Cyber Security for Monitoring Industrial IoT

ACAMP seminar

June 1st, 2016

Marius Ghinescu

Topics - Focus

- Alberta Innovates overview
- From Digital Battlefield to Digital Oilfield
- Industrial Internet of Things (IoT)
  - aka Operational Technology
- Advanced Monitoring Systems Timelines
- Data Science, Machine Learning, Artificial Intelligence
- Cyber Security Frameworks and references
- Tactical IoT Digital Security Summary

Alberta's Innovation System

Alberta Innovates offers post-secondary research support and applied research and commercialization services to enhance research and innovation in Alberta

650 staff
$160M budget
7 locations

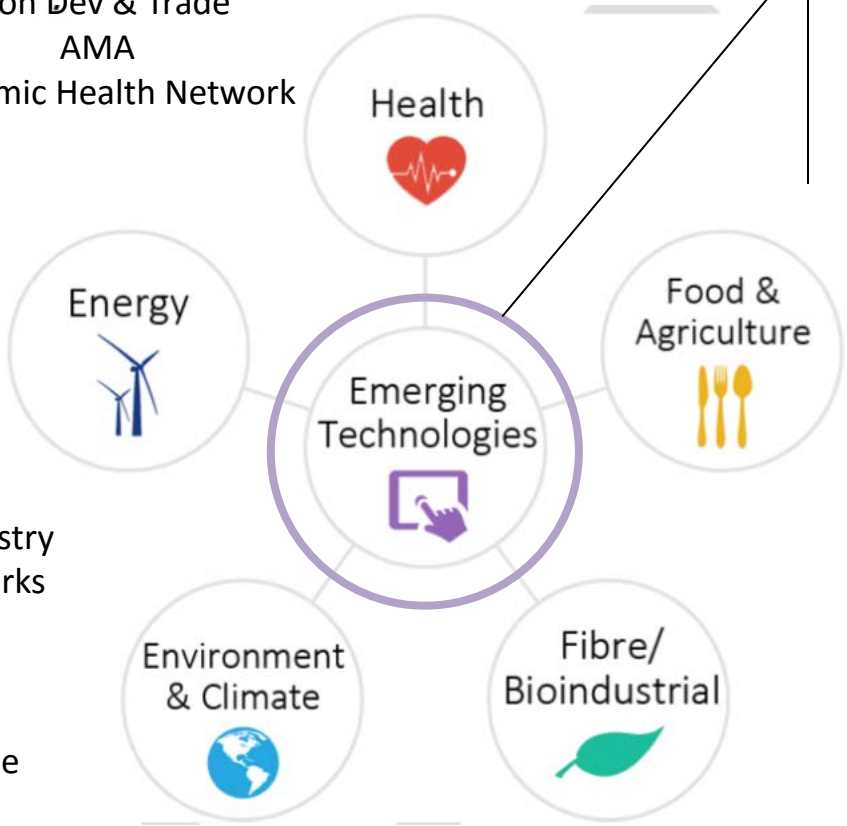
Priority Sectors – Key GoA Stakeholders

Targets and focus areas determined by GoA collaboratories

Health
Health Services
Econ Dev & Trade
AMA
Academic Health Network

Emerging Tech focuses on convergent opportunities by performing an Integrative function across all sectors and other GoA entities (e.g. Service Alberta)

Environment & Parks
Energy
Econ Dev & Trade
AER
CCEMC

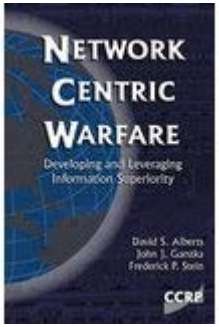


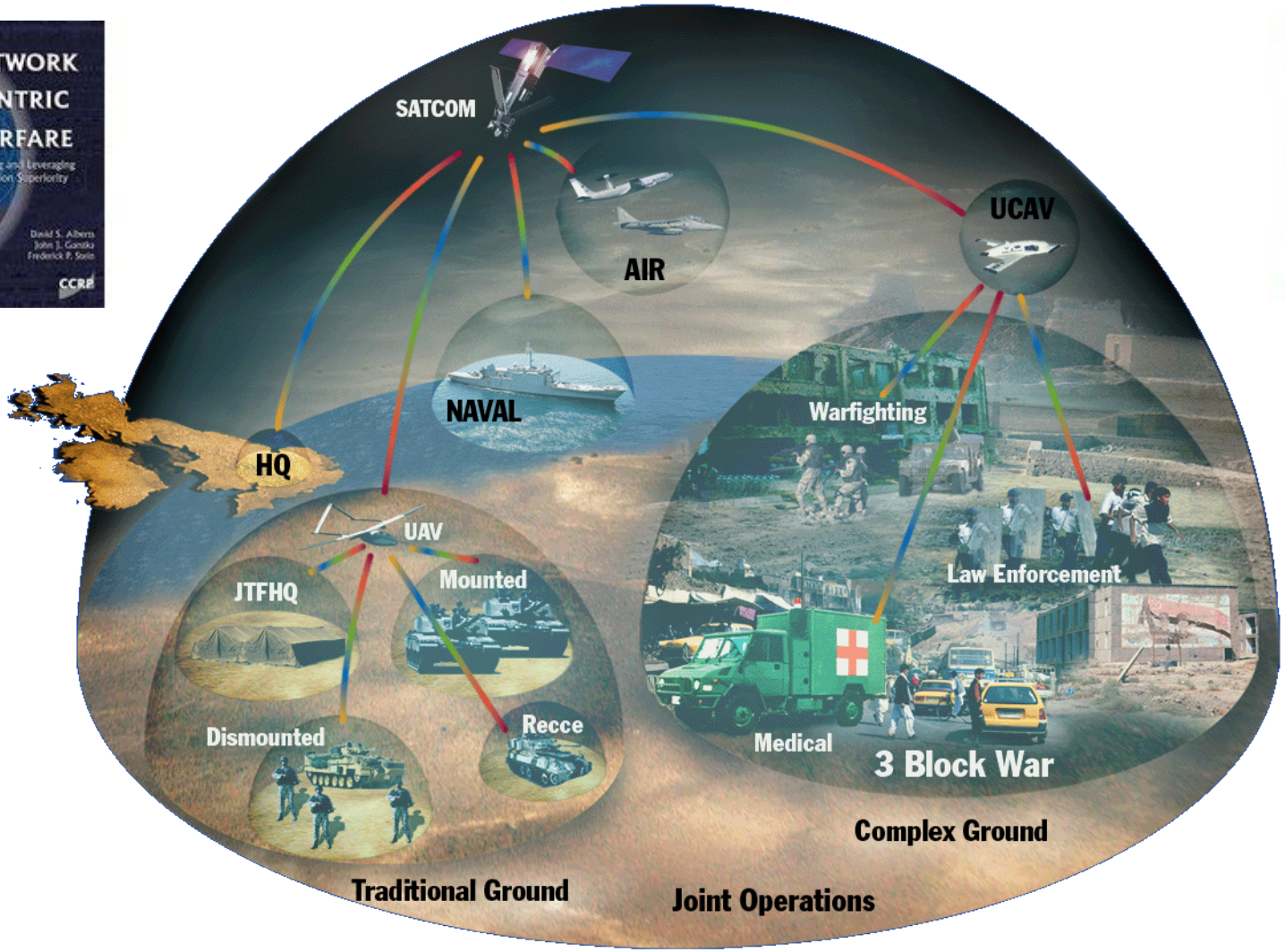
Agriculture & Forestry
Health
Econ Dev & Trade
ALMA

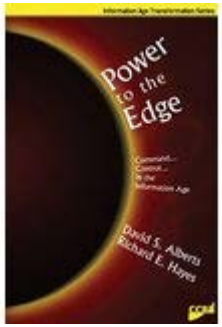
Agriculture & Forestry
Environment & Parks
Energy
Health
AER
Econ Dev & Trade
CCEMC

Agriculture & Forestry
Environment & Parks
Econ Dev & Trade

Digital Battlefield – Network Centric Operations

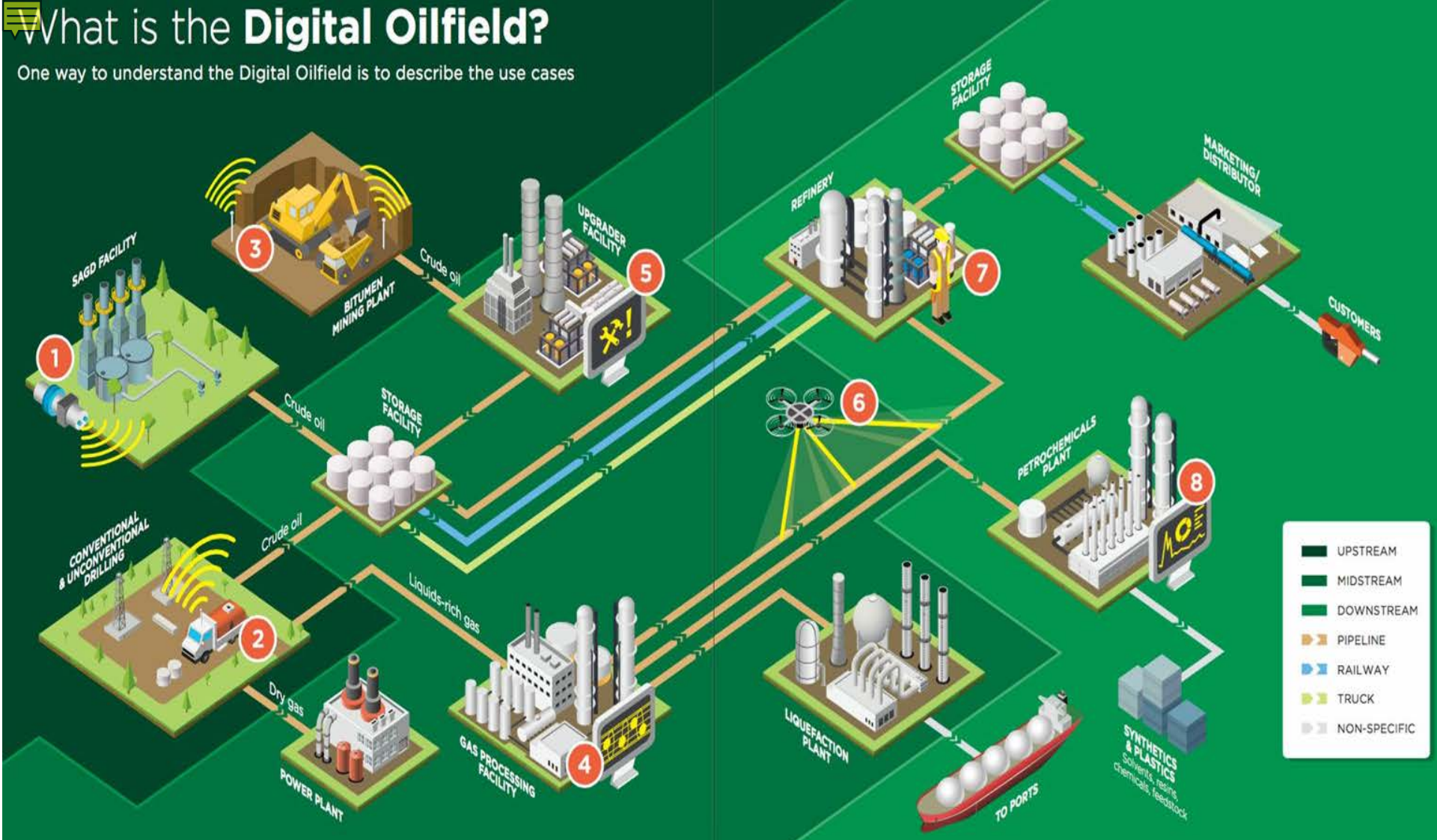






What is the **Digital Oilfield?**

One way to understand the Digital Oilfield is to describe the use cases



1

Improve SOR, asset reliability and optimize production through increased use of improved sensors, automation and connectivity to remote experts.

2

Improve fleet efficiency with vehicle identification, logistics optimization and automated loading using pervasive wireless and real-time sensor and video data analytics.

3

Provide pervasive wireless connectivity to support collaboration, knowledge access and personnel welfare in the field.

4

Use remote monitoring and inspection applications to improve security and environmental protection with predictive intrusion, leakage and deformation detection.

5

Reduce downtime and improve asset integrity with predictive maintenance using real-time analytics and immediate virtual expert support.

6

Remote monitoring of assets such as pipelines, gas plants and storage facilities via smart video surveillance, self-navigating drones and satellite.

