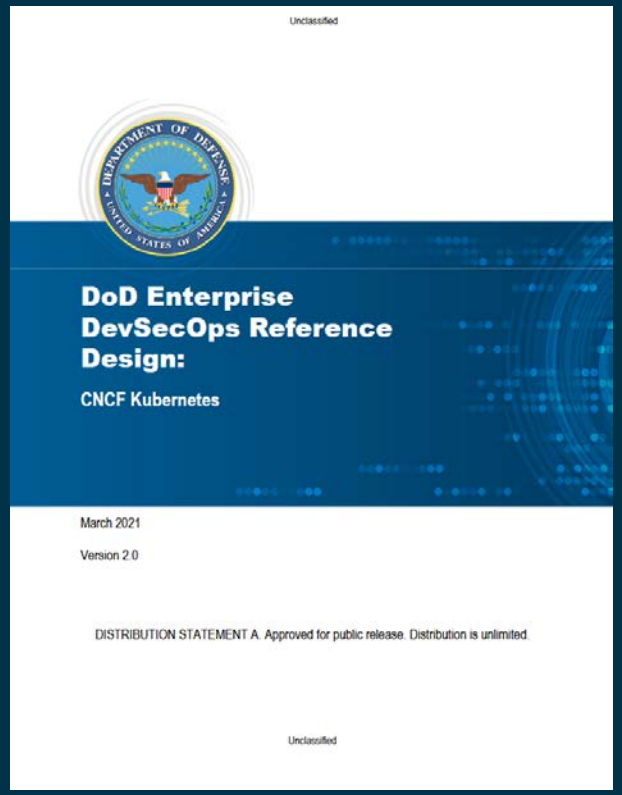
CLEARED
For Open Publication
Sep 12, 2019
Department of Defense
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

DoD Enterprise DevSecOps Reference Design

Version 1.0
12 August 2019

Department of Defense (DoD)
Chief Information Officer

DISTRIBUTION STATEMENT A. Approved for public release. Distribution is unlimited.


Unclassified

DoD Enterprise DevSecOps Reference Design:

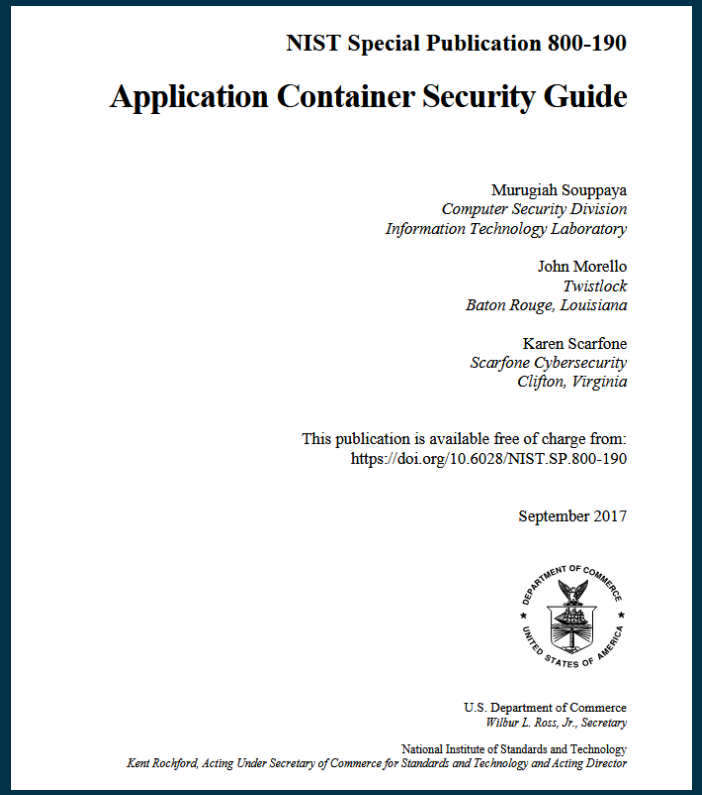
CNCF Kubernetes

March 2021

Version 2.0

DISTRIBUTION STATEMENT A. Approved for public release. Distribution is unlimited.

Unclassified


NIST Special Publication 800-190

Application Container Security Guide

Murugiah Souppaya
Computer Security Division
Information Technology Laboratory

John Morello
Twistlock
Baton Rouge, Louisiana

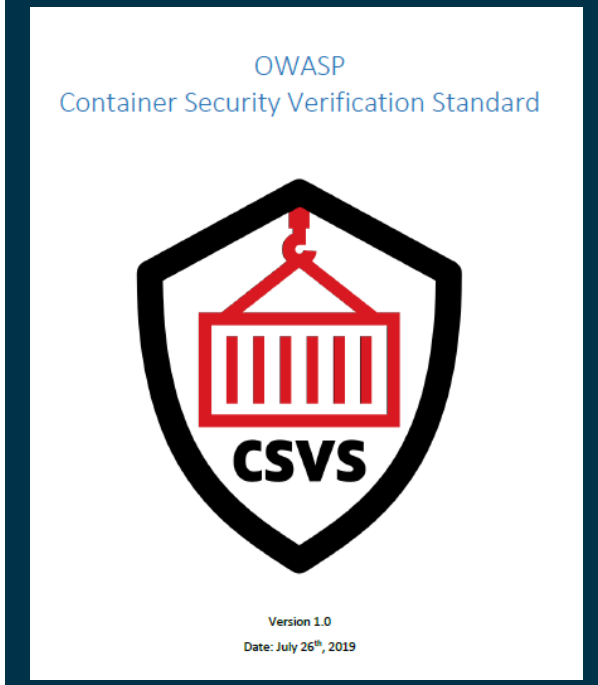
Karen Scarfone
Scarfone Cybersecurity
Clifton, Virginia

