Automotive Cybersecurity
SUMMIT & TRAINING
Chicago | May 1-8, 2018
www.sans.org/Auto-Summit
Automotive Critical Controls – A Mapping of CIS Critical Controls to Automotive Cybersecurity

Dave Bares, CISSP, PMP
Lear Corporation, E-Systems, Cybersecurity Senior Engineer
dbares@lear.com  M: +1-734-546-1725  D: +1-248-447-1682
Global Engineering & Manufacturing

257 FACILITIES
39 COUNTRIES
165,000 EMPLOYEES

#151 on Fortune 500 list

>80% of component facilities and >90% of related employment located in low-cost countries

Diverse Global Sales & Customers

By Customer
- Ford: 18%
- GM: 18%
- Daimler: 9%
- BMW: 9%
- FCA: 8%
- Jaguar/Land Rover: 8%
- Renault-Nissan: 8%
- Hyundai: 6%
- Other: 5%

By Region
- North America: 40%
- Europe and Africa: 38%
- Asia: 18%
- South America: 4%

By Segment
- Passenger Cars: 43%
- CUV/SUV: 44%
- Trucks/Vans: 13%

Serving All Of The World's Automakers With Content In More Than 400 Vehicle Nameplates

Leader in Automotive Systems

SEATING

2017 Sales of $15.9 Billion

Fastest-growing and most profitable automotive seating supplier

World leader in luxury & performance seating;
Well positioned to capitalize on mix shift toward Crossovers and SUVs

Most complete seat component capabilities with unique expertise in fabric, leather and seat cover cutting & sewing allowing the highest level of craftsmanship

Unique software capabilities enabling the innovative intelligent seat

E-SYSTEMS

2017 Sales of $4.6 Billion

Global leader in electrical architecture including high-power with wireless connectivity expertise

Well positioned to benefit from rapidly increasing demands for additional electronic content and software driven by trends in safety and fuel economy

Uniquely positioned to grow with vehicle electrification and connectivity mega-trends with industry-leading electrical distribution and gateway modules, as well as expertise in cybersecurity

Uniquely Positioned To Deliver Continued Profitable Sales Growth

E-Systems Product Portfolio

**ELECTRICAL DISTRIBUTION SYSTEMS**
- Wire Harnesses
- Power Distribution Boxes
- Alternative Wire Solutions
- Global, Low Cost Footprint

**BODY ELECTRONICS**
- Advanced, Highly Integrated Central Body Control Units
- Gateway Modules
- Seat Controllers
- Battery Monitoring Sensors

**TERMINALS & CONNECTORS**
- Standard T&Cs Systems
- High Power Box Terminals
- High Power Pin Terminals
- High Power Connectors
- Stamped & Injection Molded Components

**WIRELESS TECHNOLOGY**
- Remote Keyless Entry Systems
- Passive Entry Passive Start
- 2-Way Remote Keyless Entry
- Integrated Wireless Systems
- Remote Start Systems
- Wireless Electronics Charging

**CONNECTIVITY**
- Connected Gateway
- TeleCommunications Unit
- Over-The-Air Software
- Cyber Security
- V2X On-Board Unit
- V2X Road Side Equipment

**HIGH POWER**
- On-Board Charging Systems
- Electric Vehicle Supply Equipment
- High Power Distribution Systems
- AC Outlet Inverters
- Wireless EV Battery Charging

**JUNCTION BOX**
- Passive Junction Boxes
- Smart Junction Boxes
- Solid State Smart Junction Boxes
- Fuse & Pre Fuse Boxes

**AUDIO**
- Premium Audio Amplifiers
- Lear Proprietary Dynamic Sound Optimization (DYSOP)
- Sound System Integration and Tuning Expertise

**48V TECHNOLOGIES**
- Dual Voltage Architectures
- 48V Wire Harnesses
- 48V MAK 8/12 T&Cs
- 48V DC-DC Converters
- 48V Smart Junction Boxes
- 48V Power Distribution Box