7

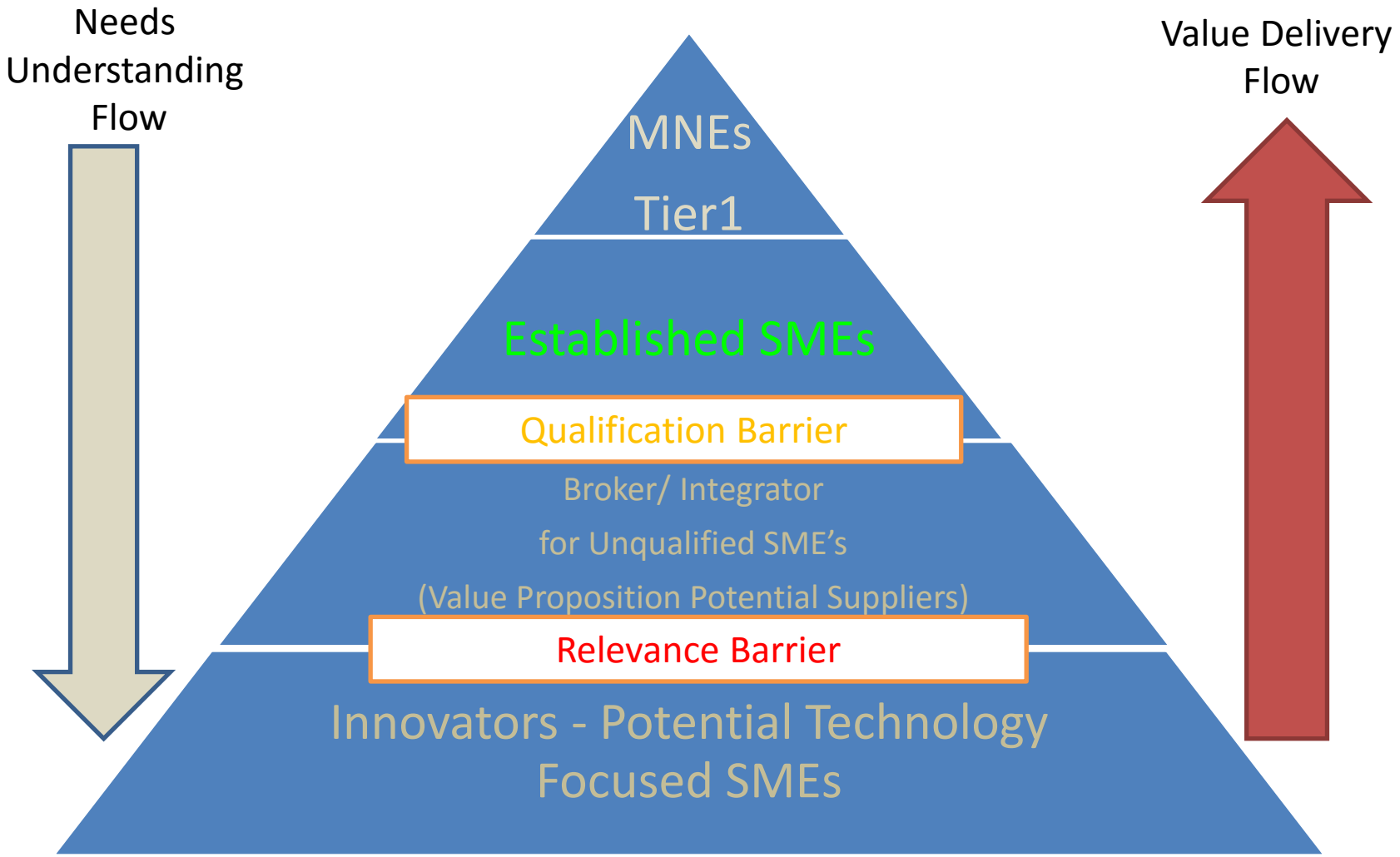
Improve personnel safety and optimize processes with wireless real-time tracking, video analytics and automated incident response.

8

Perform analytics on collected data to identify operating insights that can be used to enhance decision making.

Source: Digital Oilfield Outlook Report, Opportunities &Challenges for Digital Oilfield Transformation, JWN Energy/GE/Accenture Oct. 2015

Canada Defence Procurement Strategy:
ITB Policy Value Proposition - 15% SMEs Content



http://www.ic.gc.ca/eic/site/086.nsf/eng/00006.html

IoT Definition

The Internet of Things (IoT) has been defined in Recommendation ITU-T Y.2060 (06/2012) as a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.*

Industrial IoT: A standardization initiative on the Industrial IoT covering the Industry 4.0, Smart factory or Smart manufacturing (ITU-T SG20)

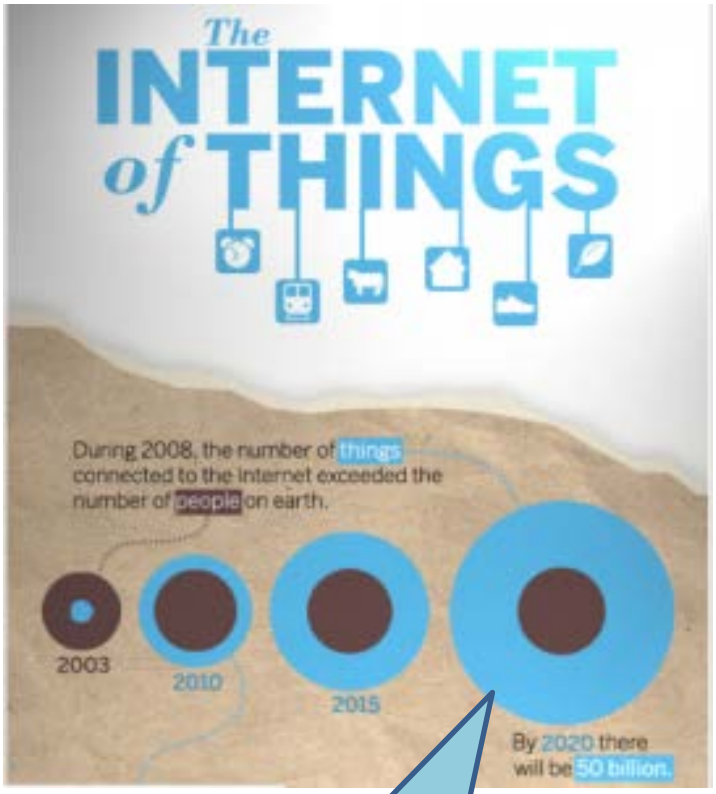
The real opportunity for change... surpassing the magnitude of the consumer Internet... is the Industrial Internet, an open, global network that connects people, data, and machines.

Jeff Immelt
GE Chairman & CEO

industrial internet CONSORTIUM

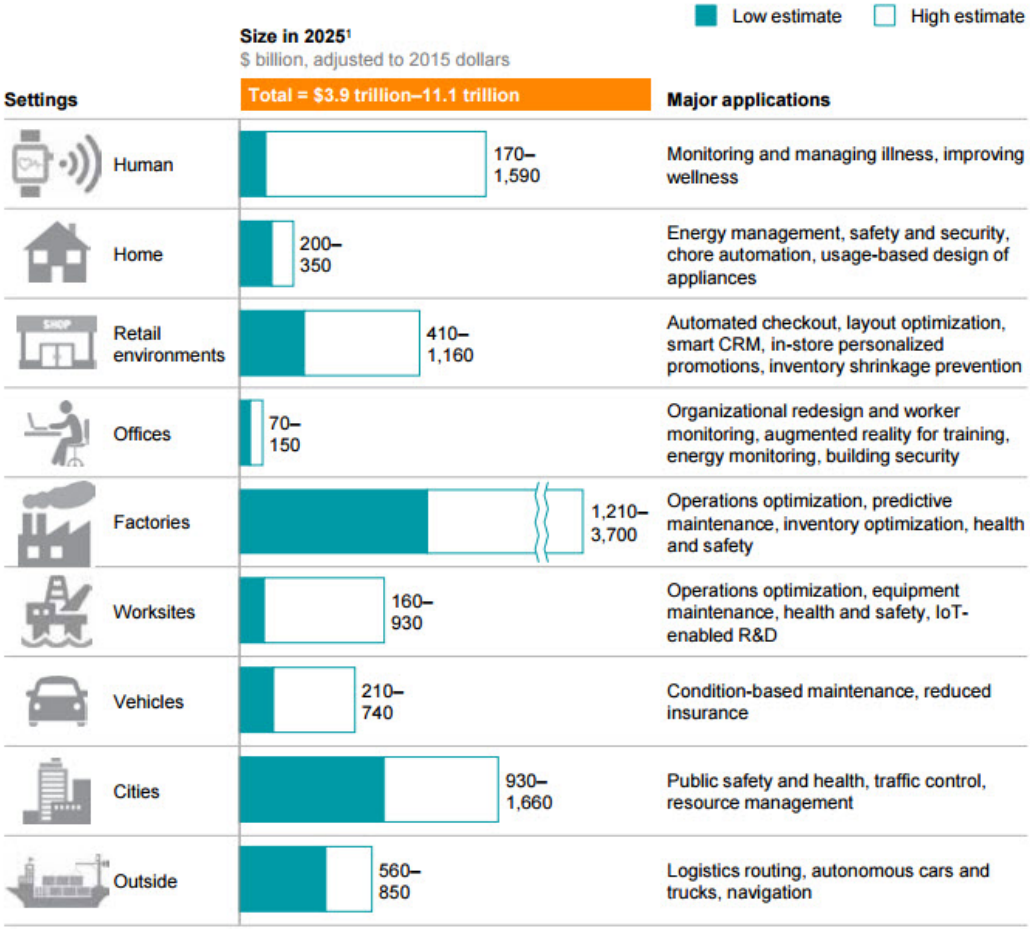
*Internet of Thighs Global standards Initiatives

IoT economic impact



Source IDC: $29.5 billion in 2020, from $10.3 billion in 2014

Potential economic impact of IoT in 2025, including consumer surplus, is $3.9 trillion to $11.1 trillion



1 Includes sized applications only.
NOTE: Numbers may not sum due to rounding.

SOURCE: McKinsey Global Institute analysis

Cyber Security Defence Market size per Sub-Sectors

Sector	Sub-Sectors	Description
Cyber Security	Network Security	This segment includes all processes, mechanisms, software and hardware that are used in securing a computer network infrastructure. These mechanisms prevent unauthorized access into the network while ensuring data availability to a legitimate user.
	Data Security	This segment includes all processes, mechanisms, software and hardware that are used to protect unauthorized personnel from gaining access to databases or information repositories. These mechanisms also ensure that the data is free of malware or any other sort of corruption
	Identity and Access	This segment is a framework for computer networks and processes that facilitates the management of electronic identities. The framework includes the technology needed to support identity management.
	Cloud Security	This segment refers to the set of procedures, processes and standards designed to provide information security assurance in a cloud computing environment

Region	(All)										
	Values (in US$ Millions) per Year										
Sub-Sectors	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023
Identity & Access	2,543	2,658	2,901	3,099	3,288	3,432	3,499	3,735	3,896	4,185	4,427
Network Security	4,003	4,094	4,399	4,524	4,793	5,012	5,285	5,628	5,852	5,783	6,101
Cloud Security	1,576	1,774	2,027	2,180	2,406	2,529	2,686	2,889	3,026	3,286	3,517
Data Security	2,968	3,114	3,397	3,628	3,853	4,029	4,261	4,541	4,742	5,089	5,381
Grand Total	11,090	11,641	12,723	13,431	14,340	15,002	15,731	16,792	17,516	18,343	19,426

*Frost and Sullivan 2013

Internet of Things Reference Model

Levels

7 **Collaboration & Processes**
(Involving People & Business Processes)

6 **Application**
(Reporting, Analytics, Control)

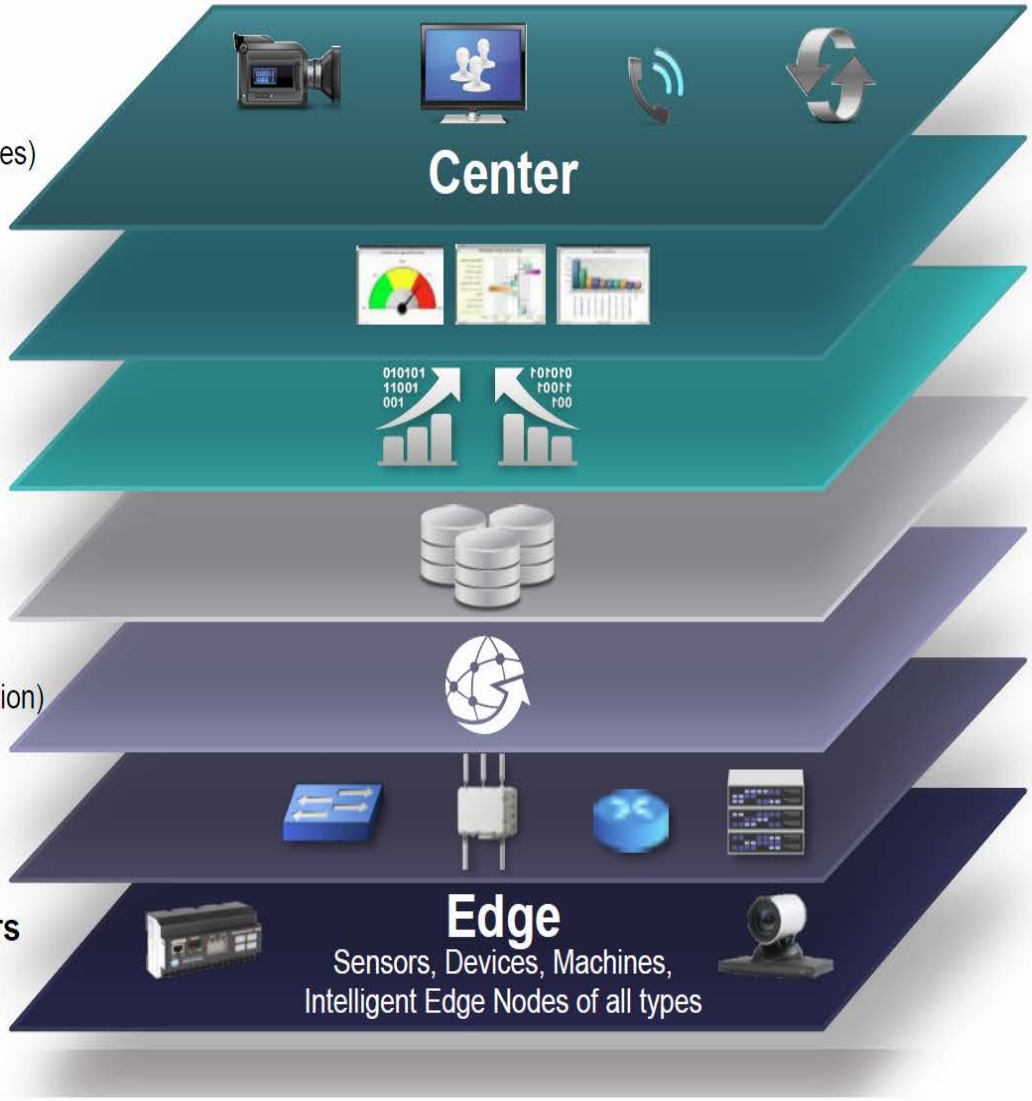
5 **Data Abstraction**
(Aggregation & Access)

