2019 NDIA GROUND VEHICLE SYSTEMS ENGINEERING AND TECHNOLOGY SYMPOSIUM
GROUND SYSTEMS CYBER ENGINEERING TECHNICAL SESSION
AUGUST 13-15, 2019 - NOVI, MICHIGAN

DEMYSTIFYING PLATFORM CYBER RESILIENCE

Cheri Lofy[1], **Dr. Mark Vriesenga**[2]

[1]C4ISR Mission Systems, BAE Systems, San Diego, CA 92127
[2]FAST Labs Cyber Technology, BAE Systems, San Diego, CA 92127

ABSTRACT

Today's platform systems (satellites, aircraft, surface ships, ground vehicles, and subsurface vehicles) have large numbers of electronic components including microprocessors, microcontrollers, sensors, actuators, and internal (onboard) and external (off-board) communication networks. Hardening and securing these systems is currently performed using checklist approaches like the Risk Management Framework (RMF) that derive from decades of information technology (IT) best practices. However, these approaches do not translate well to platforms because they inadequately address security issues that are unique to cyber-physical and the embedded nature of platform systems.

In this paper, we describe key resilience concepts and two analytic models for improving platform cyber resilience. These models balance knowledge of offensive attack vectors with Resilience-in-Depth™ controls. The Platform Cyber Attack Model (PCAM) provides a multi-scale construct for identifying, describing, and understanding cyber-attacks that are relevant to platform systems in their operating environment. The corresponding Platform Cyber Defense Model (PCDM) determines resiliency controls needed to respond to and recover from high-likelihood, high-severity cyber-attacks. These analytic models provide a foundation for building on RMF and guides implementation of relevant cyber resilience capabilities for platform systems. We conclude this paper with a simplified process for developing the PCAM and PCDM models and with recommendations for next steps in implementing platform cyber resilience.

1. INTRODUCTION

Our adversaries are rapidly maturing their offensive cyber operations (OCO) capabilities to achieve parity with US cyber forces and to deliver kinetic effects through the cyber domain. In many cases, our adversaries acquire these OCO capabilities at low cost and with little historical investment. This pairing of 'significant lethality' with a 'low barrier of acquisition' makes cyber warfare a significant concern for defense planners and makes the topic of Platform Cyber Resiliency timely, relevant, and essential to our future warfighting success.

As shown in Figure 1, DoDIN, DISA, MITRE, NIST, INCOSE, and other organizations across the defense, federal, and civilian communities are rapidly developing and deploying strategic-level perspectives and guiding documents on cyber security and cyber resilience. While these high-level constructs are necessary for thinking about and understanding cyber resiliency, they do little to make product-level cyber resilient solutions intuitive, actionable, and affordable. Based on our experience, most engineering teams struggle while crossing the chasm between the guiding documents and the development of platform specific technical architectures, designs, and build plans. We call this chasm the "Fog of Platform Cyber Resilience."

In this paper, we describe key resilience concepts and two analytic models for improving platform cyber resilience. These models provide critical insights needed to remove the fog from engineering teams and to enable design and development of robust resilience solutions on platform programs. Specifically, we describe the difference between cybersecurity engineering and cyber resilience engineering, we define the concept of Resilience-in-Depth, and we introduce tactical visualization models that enable cyber resilience engineering. The models include a Platform Cyber Attack Model (PCAM) allowing visualization of the platform attack surface and a Platform Cyber Defense Model (PCDM) allowing visualization of the platform resilience surface. We provide an unclassified example of these models for a fictitious platform system, and we conclude with a brief description of a process for developing the PCAM and PCDM artifacts.

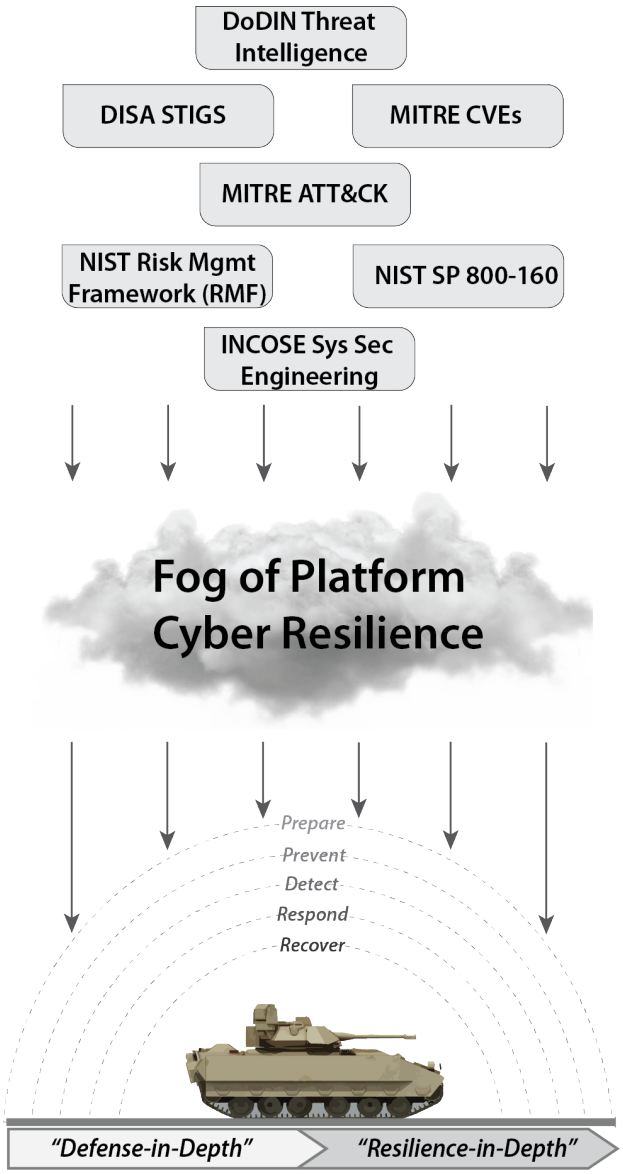


Figure 1 – The Fog of Platform Cyber Resilience: Policies, Frameworks, and Guidelines are emerging rapidly in the field of cyber security and cyber resilience. Unfortunately, application of this foundational infrastructure is not well applied by many engineering teams making the realization of cyber resilience solutions in platform systems inconsistent and incomplete.

2. PRIOR SOLUTIONS

Many commercial and military platform integrators use a holistic cyber defense strategy guided by well-established frameworks, standards, and engineering processes. Over the last decade, these techniques have served these industries well and have protected platform operators from harm.

Figure 2 provides a simplified view of present tradecraft used to implement *platform defense capabilities*. Threat Intelligence [1, 2, 3] and Attack Models [4] describe adversarial threats in a platform's operational environment. These models are usually static and provide offensive knowledge needed to make defensive design decisions. Similarly, Vulnerability Information characterizes access points through which attackers may enter the targeted system or subsystems during the course of an attack. These three elements of information are integrated using Defense-in-Depth engineering processes [5], whereby the selection and precise placement of security controls disrupt cyber-attack vectors. Additionally, we harden specific system elements and interfaces through the application of Security Technical Implementation Guides (STIGs) [6] applied to the platform's systems and subsystems.

