Setting the Standard for Automation™

How are cyber security standards and technologies relevant to Drilling Control Systems?

Standards

Certification

Education & Training

Publishing

Conferences & Exhibits

Presenter

Kenneth.Frische@aesolns.com

Industrial Cyber Security Principal

CISSP, C|EH, PMP, MBA, SS DBA, Agile ScrumMaster

Kenneth Frische ("frish") has over 25 years experience in providing IT & OT Solutions to Oil & Gas, Pharma, Food & Beverage, Packaging, Chemical, Water/ Wastewater, and Correctional Facilities.

From hands-on coding to management and consulting, Kenneth Frische has worn many hats to include: IT Director, Solutions Architect, Enterprise Architect, Project Manager, Req/Tech Spec Writer, and Programmer Lead.

His domain expertise includes Process Control Systems, HMI Systems Development, MES integration, Database Design, Business Intelligence, Business Process Improvement, and Data Warehousing.

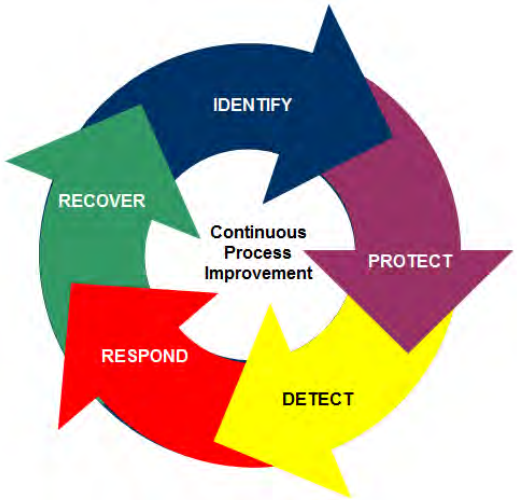
Kenneth Frische currently provides risk assessment services, cyber security consulting, and ISA IC32 Training as a member of the Cyber Security Services department at aeSolutions.

How are cyber security standards and technologies relevant to Drilling Control Systems?

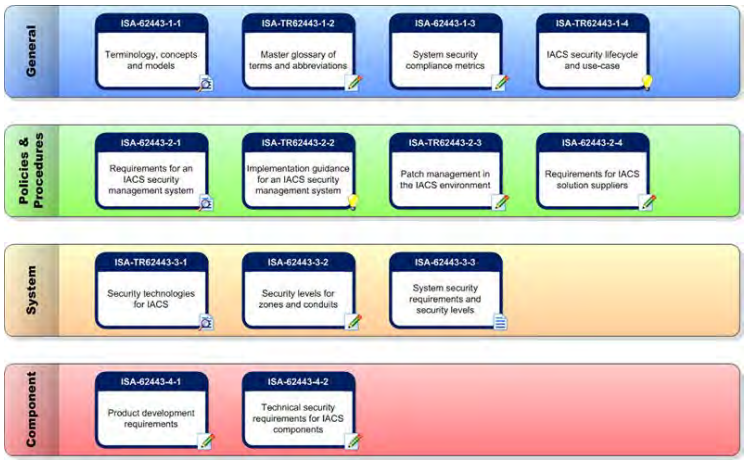
This presentation is focused on providing a high level understanding of the ISA cyber security standards and how they may be applied to the process control and safety systems relevant to drilling control systems.

Discussion will include the following:

- ISA Standards
- Increased Automation and Real-world Threats
- Risk Assessments
- Mitigation Techniques
- New Technologies and Interoperability



NIST to ISA



Agenda

- ISA Standards
- Increased Automation and Real-world Threats
- Risk Assessments
- Mitigation Techniques
- New Technologies and Interoperability