4 **Data Accumulation**
(Storage)

3 **Edge (Fog) Computing**
(Data Element Analysis & Transformation)

2 **Connectivity**
(Communication & Processing Units)

1 **Physical Devices & Controllers**
(The "Things" in IoT)

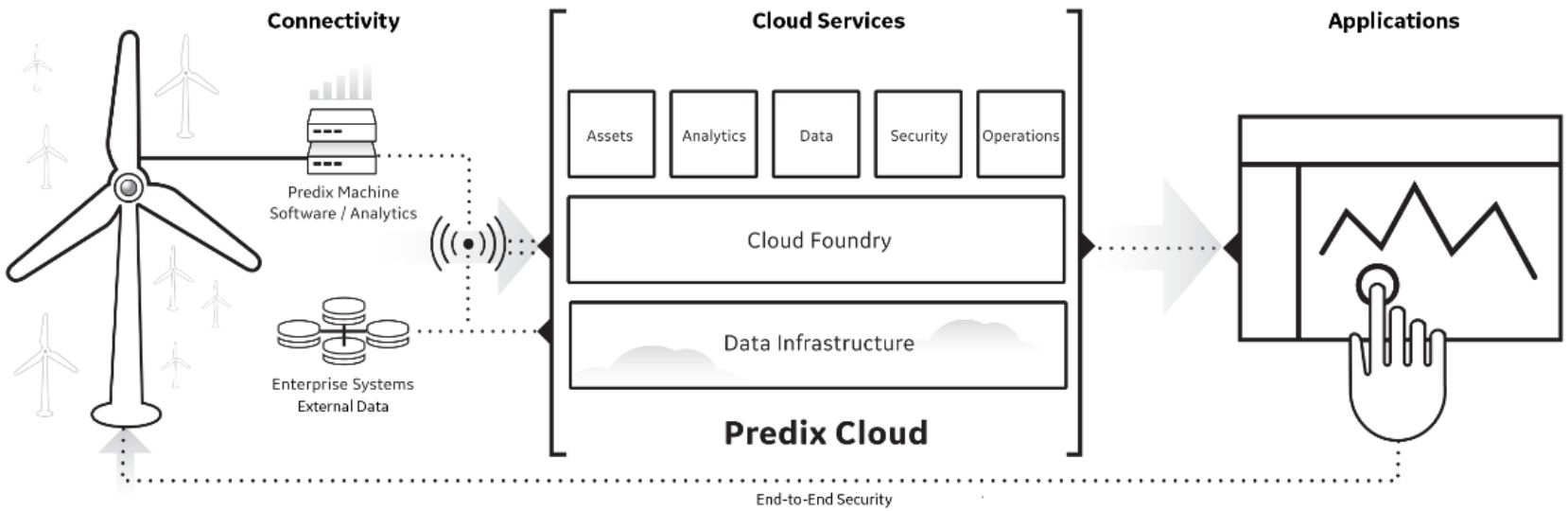


Data at Rest

Data in Motion

End to End Security “baked-in”

Built on Cloud Foundry, Predix is optimized for secure connectivity and analytics at scale - in the Cloud and on the Edge



GE Imagination at work

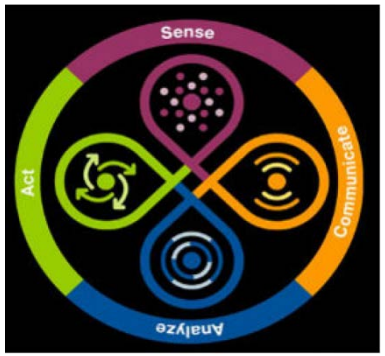
IoT Security Testing and Certification Labs

The ICSA Labs Product Assurance Report found the majority of security devices fail to perform as intended*

IoT Security Testing Categories	
Alerting/Logging	Cryptography
Authentication	Physical Security
Communications	Platform Security

*Validation vs Verification, Qualification, Certification

Hype



BRUCE SCHNEIER 01.06.14 6:30 AM

THE INTERNET OF THINGS IS WILDLY INSECURE — AND OFTEN UNPATCHABLE

"Internet of Things" security is hilariously broken and getting worse

Shodan search engine is only the latest reminder of why we need to fix IoT security.

by J.M. Porup (UK) - Jan 23, 2016 7:30am PST

Share Tweet Email 135

As IoT takes center stage at CES 2016, security gets lost in the wings

Analysis: Now more than ever, toymakers and smart home device manufacturers have to put security first.

By Zack Whittaker for Zero Day | January 6, 2016 -- 17:42 GMT (09:42 PST) | Topic: Security

CRUNCH NETWORK

Who Will Step Up To Secure The Internet Of Things?

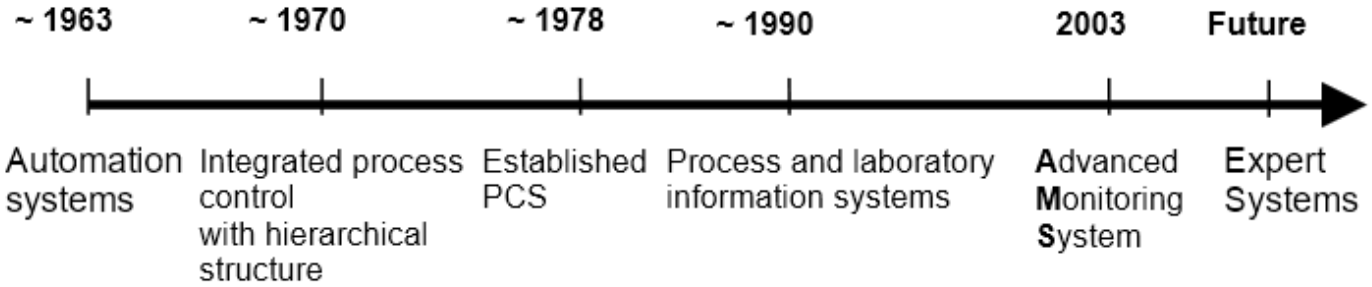
Posted Oct 2, 2015 by John Dixon (@JohnDixonIoT)

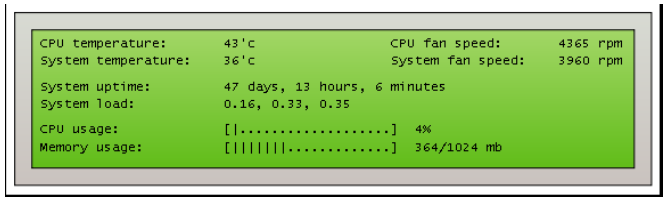
NEWS ANALYSIS

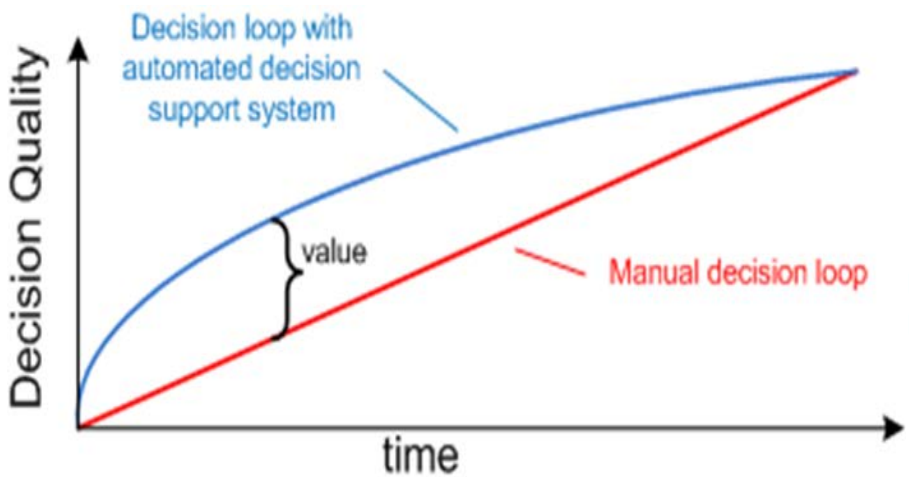
Going dark debunked: Boundless surveillance opportunities via the Internet of Things

