United States
Department of Energy
National Nuclear Security Administration

International Nuclear Security

The Cyber Insider in the Supply Chain

Shannon Eggers, Idaho National Laboratory

WINS International Best Practices Workshop on Mitigating Cyber Insider Threat in the Nuclear Sector
03-05 September 2024

INL/MIS-24-80003

INS International Nuclear Security
Reducing Risk of Nuclear Terrorism

What is the Supply Chain Cyber-Attack Surface?

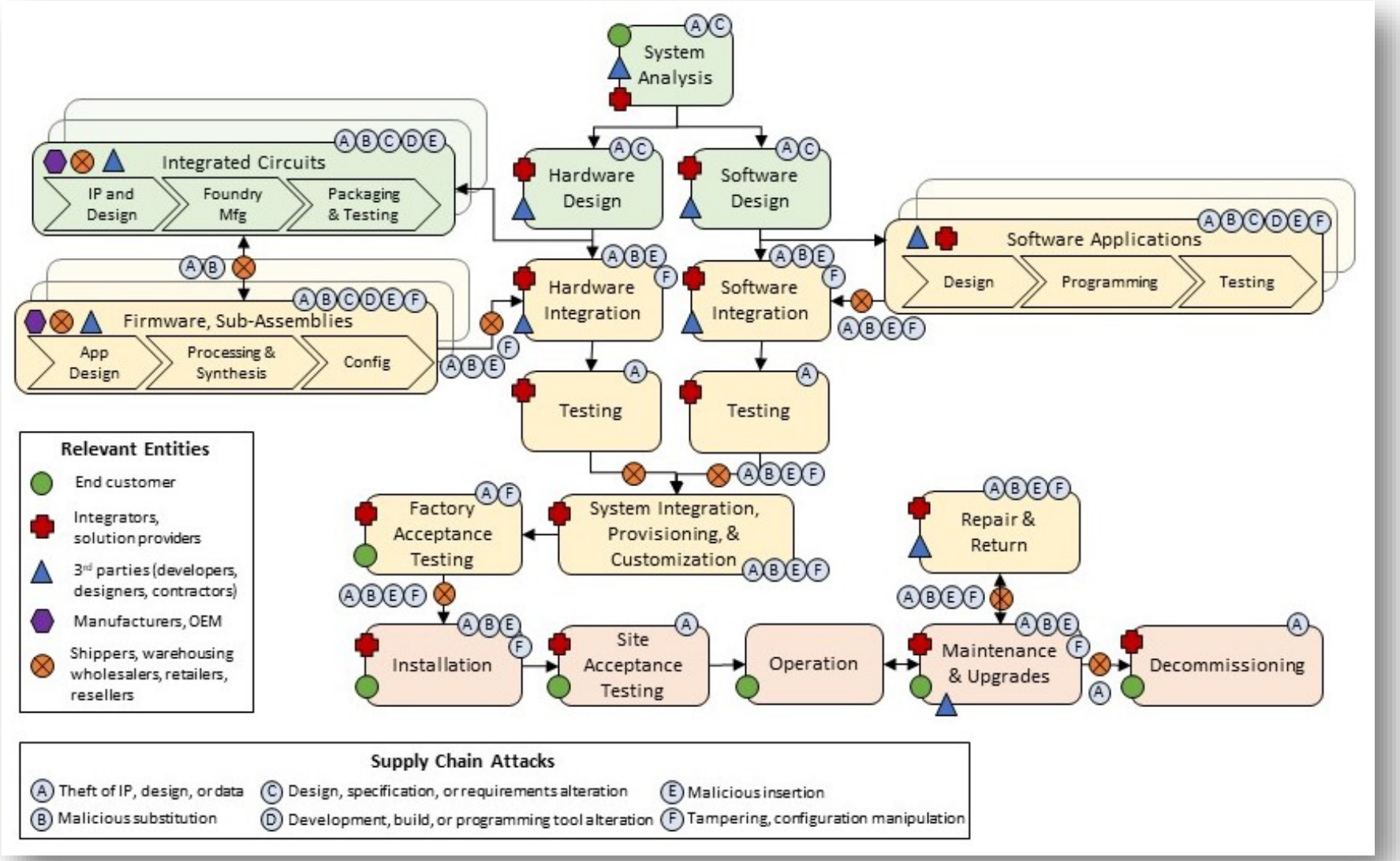
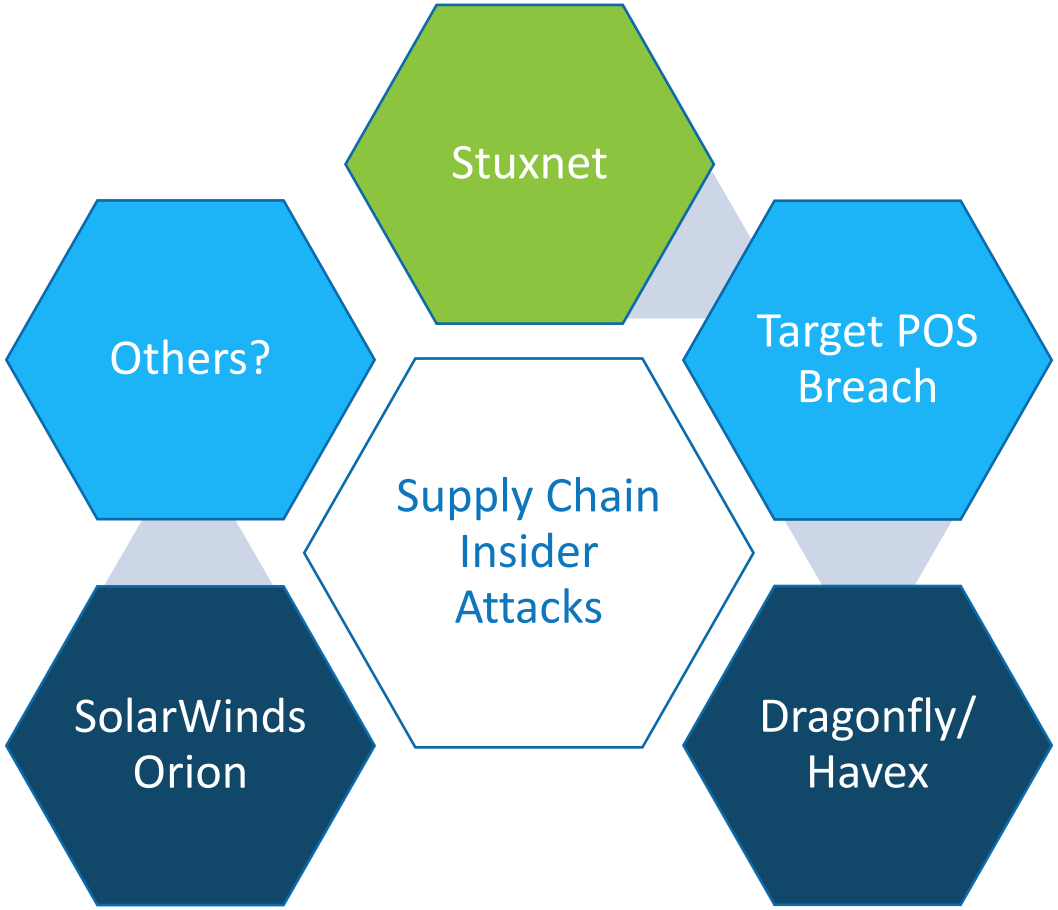