Today, standards organizations and think-tanks are establishing new frameworks, processes, tools, and technologies for implementing future *platform resilience capabilities*. The National Institute of Standard (NIST) is leading the way by developing system security frameworks and by identifying the critical challenges in implementing resilient cyber solutions. The NIST SP 800-160 volume 1 and 2 documents [7, 8] provide an excellent starting point for development organizations to learn about cyber security and cyber resilience. These two documents also offer a point-of-departure for developing industry and product-line specific engineering processes needed to implement cyber resilience functions.

While these historical and current approaches provide the necessary foundation for cyber resilience, they are not sufficient to enable tactical implementation of cyber resilience solutions on platform programs. The remainder of this paper focuses on demystifying platform cyber resilience from a tactical perspective and on enabling the implementation of resilience solutions.

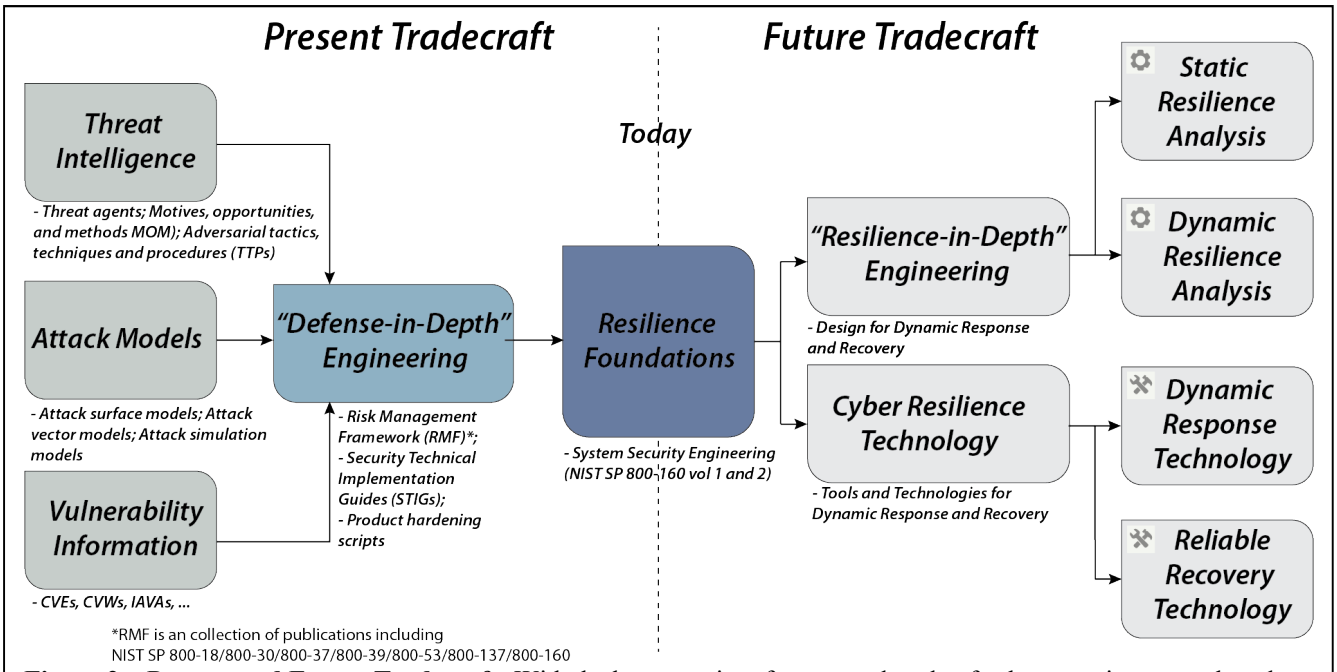


Figure 2 – Present and Future Tradecraft: With the best practices for over a decade of cyber security research and the thought leadership provided by organizations like NIST, we are well positioned to invent Resilience-in-Depth engineering practices and Cyber Resilience Technologies to implement responsive and recoverable security solutions.

3. DESIGNING AND IMPLEMENTING PLATFORM CYBER RESILIENCE

The Department of Defense (DoD) is challenging its contractors to develop platforms and systems that are protected against cyber-attacks as effectively as they are protected against kinetic attacks. To accomplish this goal, platform integrators are moving beyond traditional cyber defense techniques to cyber resilience techniques.

3.1. Demystifying Cyber Resilience

The NIST SP 800-160 Volume 2 defines Cyber Resilience as *"The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources."* At BAE Systems, we adopt this definition and further organize our cyber resilience engineering practices around five pillars:

1. **Prepare** – Identification of relevant cyber threats and attack vectors; understanding the consequences of a cyber-attack; analyzing attack pathways using tools like Cyber Failure Mode, Effects, and Criticality Analysis (Cyber FMECA).
2. **Prevent** – Harden the system environment using cybersecurity best practices including, High Availability Design, Risk Management Framework (RMF), and Defense-in-Depth techniques.
3. **Detect** – Monitor the system and its operating environment for signs of intrusion and provide reliable notifications to security monitors.
4. **Respond** – Dynamically react to cyber-attacks to reduce or eliminate harmful impacts; responds to the adversary by 'shutting down their attack process' (responsive action).
5. **Recover** – Autonomously repair damage from a cyber-attack to assure continuity of operations (in partial or full capacity).

The well understood Prepare/Prevent pillars provide a foundation for Defense-in-Depth solution design and traditional RMF accreditations. The Detect/Respond/Recover pillars introduce new dimensions of design and provide a foundation for Resilience-in-Depth.

The differences between cyber defense and cyber resilience become clear by analyzing these five pillars. Figure 3 shows how Resilience Engineering builds on a foundation provided by Defense Engineering techniques like those prescribed by RMF.

	Defense Engineering Approach	Resilience Engineering Approach
Offensive Knowledge	***NIST SP 800-160 System Security Engineering*** – provides guidance for principles and concepts on defensive security engineering process; identifies relevant cyber resilience issues to be addressed during the system architecting process.	***Platform Cyber Attack Model (PCAM)*** – extends NIST SP 800-160 by providing a model for describing platform specific cyber attacks thereby providing context for developing cyber resilient platform systems.
Defensive Knowledge	***Risk Management Framework (RMF)***– provides defensive security analysis and layered security controls for IT and Platform IT systems.	***Platform Cyber Defense Model (PCDM)*** – extends RMF by aligning platform specific cyber attacks with cyber defense and resilience controls. PCAM and PCDM allow visualization of a platform's attack and corresponding defense surface.
Architecture Approach	***Defense-in-Depth*** – places multiple layers of security controls throughout the system, providing defensive redundancy to displace cyber attacks.	***Resilience-in-Depth*** – extends Defense-in-Depth architectures to include attack detection, response and recovery capabilities across scales (chip-to-platform).
Engineering Approach	***Cyber Security Engineering*** – uses functional architecture descriptions consisting of largely structural design models to develop integrated defense-in-depth solutions.	***Cyber Resilience Engineering*** – uses dynamic architecture models to reason over the functional architecture about cyber attacks and responsive/recovery options. These models also include attack surface and dynamic response planning models.
Testing Approach	***Nominal Analysis and Design*** – uses traditional engineering processes and RMF to design platforms that satisfy well-defined functional requirements and implement nominal system behaviors.	***Off-Nominal Analysis and Design*** – uses adversarial knowledge to design platforms that adapt and respond to use-cases outside the scope of the traditional requirement (functional and performance) space.