s

Advanced Monitoring Systems Time lines

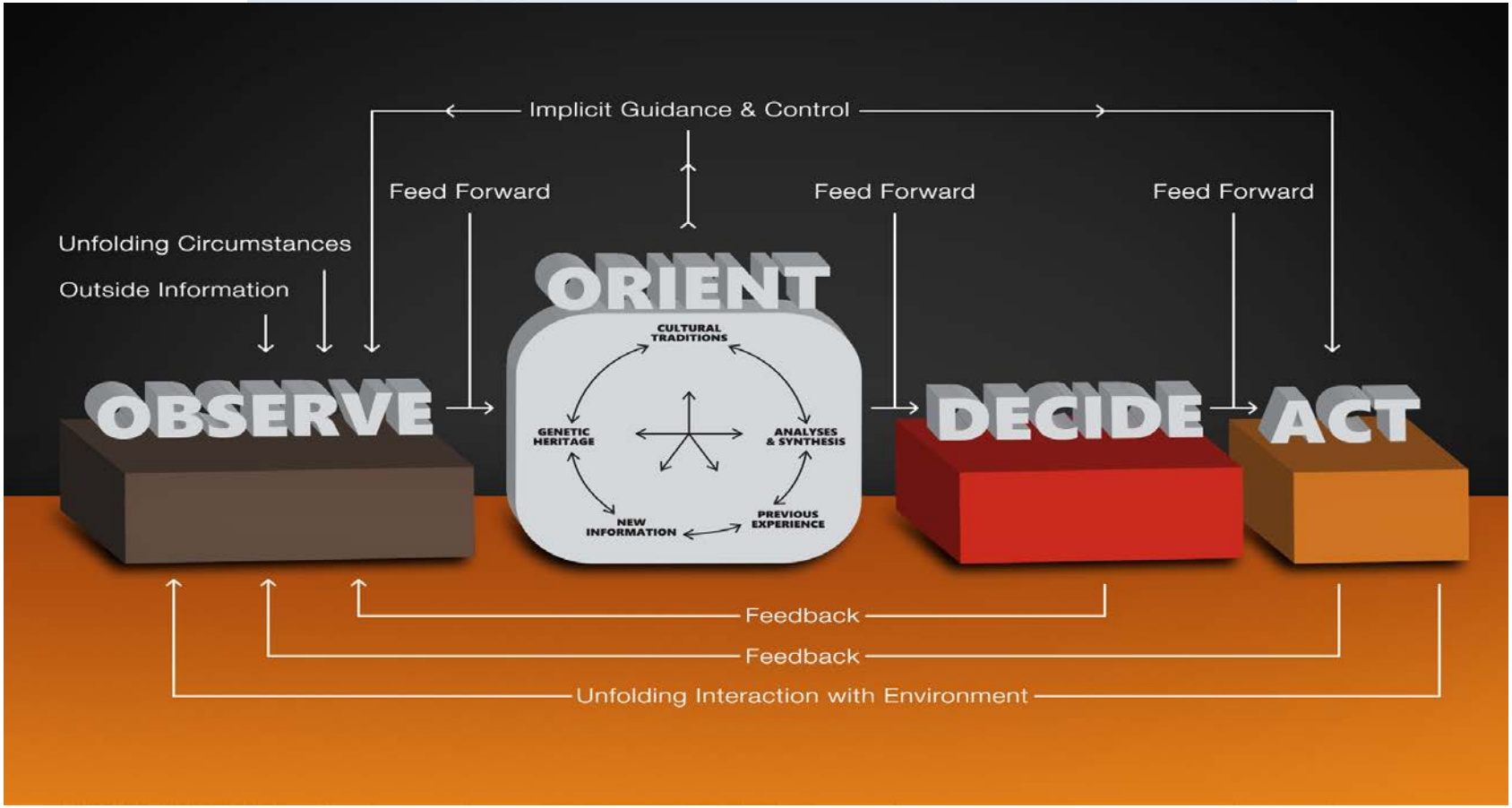




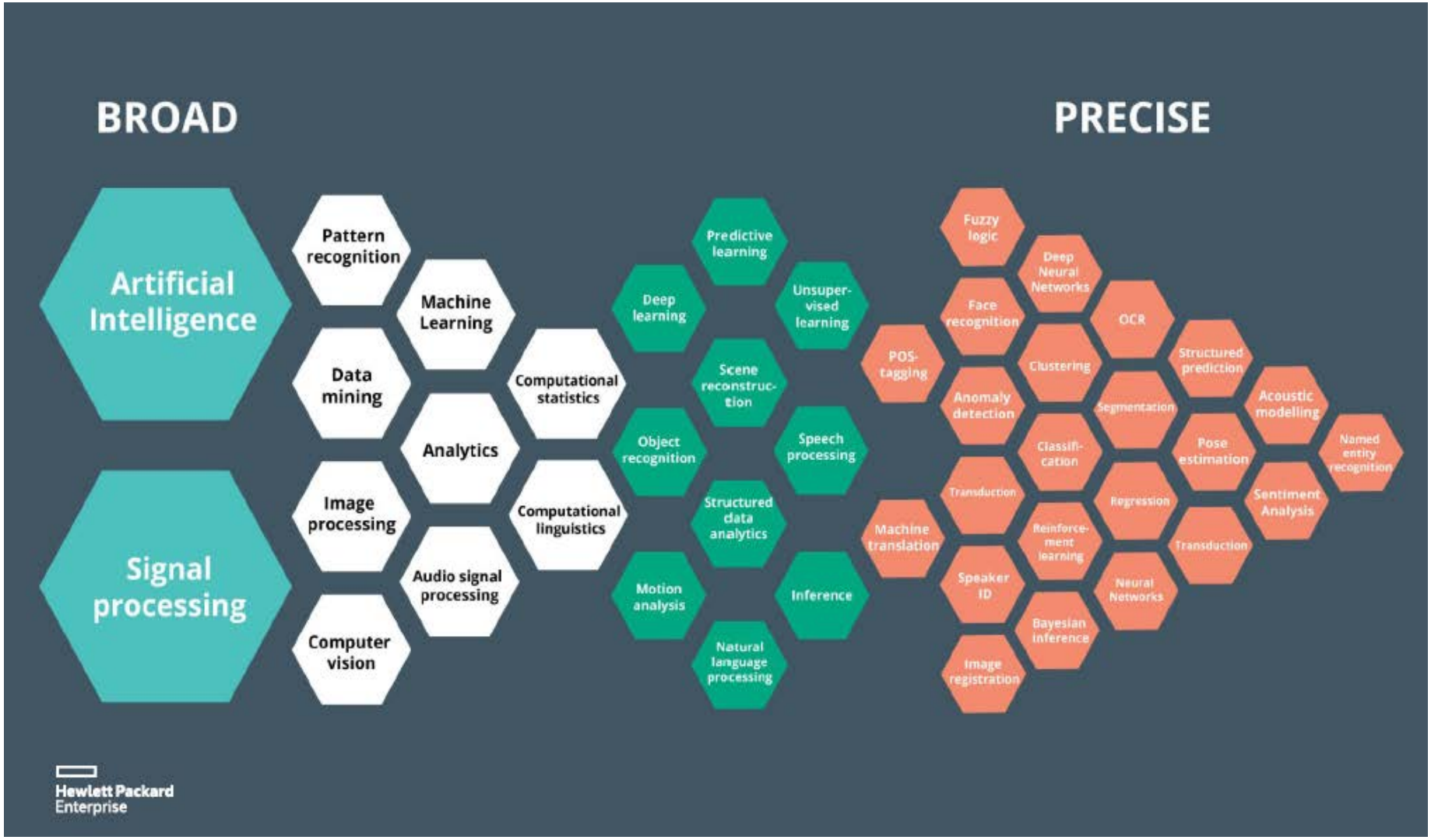


One of the bigger challenges in securing IoT entails changes required in the IoT sensors and protocols that have evolved from more functional requirements. *The Economic times

OODA Loop – IoT Capabilities



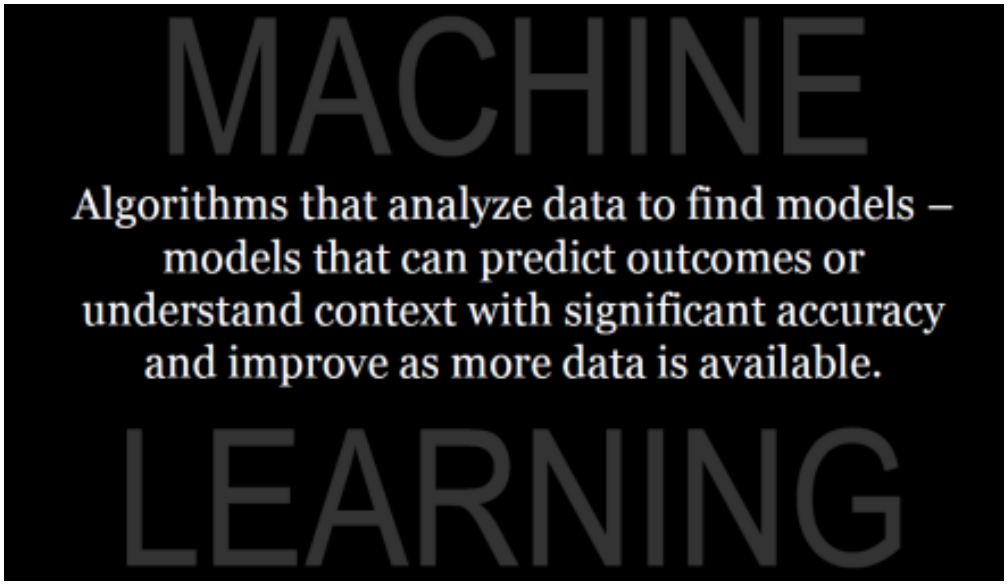
Focus – What is your System loop?



Machine Learning and Artificial Intelligence

vicarious

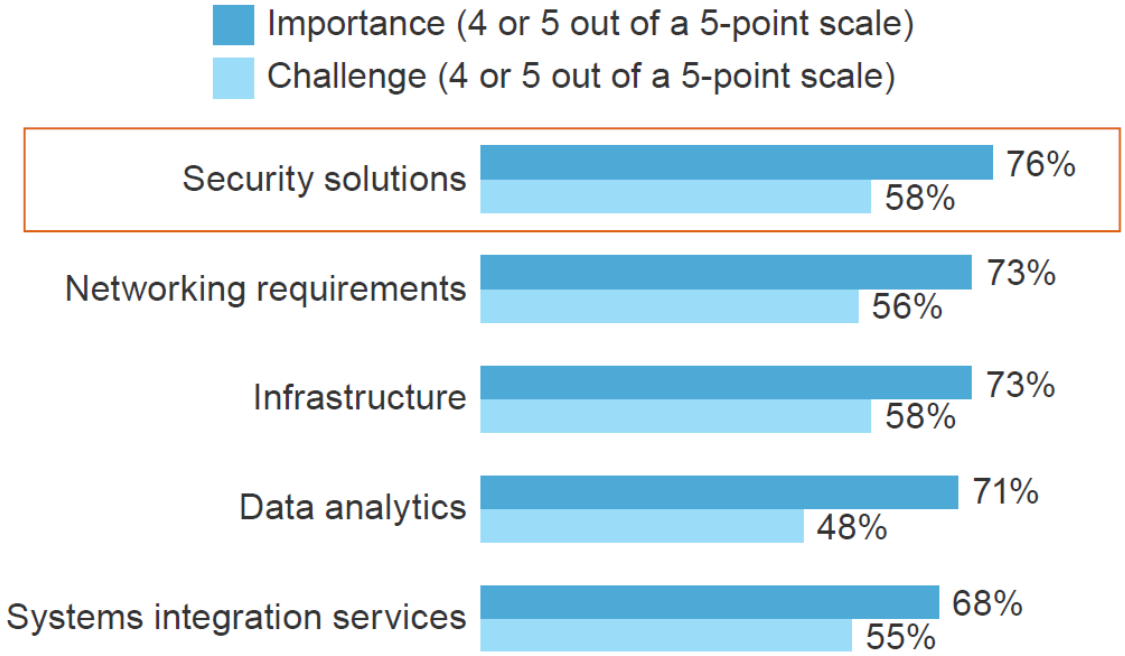
"…We are building a **unified algorithmic architecture** to achieve human-level intelligence in vision, language, and motor control. Currently, we are focused on visual perception problems, like recognition, segmentation, and scene parsing. We are interested in general solutions that work well across multiple sensory domains and tasks."



Security – Top of mind

"Please rate the following elements based on how *important* and how much of a *challenge* each element is to implementing applications and solutions that use the *'intelligent connectivity of physical devices'* in your organization."

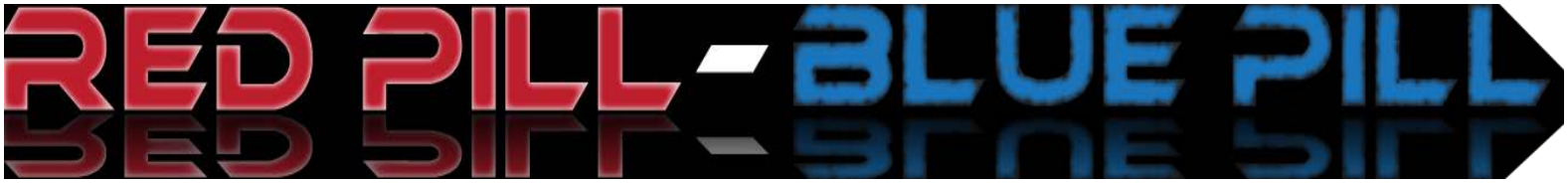
(Rate on a 1-to-5 point scale, showing top 5 in importance)



Base: 336 Internet-of-Things decision-makers

Source: A commissioned study conducted by Forrester Consulting on behalf of Cisco, November 2014

Cyber Security– Reality Check



Truth leads to enlightenment, which compels action

Bliss fosters naiveté, which leads to status quo

The Sliding Scale of Cyber Security

SANS ICS410
ICS/SCADA Security Essentials

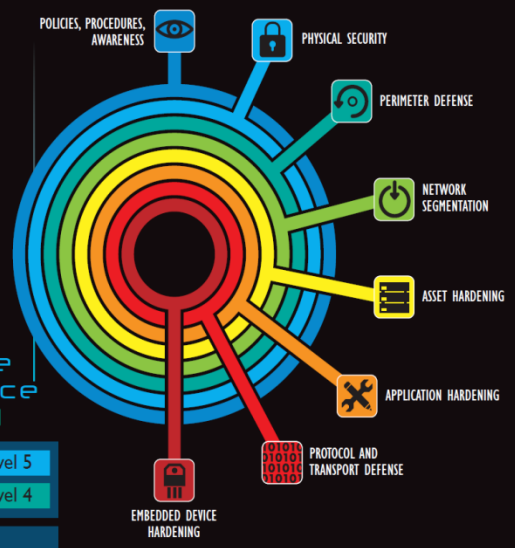
SANS has joined forces with industry leaders to equip security professionals and control system engineers with the cybersecurity skills they need to defend national critical infrastructure. **ICS410: ICS/SCADA Security Essentials** provides a foundational set of standardized skills and knowledge for industrial cybersecurity professionals. The course is designed to ensure that the workforce involved in supporting and defending industrial control systems is trained to keep the operational environment safe, secure, and resilient against current and emerging cyber threats.

SANS ICS515
ICS Active Defense and Incident Response

ICS515: ICS Active Defense and Incident Response empowers students with the ability to understand and utilize active defense mechanisms in concert with incident response for industrial control system networks in order to respond to and deny cyber threats. The course uses a hands-on approach to give students a technical understanding of concepts such as generating and using threat intelligence, communicating control system needs to information technology personnel to deploy appropriate defenses, detecting malicious actors or threats on control system networks, and performing threat triage and incident response to ensure the safety and reliability of operations technology.