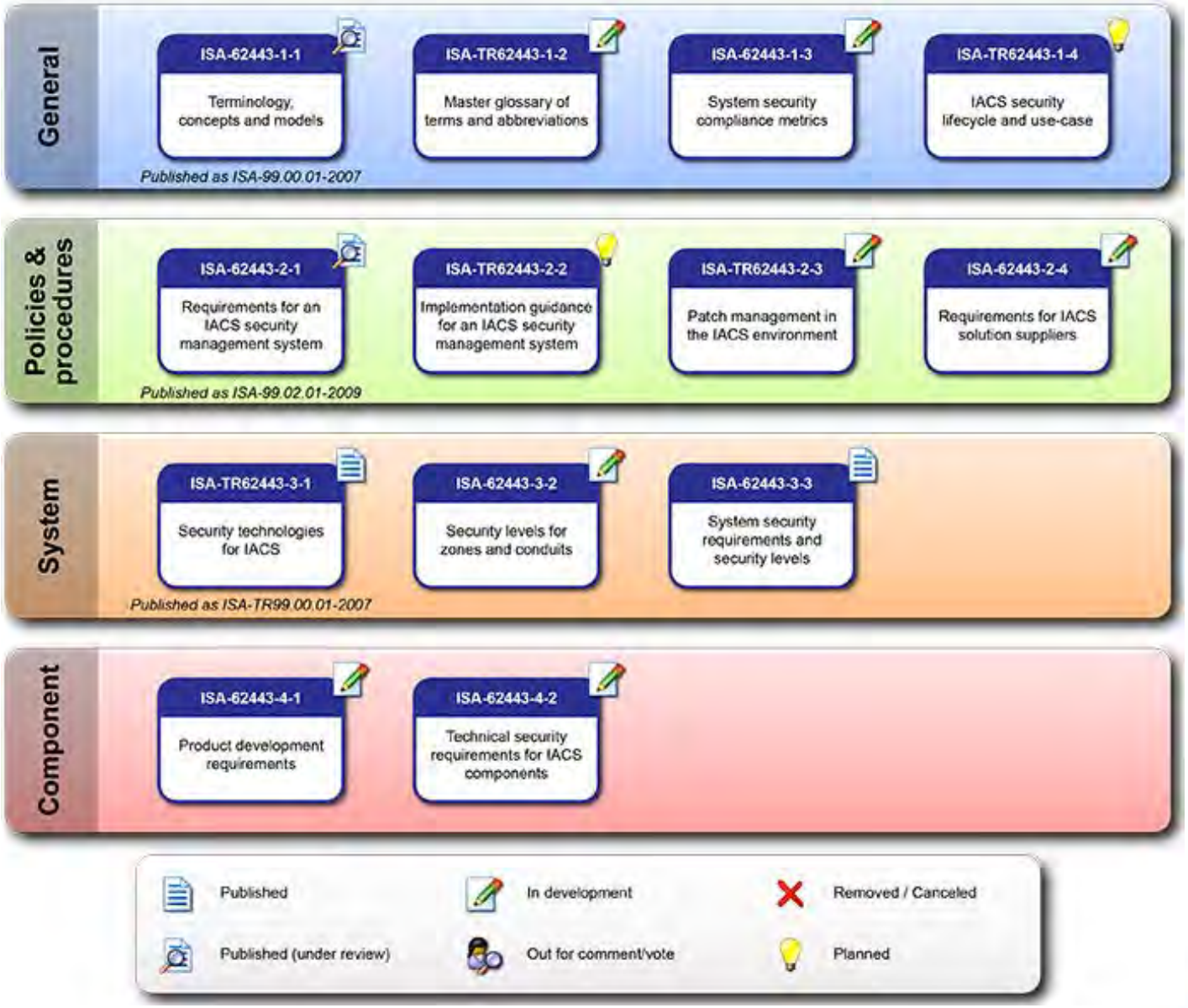
NIST Framework Core
Common Categories for Critical Infrastructure

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Source: Framework for Improving Critical Infrastructure Cybersecurity
Version 1.0 National Institute of Standards and Technology February 12, 2014

ISA Standards

Best Practice Guides for Compliance Measurement, Risk Measurement, and Risk Mitigation



NIST Framework Core - Sample

PROTECT (PR)	**Access Control (PR.AC):** Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are managed for authorized devices and users	· **CCS CSC** 16 · **COBIT 5** DSS05.04, DSS06.03 · **ISA 62443-2-1:2009** 4.3.3.5.1 · **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 · **ISO/IEC 27001:2013** A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3 · **NIST SP 800-53 Rev. 4** AC-2, IA Family
		PR.AC-2: Physical access to assets is managed and protected	· **COBIT 5** DSS01.04, DSS05.05 · **ISA 62443-2-1:2009** 4.3.3.3.2, 4.3.3.3.8 · **ISO/IEC 27001:2013** A.11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.3 · **NIST SP 800-53 Rev. 4** PE-2, PE-3, PE-4, PE-5, PE-6, PE-9
		PR.AC-3: Remote access is managed	· **COBIT 5** APO13.01, DSS01.04, DSS05.03 · **ISA 62443-2-1:2009** 4.3.3.6.6 · **ISA 62443-3-3:2013** SR 1.13, SR 2.6 · **ISO/IEC 27001:2013** A.6.2.2, A.13.1.1, A.13.2.1 · **NIST SP 800-53 Rev. 4** AC-17, AC-19, AC-20
		PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	· **CCS CSC** 12, 15 · **ISA 62443-2-1:2009** 4.3.3.7.3 · **ISA 62443-3-3:2013** SR 2.1 · **ISO/IEC 27001:2013** A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4 · **NIST SP 800-53 Rev. 4** AC-2, AC-3, AC-5, AC-6, AC-16
		PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate	· **ISA 62443-2-1:2009** 4.3.3.4 · **ISA 62443-3-3:2013** SR 3.1, SR 3.8 · **ISO/IEC 27001:2013** A.13.1.1, A.13.1.3, A.13.2.1 · **NIST SP 800-53 Rev. 4** AC-4, SC-7

Source: Framework for Improving Critical Infrastructure Cybersecurity
Version 1.0 National Institute of Standards and Technology February 12, 2014

Your operations are a target ….do you mind?