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-190

September 2017

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Kent Rochford, Acting Under Secretary of Commerce for Standards and Technology and Acting Director


OWASP
Container Security Verification Standard

CSVS

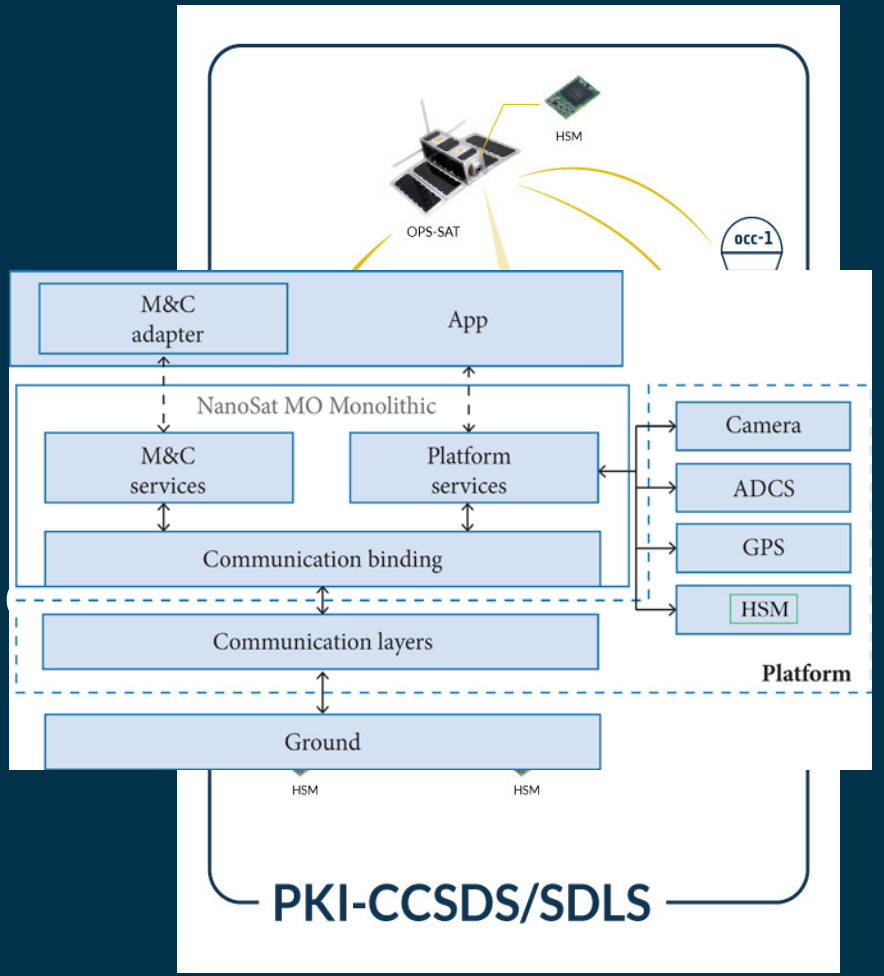
Version 1.0
Date: July 26th, 2019

OPS-SAT Security experiment

- OPS-SAT a 3U cubesat launched December 2019
- 4x higher uplink rate than any ESA spacecraft
- Reconfigurable FPGA
- On-board Linux OS
- Apps in space and IOD of experiments executed by remote experimenters
- Implements Space Packet Protocol, FBO/CFDP and Mission Operations Services through an innovative NanoSat MO Framework (NMF)

OPS-SAT Security experiment

- Definition of MO Security Service
- Definition of CCSDS-compliant Public Key Infrastructure (PKI)
- Implementation of MO Security Service in the NMF using HSM
- NMF App, to be demonstrated on OPS-SAT (if availabl
  - Secure login service using RBAC for inter-app security
  - E2E encryption/digital signature of a file sent from the satellite to the ground



FPGA implementation of (extended) SDLS/EP

- OPS-SAT activity builds upon ongoing work looking into demonstration of HSM-based CCSDS-compliant PKI implementation

3.3 SERVICES PROVIDED BY ADDITIONAL SDLS EXTENDED PROCEDURES

3.3.1 GENERAL

The additional SDLS Extended Procedures provide two different services:

a) Session Management Service;

b) Public Key Infrastructure Service.

- Session Management Services based on Elliptic Curve Diffie-Hellmann (ECDH) for key exchange. Edwards-curve Digital Signature algorithm for authentication and identity verification (EdDSA)

SpaceOps 2021 paper

SpaceOps-2021,14,x1539

SEC_LAB: A Secure Communications Testbed for Space Missions

Marcus Wallum[a], Daniel Fischer[a], Jadwiga Nowotnik[b], Łukasz Pieczonka[b], Mariusz Tkaczyk[b]

[a] Ground Systems Engineering & Innovation Department, Directorate of Operations, European Space Agency, Robert-Bosch-Str. 5, D-64392 Darmstadt, Germany, *marcus.wallum@esa.int*, *daniel.fischer@esa.int*

[b] *Newind Inc, ul. Ostrowskiego 7, 53-238 Wrocław, Poland,* jadwiga.nowotnik@newind.pl, lukasz.pieczonka@newind.pl, mariusz.tkaczyk@newind.pl

www.esa.int