Figure 3 – Capability Evolution for Cyber Resilience: Developing and deploying cyber resilient solutions requires new processes, tools, techniques, and technologies that extend beyond that of today's static Defense-in-Depth techniques.

3.2. Demystifying Resilience-in-Depth

As we seek to develop resilient cyber solutions, we frequently find ourselves working at a single level of scale. For example, while designing a combat vehicle, we often evaluate our security architecture only at a platform and major subsystem level. This restricted view of cyber resilience leaves implemented systems vulnerable to attack at lower levels of scale and sometimes with significant consequences.

Resilience-in-Depth™ is an architectural property whereby a system detects, responds, and recovers from cyber attacks within and across levels of scale. For our work, we define five levels of scale ranging from the individual microchip to the fully integrated platform vehicle. Figure 4 shows the five levels of scale in context.

At each level, preventative defensive security controls are placed in strategic locations specifically to break attack vectors and to provide a layered defense. This action provides a core level of defensive capability. Next, resiliency controls are added to the defensive controls to address the dynamic aspects of attack detection, response, and recovery. This action provides a core level of resilience at each of the five levels of scale.

It is important to note that system designs at each of the five levels of scale are not independent. After allocating controls structurally at each level of design, we cross-connect the five levels and deploy control logic to synchronize and coordinate dynamic responses across scales. This activity turns the resiliency solution into a three-dimensional architecture where cyber attacks are actively deterred (detect, respond, and recover) across horizontal (same level of scale) and vertical (across levels of scale) planes of the platform design.

Today, cyber resilience engineering processes are actively being developed to strengthen the design of military platforms. Due to the complexity of performing both static and dynamic analysis across scales for nominal and off-nominal system modes, BAE Systems is pioneering new model-based engineering (MBE) techniques to organize project data, manage complexity, and analyze dynamic relationships among security and resiliency controls.

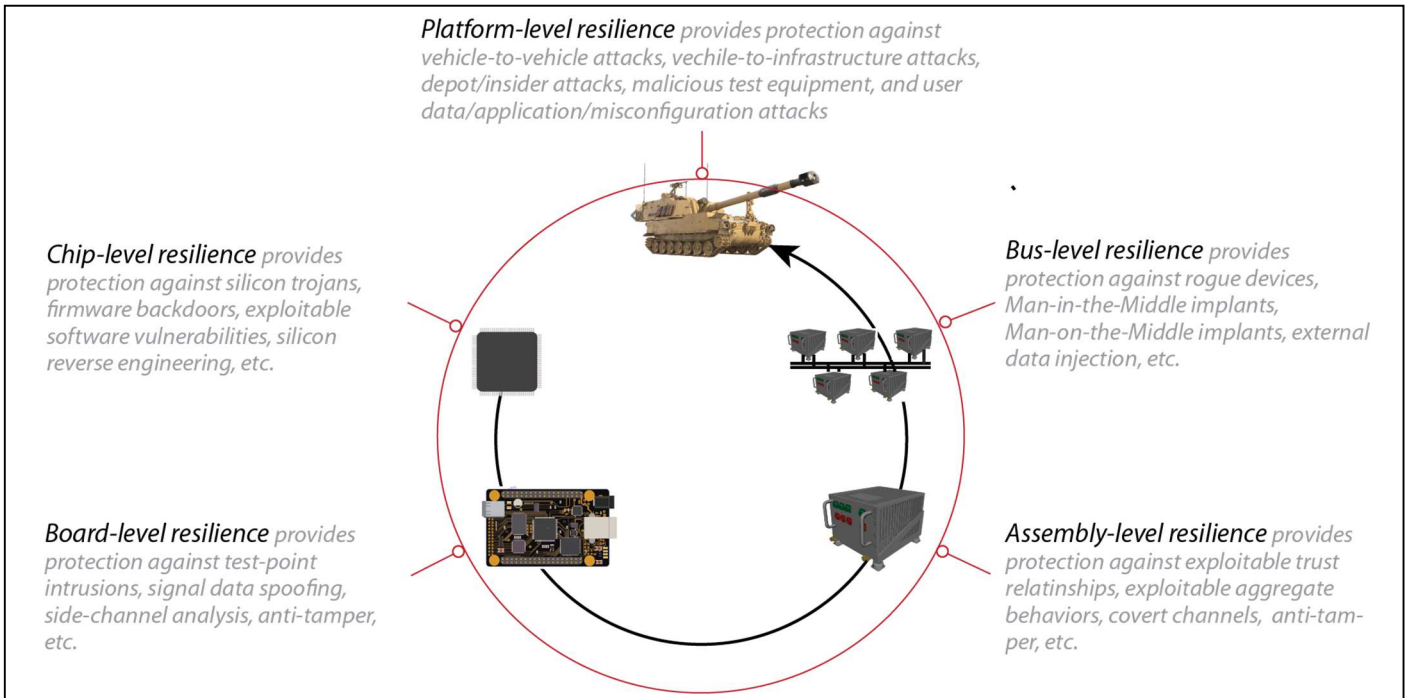


Figure 4 – Five Levels of Scale for Resilience-in-Depth: Platform cyber resilience solutions must integrate detection, response, and recovery functions across five levels of scale to improve effectiveness, dependability, and trustworthiness of the resulting defense and resilience solutions.

3.3. Demystifying Platform Cyber Attack

Developing Resilience-in-Depth solutions requires platform integrators to understand platform cyber-attacks. To address this need, BAE Systems uses a Platform Cyber Attack Model (PCAM) to assist with visualization, analysis, and understanding of platform-specific attack surfaces. Figure 5 shows an unclassified example of a PCAM tailored to a fictitious vehicle. The full PCAM is a repository of known and relevant platform cyber-attacks and enables rapid integration of offensive cyber data into the defensive design process. It provides a kick-start for engineering teams tasked with both implementing cyber resilience solutions for new platform designs and with retrofitting cyber resilience into existing platforms designs.

The modeling process begins with engineering teams identifying relevant cyber threats and cyber-attacks for their specific platform. The resulting adversarial data is integrated into a tailored PCAM that is stored in the project's MBE repository. This adversarial data is then linked via the MBE toolset to traditional design artifacts (those prescribed by the local engineering processes) to be considered throughout platform design, development, and testing.

While applying the PCAM to production programs, BAE Systems has identified the following four best practices. First, it is vital to prioritize the selected attacks based on the likelihood that a cyber adversary will implement them to ensure coverage of the most critical attacks. From this prioritized list, select the top 5-10 attacks to start and incorporate additional attacks as time and budget allow. Our experience suggests that a small set of relevant orthogonal attacks quickly drives the convergence of a robust defensive and resilient security design.