Image source: IAEA TDL-011

Taxonomy of Supply Chain Cyber-Attack Types

Attack Type	Description	Publicly Acknowledged Attacks
Theft of IP, design, or data	Unauthorized disclosure of information from a stakeholder who has a trust relationship with the end target, enabling future attacks and/or causing economic loss. This may include but is not limited to intellectual property (IP), design information, operational/configuration data, or stored secrets (i.e., private key, digital certificates).	Stuxnet, Target breach, Duqu 2.0, CCleaner attack
Malicious substitution	Complete replacement of digital technology, including hardware, firmware, and/or software. Hardware clones or counterfeits may not impact all end users depending on the distribution, whereas a substituted software package may compromise all end users even if only a few were targeted.	ShadowHammer, Dragonfly/Havex, Solarwinds Orion (Sunspot), CCleaner attack
Design, specification, or requirements alteration	Unauthorized modification of design, specifications, or requirements that compromises the design stages and results in the purposeful inclusion of latent design deficiencies (e.g., requirements that result in vulnerabilities) or built-in backdoors.	Dual_EC_DRBG random number generator backdoor
Development, build, or programming tool alteration	Unauthorized modification of the development environment, including platform, build and programming tools, with the intent to corrupt the device under development.	Xcode-Ghost, SolarWinds Orion (Sunspot)
Malicious insertion	Addition or modification of information, code, or functionality directly into a device to cause malicious intent, such as impairing or altering device operation or function.	Stuxnet, Target breach, SolarWInds Orion (Sunburst), NotPetya Ransomware, Kaseya (REvil Ransomware)
Tampering, configuration manipulation	Unauthorized alteration or fabrication of configuration, non-executable data, or sending of unauthorized commands with the goal of impacting device operation or function.	SQL Slammer worm

Are any of these Supply Chain Attacks by an Insider?



- Stuxnet
  - Malware on air gapped system
  - Stuxnet driver was signed with a valid certificate. Twice.
- Target Point of Sale (POS) Breach
  - 3rd party contractor's credentials were stolen and used for access
- Dragonfly/Havex
  - Vendor websites were compromised
  - Malware was inserted into legitimate software and downloaded by customers
- SolarWinds Orion
  - Sunspot: Deployed in build environment; replaces source file with one with Sunburst malware backdoor
  - Software update included Sunburst; downloaded by customers which then allowed further compromise