**LIGHTING**
- Exterior Lighting Control Modules
- Interior Ambient Light Control
- Adaptive Front Light Control Modules
- LED Matrix Beam Control Modules

Capitalizing On Traditional Electrical Opportunities And Growth In Emerging Industry Trends

Integrated Vehicle Cybersecurity

Secure External Communications
1. Block access to vehicle networks (Firewall)
2. Authenticate and Encrypt Data Exchange
3. Ensure Data Privacy

Remote Updates and Analytics
1. Record and Maintain History
2. OTA Security Updates
3. Cloud-based Analytics

Protect Computing Platform
1. Secure boot
2. Hypervisor
3. Sec. Env. & integrity monitoring

Development Process
1. Secure development and production processes
2. Penetration testing
3. Industry standards (SAE J3061)

Secure & Monitor Vehicle Networks
1. Authenticate and/or encrypt vehicle network comm.
2. Anomaly Detection & Prevention
3. Smart firewall

Recognized As A Leader In Connected Vehicle Solutions and Cybersecurity
Automotive Critical Controls –
A Mapping of CIS Critical Controls
to Automotive Cybersecurity

Dave Bares, CISSP, PMP
Lear Corporation, E-Systems, Cybersecurity Senior Engineer
dbares@lear.com  M: +1-734-546-1725  D: +1-248-447-1682
SANS CIS Controls Overview

CIS Controls™

Basic
1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6. Maintenance, Monitoring and Analysis of Audit Logs

Foundational
7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols, and Services
10. Data Recovery Capabilities
11. Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control

Organizational
17. Implement a Security Awareness and Training Program
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

SANS CIS Controls available from: http://www.cisecurity.org/critical-controls/
CIS Control 1: Inventory and Control of Hardware Assets

- Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.
CIS Control 2: Inventory and Control of Software Assets

- Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.

Digital Signatures/Software Authentication

Patch Management Strategy

Over the Air Updates

Signing/Verification graphic from: https://commons.wikimedia.org/wiki/File:Digital_Signature_diagram.svg
CIS Control 3: Continuous Vulnerability Management

- Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers. (up from #4 in v6.1)

LOC graphic from: http://www.electronicdesign.com/automotive/automotive-security-can
SIEM graphic from: https://www.cptech.com/cyber-security/

More code implies more vulnerabilities
CIS Control 4: Controlled Use of Administrative Privileges

- The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications. (up from #5 in v6.1)

Don’t run everything as root!

Diagnostic Seed/Key → Challenge/Response

Apply least privilege & separation of duties
CIS Control 5: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

- Establish, implement, and actively manage (track, report on, correct) the security configuration of mobile devices, laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings. *(down from #3 in v6.1)*
CIS Control 6: Maintenance, Monitoring and Analysis of Audit Logs

- Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.
CIS Control 7: Email and Web Browser Protections

- Minimize the attack surface and the opportunities for attackers to manipulate human behavior through their interaction with web browsers and email systems.

CIS Control 8: Malware Defenses

- Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action.


CIS Control 9: Limitation and Control of Network Ports, Protocols, and Services

- Manage (track/control/correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers.

CIS Control 10: Data Recovery Capabilities

- The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.

---


Warning sign from: [http://www.bandsbodyshop.com/Direct-Repair-Program](http://www.bandsbodyshop.com/Direct-Repair-Program)


---

Wishlist

- Popular?
- Ambiguous?
- Alternatives?
- Conflicting?
- Dependent?
- Technical
- Economic
- Schedule
- Compliance
- Feasible?
- Operational

KWP2000
CCP/XCP
UDS
E/J-OBD
OBDII
CARB

---

Approved for Public Release
CIS Control 11: Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

...very similar to CIS Control 5 without end-user/HMI considerations

• Establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings

Apply layered security & hardening

HSM logo from: http://www.hardware-security-module.com/

CIS Control 12: Boundary Defense

- Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.