Second, the PCAM provides data needed to analyze the platform's cyber-attack surface. This analysis may include techniques like Cyber FMECA and Attack Vector Composition Analysis to understand the impacts of sophisticated cyber-attacks better. In some cases, this also leads to an ability to prove cyber resilience based on a finite set of offensive and defensive assumptions.

Third, the PCAM allows consideration of off-nominal (misuse) behaviors caused by cyber-attacks. It is important to understand that cyber-attacks frequently use systems in unintended and unplanned ways to gain an advantage for the attacker. The consideration of off-nominal behaviors allows identification of unintended system behaviors that may work to an adversary's advantage and that may lead to system compromise.

Finally, the PCAM speeds development of adversarial test cases used to validate platform defense and resiliency. Red Teams commonly perform adversarial testing. We recommend that these tests be added to the standard test and evaluation process to properly assess the functioning of dynamic resilience controls.

To better illustrate insights provided by the PCAM, we briefly describe five frequently occurring attacks at each of the five levels of scale. Most readers will recognize some of these attacks and will awaken to others. This awakening is an intended effect as it enables *offensive thinking to solve defensive problems*.

Chip-Level Attacks

At the chip-level, functional structures are 'integrated into silicon' to form microcontrollers, microprocessors, field-programmable gate arrays (FPGAs), and static read-only memory (ROM). These structures sometimes contain cryptographic key material and algorithms, proprietary programming, finite-state machines (FSMs), and decision logic. Five common attacks at the chip-level include:

- **IC Reverse Engineering -** Extraction of circuit design, proprietary hardware designs, embedded firmware, and cryptographic keys from analysis of transistors on a silicon die. Micro-probing techniques provide dynamic exploitation of silicon die, including a bypass of cryptographic security of embedded firmware.

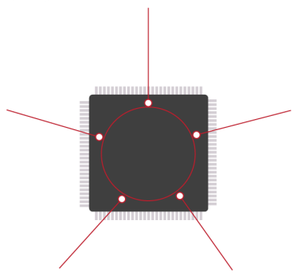
Platform Cyber Attack Model (PCAM)

BAE SYSTEMS

Chip-Level Attacks

IC reverse engineering - *allows mapping and analysis of IC designs; extraction of internal ROM programming; extraction of cryptographic materials*

Fault induction - *rapid writing of memory cells to flip bits in adjacent cells; row-hammer attack*



Silicon malware - *backdoors, kill switches, and trojans (intended and unintended) built into the silicon level of an integrated circuit*

Firmware/software glitching - *uses partial clock cycles, power faults, RF fault injection, and laser fault injection to alter execution of embedded programming; allows bypass of firmware security functions*

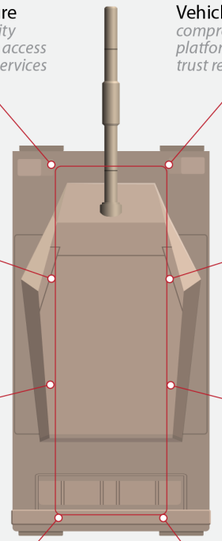
Side-channel analysis - *timing, power, thermal, and radio frequency emissions allow side-channel attacks on embedded application programming and cryptography; password brute-forcing*

Prepare - Prevent - Detect - Respond - Recover

Platform-Level Attacks

Vehicle-to-infrastructure (V2I) - *network connectivity provides local and remote access to vehicular systems and services*

Vehicle-to-vehicle (V2V) - *compromised vehicles provide a platform for moving laterally in a trust relationship*



Malicious maintenance equipment - *test stands and maintenance equipment provide a pre-authenticated connection to sensitive functions on the platform*

Radio frequency apertures - *network connectivity over radio carrier provides remote access to vehicular systems or presenation of false data (e.g., spoofed GPS)*

Open test ports - *test ports that do not support device authentication provide open access to attackers*

Open data ports - *allows transport of applications and data to on-board computing systems without checking access permissions or performing data sanitization*

Supply chain - *supply chain poisoning (intentional and unintentional) provides local and remote backdoors through compromised hardware, software and firmware*

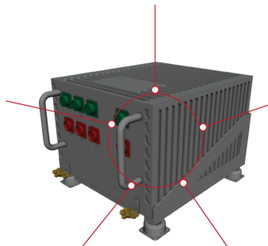
Malicious Insider - *a malicious insider changes the configuration of equipment and/or software to compromise the platform*

**NOTE: This is a fictitious vehicle. Any resemblance to a real world military vehicle is unintended and is purely coincidental.*

Assembly-Level Attacks

Backplane intrusion - *reading/writing backplane signals used for cross-board communication to disclose information, reconfigure devices, change execution flow and insert malware*

Embedded behavior - *exploitation of defaults LRU/ECU behaviors (fault response, default configurations)*



Cross-board trust relationships - *unauthenticated/implicit trust between boards*

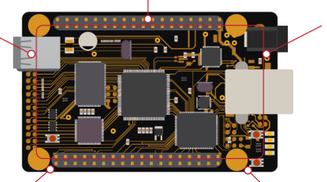
Unsecured data storage - *manipulation of local data stores to compromise data confidentiality and integrity*

Malicious/vulnerable boards - *tampering or compromising less secure boards to access highly secure boards*

Board-Level Attacks

PCB reverse engineering - *allows mapping and analysis of PCB designs; loss of intellectual property and trade secrets*

Hardware implants - *insertion of malicious circuits to alter/control the host hardware environment*



Embedded OS and applications - *attacks on the embedded software applications (L:inux, RTOS, drivers, embedded software)*

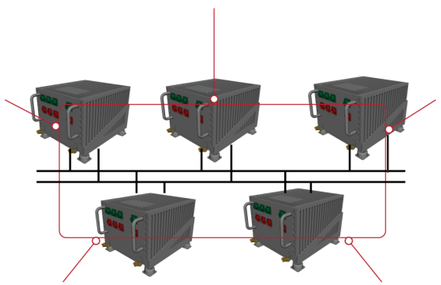
Test-point intrusion - *use of UART, JTAG and other test-points to disclose information, reconfigure devices, change execution flow and insert malware*

Bus intrusion - *reading/writing bus signals (I2C/SPI/...) to disclose information, reconfigure devices, change execution flow and insert malware*

Bus-Level Attacks

External message manipulation - *message data bridged across gateways allow message sniffing, replay and injection*

Sensor data manipulation - *tampering with sensor data allows attackers to set LRU/ECU state and response*



Actuator data manipulation - *tampering with actuation data allows attackers to set LRU/ECU state and response*

Bus Man-on-the-Middle (MOTM) - *rogue devices sit on the the bus and sniff, modify, replay, and inject malicious message traffic*

Bus Man-in-the-Middle (MITM) - *rogue devices split the bus into two physical buses and modifies message traffic inflight*

Figure 5 - Platform Cyber Attack Model (PCAM) – The PCAM is an engineering analysis and design artifact that identifies and prioritizes attack vectors that are likely to be manifested in a platform's operating environment. The accumulation of PCAM diagrams over a portfolio of programs provides a product-line attack vector catalog that is useful for developing completeness criteria for platform resilience solutions.