- July 2012: Hacker g
  successfully hacked
  companies operating in
  company email add
  …acted in support of env
  Greenpeace and tha
  and gas drilling on t
  …. The companies affect
  Global, ExxonMobil

- Aug 2012: Aramco S
  infected; 20,000 PC

- Aug 2014: Ongoing
  worldwide

HOUSTON CHRONICLE
ENERGY

SPORTS BUSINESS OPINION ARTS & ENTERTAINMENT LIFESTYLE INSIDER

Week Medical Retail Technology Personal Finance Chronicle 100 Markets Bloomberg

Malware on oil rig computers raises security fears

By Zain Shauk

February 22, 2013 | Updated: February 23, 2013 8:29am

Malicious software unintentionally downloaded by offshore oil workers has incapacitated computer networks on some rigs and platforms, exposing gaps in security that could pose serious risks to people and the environment, cybersecurity professionals told the Houston Chronicle.

Svell: Tabenkova

Oil industry under attack by hackers

August 27, 2014

SHARE

UPDATED: State authorities are warning as many as 300 companies in the country's major oil and energy industries this week that they're the targets of the largest coordinated hacker attack ever registered in Norway. Attacks have …mpanies, including Statnett, and the authorities

…gest company, state-controlled Statoil, has confirmed that it's …panies that's been warned they're under attack by coordinated hackers. PHOTO: Statoil/Øyvind Hagen

…heir logs," Hans Christian Pretorius, director of the …This is the largest warning we have ever carried out."

…s thousands of oil and gas industry executives from all …s oil capital of Stavanger for the huge Offshore …ar whether non-Norwegian oil and gas companies were …wned operator of Norway's energy system, confirmed

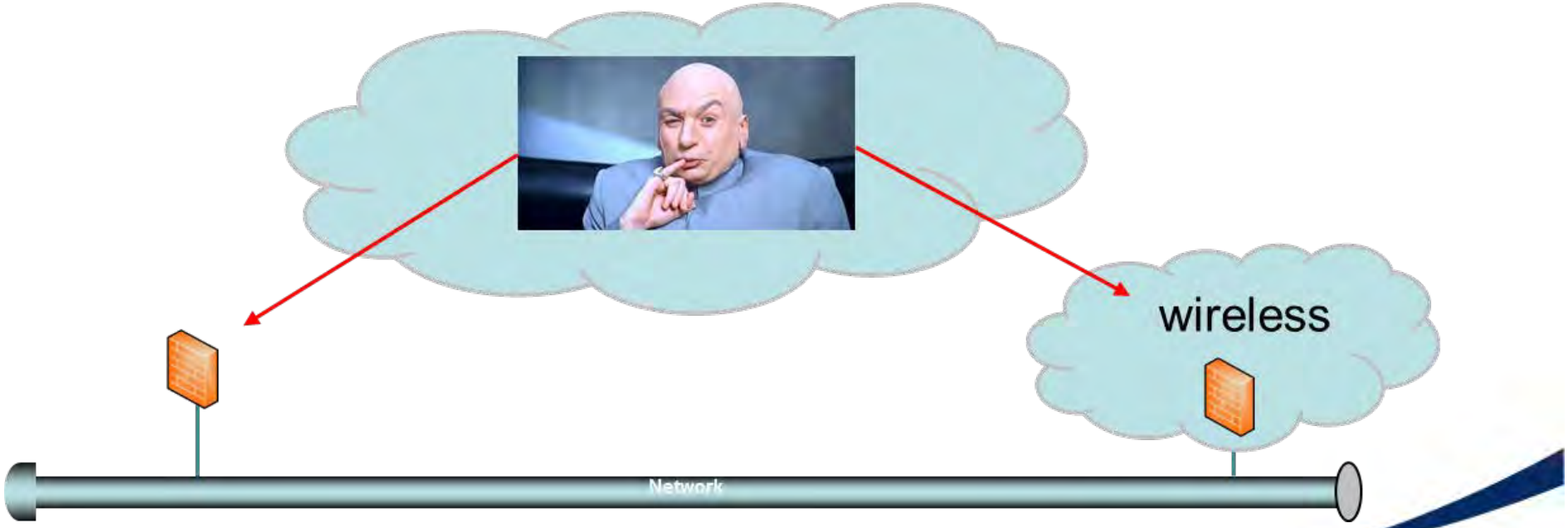
Typical Crack Sequence

1. Get access to one device: onsite or will be onsite

Top Successful Approaches to Infect your System(s)