Hypothetical Supply Chain Insider Attack #1—Software Update Compromise

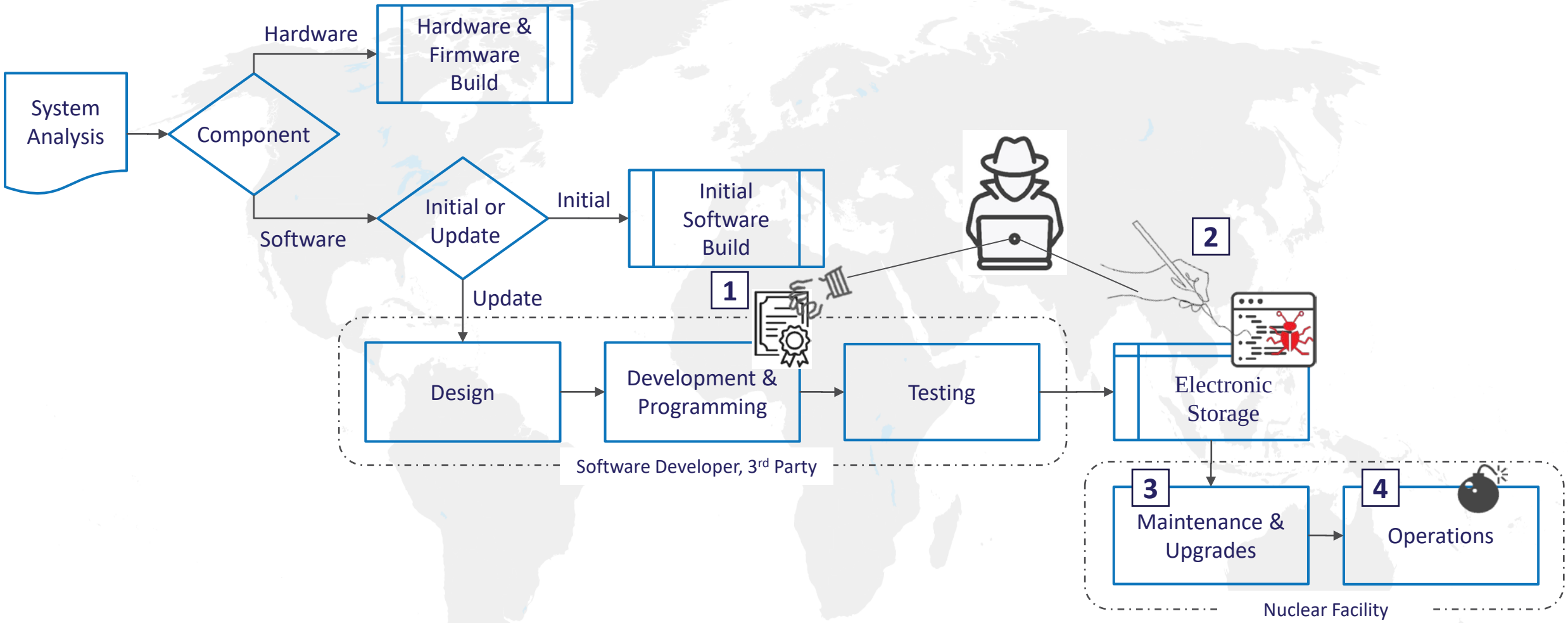


Image sources: www.shutterstock.com

Hypothetical Supply Chain Insider Attack #2—Hardware Configuration Manipulation

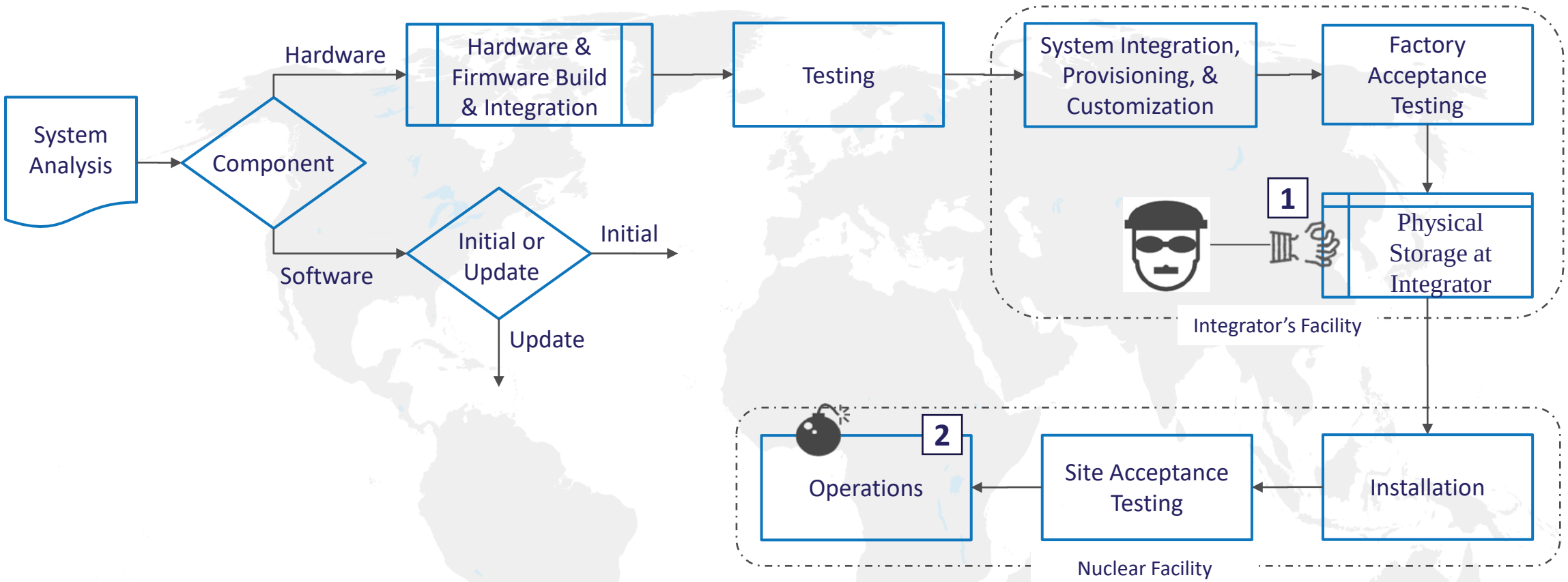


Image sources: www.shutterstock.com

Hypothetical Supply Chain Insider Attack #3—Theft and Release of Confidential Information

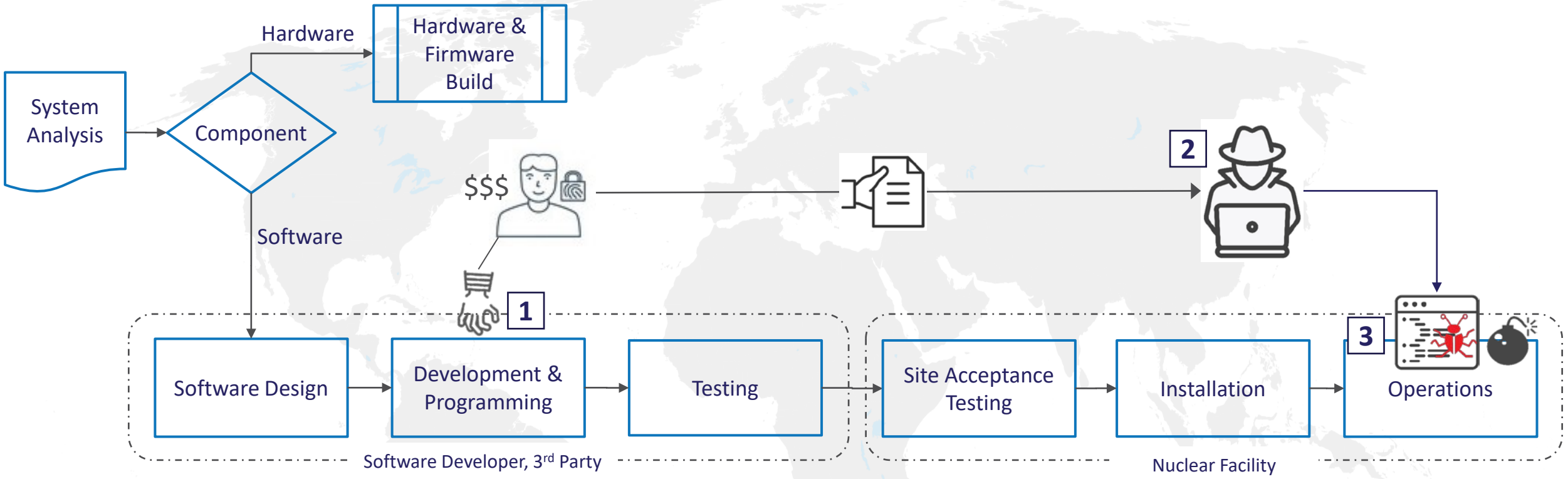


Image sources: www.shutterstock.com

Mitigations for Insiders in the Supply Chain

- Risk-informed approach: Focus first on the sensitive digital asset (SDA) supply chain
- Map the supply chain: Understand the supply chain attack surface for the SDAs; include service providers
- Establish supplier trustworthiness:
  - Establish and verify supplier security capabilities
    - Understand their insider threat mitigation processes
    - Visit and audit/assess suppliers, if possible (could be 3rd party verification)
  - Maintain approved supplier lists
  - Monitor and review supplier's security periodically