- **Silicon Malware** – Backdoors (intentional and unintentional) and hidden embedded functions (reset, administration, security functions) in silicon allow access to critical chip-level functions. Chip designers often mistakenly assume that the exploitation of these vulnerabilities requires human interaction.
- **Side-Channel Analysis** – Timing, power, and RF side channel analysis used to extract cryptographic keying materials from chips running block ciphers (e.g., DES and AES).
- **Glitching** – Technique of injecting momentary faults onto the chip to cause changes in firmware and software execution. Power glitching introduces transient power faults, and clock glitching introduces corruption to the clock waveforms to transition abnormally into execution of normally protected processing paths. RF glitching uses electromagnetic pulses to change the flow of execution of the chip-state.
- **Inductive Bit-Flipping** – Inductively flipping individual memory cells (bits) as the transistor density on modern chips increases can cause changes to adjacent memory cells. Using this technique, it is possible to change security bits on microcontrollers and microprocessors to enable and access privileged chip functions.

Board-Level Attacks

At the board-level, analog and digital electronic components form single board computers, controller/actuator cards, and RF tuners and receivers when aggregated. These boards generally contain secure boot functions, static firmware loads, embedded operating systems, embedded application code, FPGA bit streams, unprotected data and control busses, and sensor/actuator logic. Five common attacks at the board-level include:

- **Printed Circuit Board (PCB) Reverse Engineering** – Extraction of proprietary hardware designs, embedded firmware, and cryptographic keys from analysis of PCB layers allows identification of attack insertion points. In some cases, small board modifications allow insertion of malicious implants.
- **Embedded OS and Applications** – Embedded software applications may be altered or exploited allowing access to critical system functions. This includes alteration of runtime configuration files, changing software behaviors, and implanting malicious applications.
- **Bus Intrusion** – Lack of secure message transport exposes board-level signals and allows monitoring, capture, replay, spoofing, and injection of low-level messages (data and control). Adversaries conduct these attacks using unprotected PCB traces between chips on the board.
- **Test-point Intrusion** – On many commercial boards, test points are frequently enabled allowing low-level control of hardware features. Common test-points include UART/RS-232, JTAG, USB, SPI and I2C connectors printed on circuit boards. Attackers use these test points to gain access to disclose sensitive information and to alter board-level functions.
- **Hardware Implants** – Small electronic devices can tap into PCB test-points, board traces, and chip pins to alter board functions, alter message traffic, and implant malware into the running system.

Assembly-Level Attacks

At the assembly-level, integrated components create major platform subsystems such as Line Replaceable Units (LRUs) and Electronic Control Units (ECUs). These subsystems generally contain power supplies, power distribution backplanes, control signal backplanes, sensors, processors, and actuators. Five common attacks at the assembly-level include:

- **Backplane Intrusions** – Insertion of malicious implants allow monitoring, capture, replay, spoofing, and injection of low-level command traffic.
- **Cross-Board Trust Relationships** – Most boards in an assembly implicitly trust each other to generate the correct stimulus-response behaviors. Performing little or no authentication of cross-board traffic to verify the authenticity of messages can be a significant vulnerability. This allows a compromised board to laterally affect other boards in the assembly and potentially cause great damage to the host platform.
- **Malicious/Vulnerable Boards** – Successful attacks against a weakly secured board allows alteration of performance characteristics and provides a pivot

point for lateral movement to other boards within the assembly.

- **Unsecured Data Storage -** Many systems rely on configuration files to define post-boot operations and rules-for-operation. These files are frequently unprotected at the assembly and board levels allowing attackers to change configurations and operational behaviors of the platform systems.
- **Embedded Behavior** – The design of most hardware systems use a stimulus-response paradigm that results in implicit assembly-level behaviors. Triggering these behaviors by providing malicious stimulus from compromised sensor or control allows an attacker to invoke embedded behaviors.

Bus-Level Attacks

At the bus-level, integrated assemblies form subsystems for platform physical control, weapon system control, and information and Human-Machine Interface (HMI) systems. These subsystems generally contain assemblies from a diverse set of manufacturers, data and control buses (e.g., CAN, Ethernet, MIL-STD-1553), sensors, processors, and actuators. Five common attacks at the bus-level include:

- **External Message Manipulation** – Many platforms contain dedicated buses assigned to specific functions (e.g., Platform Physical Control, Weapon System Control). Messages commonly cross over from one bus to an adjacent bus using a message gateway. Manipulating messages on one bus may cause collateral messages to appear on nearby buses that implement the attacker's intent.
- **Actuator Data Manipulation** – The connection of actuators and sensors frequently form a feedback loop. Spoofing and manipulation of actuator data allows activation of platform functions at the discretion of an attacker.
- **Man-in-the-Middle Attacks (MITM)** – Rogue or infected assemblies can alter messages while being transported on the bus thereby allowing attackers to invoke trusted system functions and capabilities.
- **Man-on-the-Middle Attacks (MOTM)** – Rogue or infected assemblies can generate messages allowing attackers to invoke trusted system functions and capabilities on adjacent assemblies.
- **Sensor Data Manipulation** – Sensors provide measurement data to assemblies (LRUs/ECUs) over data buses. Intercepting and manipulating this data can trigger platform functions at the discretion of an attacker.

Platform-Level Attacks

At the platform-level, we integrate subsystems to perform on-board and off-board functions such as vehicle-to-infrastructure interaction, vehicle-to-vehicle interaction, platform system management, and warfighting functions. Five common attacks at the platform-level include:

- **Vehicle-to-Infrastructure (V2I)** – Data transmitted over trusted data links may be unauthenticated and inadequately checked for authenticity, integrity, and validity. This allows attackers to pivot from compromised infrastructure into the platform system.
- **Vehicle-to-Vehicle (V2V)** – Data transmitted over trusted data links is sometimes unauthenticated and inadequately checked for authenticity, integrity, and validity. This allows attackers to pivot from one compromised platform to a second platform over a shared communication pathway.
- **Radio Frequency Apertures** – RF apertures and communication protocols provide an opportunity to inject data into the platform systems. RF apertures include military radios, Wi-Fi radios, Bluetooth radios, and GPS receivers.
- **Open Test/Data Ports** – Plugging hardware implants into unsecured test and data ports allow dynamic and over-the-air reconfiguration of the platform systems.
- **Malicious Maintenance Equipment** –Maintenance equipment (e.g., Test stands, maintenance laptops, diagnostic equipment, and spare parts) is not well secured in some operational environments. This equipment provides an opportunity to misconfigure or infect the platform to achieve an attacker's intent.

Identifying the most important cyber-attacks across the five levels of scale allows engineering teams to make more informed design decisions and provides a starting point for the development of cyber resilience designs.

3.4. Demystifying Platform Cyber Defense

With an understanding of platform cyber-attack, we now select appropriate resilience controls leading to a Resilience-in-Depth solution. BAE Systems' Platform Cyber Defense Model (PCDM) provides a tool for identifying 'resiliency controls' across the five levels of scale. Figure 6 shows a simplified version of the PCDM tailored to a fictitious vehicle to avoid disclosure of platform-sensitive information. Like the previously described attack framework, the full PCDM is a repository of proven platform resilience controls and enables the rapid synthesis of resilient architectures based on best practice. It also provides a kick-start for engineering teams tasked with both creating new platform designs and with retrofitting cyber resilience into existing platforms designs.