1. User Pull: Trojan via file download
2. User Pull: Trojan via USB or use of other ports by personal devices
3. User Pull: Script insertion (cross site scripting) from visiting web site

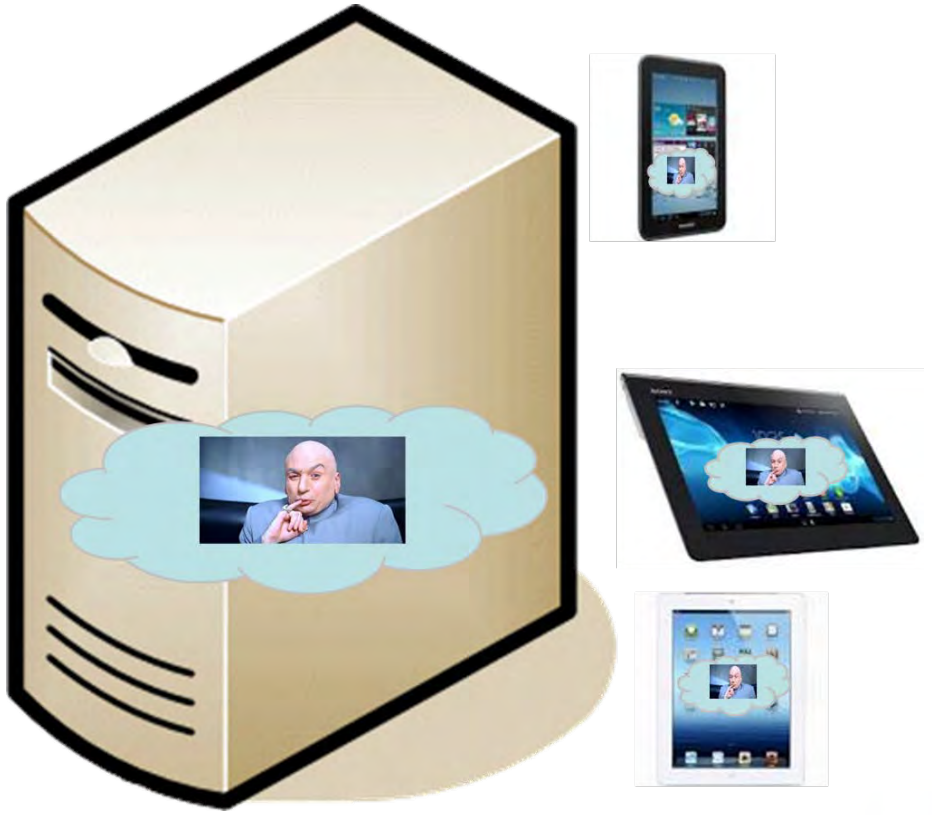
4. Hacker Push: Web Site Vulnerability (modify for script insertion on User Pull)
5. Hacker Push: Web Site/App Vulnerability (use SQL insertion to hack into system)
6. Hacker Push: Hack through Firewall (access internal devices/OS)



