



## Who am I?

Name:	Chris Sandford
Job Title:	Director of Global Security Services
Background:	20 Years working in IT and Security, with over 10 years focusing on Industrial Security. Worked with Shell, Kraft Foods, European Space Agency.
Highlights:	<ul style="list-style-type: none"><li>• Designed a secure architecture framework for oil and gas company.</li><li>• Engineered the network and security infrastructure at numerous offshore, oil processing facilities, pipeline and production facilities.</li><li>• Rolled out a security framework for a utility and offshore drilling company.</li><li>• Created numerous risk assessment methodologies for companies as well as conducting risk assessments.</li><li>• Taught industrial cyber security courses.</li><li>• Presented at numerous conferences on industrial cyber security.</li></ul>

### The Consequence of a Cyber Security Incident

- Unexpected production outage investigating an incident or applying a reactive patching strategy
- Reputation loss due to public disclosure, delay in production improvements
- Retro-fitting security into existing production facilities after an incident has a significant higher cost
- Supply chain impact due to unplanned shutdown
- A recent case-study by Wurdtech found that it cost a US energy company the following:
  - \$1M in additional manpower and maintenance for resolving an incident
  - \$2M+ for post-incident updates, excluding unplanned production outages
  - Excludes production loss during the original incident and costs to delayed maintenance and improvement activities



wurdtech

### Risk Assessment

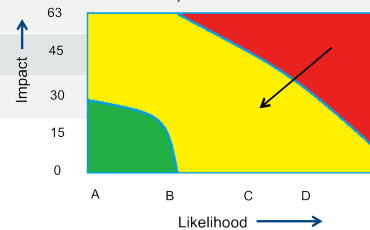
- Process for identifying and analyzing risks, and understanding what is the impact of a potential threat within a Process Control Infrastructure
- Impact can be: production interruption, reputation, loss of revenue, fines, safety, environment etc.
- Threat can be: accidental, insider malicious, outside malicious, organized crime, Hacktivism
- Standard are NIST SP 800-30, 800-39, NSTR 7628 Industry Standards and OCTAVE Allegro methodology



wurdtech

### Risk Assessment Methodology

Title	System hardening (host)
Description	Systems should have unnecessary services disabled and software removed
Business Impact	Attacks of various sources may compromise process control or availability. Impact varies based on affected systems
Risk Level	<b>D45</b>
Mitigating Controls	Harden systems, regular procedures for checking systems, network segregation, IDS enabled on plant firewall
Systems Affected	All Windows platforms
Recommendations	Remove unnecessary software and services, create and enforce hardening procedures
Cost of Mitigation	Minimal
Residual Risk	<b>C15</b>



wurldtech

### Benefits

- By understanding the risk, the business is able to make informed decisions to either accept or mitigate a risk
- Create a prioritized roadmap for monitoring and mitigating the risks which will improve the safety and reliability of your Process Control Infrastructure
- Support a business case for funding upgrading projects
- Conducting risk assessments across multiple sites will identify similar risks, such as lack of procedures; the mitigation plan can then be rolled out across the organization.
- Apply good practices that are performed at one site to others
- Ability to mature the security of the production facility in concrete steps, including having standard security requirements for vendors (IEC62443/WIB).

wurldtech

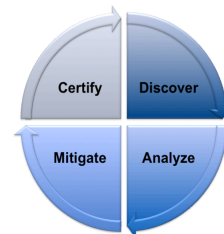
## Thank you

- Questions

wurldtech

## Company Overview

- Industrial Security Company, headquartered in Vancouver with offices in US and Europe
- Discover security gaps, analyze vulnerabilities and threats, mitigate with tailored solutions and certify products and devices
- Sectors are Energy, Oil & Gas, Medical and Process Automation
- Portfolio includes device testing and fuzzing solutions, security and risk assessments, vulnerability analysis, industrial threat protection and security training



wurldtech

*Protecting Critical Infrastructure from Cyber Attack*

© 2013 Wurldtech Security Technologies Inc. – Confidential Page 8