Application of the PCDM requires platform-engineering teams to select and prioritize appropriate resilience controls and technologies for their specific platform. While these controls include IT controls specified by RMF, a resilience solution frequently includes additional dynamic controls that are unique to cyber-physical systems. Integrating the selected controls into a tailored PCDM stored in the project's MBE repository, each control links via the MBE toolset to traditional design artifacts (those prescribed by the local engineering processes). Linking the controls to specific design artifacts ensures that they are considered during the functional design development, integration of the platform system, and testing of the final platform product.

While applying the PCDM to production programs, BAE Systems has identified the following five best practices. First, it is essential to remember that platform cyber resilience builds on platform cyber defense. RMF is still required on all platform designs to provide relevant foundational security controls and to provide relevant system hardening.

Second, it is important to select resilience controls linked to the platform-specific cyber-attack models that have a proven ability to disrupt the attacks identified in the PCAM.

Third, each configured resilience control detects, responds, and recovers based on the characteristics of the platform-specific cyber-attacks and the specific platform design parameters. This reduces the likelihood for replication of vulnerabilities on one type of platform to other platform systems. For example, using the common rule-set for a bus-level intrusion detection system may result in a common vulnerability on all platforms that use that rule set. These common rule-sets allow adversaries to move laterally from one type of compromised platform (e.g., a fuel truck) to the second type of uncompromised platform (e.g., a battle tank) using the same attack vector.

Fourth, appropriately configuring the resilience controls to interoperate is required because they are active elements in the system design. Failure to design the proper system dynamics results in unintended and undesirable emergent system behavior that may also be potentially exploitable. For example, inaccurate bus-level Intrusion Detection System (IDS) detections may trigger a dynamic response that shuts-down platform functions, thereby threatening operator safety and reducing mission effectiveness.

Finally, integrating resilience controls across the five levels of scale may improve the reliability of attack detections. Many detectors use rule-sets, physical models, and machine learning to detect cyber-attacks. In many cases, having a richer set of data types available from the platform allows the definition of more reliable decision criteria, thereby making the overall resilience mechanisms more trustworthy.

To better illustrate the value provided by the PCDM, we briefly describe common defense and resilience controls at each of the five levels of scale. Most readers will recognize some defenses and will learn about others. This is the intended outcome as we want to ensure that best-practice resilience technologies are selected, integrated, and configured appropriately for the platform at hand.

BAE SYSTEMS

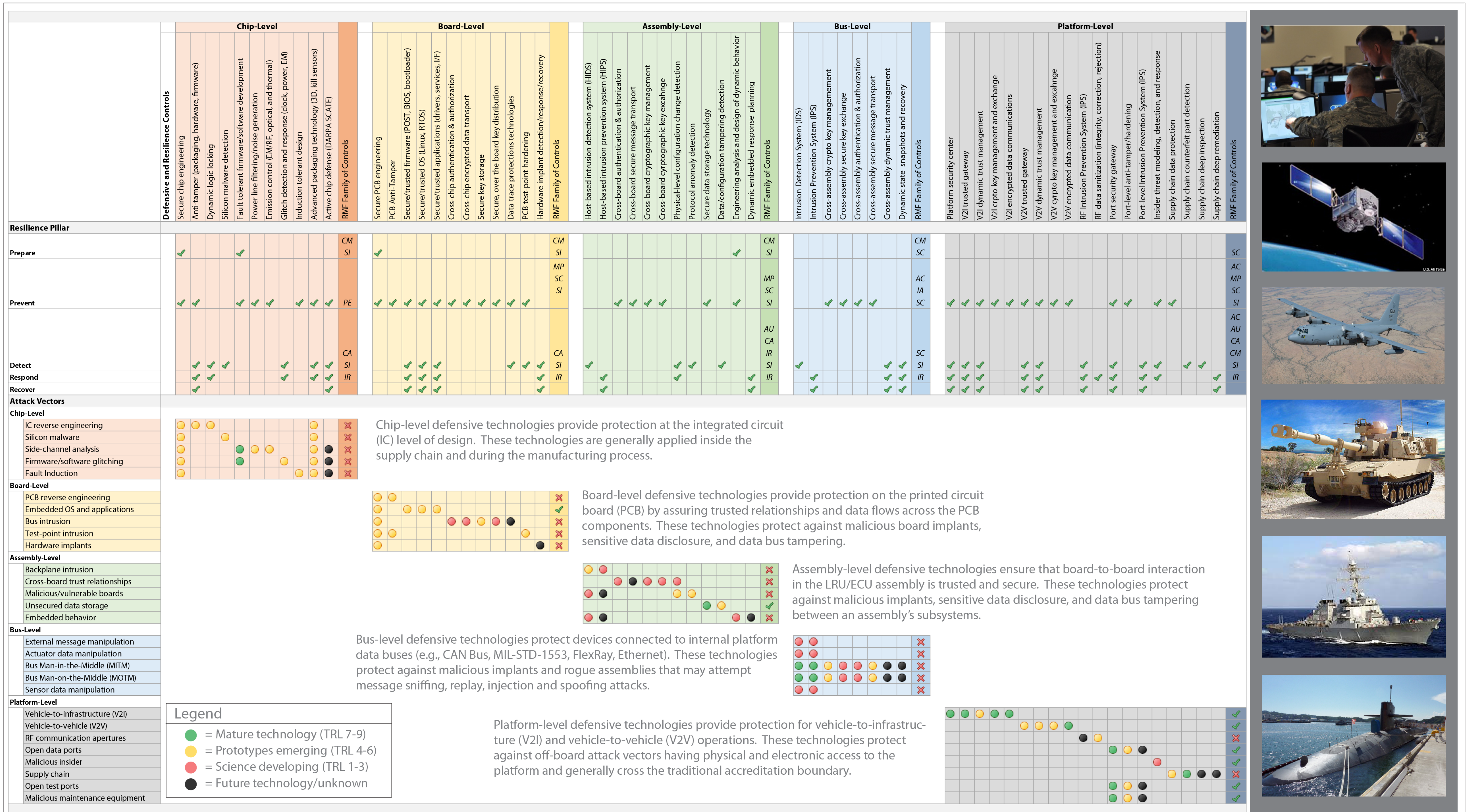


Figure 6 – Platform Cyber Defense Model (PCDM) – The PCDM is an engineering analysis and design artifact that is tailored to each specific project and provides a mapping of resilience controls to attack vectors across 5 levels of scale. This mapping provides a foundation for developing and delivering Resilience-in-Depth solutions into operational platforms.