Typical Crack Sequence

2. Establish Beach head

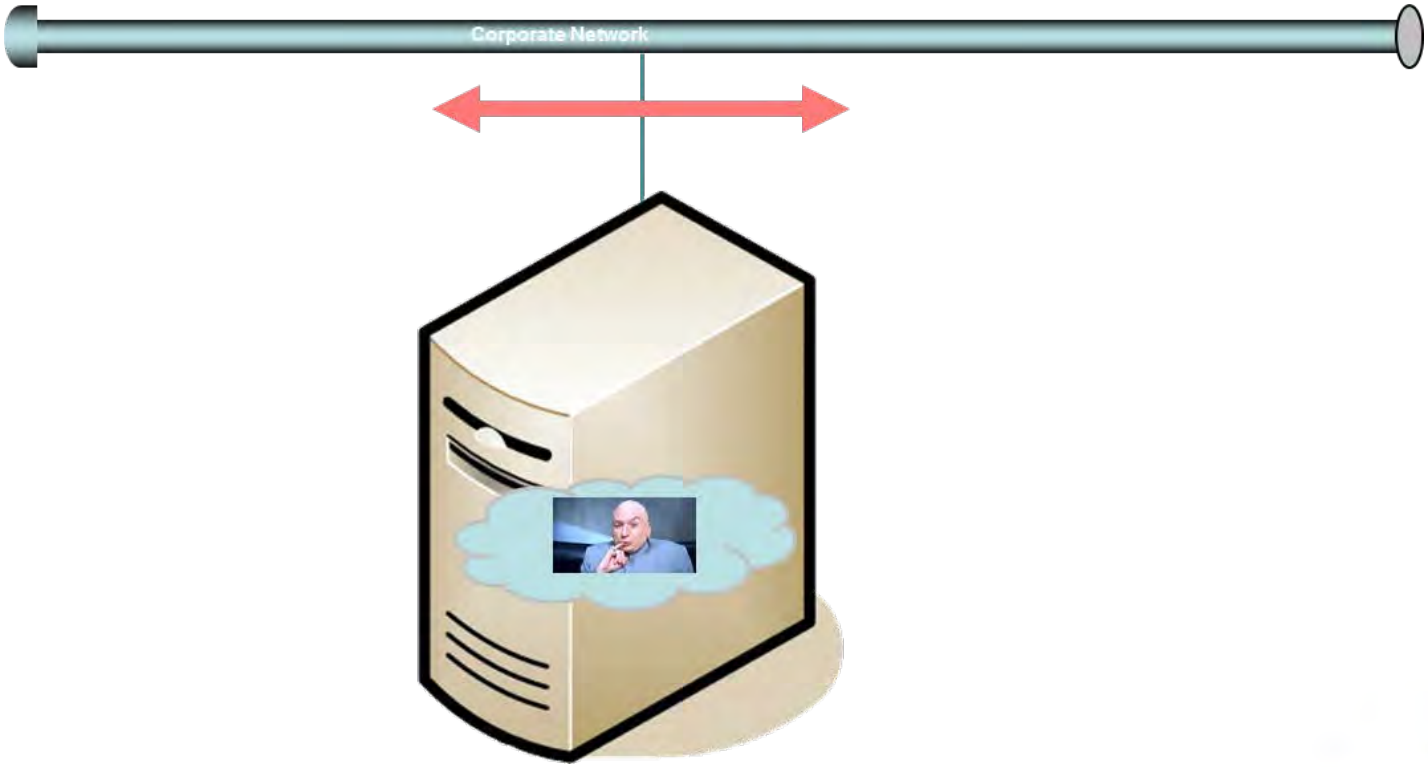
- Enumerate local SAM
- Determine Admin Level Users
- Crack Passwords (9 chars, upper, lower, special, no Dic or keywords)
- Elevate Privileges to Admin
- Handicap Defenses
- Embed Trojans and Hide
- Install tools



Typical Crack Sequence

3. Investigate Network

- Sniff network
- Develop Network Topology to determine targets

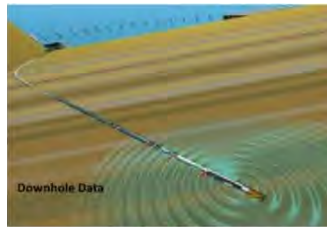


Typical Crack Sequence

4. Use and Abuse

Drilling Operations Focus

- Directly access PLCs/Devices:
  - WIT/WITSML, Profibus, Modbus, OPC, DDE, CIP, etc..
- Data Collection:
  - Proprietary Methods and Data



- Production:
  - Manipulating Pressure for Blowout / Reservoir Failure
- Drilling:
  - HMI Display and Controls Manipulation
  - Pump Failure
  - Control Speed/Trigger Manipulation

IT Focus

- Replicate and Establish Botnet: command and control of many devices for later use (attack or proxy)
- Harvest login/passwords: loggers with send
- Spoofing or MITM: hijack sessions for immediate access to secured systems
- Access and steal sensitive data
- Use as Stepping Stone

Risk Assessments

Cyber PHA Example

PHA-Pro 8 - [Cyber PHA Example *]