ARCHITECTURE | PASSIVE DEFENSE | ACTIVE DEFENSE | INTELLIGENCE | OFFENSE

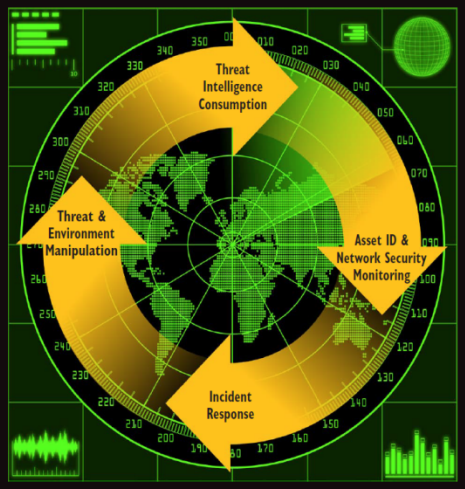
Layers of ICS Defense In Depth



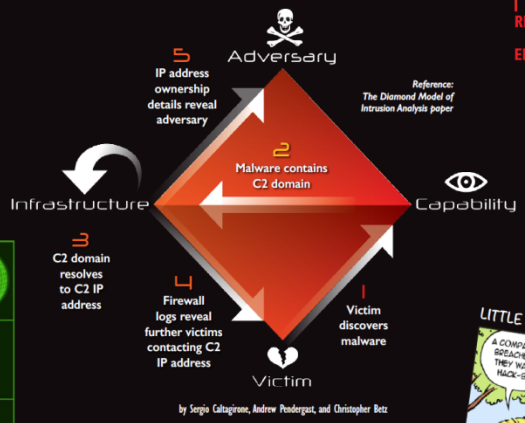
Purdue Reference Model

ENTERPRISE ZONE	Level 5
	Level 4
DMZ	
MANUFACTURING ZONE	Level 3
CELL/AREA ZONE	Level 2
	Level 1
	Level 0

Active Cyber Defense Cycle



The Diamond Model



by Sergio Caltagirone, Andrew Pendergast, and Christopher Betz

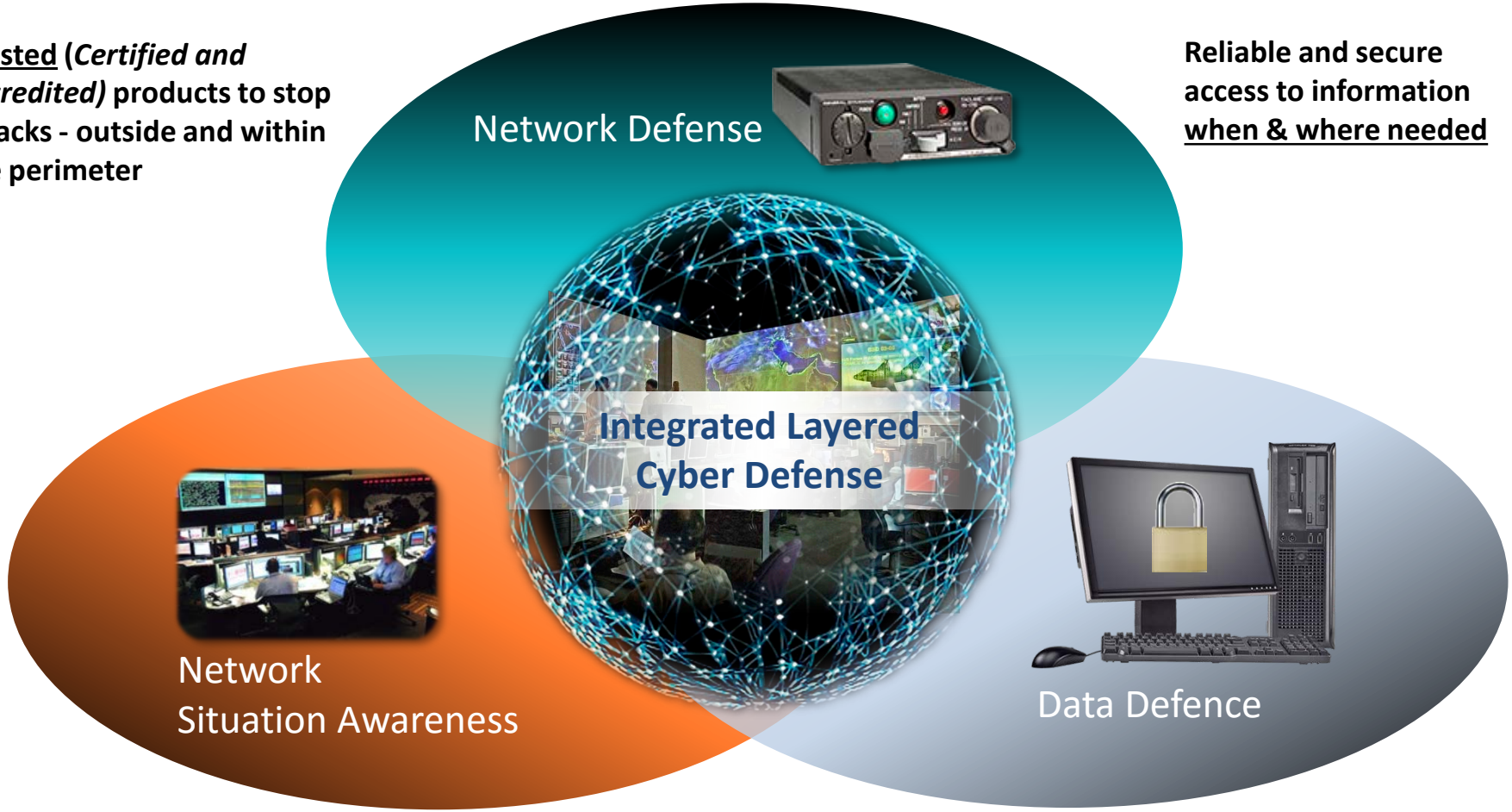
NOT RECOMMENDED IN ICS ENVIRONMENTS

by Robert M. Lee and Jeff Haas

Digital Battlefield - Cyber Defense

<u>Trusted</u> (*Certified and accredited)* products to stop attacks - outside and within the perimeter

Reliable and secure access to information <u>when & where needed</u>



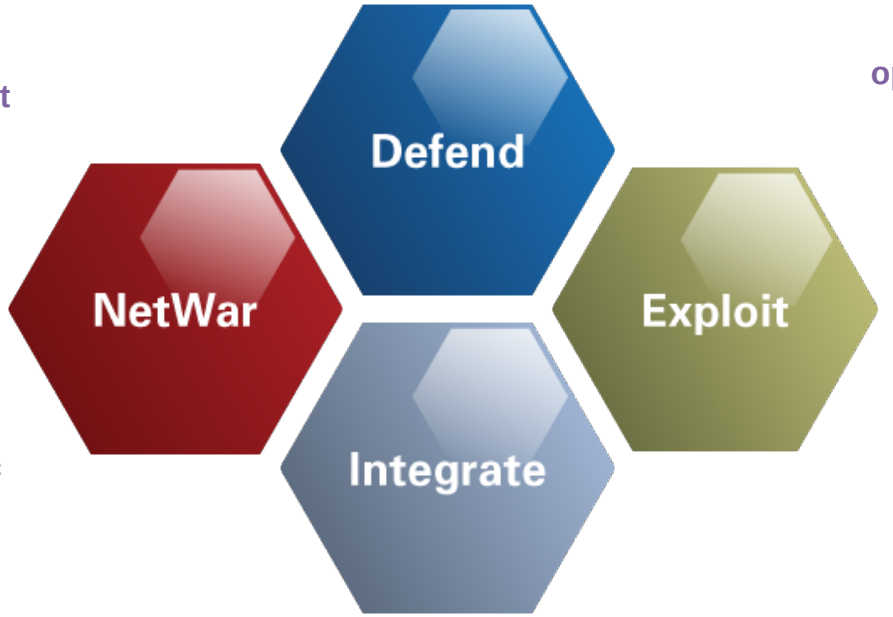
<u>Reduce time</u> to successfully resolve an attack

Defend the information <u>outside the network</u>

Cyber Security Framework – Expanded Defense example

Defend
Providing the personnel and electronic systems that government organizations need to actively defend their networks against external attacks

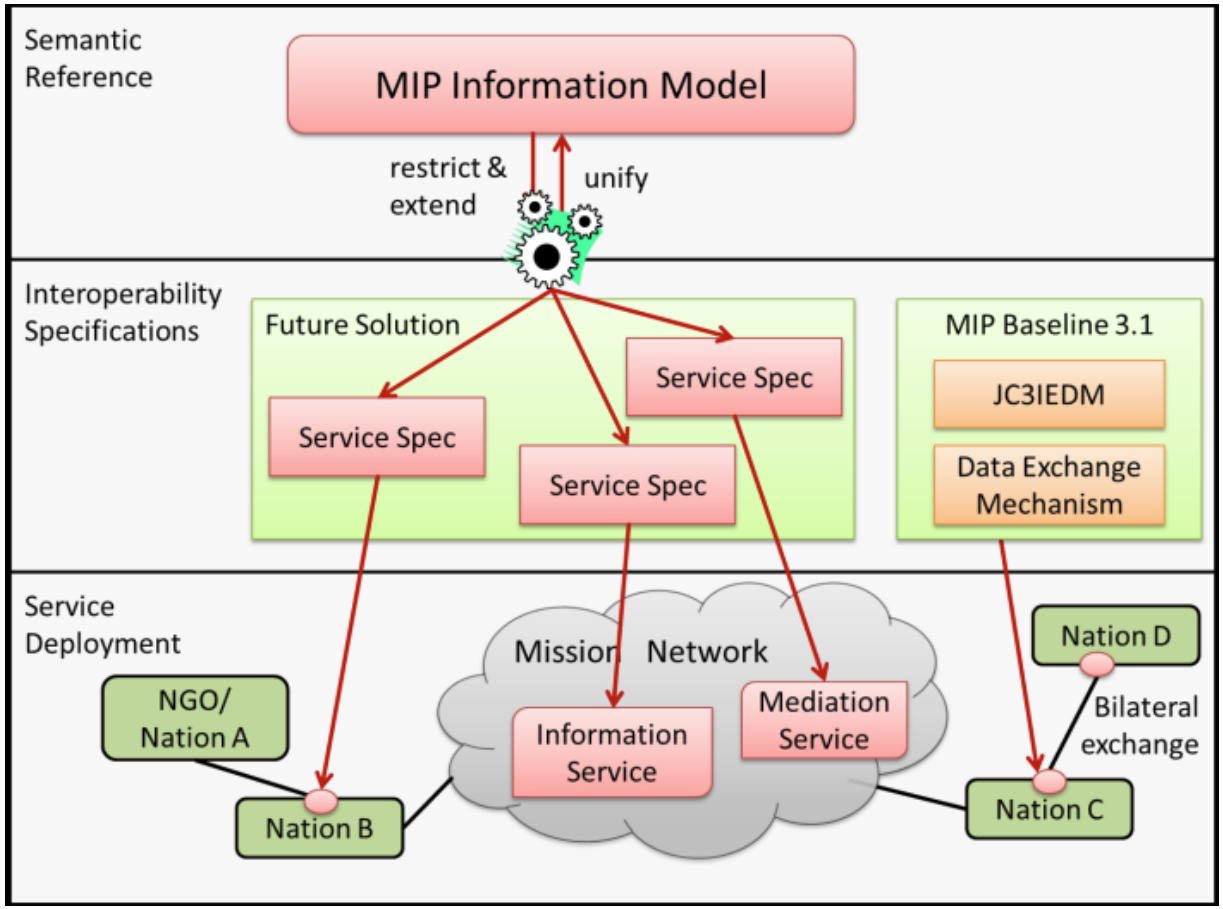
Exploit
Using broad information-operations expertise to identify and assist in understanding adversaries' (offensive).



NetWar
Use networked electronic communications to disrupt adversaries' abilities to function.

Integrate
Incorporating protective measures into the design and operations of networks to avoid vulnerabilities.

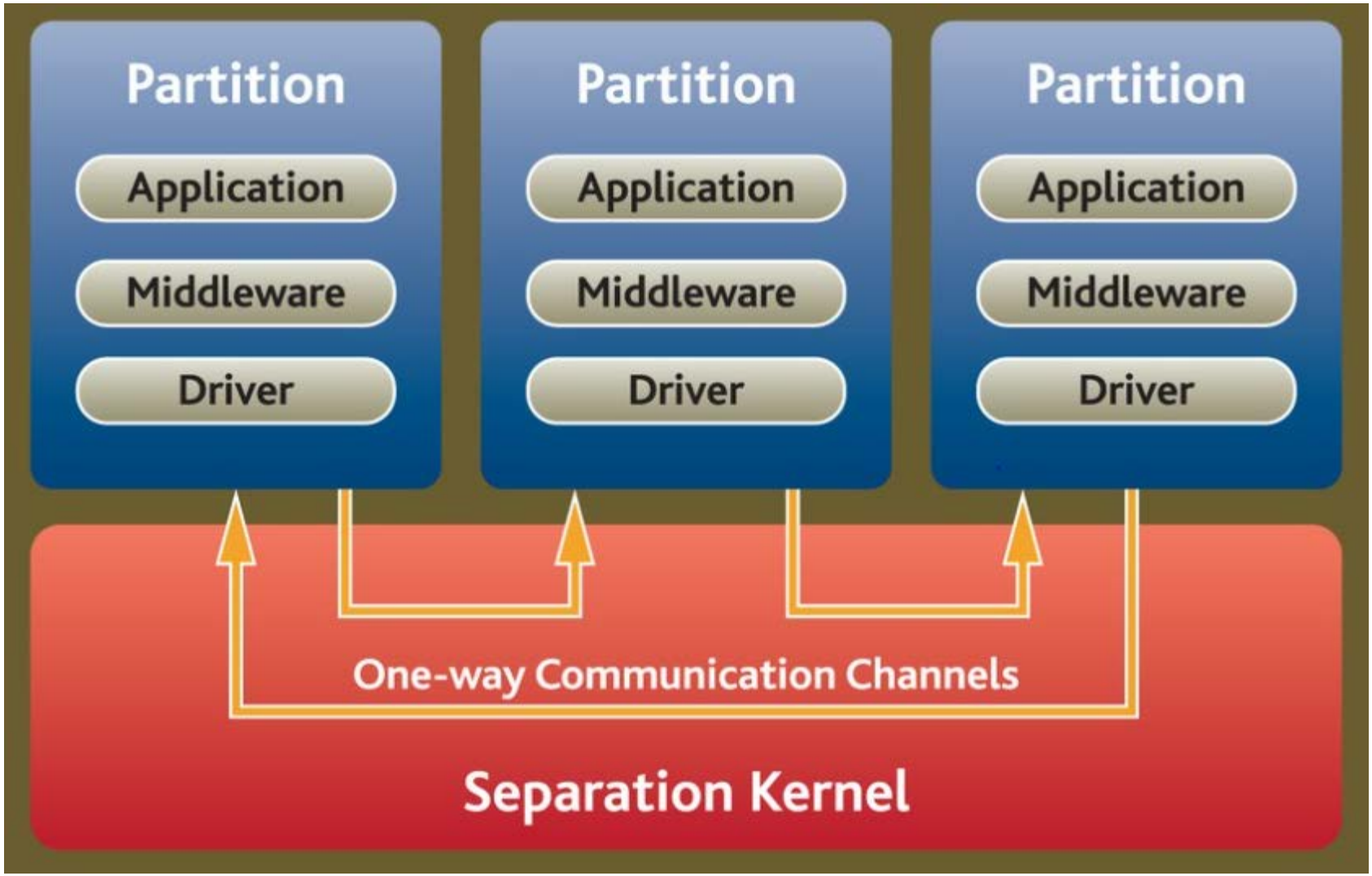
MIP Information Model



The **Joint Command, Control and Consultation Information Exchange Data Model (**JC3IEDM) is first and foremost an information exchange data model