Chip-Level Resilience

Chip-level resilience technologies protect at the integrated circuit (IC) level of design. Applying these technologies happens inside the supply chain and during the manufacturing process. Chip-level defenses include:

- **Secure Chip Design** – Design and develop future ICs with an understanding of chip-level attacks. Designers frequently focus exclusively on the functional properties of their products and not on the security issues that may drive alternative designs.
- **IC Anti-Tamper** – Reverse engineering ICs to extract designs, data, and intellectual property is a mature and proven science. Future IC designs need to incorporate active anti-tamper (AT) techniques (e.g., external storage of cryptographic keys) to deter adversarial reverse engineering.
- **Emissions Management** – To disrupt side-channel attacks, it is essential to understand the nature of each emission and to disrupt each of them appropriately. This includes the application of capacitive filtering and noise generation for power lines, development of constant-time firmware, and spreading of thermal and radiated energy patterns.
- **Protection of Security Functions** – Implementing security functions at the chip level is a difficult task and frequently involves security fuses, focused ion beam implants, and camouflage. Logic hardening techniques have been proposed at the circuit level, specifically against non-invasive and semi-invasive attacks. These hardening approaches include planning and managing the electromagnetic cross-coupling near security fuses and security bits and application of advanced packaging technologies to defend against inductive attacks.
- **Active Chip Defense** – DARPA is investigating a new generation of technologies for sensing and protecting against cyber-attacks at the chip-level. These technologies will be available for use in military systems in the next three to five years. Anticipated technologies include detection and recovery from glitching, side-channel, and fault induction attacks.

Board-Level Resilience

Board-level resilience technologies protect the printed circuit board (PCB) by assuring trusted relationships and data flows across the PCB components. These technologies protect against malicious board implants, sensitive data disclosure, and data bus tampering. Board-level defenses include:

- **Secure Board-Level Design** – Design and develop future PCBs with an understanding of board-level attacks. Designers frequently focus exclusively on the functional properties of their products and not on the security issues that may drive different design decisions.
- **PCB Anti-Tamper (AT)** – Reverse engineering PCBs to extract designs, data, and intellectual property is a mature and proven science. Future PCB designs need to incorporate active AT to deter adversarial reverse engineering.
- **PCB Test-Point Hardening** – Many board designers integrate test-points on PCBs to support firmware installation, product testing, defect detection, and repair. Future board designs need to reduce or eliminate test-points as they provide physical access to sensitive board-level functions such as providing control of on/off switching.
- **IC-to-IC Encrypted Data Transport** – Data buses provide entry points for reverse engineering and malicious implants. Data should be encrypted during transport to preserve data and message integrity between board-level subsystems.
- **Secure/Trusted Firmware, OS, and Applications** – Many embedded software loads (firmware, OS, and applications) contain poorly written and poorly tested code. Future embedded software loads should be rigorously inspected and certified since hardware forms the root-of-trust for most systems.

Assembly-Level Defense

Assembly-level defensive technologies ensure that board-to-board interaction inside the LRU/ECU assembly is trusted and secure. These technologies protect against malicious implants,

sensitive data disclosure, and data bus tampering between boards in the assembly. Assembly-level defenses include:

- **Assembly-Level HIDS/HIPS** – Future assemblies should contain dedicated software or hardware to perform host-based intrusion detection (HIDS) and host-based intrusion prevention (HIPS). Passing local HIDS/HIPS data to Bus-Level IDS/IPS supports scalable detection of cyber-attacks.
- **Cross-Board Authentication & Authorization** – Techniques for establishing trust between sensors, actuators, and boards in an assembly are necessary to prevent insertion of rogue and untrusted devices (implants).
- **Cross-Board Secure Message Transport** – Today, boards in an assembly implicitly trust the signals used for control and data transfer. New techniques are needed to support secure (confidentiality, integrity, non-repudiation) message transport to prevent data and message tampering attacks.
- **Cross-Board Cryptographic Key Management** – Implementing security across boards in an assembly requires management of cryptographic keys. Future assemblies should include capabilities for secure key generation and distribution across the assembly's subsystems.
- **Protocol Anomaly Detection** – Cyber adversaries frequently attack flaws in communication protocols and their implementations. Future assemblies should validate the proper implementation of communication protocol stacks and handling of protocol anomalies in embedded software (firmware, OS, and applications).

Bus-Level Resilience

Bus-level resilience technologies protect devices connected to internal platform data buses (e.g., CAN Bus, MIL-STD 1553, FlexRay, Ethernet). These technologies protect against malicious implants and rogue LRUs/ECUs that may attempt message sniffing, replay, injection and spoofing attacks. Bus-level defenses include:

- **Bus-Level IDS/IPS** – Future bus-level defenses should contain dedicated hardware to perform intrusion detection (IDS) and intrusion prevention (IPS). Reliable detections from IDS/IPS systems enable subsequent response and recovery capabilities in the Resilience-in-Depth architecture.
- **Cross-Assembly Authentication & Authorization** – Techniques for dynamically establishing trust between assemblies on a bus are necessary to prevent insertion of rogue and untrusted devices (implants). Techniques like introduction-based routing allow bus-level assemblies to increase their trust levels based on prior 'good behavior.' New devices and implants are less trusted on the bus allowing detection of malicious interactions and activities while operating the platform system.
- **Cross-Assembly Secure Message Transport** – Today, assemblies on a bus trust the messages used for control and data transfer. New techniques are needed to support secure (confidentiality, integrity, non-repudiation) message transport to prevent data and message tampering attacks. Cryptographic techniques based on dynamic key generation and dynamic one-time pads can substantially increase the resilience of bus-level communications.
- **Cross-Assembly Cryptographic Key Management** – Implementing security across assemblies on a bus requires management of cryptographic keys. Future bus topologies should include capabilities for secure key management, including dynamic key generation and distribution to support disconnected network operations.
- **Cyber Retrofit** – The vast majority of LRUs and ECUs used in platform systems today do not incorporate sufficient security or resilience capabilities. Developing techniques like cryptographic shims and hardware monitoring boards (resilience implants) to add bus-level security and resilience functions to the existing system should be applied in both legacy and new platform designs.

Platform-Level Resilience

Platform-level resilience technologies provide active protection for vehicle-to-vehicle and vehicle-to-infrastructure operations. These technologies protect against off-board attack vectors having physical and electronic access to the

platform and generally cross the traditional accreditation boundary. Platform-level defenses include:

- **Secure Vehicle-to-Infrastructure (V2I) Gateway** – Future platforms must provide secure gateways to manage trust relationships with infrastructure systems and software. Functions of the gateway must include; key management, key distribution, authentication, authorization, trusted data transport, and trusted service access.
- **Secure Vehicle-to-Vehicle (V2V) Gateway** – Future platforms must provide secure gateways to manage trust relationships with external systems and software. Functions of the gateway must include key management, key distribution, authentication, authorization, trusted data transport, and trusted service access.
- **Port Security Gateway** – Future platforms must provide secure gateways to manage trust relationships with in-depot diagnostic tools and equipment. Functions of the gateway must include key management, key distribution, authentication, authorization, trusted data transport, and trusted service access.
- **Platform Security Center** – Future platforms must provide a central management solution for the platform-level Resilience-in-Depth architecture. This management solution integrates sensor data from the chip, board, assembly, bus, and platform levels into a platform-level operational picture and allows management of response and recovery activities.
- **Supply Chain Inspection** – Today, most platform integrators check for counterfeit parts and secure engineering data within their supply chains. However, experts estimate that many military platforms still contain compromised chips, boards, and assemblies. Future supply chain inspection procedures should perform a deep-inspection of critical system elements to ensure that parts are reliable and can be trusted.