File Edit View Insert Format Tools Data Window Help

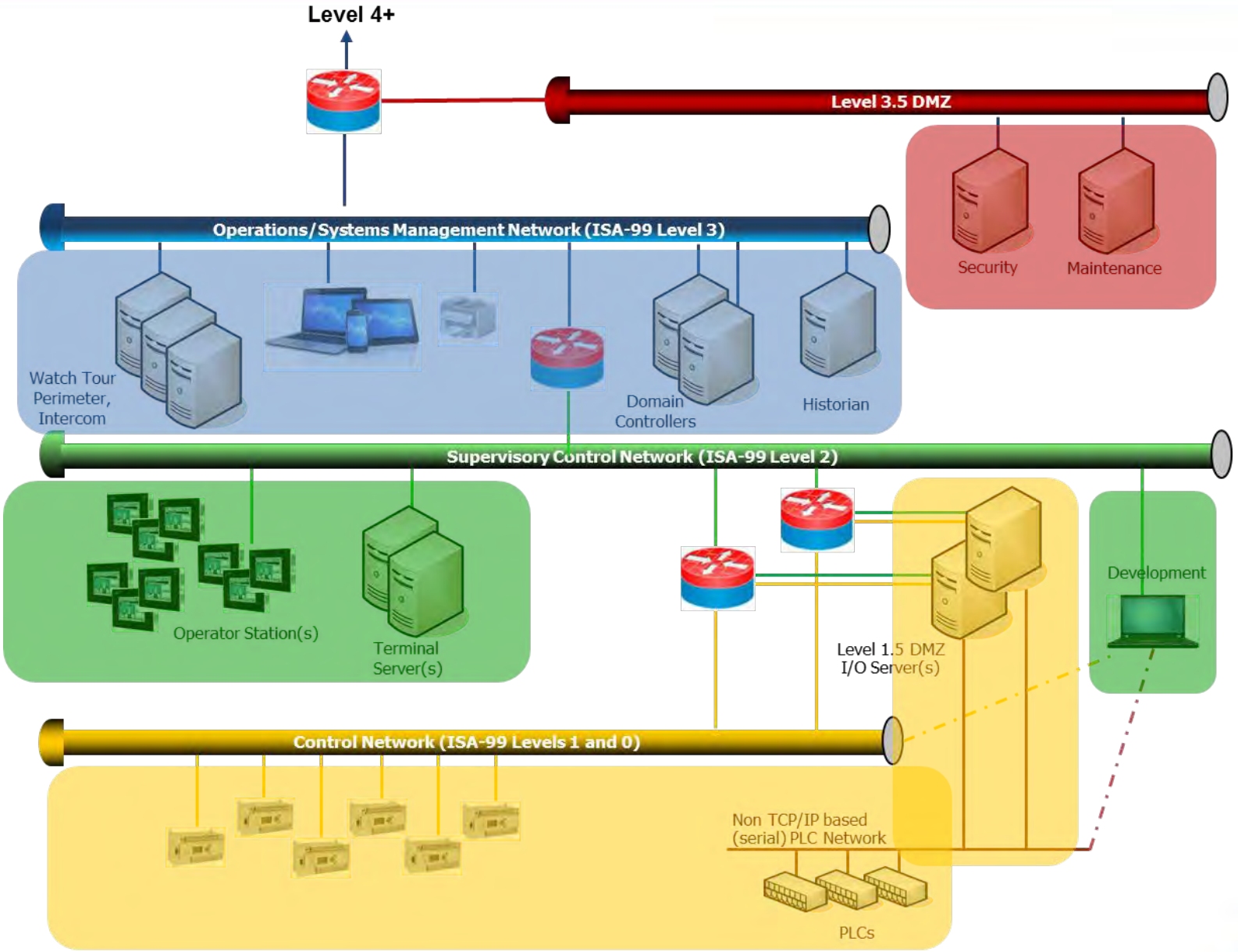
Administration | Sites | Nodes | Deviations | Worksheet | Recommendations (HAZOP) | Parking Lot | Countermeasures | Reports | Analysis | Settings | Data Check

Site: 1. Acme Chemical Company
Unit: 1. Truck Loading
Zone: 3. Control Room
Node: 2. Operator Consoles

Deviation	Causes		Vulnerability	Consequences	Risk Matrix								Countermeasures	Recommendations (HAZOP)
	Threat Agent	Threat Action			H&S	Env	Fin	Ops	Max Severity	UEL	MEL	RR		
Malware	1. Non-malicious insider	Inserts infected USB stick into computer	1. Anti-virus not updated	1. Potential process upset leading to plant shutdown	G	G	F	E	E	2	3	2	2. Physical security to access control room	3. Consider application whitelisting 4. Implemenent patch management server in DMZ 5. Implement anti-virus server in DMZ
			2. Zero-day	1. Potential process upset leading to plant shutdown	G	G	F	E	E	3	4	3	3. Physical security to access control room	3. Consider application whitelisting
			3. USB ports are accessible	1. Potential process upset leading to plant shutdown	G	G	F	E	E	2	3	2	1. Physical security to access control room	1. Disable or block USB ports on all physically accessible computers 2. Develop and enforce policy and procedures for authorized use of USB media
	2. Malicious insider	Deliberately installs malware on OWS	1. Computers are permanently logged in with admin rights	1. Potential process upset and loss of containment	D	D	D	E	D	3	3	2	4. Background checks on operators	6. If possible, operate without admin rights
			2. Remote desktop is enabled	1. Potential process upset and loss of containment	D	D	D	E	D	3	3	2		7. Implement strict controls on RDP access to OWS computers 8. Block RDP at PCN firewall (e.g. must be on PCN to RDP to OWS)
	3. Other computer on LAN	Spreads malware	1. Anti-virus not updated	1. Potential process upset and loss of containment	D	D	D	E	D	1	2	1		4. Implemenent patch management server in DMZ 5. Implement anti-virus server in DMZ
			2. Computers are permanently logged in with admin rights	1. Potential process upset and loss of containment	D	D	D	E	D	1	2	1		6. If possible, operate without admin rights
			3. Host firewall not enabled	1. Potential process upset and loss of containment	D	D	D	E	D	1	2	1		9. Implement host firewall to block unnecessary ports
			4. Zero-day	1. Potential process upset and loss of containment	D	D	D	E	D	3	4	2		3. Consider application whitelisting
Tampering	1.		1.											
Denial of Service														

