SAE International Position Paper to NIST's Call-for-Papers for EO 14028 Workshop

Standards (Area 2) – SAE International G-32 Cyber Physical Systems Security Committee:

- SAE International established the **G-32 Cyber Physical Systems Security Committee** in 2019. It has been chartered to characterize and address the risk to CPSS (Cyber Physical Systems Security), assess weaknesses and vulnerabilities, and recommend system engineering focused mitigation actions that include hardware and software assurance through the lifecycle, from initiation to disposal, and across the supply chain. The Committee's 280+ members are drawn from a broad cross-sector international stakeholder base, consisting of subject matter experts from Aerospace, Defense, Automotive, Industrial Control Systems, Industrial Internet of Things, Medical Devices, Banking and Finance, and others, with individuals from government and industry that rely on a trusted supply chain, systems and operational security. The G-32 roster also brings in key organizations such as NIST, MITRE and the research community, including academia. SAE International's standards are, and have long been, a powerful embodiment of the benefits of the public-private partnership. Government agencies such as DoD, FAA and NASA, are core constituents in the development, approval, oversight and maintenance of SAE standards and participate alongside industry partners in the technical committees to establish standards which often are aligned and mutually support government procurement and regulation through adoption.
- G-32's documents are intended for broad industry use (commercial, defense, and other high reliability and/or critical systems in aerospace, transportation, medical, finance etc.) and as such promote multi-use supply chains. The Standards currently under development are:

  - ✓ **JA7496** - Cyber Physical Systems Security Engineering Plan (CPSSEP) [post ballot]
  - ✓ **JA6678** - Cyber Physical Systems Security Software Assurance [ballot scheduled Dec 2021]
  - ✓ **JA6801** - Cyber Physical Systems Security Hardware Assurance [ballot scheduled Dec 2021]

- Due to the interconnected nature of CPS and modern supply chains, **JA7496** - Cyber Physical Systems Security Engineering Plan (CPSSEP) integrates with **JA6678**, **JA6801** holistically, connecting system engineering principles with a risk based approach supporting quantified assurance and zero trust initiatives, as next detailed. This set of standards does not attempt to reinvent the wheel, but draws from every major currently applied standard and practice from all the G-32 disciplines and sectors of interest.

"Critical Software" Criteria (Area 1) – G-32 JA6678 defines criteria for the criticality of various types and categories of CPS software and virtual elements, including:

- The physical/virtual state of the software:

  - ✓ Software within the Security Perimeter – G-32's JA6678 defines a broad range of Security topologies, including non-continuous Security Perimeters, seamlessly supporting NIST's Zero Trust Architecture, SP-800-207;
  - ✓ Software within the Trust Perimeter – G-32's JA6678 defines a broad range of Trust topologies, including non-continuous Trust Perimeters, seamlessly supporting NIST's Zero Trust Architecture, SP-800-207;
  - ✓ Software outside the Trust Perimeter;
  - ✓ Software tools and development environment software at large – a category often downplayed by existing standards and practices; this category is not confined by G-32's JA6678 to CPS software, but encompasses a variety of software types, including generic IT software.

- The security-function type of the software, in the scope of its relation to system and HW aspects:

  - ✓ Two types of security functions: (1) security measure, (2) security issue, i.e. – vulnerability, weakness, etc. ;
  - ✓ Three types of relations with non-software aspects (i.e. system, HW etc.) of the system: (1) software exclusive, (2) hybrid software and non-software, (3) non-software;
  - ✓ This taxonomy is represented by a two-dimensional matrix, the axes representing security issues .vs. security measures, each axis consisting the three relation-types.

Integrity Chains & Provenance (Area 5) – G-32's JA6678 provides CPS-specific Guidelines & Taxonomy for CPS Software Security Assurance for both the software supply / development side and the customer / OEM / integrator side, e.g.: Software supply / development side: G-32's JA6678 defines detailed software assurance processes for the entire engineering lifecycle, which aligns with organizations that produce software and, when imposed – will lead to software of high security pedigree. This software assurance process, when executed during the software lifecycle, provides the initial basis for source code provenance.