3.5. Process for Building Resilience-in-Depth

Most platform integrators have well established, proprietary engineering processes for building defense-in-depth capabilities into platform designs. During the Requirements Analysis phase of the project lifecycle, we develop and integrate PCAM and PCDM artifacts and integrate them into the MBE repository.

Figure 7 shows one approach to building these models leveraging three primary data repositories. The Adversarial Threat Agent Model repository

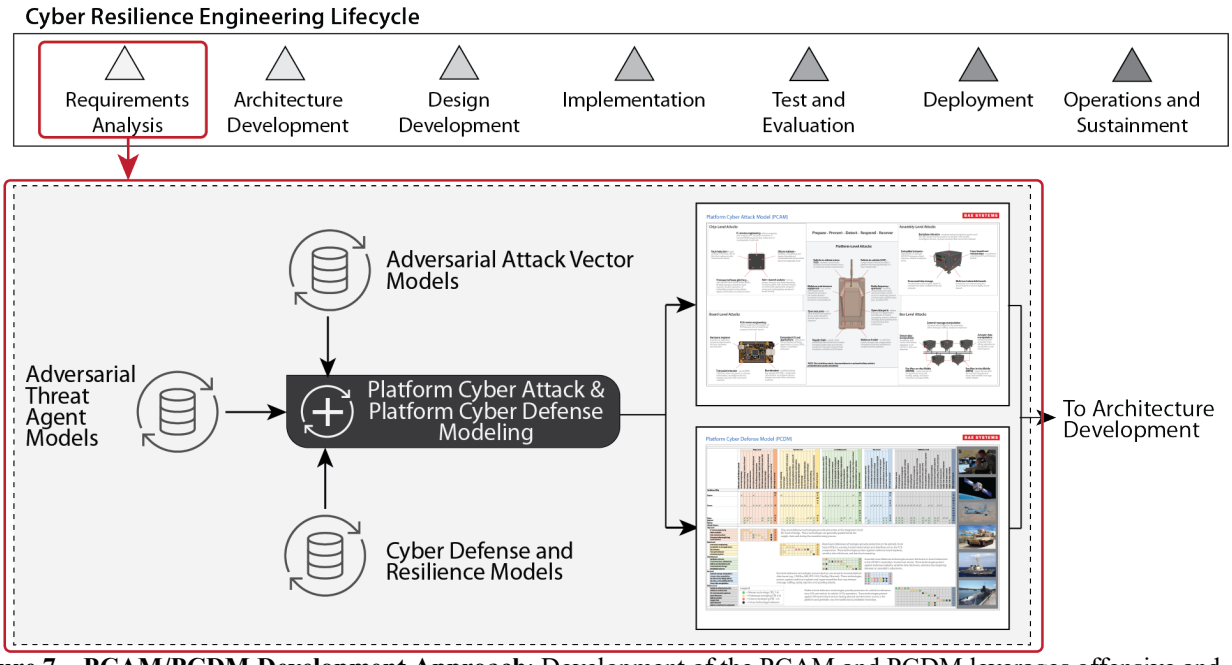


Figure 7 – PCAM/PCDM Development Approach: Development of the PCAM and PCDM leverages offensive and defensive knowledge repositories to ensure high-quality inputs early in the product development lifecycle.

contains generalized descriptions of threat agents found in operational environments. Selection of specific threat agents allows engineering teams to focus their engineering activities on a limited and relevant set of cyber resilience issues. The Adversarial Attack Vector Model repository contains PCAM data that is disassociated from specific platform implementations (to keep the data unclassified). The attack vector models in this repository allow rapid construction of platform-specific PCAM models using simple selection and tailoring activities. The Cyber Defense and Resilience Model repository contains data linking adversarial attacks to defensive and resilience controls. By combining and analyzing data from these three repositories, we rapidly produce the PCAM and PCDM models early in the project lifecycle.

4. CONCLUSIONS

As our foreign adversaries increase their platform cyber-attack capabilities, we need to shift from 'Defense-in-Depth' strategies to incorporate 'Resilience-in-Depth' strategies. At BAE Systems, we found that a necessary first step to addressing this need is to demystify platform cyber resilience and enable engineering teams to work with offensive data to solve defensive problems.

In this paper, we described several key concepts needed to enable the development of resilient solutions. These concepts included:

- Five Pillars of Cyber Resilience to delineate differences between the static defense and dynamic resilience aspects of cyber security solutions.
- Resilience-in-Depth as an extension of Defense-in-Depth requires a new emphasis on attack surface modeling, attack vector modeling, dynamic response modeling, and off-nominal system testing.
- As an approach to defining, visualizing, and understanding a specific platform's attack surface, Platform Cyber Attack Modeling (PCAM) allows engineering teams to consider adversarial behaviors while designing and developing platform systems.
- As an approach to defining, visualizing, and understanding a specific platform's defense surface, Platform Cyber Defense Modeling (PCDM) allows engineering teams to design platforms that can operate effectively in cyber contested environments.

Using these concepts, BAE Systems is taking the next steps by adding Cyber Resilience Engineering processes to our platform systems engineering process set. The resulting integrated processes provides a repeatable and measurable approach to designing and developing highly defendable and highly resilient platform systems with a fast-track to operational accreditation and with increase battlespace survivability.

5. REFERENCES

[1] BAE Systems. "BAE Systems Applied Intelligence Cyber Threat Bulletin", Internet: https://www.baesystems.com/en/cybersecurity/capability/cyber-security-services, date updated 2019 [viewed 17 June 2019].

[2] U.S. Department of Defense. "Information Sharing Environment (DISE)", Internet: https://www.dni.gov/index.php/nctc-who-we-are/organization/201-about/organization/information-sharing-environment, date updated 2019 [viewed 17 June 2019].

[3] U.S. Department of Defense. "DIBnet Portal", Internet: https://dibnet.dod.mil/portal/intranet, date updated 2017, U.S. [viewed 17 June 2019].

[4] MITRE. "ATT&CK™ Framework", Internet: https://attack.mitre.org, date updated 2019 [viewed 17 June 2019].

[5] NIST. (2013, April). *NIST Special Publication (SP) 800-53, Security and Privacy Controls for Federal Information Systems and* Organizations.

(Revision 4). [On-line]. Available: https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final [viewed 17 June, 2019].

[6] DoD Cyber Exchange. "Security Technical Implementation Guides", Internet: https://public.cyber.mil/stigs/, date updated 8 May 2019 [viewed 17 June 2019].

[7] NIST. (2018, March). *NIST Special Publication (SP) 800-160, Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*. (Volume 1). [On-line]. Available: https://csrc.nist.gov/publications/detail/sp/800-160/vol-1/final [17 June, 2019].

[8] NIST. (2018, March). *NIST Special Publication (SP) 800-160 Systems Security Engineering: Cyber Resiliency Considerations for the Engineering of Trustworthy Secure Systems*. (DRAFT) [On-line]. Available: https://csrc.nist.gov/publications/detail/sp/800-160/vol-1/final (Volume 2).