Mitigation Techniques

Zones and Conduit Definition and Enforcement

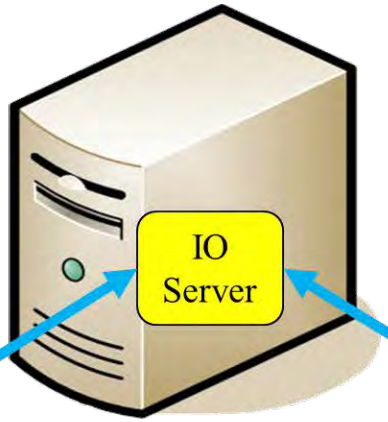


Old Tech and Interoperability

WIT/WITSML, OPC, Profibus, CIP, Modbus, DDE, etc…

Issues

- Protocols Not Secure
- IO Server Approach: Flat Tag Structure
- PLC Direct Approach: Reduced Interoperability



Motors – Dry Works (Cable, Spool,..)
Motors – Rotation
Pumps
Other: Blowers, Coolers, Brakes, …

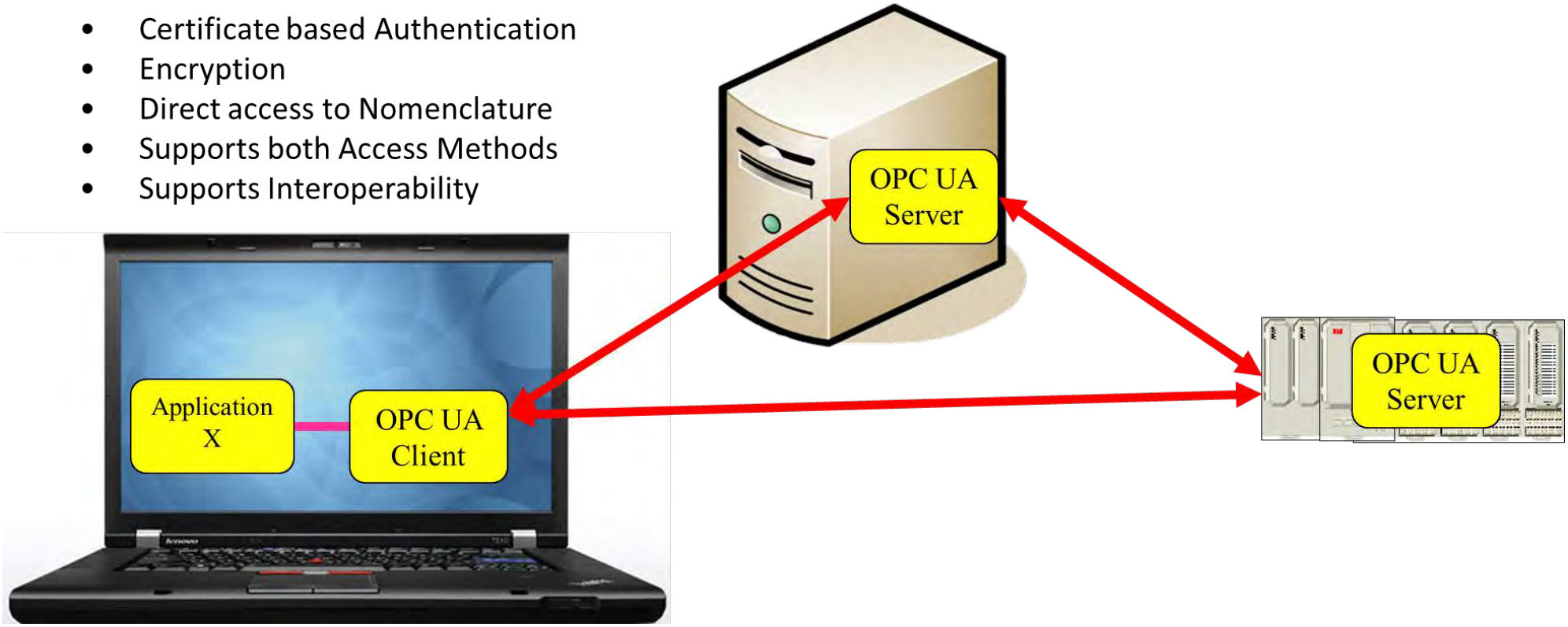
1. HMI Application to PLC through IO Server
2. HMI Application direct to PLC

