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

Kenneth.Frische@aesolns.com

Industrial Cyber Security Principal

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

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

--- Once size does not fit all ----
# NIST Framework Core
Common Categories for Critical Infrastructure

<table>
<thead>
<tr>
<th>Function</th>
<th>Category</th>
<th>Function</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify</td>
<td>ID.AM</td>
<td>ID.BE</td>
<td>Business Environment</td>
</tr>
<tr>
<td></td>
<td>ID.GV</td>
<td>ID.RA</td>
<td>Governance</td>
</tr>
<tr>
<td></td>
<td>ID.RM</td>
<td></td>
<td>Risk Assessment</td>
</tr>
<tr>
<td>Protect</td>
<td>PR.AC</td>
<td>PR.AT</td>
<td>Awareness and Training</td>
</tr>
<tr>
<td></td>
<td>PR.DS</td>
<td>PR.IP</td>
<td>Data Security</td>
</tr>
<tr>
<td></td>
<td>PR.MA</td>
<td>PR.PT</td>
<td>Information Protection Processes and Procedures</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Maintenance</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Protective Technology</td>
</tr>
<tr>
<td>Detect</td>
<td>DE.AE</td>
<td>DE.CM</td>
<td>Anomalies and Events</td>
</tr>
<tr>
<td></td>
<td>DE.DP</td>
<td></td>
<td>Security Continuous Monitoring</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Detection Processes</td>
</tr>
<tr>
<td>Respond</td>
<td>RS.RP</td>
<td>RS.CO</td>
<td>Response Planning</td>
</tr>
<tr>
<td></td>
<td>RS.AN</td>
<td>RS.IM</td>
<td>Communications</td>
</tr>
<tr>
<td></td>
<td>RS.MI</td>
<td></td>
<td>Analysis</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Mitigation</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Improvements</td>
</tr>
<tr>
<td>Recover</td>
<td>RC.RP</td>
<td>RC.IM</td>
<td>Recovery Planning</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RC.CO</td>
<td>Improvements</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Communications</td>
</tr>
</tbody>
</table>

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) | Source: Framework for Improving Critical Infrastructure Cybersecurity  
Version 1.0 National Institute of Standards and Technology February 12, 2014 |
|--------------|------------------------------------------------------------------|
| **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 433.5.1  
- 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  
- 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 433.3.2, 433.3.8  
- 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 433.6.6  
- ISA 62443-3-3:2013 SR.1.13, SR.2.6  
- 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 433.7.3  
- ISA 62443-3-3:2013 SR.2.1  
- 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 433.3.4  
- ISA 62443-3-3:2013 SR.3.1, SR.3.8  
- NIST SP 800-53 Rev. 4 AC-4, SC-7 |
Your operations are a target ....do you mind?

- July 2012: Hacker group Anonymous said it had successfully hacked into the servers of five oil and gas companies operating in the Arctic, posting hundreds of company email addresses online. They acted in support of environmental organization Greenpeace and the drive to cease oil and gas drilling on the Arctic shelf. The companies affected were Shell, BP, Global, ExxonMobil, and Gazprom.

- Aug 2012: Aramco Shamoon Work Hack: 30,000 infected; 20,000 PCs had data deleted.

- Aug 2014: Ongoing hack operations Oil & Gas worldwide.
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

<table>
<thead>
<tr>
<th>Deviation</th>
<th>Threat Agent</th>
<th>Threat Action</th>
<th>Vulnerability</th>
<th>Consequences</th>
<th>Risk Matrix</th>
<th>Countermeasures</th>
<th>Recommendations (HAZOP)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malware</td>
<td>Non-malicious insider</td>
<td>Inserts infected USB stick into computer</td>
<td>1. Anti-virus not updated</td>
<td>1. Potential process upset leading to plant shutdown</td>
<td>G G F E E</td>
<td>2 2</td>
<td>2. Physical security to access control room</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>4. Implement patch management server in DMZ</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>5. Implement anti-virus server in DMZ</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>6. Consider application whitelisting</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>7. Implement anti-virus server in DMZ</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>8. Implement host firewall to block unnecessary ports</td>
</tr>
<tr>
<td></td>
<td>Malicious insider</td>
<td>Deliberately installs malware on OWS</td>
<td>1. Computers are permanently logged in with admin rights</td>
<td>1. Potential process upset and loss of containment</td>
<td>D D D D D</td>
<td>3 3</td>
<td>2. Background checks on operators</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>7. Implement strict controls on RDP access to OWS computers</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>8. Block RDP at PCN firewall (e.g. must be on PCN to RDP to OWS)</td>
</tr>
<tr>
<td></td>
<td>Other computer on LAN</td>
<td>Spreads malware</td>
<td>1. Anti-virus not updated</td>
<td>1. Potential process upset and loss of containment</td>
<td>D D D D D</td>
<td>1 2</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>5. Implement anti-virus server in DMZ</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>6. If possible, operate without admin rights</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>7. Implement host firewall to block unnecessary ports</td>
</tr>
<tr>
<td>Tampering</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>3. Consider application whitelisting</td>
</tr>
<tr>
<td>Denial of Service</td>
<td>1.</td>
<td>1.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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

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

Motors – Dry Works (Cable, Spool,..)
Motors – Rotation
Pumps
Other: Blowers, Coolers, Brakes, …
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
Secure Two-Way Comm

- Wired BHA
- Interface Sub
- Downhole Drilling
  Dynamics Sub
- BHA
- Mud Motor or RSS
- Bit
- Along-String Measurements
  Bi-Directional High Speed Communication

- Top Drive
- Swivel Joint
- Automated Controls Platform
- Rig Floor Visualisation
- APPS
  1. Surface Drilling Optimizer
  2. Realtime ADS
  3. Well Placement
  4. DD
  5. Solids Control
  6. Downhole Drilling Optimizer

- Tool Communications
- Downhole Data
  DWOB, DTOR,
  Pressure, VIS
  RPM, Stick Slip

- Draw Works
- Pumps
- Remote Comms
  Satellite to RTTC
- Top Drive
Thank you for your time

Kenneth.Frische@aesolns.com
Industrial Cyber Security Principal
C|EH, PMP, MBA, SS DBA, Agile ScrumMaster

mobile: 423.413.3520