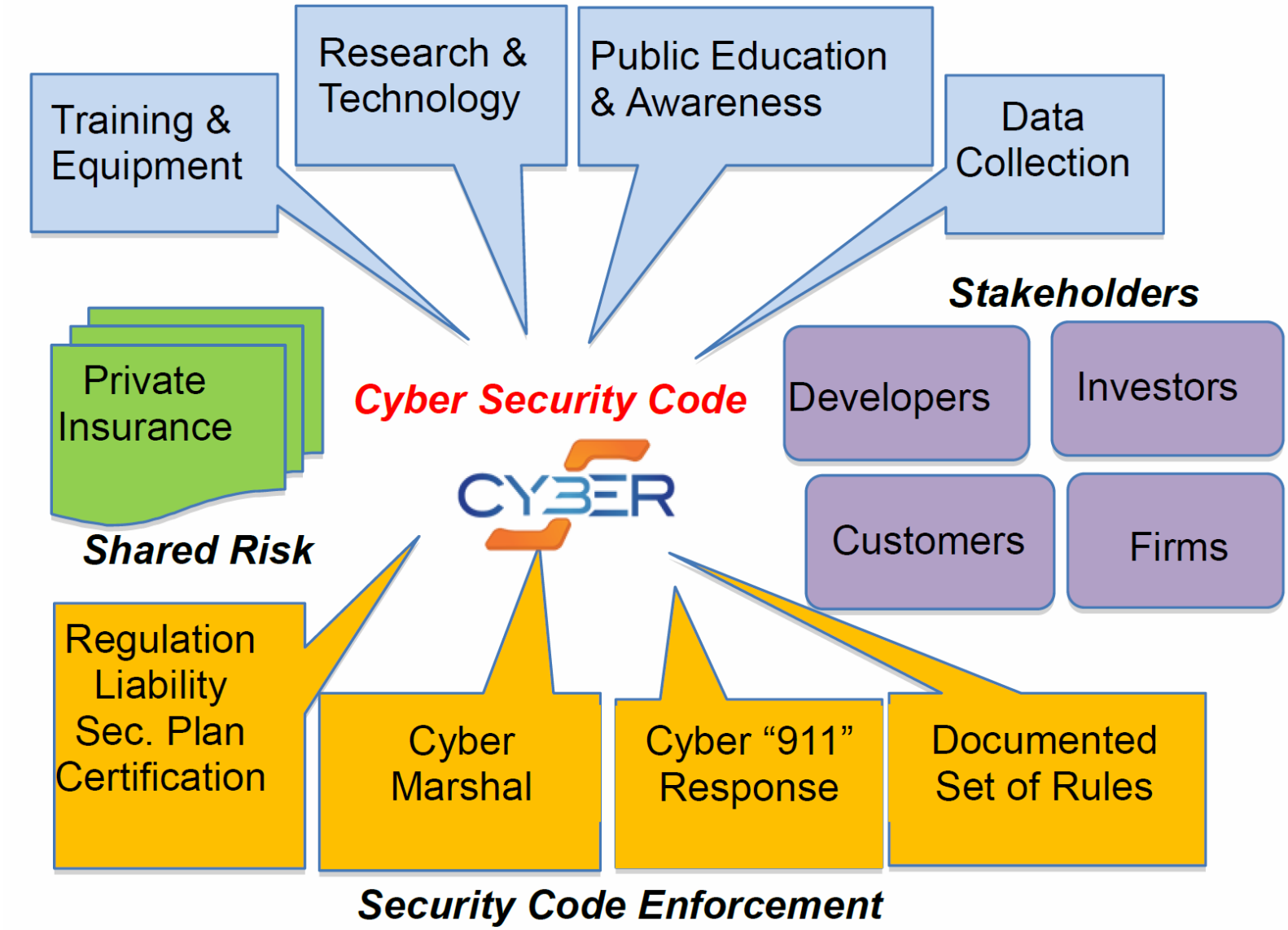
@MIP Public Home https://mipsite.lsec.dnd.ca/Pages/Default.aspx

MILS (Multiple Independent Levels of Security) High-Assurance Architecture



http://mil-embedded.com/articles/open-mls-systems-integration/

Risk Management



*https://www.ncoic.org/images/technology/whitepapers/NCOIC_Cybersecurity_Landscape_WhitePaper_v1.0.pdf

An Enterprise Approach to Security - Commercial

- An enterprise security architecture for the **whole** of the network
- Protects against **external and internal** attackers
- Define the **what** and **when** for all the security capabilities of the network and defend accordingly
- Define supporting **policies and principals** to support active defence
- Focus on the **holistic, integrated solution** rather than the piecemeal/license driven model

Computer Network Defence

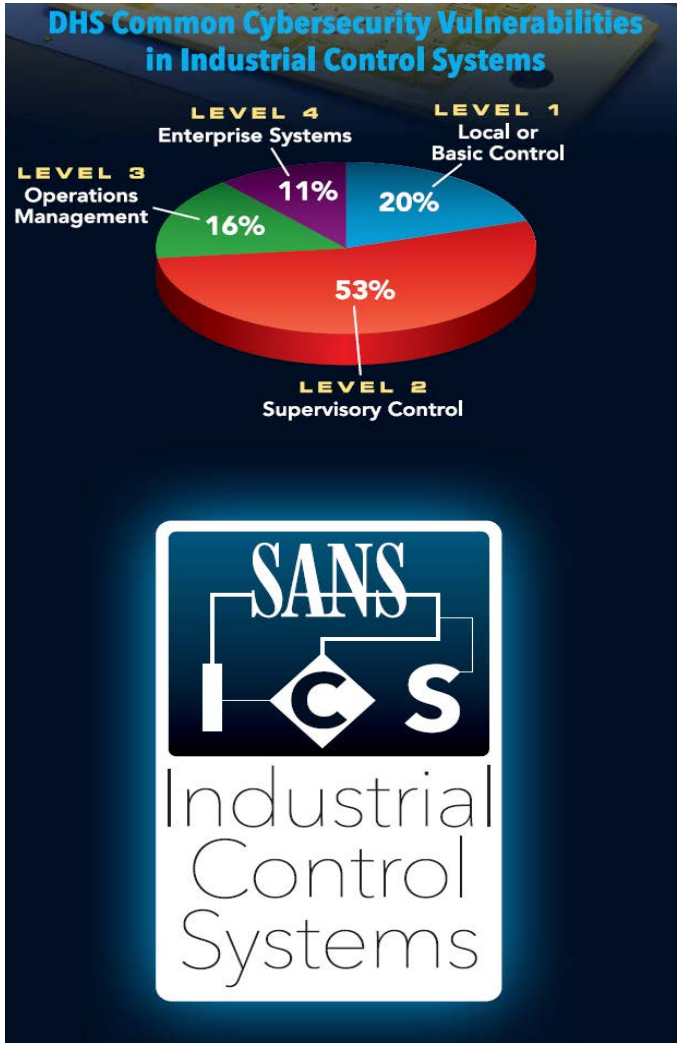
Outside attackers

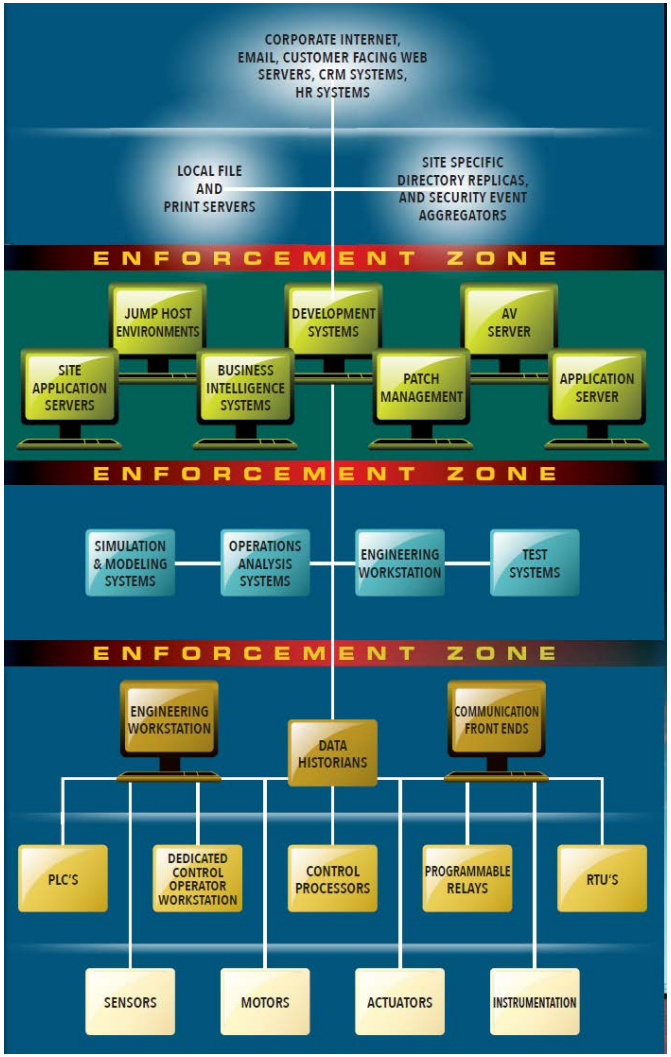
1. Defend the assets
2. Identify the attackers
3. React accordingly