- Customer / OEM / integrator side: G-32 JA6678 defines standard procedures for the integration of various types of software produced outside the scope of a given development project. Such JA6678 standard procedures for externally developed software are, for instance:

- ✓ For externally developed software items that need to be integrated into the system inside the security perimeter, the establishment of Trustworthiness is required, and until/unless such Trustworthiness is established, this software item is considered a "Vulnerability" for all Security Risk Assessments;
- ✓ For externally developed software items with which the developed system needs to interact, but are outside the security perimeter, the assessment of Trustworthiness is required, and until/unless such Trustworthiness is established, this software item is considered a "Potential Attack Source" for all Security Risk Assessments.

Security Measures Guidelines (Area 3) – CPS-specific Guidelines and Taxonomy are applied by JA6678 for CPS Software Security Assurance development processes, as security procedural measures, e.g.:

- ➢ G-32 JA6678/JA6678/JA6801 are based on the solid foundations of generic system-engineering quality/process assurance and software quality assurance, as practiced by such commonly practiced standards as ISO15288, ISO12207 etc. as appropriate for Cyber Physical Systems' lifecycle. The security foundational aspects of JA6678 are commonly used practices such as NIST SP800-160 and NIST SP-800-82, as appropriate for security system-engineering in general, and for cyber-physical systems in particular – but it also builds on specific sectors' existing practices, such as critical-infrastructure (e.g. power-plants), aerospace and automotive security standards.
- ➢ Such a system/SW/HW holistic framework enables JA6678, for instance, to be closely coordinated with the system level criticality-levels with a unified scale that is also coherent with most other industry standards and best practices, and apply practices such as using the hardware as a "Trust Anchor" for software or "Trust Chains" for supply chains.
- ➢ Thus – applying JA7496/JA6678 should be a relatively low-effort proposition for sectors and organizations already applying such practices, unlike "disruptive" new practices, while sectors or organizations that do not have such existing infrastructure would, as a by-product need to undergo a preliminary process that would bring them to a similar level system-engineering and software-development good-practices as the more mature sectors, considerably enhancing their overall quality even before managing security. G-32's JA6678 compliments existing standards by applying sound software assurance practices.

Software Testing/Verification (Area 4) – A major contribution of G-32's JA6678 is the definition of a Cyber Physical Systems (CPS) specific taxonomy for Software Review, Test and Analysis as Verification Means of security requirements for CPS Software Security Assurance, e.g.:

- ➢ Classic security verification approaches are mostly rigid, assuming either full knowledge of how software was developed, including source code, or no knowledge at all, but for the binary code, at most. In practice, however, Systems' architectures are hybrid, consisting components inherited without full information, and in general – various degrees of information. The intent of JA6678's verification taxonomy is to provide the verifier with the tools to test security objectives over a range of verification categories, the main distinguishable categories being:
  - ✓ Full knowledge and security requirements (white box)
  - ✓ Partial knowledge, security documentation and configuration (gray box)
  - ✓ No knowledge (black box)
- ➢ Classic security testing techniques are also mostly rigid, applying either fully static or fully dynamic testing. G-32's JA6678 diversifies the selection of such techniques, allowing: 1) static analysis, 2) dynamic analysis, and 3) hybrid approach. JA6678 provides methodologies to apply testing in specific situations to achieve optimal test results, providing a verification metric information that can be analyzed.
- ➢ In addition to providing a solid software development process and verification test guidance for software, the document is also explicit about analyzing and reporting metrics of the security test and their communication to stakeholders. Metrics reported via a risk-based expression denote to which extent the security objectives have been met, allowing the software stakeholders to make risk-based decisions within the organization's risk tolerance envelope.

SAE International proposes using the G-32 products as NIST's Cyber-Physical-Systems Acceptable-Means-of-Compliance for EO14028, in accordance with OMB Circular A-119

Proposed Speaker: Christopher Sundberg, Co-Chair of G-32 Software Assurance Task Group
Product Cyber Security Engineer, Woodward Inc.
(970)498-3383
christopher.sundberg@woodward.com