Flat bus topologies shifting toward functional domains with varied CIA requirements

Domain based vehicle topology graphic from: https://automotive.electronicspecifier.com/air-conditioning/real-time-automotive-ethernet
CAN schematic from: https://commons.wikimedia.org/wiki/File:CAN_Bus_Elektrische_Zweidrahtleitung.svg
Approved for Public Release
CIS Control 13: Data Protection

- The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.

VIN, Owner info, Vehicle health, Geolocation, Speed, etc.

PII = personally identifiable information
CIS Control 14: Controlled Access Based on the Need to Know …very similar to CIS Control 4 with extension beyond ‘Admin’

- The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.

Don’t run everything as root!

Apply least privilege & separation of duties

CIS Control 15: Wireless Access Control
...a specific case of CIS Controls 9 and 12 when applied to automotive

- The processes and tools used to track/control/prevent/correct the security use of wireless local area networks (WLANs), access points, and wireless client systems.

CIS Control 16: Account Monitoring and Control
...‘housekeeping’ of CIS Controls 4 and 14

- Actively manage the life cycle of system and application accounts - their creation, use, dormancy, deletion - in order to minimize opportunities for attackers to leverage them.

Interconnectivity depiction from: http://www.autopinas.com/14-year-old-boy-hacks-car/
CIS Control 17: Implement a Security Awareness and Training Program

• For all functional roles in the organization (prioritizing those mission-critical to the business and its security), identify the specific knowledge, skills and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs.

CIS Control 18: Application Software Security

• Manage the security life cycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses.


[Digital car graphic from: https://www.ccn.com/hackethon-bring-data-analytics-smart-contracts/]

Approved for Public Release
CIS Control 19: Incident Response and Management

• Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight) for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.

CIS Control 20: Penetration Tests and Red Team Exercises

• Test the overall strength of an organization's defense (the technology, the processes, and the people) by simulating the objectives and actions of an attacker.

Penetration Testing graphic from: https://trashieldinc.com/services/risk-assessments/penetration-testing/
The ‘Secure’ Car

(1) Includes immutable cryptographic identities – as building blocks for other features/services

(1) & (2) Includes full traceability of all replaceable hardware and soft inventory line items throughout entire product lifecycle

(2) Only uses authenticated software providing mechanisms to vet and authenticate non-traditional sources

(2) Offers secure remote updates assisting timely proactive and reactive response/update actions

(2) Utilizes end-to-end mutual authentication for integrity and non-repudiation within a comprehensive managed update/patch framework

(3) Provides feedback to SIEM for aggregation & correlation

(4) Applies and enforces least privilege, separation of duties, properly authenticated privilege escalation

(4) & (12) Includes physically and/or logically separate domains – function, safety/security, etc. – enforcing MAC

(4) Enforces role-based DAC for diagnostics and repair/update operations ensuring safety & security throughout

(5) Assumes and provides a secure operating environment

(6) Operations, health, anomalies, etc. reported to and monitored by IDS and SOC

(7) Provides secure M2M and HMI interactions

(8) Is malware resilient – primarily via sound code hygiene and data interchange practices

(9) Exposes only essential ports/services – no more, no less

(10) Includes appropriate redundancy and data recovery mechanisms

(11) Assumest and provides a secure intercommunication environment

(12) Provides domain separation, filtering, and isolation or allowed transitions

(13) Protects sensitive information – at rest, in transit, in use

(14) Facilitates authorized forensic review and analysis

(15) Adheres to prescribed communication models

(16) Adheres to account/access privileges and revocations

(17) Designed, built, and maintained by subject matter experts

(18) Coded & constructed via secure development processes

(19) Includes full lifecycle support including incident response when need

(20) Completed full testing/validation including adversarial penetration tests/attack emulation

Discussion & Questions

Dave Bares, CISSP, PMP
Lear Corporation, E-Systems, Cybersecurity Senior Engineer
dbares@lear.com M: +1-734-546-1725 D: +1-248-447-1682
Sources and Related Reading