Unauthorized release

Data Loss Prevention

Industrial Control Systems





https://www.sans.org/security-resources/posters/

CIS Critical Security Controls

CIS CRITICAL SECURITY CONTROL	NIST 800-53 rev4*	NIST Core Framework	DHS CDM Program	ISO 27002:2013	ISO 27002:2005	NSA MNP	Au Top 35	NSA Top 10	GCHQ 10 Steps	UK Cyber Essentials	UK ICO Protecting Data	PCI DSS 3.0	HIPAA	FFIEC Examiners Handbook	COBIT 5	NERC CIP v5	NERC CIP v4	NERC CIP v3	Cloud Security Alliance	FY15 FISMA Metrics	ITIL 2011 KPIs
1 Inventory of Authorized & Unauthorized Devices	CA-7 CM-8 IA-3 SA-4 SC-17 SI-4 PM-5	ID.AM-1 ID.AM-3 PR.DS-6	• IDAM: Hardware Asset Management	A.8.1.1 A.9.1.2 A.13.1.1	A.7.1.1 A.10.6.2 A.10.6.1 A.11.4.6	• Map Your Network • Baseline Management • Document Your Network • Personal Electronic Device Management • Network Access Control • Log Management					• Inappropriate Locations for Processing Data	2.4	• 164.310(b) Workstation Use - R • 164.310(c) Workstation Security - R	• Asset Security • User Equipment Security (Workstation, Laptop, Handheld)	• APO13: Manage Security • DSS05: Manage Security Services • BAI09: Manage Assets	CIP-002-5 R1 CIP-003-5 R2	CIP-002-4 R1 CIP-003-4 R2 CIP-005-4 R2 CIP-006-4 R2 CIP-007-4 R5	CIP-002-3 R1 CIP-003-3 R2 CIP-005-3 R2 CIP-006-3 R2 CIP-007-3 R6	CSC-01 MOS-09 MOS-15	1: System Inventory 2: Continuous Monitoring	Information Security Management
2 Inventory of Authorized & Unauthorized Software	CA-7 CM-8 SA-4 SI-4 CM-2 CM-10 SC-18 PM-5 CM-11 SC-34	ID.AM-2 PR.DS-6	• IDAM: Hardware Asset Management • DAM: Software Asset Management	A.12.5.1 A.12.6.2		• Baseline Management • Executable Content Restrictions • Configuration and Change Management	1 14 17	• Application Whitelisting			• Decommissioning of Software or Services		• 164.310(b) Workstation Use - R • 164.310(c) Workstation Security - R	• Asset Security • User Equipment Security (Workstation, Laptop, Handheld)	• APO13: Manage Security • DSS05: Manage Security Services				CCC-04 MOS-3 MOS-04 MOS-15	1: System Inventory 2: Continuous Monitoring	Information Security Management
3 Secure Configurations for Hardware & Software	CA-7 CM-6 CM-11 SC-15 CM-2 CM-7 PM-6 SC-34 CM-3 CM-9 MA-5 SI-2 CM-5 CM-9 SA-4 SI-4	PR.IP-1	• CSM: Configuration Settings Management	A.14.2.4 A.14.2.8 A.18.2.3	A.15.2.2	• Patch Management • Baseline Management • Data-at-Rest Protection • Configuration and Change Management	2-5 21	• Control Administrative Privileges • Set a Secure Baseline Configuration • Take Advantage of Software Improvements	• Secure Configuration	• Secure Configuration • Patch Management		2.2 2.3 6.2 11.5	• 164.310(b) Workstation Use - R • 164.310(c) Workstation Security - R	• Asset Security • User Equipment Security (Workstation, Laptop, Handheld)	• APO13: Manage Security • DSS05: Manage Security Services • BAI10: Manage Configuration	CIP-007-5 R2 CIP-010-5 R2	CIP-003-4 R6 CIP-007-4 R2	CIP-003-3 R6 CIP-007-3 R2	VM-07 MOS-15 MOS-19 PM-02	2: Continuous Monitoring	Information Security Management
4 Continuous Vulnerability Assessment & Remediation	CA-2 RA-5 SI-4 CA-7 SC-34 SI-7	ID.RA-1 DE.CM-8 ID.RA-2 RS.MI-3 PR.IP-12	• VUL: Vulnerability Management	A.12.6.1 A.14.2.8	A.12.6.1 A.13.1.2 A.15.2.2	• Patch Management • Log Management • Configuration and Change Management	2 5	• Take Advantage of Software Improvements		• Patch Management	• Software Updates	6.1 6.2 11.2	• 164.310(b) Workstation Use - R • 164.310(c) Workstation Security - R	• Asset Security • User Equipment Security (Workstation, Laptop, Handheld)	• APO13: Manage Security • DSS05: Manage Security Services	CIP-007-5 R2 CIP-010-5 R3	CIP-005-4 R4 CIP-007-4 R3 CIP-007-4 R8	CIP-005-3 R4 CIP-007-3 R3 CIP-007-3 R8	VM-05 MOS-15 MOS-19 PM-02	2: Continuous Monitoring	Information Security Management
5 Controlled Use of Administrative Privileges	AC-2 AC-19 IA-5 AC-6 CA-7 IA-4 AC-17 IA-4	PR.AC-4 PR.MA-2 PR.AC-2 PR.PT-3		A.9.1.1 A.9.2.2 - A.9.2.6 A.9.3.1 A.9.4.1 - A.9.4.4	A.10.4.4 A.11.5.1 - A.11.5.3	• User Access • Baseline Management • Log Management	4 9 11 35	• Control Administrative Privileges	• Monitoring	• Access Control	• Configuration of SSL and TLS • Default Credentials	2.1 7.1 - 7.3 8.1 - 8.3 8.7	• 164.310(b) Workstation Use - R • 164.310(c) Workstation Security - R	• Authentication and Access Controls	• APO13: Manage Security • DSS05: Manage Security Services	CIP-004-5 R4 CIP-006-5 R1 CIP-007-5 R5	CIP-005-4 R5 CIP-004-4 R4 CIP-005-4 R2 CIP-007-4 R5	CIP-005-3 R5 CIP-006-3 R4 CIP-005-3 R2 CIP-007-3 R5	IAM-09 - IAM-15 MOS-16 MOS-20	3: Identity Credential & Access Management	Information Security Management
6 Maintenance, Monitoring, & Analysis of Audit Logs	AC-23 AU-6 AU-11 IA-10 AU-2 AU-7 AU-12 SI-4 AU-3 AU-8 AU-13 AU-9 AU-4 AU-14 AU-5 AU-10 CA-7 DE.DP-1 DE.DP-4 DE.DP-2 DE.DP-3 DE.DP-5	PR.PS-1 DE.AE-3 DE.DP-4 DE.DP-1 DE.DP-5 DE.DP-2	• Generic Audit Monitoring	A.12.4.1 - A.12.4.4 A.12.7.1	A.10.10.1 - A.10.10.3 A.10.10.6	• Log Management	15-16 15		• Monitoring			10.1 - 10.7	• 164.308(a)(1) Security Management Process - Information System Activity Review R • 164.308(a)(5) Security Awareness and Training - Log-in Monitoring A	• Security Monitoring	• APO13: Manage Security • DSS05: Manage Security Services	CIP-007-5 R4	CIP-005-4 R3 CIP-007-4 R6	CIP-005-3 R3 CIP-007-3 R6	MV-01 MV-03		Information Security Management
7 Email & Web Browser Protections	CA-7 CM-6 CM-11 SC-15 CM-2 CM-7 MA-4 SC-34 CM-3 CM-9 MA-5 SI-2 CM-5 CM-9 SA-4 SI-4	PR.IP-1	• CSM: Configuration Settings Management	A.14.2.4 A.14.2.8 A.18.2.3	A.15.2.2	• Patch Management • Baseline Management • Data-at-Rest Protection • Configuration and Change Management	2-5 21	• Control Administrative Privileges • Set a Secure Baseline Configuration • Take Advantage of Software Improvements	• Secure Configuration	• Secure Configuration • Patch Management		2.2 2.3 6.2 11.5	• 164.310(b) Workstation Use - R • 164.310(c) Workstation Security - R	• Asset Security • User Equipment Security (Workstation, Laptop, Handheld)	• APO13: Manage Security • DSS05: Manage Security Services • BAI10: Manage Configuration	CIP-007-5 R2 CIP-010-5 R2	CIP-003-4 R6 CIP-007-4 R2	CIP-003-3 R6 CIP-007-3 R2	VM-07 MOS-15 MOS-19 PM-02	2: Continuous Monitoring	Information Security Management
8 Malware Defenses	CA-7 SC-44 SI-4 SC-39 SI-3 SI-8	PR.PS-2 DE.CM-4 DE.CM-5		A.8.3.1 A.12.2.1 A.12.2.5	A.10.4.1 - A.10.4.2 A.10.7.1	• Device Accessibility • Virus Scanners & Host Intrusion Prevention Systems • Security Gateways, Proxies, & Firewalls • Network Security Monitoring • Log Management	7 26 17 30 22	• Use Anti-Virus File Reputation Services • Enable Anti-Exploitation Features	• Removable Media Controls • Malware Protection	• Malware Protection		5.1 - 5.4	• 164.308(a)(5) Security Awareness and Training - Protection from Malicious Software A • 164.310(d)(1) Device and Media Controls - Accountability A • 164.310(b) Workstation Use - R • 164.310(c) Workstation Security - R	• Asset Security • User Equipment Security (Workstation, Laptop, Handheld)	• APO13: Manage Security • DSS05: Manage Security Services	CIP-007-5 R3	CIP-007-4 R4	CIP-007-3 R4	MOS-01 MOS-15 TPM-01 TPM-02	4: Anti-Phishing & Malware Defense	Information Security Management
9 Limitation & Control of Network Ports	AC-1 AC-4 PM-13 AC-2 SA-19 PM-14 AC-3 SA-18 PM-16	PR.AC-5 DE.AE-1	• Boundary Protection	A.9.1.2 A.13.1.1 A.13.1.3 A.14.1.3	A.10.6.1 - A.10.6.2 A.11.4.4	• Baseline Management • Configuration and Change Management	2 - 13 3 - 22 12	• Limit Workstation-to-Workstation Communication	• Network Security		• Decommissioning of Software or Services • Unnecessary Services	1.4	• 164.310(b) Workstation Use - R • 164.310(c) Workstation Security - R	• Network Security	• APO13: Manage Security • DSS05: Manage Security Services	CIP-007-5 R1	CIP-007-4 R2	CIP-007-3 R2	DCI-02 MV-04 IPT-04		Information Security Management
10 Data Recovery Capability	CP-9 CP-10 MP-4	PR.IP-4		A.10.5.1 A.12.3.1	A.10.5.1 A.10.8.3	• Backup Strategy						6.3 9.5 - 9.7	• 164.308(a)(7) Contingency Plan - Data Backup Plan R • 164.308(a)(7) Contingency Plan - Disaster Recovery Plan R • 164.308(a)(7) Contingency Plan - Testing & Revision Procedure A • 164.310(d)(1) Device & Media Controls - Data Backup & Storage A	• Encryption	• APO13: Manage Security • DSS05: Manage Security Services		CP-009-4 R4 CP-009-4 R5	CP-009-3 R4 CP-009-3 R5	MOS-11		Information Security Management
11 Secure Configurations for Network Devices	AC-4 CA-9 CM-5 MA-4 CA-3 CM-2 CM-6 SC-24 CA-7 CM-3 CM-8 SI-4	PR.AC-5 PR.IP-1 PR.PT-4	• CSM: Configuration Settings Management • Boundary Protection	A.9.1.2 A.13.1.1 A.13.1.3	A.10.6.1 - A.10.6.2 A.11.4.5 A.11.4.7 A.11.5.1 - A.11.5.3	• Map Your Network • Patch Management • Baseline Management • Document Your Network • Security Gateways, Proxies, and Firewalls • Configuration and Change Management	2 5 16	• Set a Secure Baseline Configuration • Segregate Networks and Functions	• Secure Configuration • Network Security	• Boundary Firewalls & Internet Gateways • Secure Configuration • Patch Management	• Software Updates • Inappropriate Locations for Processing Data	1.1 - 1.2 2.2 6.2		• Network Security	• APO13: Manage Security • DSS05: Manage Security Services • BAI10: Manage Configuration	CIP-005-5 R1 CIP-007-5 R2	CIP-003-4 R6 CIP-004-4 R4 CIP-005-4 R2	CIP-006-4 R3 CIP-007-4 R3	CIP-003-3 R6 CIP-006-3 R3 CIP-006-3 R2	CIP-007-3 R3	DSI-02 IVS-09 IAM-03 MOS-19 IVS-06 TVM-02	3: Identity Credential & Access Management	Information Security Management
12 Boundary Defense	AC-4 CA-7 SC-7 AC-17 CA-9 SC-8 AC-20 CM-2 SI-4 CA-3 SA-9	PR.AC-5 PR.AC-6 PR.MA-2 DE.AE-1	• Boundary Protection	A.9.1.2 A.12.4.1 A.12.5.1 A.12.2.1	A.10.6.1 - A.10.6.2 A.11.5.1 - A.11.7.2 A.10.10.2 A.11.4.5 A.11.4.6 A.11.4.7	• Map Your Network • Network Architecture • Baseline Management • Document Your Network • Personal Electronic Device Management • Security Gateways, Proxies, and Firewalls • Remote Access Security • Network Security Monitoring • Log Management	10-11 18-20 23 32-34	• Segregate Networks and Functions	• Home and Mobile Working • Monitoring • Network Security	• Boundary Firewalls & Internet Gateways	• Configuration of SSL and TLS • Inappropriate Locations for Processing Data	1.1 - 1.3 8.3 10.8 11.4		• Network Security • Security Monitoring	• APO13: Manage Security • DSS05: Manage Security Services	CIP-005-5 R1 CIP-005-5 R2 CIP-007-5 R4	CIP-005-4 R3 CIP-007-4 R6	CIP-005-3 R3 CIP-007-3 R6	DSI-02 MV-01 MV-04 MV-09 MOS-18	3: Identity Credential & Access Management 4: Network Defense 7: Boundary Protection	Information Security Management
13 Data Protection	AC-3 CA-9 SC-8 SI-4 AC-4 IR-9 SC-28 AC-23 MP-5 SC-31 CA-7 SA-18 SC-41	PR.AC-5 PR.DS-2 PR.DS-5 PR.PT-2		A.8.3.1 A.10.1.1 - A.10.1.2 A.15.2.3 A.18.1.5	A.10.7.1 A.12.2.1 - A.12.2.2 A.12.5.4 A.15.1.6	• Network Architecture • Device Accessibility • Security Gateways, Proxies, and Firewalls • Network Security Monitoring	24		• Removable Media Controls			3.6 4.1 - 4.3	• 164.308(a)(4) Information Access Management - Isolating Health Care Clearinghouse Function R • 164.310(d)(1) Device and Media Controls - Accountability A • 164.312(a)(2) Access Control - Encryption and Decryption A • 164.312(e)(1) Transmission Security - Integrity Controls A • 164.312(e)(2) Transmission Security - Encryption A	• Encryption • Data Security	• APO13: Manage Security • DSS05: Manage Security Services	CIP-011-5 R1			DSI-02 DSI-05 IEM-01 - IEM-04 MOS-11	5: Data Protection	Information Security Management
14 Controlled Access Based on the Need to Know	AC-1 AC-6 RA-2 AC-2 AC-24 SC-16 AC-3 CA-7 SI-4 MP-3	PR.AC-4 PR.DS-2 PR.AC-5 PR.PT-2 PR.DS-1 PR.PT-3	• TRUST: Access Control Management • PRIV: Privileges	A.8.3.1 A.9.1.1 A.10.1.3	A.10.7.1 A.10.10.1 - A.10.10.3 A.11.4.5 A.11.4.7 A.11.6.1 - A.11.6.2 A.12.5.4	• Network Architecture • Device Accessibility • User Access • Data-at-Rest Protection • Log Management	24	• Segregate Networks and Functions	• Managing User Privileges • Network Security	• Access Control	• Inappropriate Locations for Processing Data	1.3 - 1.9 4.3 7.1 - 7.3 8.7	• 164.308(a)(3) Security Management Process - Information System Activity Review R • 164.308(a)(4) Information Access Management - Isolating Health Care Clearinghouse Function R • 164.308(a)(4) Information Access Management - Access Authorization A • 164.312(a)(1) Access Control - Encryption and Decryption A • 164.312(a)(1) Access Control - Unique User Identification R • 164.312(a)(1) Access Control - Automatic Logoff A • 164.312(d) Person or Entity Authentication - R • 164.312(e)(1) Transmission Security - Integrity Controls A • 164.312(e)(2) Transmission Security - Encryption A	• Authentication and Access Controls • Encryption • Data Security	• APO13: Manage Security • DSS05: Manage Security Services	CIP-005-5 R1 CIP-005-5 R2 CIP-007-5 R4 CIP-013-5 R1	CIP-003-4 R5 CIP-004-4 R4 CIP-005-4 R2 CIP-006-4 R2	CIP-003-3 R5 CIP-004-3 R4 CIP-005-3 R2 CIP-006-3 R2	DSI-02 IVS-09 MOS-11	3: Identity Credential & Access Management	Information Security Management
15 Wireless Access Control	AC-18 CM-7 SC-40 AC-19 IA-3 SI-4 CA-3 SC-8 CA-7 SC-17			A.10.1.3 A.12.4.1 A.12.2.1		• Map Your Network • Baseline Management • Document Your Network • Personal Electronic Device Management • Network Access Control			• Monitoring • Network Security			4.1 11.1		• Network Security • Encryption • Security Monitoring	• APO13: Manage Security • DSS05: Manage Security Services	CIP-007-5 R4	CIP-005-4 R3 CIP-007-4 R6	CIP-005-3 R3 CIP-007-3 R6	IVS-01 IVS-06 IVS-12 MOS-11		Information Security Management
16 Account Monitoring & Control	AC-2 CA-7 AC-3 IA-5 AC-7 IA-10 SI-4 AC-11 SC-17 AC-12 SC-23	PR.AC-1 PR.AC-4 PR.PS-3	• CRED: Credentials and Authentication Management	A.9.1.1 A.9.2.1 - A.9.2.6 A.9.3.1 A.9.4.1 - A.9.4.3 A.11.2.8	A.8.2.3 A.11.2.1 A.11.2.3 - A.11.2.4 A.11.2.5 - A.11.2.6 A.11.5.5 - A.11.5.6	• User Access • Baseline Management • Log Management	35		• Managing User Privileges	• Access Control	• Configuration of SSL and TLS	7.1 - 7.3 8.1 - 8.8	• 164.308(a)(3) Security Management Process - Information System Activity Review R • 164.308(a)(4) Information Access Management - Access Authorization A • 164.308(a)(4) Information Access Management - Access Establishment and Modification A • 164.308(a)(5) Security Awareness and Training - Password Management A • 164.312(a)(1) Access Control - Unique User Identification R • 164.312(a)(1) Access Control - Automatic Logoff A • 164.312(d) Person or Entity Authentication - R • 164.312(e)(1) Transmission Security - Integrity Controls A • 164.312(e)(2) Transmission Security - Encryption A	• Authentication and Access Controls	• APO13: Manage Security • DSS05: Manage Security Services	CIP-005-5 R1 CIP-005-5 R2 CIP-007-5 R4	CIP-005-4 R2 CIP-007-4 R5 CIP-007-4 R6	CIP-005-3 R2 CIP-007-3 R5 CIP-007-3 R6	IAM-02 IAM-09 - IAM-13 MOS-14 MOS-16 MOS-20	3: Identity Credential & Access Management	Information Security Management
17 Security Skills Assessment and Appropriate Training to Fill Gaps	AT-1 AT-4 PM-13 AT-2 SA-11 PM-14 AT-3 SA-16 PM-16	PR.AT-1 PR.AT-4 PR.AT-2 PR.AT-5 PR.AT-3	• BEHR: Security-Related Behavior Management	A.7.2.2	A.8.2.2	• Training	28		• User Education & Awareness			12.6	• 164.308(a)(5) Security Awareness and Training - Security Reminders A • 164.308(a)(5) Security Awareness and Training - Protection from Malicious Software A • 164.308(a)(5) Security Awareness and Training - Log-in Monitoring A • 164.308(a)(5) Security Awareness and Training - Password Management A	• Personnel Security	• APO13: Manage Security • DSS05: Manage Security Services	CIP-004-5 R1 CIP-004-5 R2	CIP-004-4 R1 CIP-004-4 R2	CIP-004-3 R1 CIP-004-3 R2	HRS-10 MOS-05	8: Training and Education	Information Security Management
18 Application Software Security	SA-13 SA-20 SI-11 SA-15 SA-21 SI-15 SA-16 SC-39 SI-16 SA-17 SA-18	PR.DS-7	• VUL: Vulnerability Management	A.9.4.5 A.12.3.1 A.14.2.1 A.14.2.6 - A.14.2.8	A.10.1.4 A.12.5.2 A.12.2.1 A.12.5.5 A.12.2.4	• Training	24				• SQL Injection	6.3 6.5 - 6.7		• Application Security • Software Development & Acquisition	• APO13: Manage Security • DSS05: Manage Security Services				MOS-01 CCC-02 MOS-03 CCC-03 MOS-04 MOS-08 CCC-01		Information Security Management
19 Incident Response & Management	IR-1 IR-4 IR-7 IR-2 IR-5 IR-8 IR-3 IR-6 IR-10	PR.IP-10 RS.RP-1 RS.AN-1 RS.AN-4 DE.AE-2 DE.AE-4 DE.DP-4 RS.CO-1 RS.AP-1 RS.CO-2 RS.MI-1 RS.CO-3	• Plan for Events • Respond to Events	A.6.1.3 A.7.2.1 A.16.1.2 A.16.1.4 - A.16.1.7	A.6.1.6 A.8.2.1 A.13.1.1 A.13.2.1 - A.13.2.2	• Incident Response and Disaster Recovery Plans			• Incident Management			12.10	• 164.308(a)(6) Security Incident Procedures - Response and Reporting R		• APO13: Manage Security • DSS05: Manage Security Services • DSS02: Manage Service Requests and Incidents	CIP-008-5 R1 CIP-008-5 R2 CIP-008-5 R3	CIP-008-4 R1 CIP-008-4 R2	CIP-008-3 R1 CIP-008-3 R2	SEI-01 - SEI-05	9: Incident Response	Information Security Management
20 Penetration Tests & Red Team Exercises	CA-2 CA-8 PM-14 CA-5 RA-6 PM-14 CA-6 SI-6			A.14.2.8 A.18.2.1 A.18.2.3	A.6.1.8 A.15.2.2 A.15.3.1	• Audit Strategy						11.3			• APO13: Manage Security • DSS05: Manage Security Services • MEA02: Monitor, Evaluate and Assess the System of Internal Control							Information Security Management