Mitigations for Insiders in the Supply Chain (continued)

- Maintain your own facility's supply chain best practices
  - Establish cyber supply chain risk management (C-SCRM) policies and procedures
  - Include cybersecurity in procurement specifications
  - Perform inspections (supplier, on-receipt, prior to use, etc.)
  - Identify and train employees in C-SCRM
  - Maintain existing programs [e.g., Counterfeit, Fraudulent, Suspect Items (CSFI), Nuclear Quality Assurance (NQA-1), etc.]
  - Maintain detection and response capabilities
- Maintain your own facility's insider threat best practices

DISCUSSION

A Selection of Supply Chain References

Domain	Publication
Aerospace	SAE AS5553C, Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition
	SAE AS6081, Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition-Distributors
	SAE ARP9134A, Supply Chain Risk Management Guideline
Defense	DoDI 5000.44, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks
	Defense Acquisition Guidebook, Chapter 9—Program Protection
	DFARS 252.246-7007, Contractor Counterfeit Electronic Part Detection and Avoidance System
	DFARS 252.246-7008, Sources of Electronic Parts
	DoDi 5000.02, Operation of the Defense Acquisition System
	DoDD 5200.47E, Anti-Tamper
	Cybersecurity Maturity Model Certification (CMMC)
Energy	DOE Cybersecurity Capability Maturity Model (C2M2)
	EPRI Cyber Security Procurement Methodology for Power Delivery Systems
	ESCSWG, Cybersecurity Procurement Language for Energy Delivery Systems
	NERC CIP-013-1, Cyber Security-Supply Chain Risk Management
Nuclear	EPRI Cyber Security in the Supply Chain: Cyber Security Procurement Methodology
	EPRI Secure Development, Integration, and Delivery (SDID) Audit Topical Guide
	NEI 08-09 Addendum 3, Cyber Security Plan for Nuclear Power Reactors, Systems and Services Acquisition
ICS	DHS Cyber Security Vendor Procurement Language for Control Systems
	IEC 62443-2-4, Security Program Requirements for IACS Solution Suppliers
	IEC 62443-4-1, Secure Product Development Lifecycle Requirements
	UL 2900-2-2, Part 2-2, Particular Requirements for Industrial Control Systems

A Selection of Supply Chain References (continued)

Domain	Publication
ICT	CISA, Vendor Supply Chain Risk Management (SCRM) Template
	CISA, Threat Evaluation Working Group: Supplier, products, and services threat evaluation
	CISA, Mitigating ICT Supply Chain Risks with Qualified Bidder and Manufacturer Lists
	Crossley, C., Software Supply Chain Security: Securing the End-to-End Supply Chain for Software, Hardware, and Firmware
	ENISA, Good Practices for Supply Chain Cybersecurity
	ENISA, Threat Landscape for Supply Chain Attacks
	ISO/IEC 27036-3, Information Security for Supplier Relationships, Part 3, Guidelines for ICT Supply Chain Security
	ISO/IEC 20243-1, Information Technology-O-TTPS-Mitigating maliciously tainted and counterfeit products
	NISTIR 7622, Notional Supply Chain Risk Management Practices for Federal Information Systems
	NIST SP 800-82, Guide to Industrial Control Systems (ICS) Security
	NIST SP 800-147, BIOS Protection Guidelines
	NIST SP 800-147b, BIOS Protection Guidelines for Servers
	NIST SP 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations
	UL 2900-1, Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements
Software	SAFECode, Fundamental Practices for Secure Software Development
	SAFECode, The Framework for Software Supply Chain Integrity
	SAFECode, Managing Security Risk Inherent in the use of Third-Party Components
	CISA, Defending Against Software Supply Chain Attacks
	NTIA, Framing Software Component Transparency: Establishing a Common Software Bill of Materials

INS International Nuclear Security

Reducing Risk of Nuclear Terrorism