New Tech and Interoperability

OPC UA – Authentication, Encryption, and Nomenclature

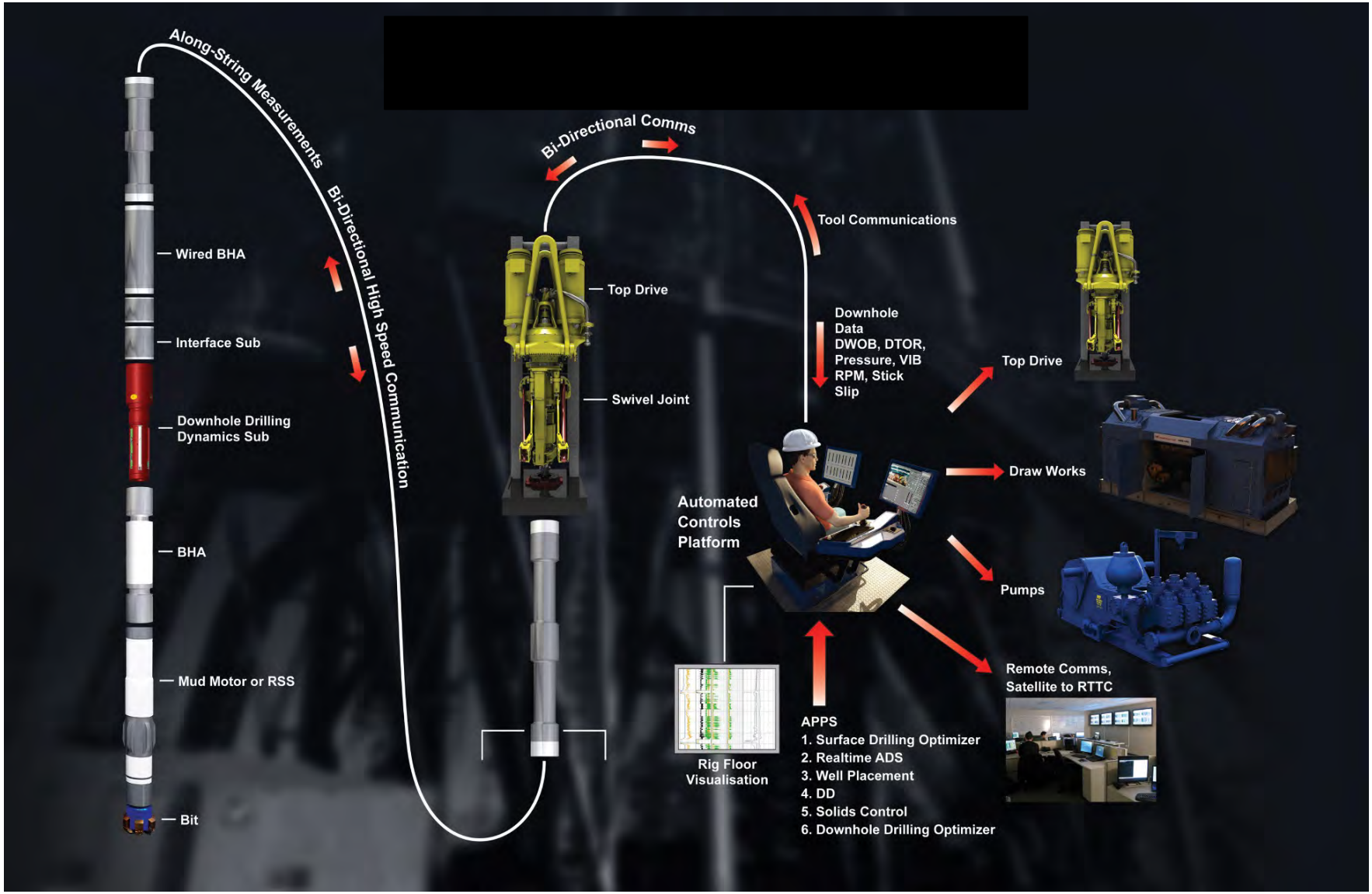
Benefits

- Certificate based Authentication
- Encryption
- Direct access to Nomenclature
- Supports both Access Methods
- Supports Interoperability



New Tech and Interoperability

SecureTwo-Way Comm



Thank you for your time

Kenneth.Frische@aesolns.com

Industrial Cyber Security Principal

CISSP, C|EH, PMP, MBA, SS DBA, Agile ScrumMaster

mobile: 423.413.3520