SANS PRESENTS CIS Critical Security Controls POSTER 4TH EDITION

https://www.sans.org/security-resources/posters/

Cyber Security Certification Programs

- Information System Security Certification Consortium, Inc.
  - (ISC)²®develops and maintains the Critical Body of Knowledge (CBK) which is a compendium of information security topics.
  - Facilitate accreditation for a number of industry recognized certification programs

CISSP® Certified Information Systems Security Professional — Certified Information Systems Security Professional (CISSP)

SSCP® Systems Security Certified Practitioner — Systems Security Certified Practitioner (SSCP)

CAP® Certified Authorization Professional — Certified Authorization Professional (CAP)

CSSLP® Certified Secure Software Lifecycle Professional — Certified Secure Software Lifecycle Professional (CSSLP)

CCFP® Certified Cyber Forensics Professional — Certified Cyber Forensic Professional (CCFP)

HCISPP® HealthCare Information Security and Privacy Practitioner — HealthCare Information Security Privacy Practitioner (HCISPP)

CCSP® Certified Cloud Security Professional — Certified Cloud Security Professional (CCSP)

CISSP® Certified Information Systems Security Professional ISSAP® Architecture — Information Systems Security Architecture Professional (CISSP-ISSAP)

CISSP® Certified Information Systems Security Professional ISSEP® Engineering — Information Systems Security Engineering Professional (CISSP-ISSEP)

CISSP® Certified Information Systems Security Professional ISSMP® Management — Information Systems Security Management Professional (CISSP-ISSMP)

Future trends

- Drive to the Cloud
  - Security-as-a-Service
  - Shared defence amongst partners
- Active and pro-active defence of the network
  - Identify vulnerabilities and countermeasures in advance
  - Aggressive response to attackers
  - Active defence of network and data
- Big, fast data drowning out the human
  - More automation, active and reactive
  - Artificial Intelligence and Expert Systems
    - Specialized services and tools to identify the interesting bits

Tactical Industrial IoT Security Summary

At a tactical level, every IOT project can follow these security measures:

♦ **Build security into IOT architecture with relevant components:** Doing so will provide around the box security till the time IOT protocols can be secure by design. This requires adhering to fundamentals including authentication, access control, and encryption.

♦ **Build monitoring controls at different levels:** This step covers IOT gateways, IOT management platform, IT infrastructure, and cloud monitoring to ensure that attacks are caught early.

♦ **Detailed security assessment and penetration testing:** These tests are imperative for secured IOT infrastructure before roll out and on a periodic basis.

Read more at:
http://economictimes.indiatimes.com/articleshow/51250695.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst

IoT Embedded Software and Systems Security Summary

- Procurement process to include ESS security reviews of components, open-source and sub-systems; align to MNEs
- Structure ESS development to include cyber security expertize
- Develop roadmaps using digital security frameworks with clear Measure of Effectiveness (MoE)

"We're not in Kansas anymore"

Back-up Slides

Secure IoT Devices - Mitigation

Unfortunately, it is difficult for a user to secure their IoT devices themselves, as most devices do not provide a secure mode of operation. Nonetheless, users should adhere to the following advice to ensure that they reduce the risk of these attacks:

- Use strong passwords for device accounts and Wi-Fi networks
- Change default passwords
- Use a stronger encryption method when setting up Wi-Fi networks such as WPA2
- Disable or protect remote access to IoT devices when not needed
- Use wired connections instead of wireless where possible
- Be careful when buying used IoT devices, as they could have been tampered with
- Research the vendor's device security measures
- Modify the privacy and security settings of the device to your needs
- Disable features that are not being used
- Install updates when they become available
- Use devices on separate home network when possible
- Ensure that an outage, for example due to jamming or a network failure, does not result in a unsecure state of the installation
- Verify if the smart features are really required or if a normal device would be sufficient

Manufacturers of smart home devices should ensure that they implement basic security standards at the very least:

- Use SSL/TLS-encrypted connections for communication
- Mutually check the SSL certificate and the certificate revocation list
- Allow and encourage the use of strong passwords
- Require the user to change default passwords
- Do not use hard-coded passwords
- Provide a simple and secure update process with a chain of trust
- Provide a standalone option that works without internet and cloud connections
- Prevent brute-force attacks at the login stage through account lockout measures
- Secure any web interface and API from bugs listed in the OWASP List of Top Ten Web vulnerabilities
- Implement a smart fail-safe mechanism when connection or power is lost or jammed
- Where possible, lock the devices down to prevent attacks from succeeding
- Remove unused tools and use whitelisting to only allow trusted applications to run
- Use secure boot chain to verify all software that is executed on the device
- Where applicable, security analytics features should be provided in the device management strategy

https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/insecurity-in-the-internet-of-things.pdf

Big Data Landscape 2016 (Version 3.0)

Infrastructure

- Hadoop On-Premise
- Hadoop in the Cloud
- Spark
- Cluster Services
- NoSQL Databases
- NewSQL Databases
- Graph Databases
- MPP Databases
- Cloud EDW
- Data Transformation
- Data Integration
- Management / Monitoring
- Security
- Storage
- App Dev
- Crowd-sourcing

Analytics

- Analyst Platforms
- Analytics Platforms
- Data Science Platforms
- Visualization
- BI Platforms
- Statistical Computing
- Log Analytics
- Social Analytics
- Real-Time
- Machine Learning
- Speech & NLP
- Horizontal AI
- Search
- Data Services
- For Business Analysts
- Web / Mobile / Commerce

Applications

- Sales & Marketing
- Customer Service
- Human Capital
- Legal
- Ad Optimization
- Security
- Vertical AI Applications
- Publisher Tools
- Govt / Regulation
- Finance
- Education/ Learning
- Life Sciences
- Industries

Cross-Infrastructure/Analytics

Open Source

- Framework
- Query / Data Flow
- Data Access
- Coordination
- Real-Time
- Stat Tools
- Machine Learning
- Search
- Security
- Visualization

Data Sources & APIs

- Health
- IOT
- Financial & Economic Data
- Air / Space / Sea
- Location / People / Entities
- Other

Incubators & Schools

Last Updated 3/23/2016

FIRSTMARK

CYBERSECURITY CAPABILITY MATURITY MODEL (C2M2)

Version 1.1
February 2014