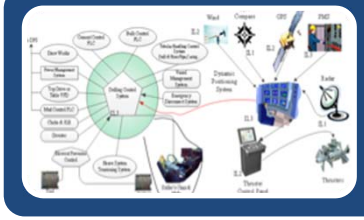
ABS Group

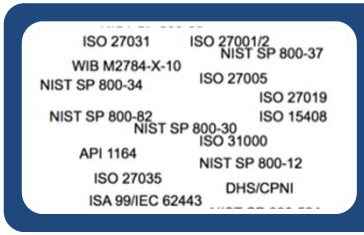
Cybersecurity Activities in the Oil and Gas Sector

Agenda

Software Integrity



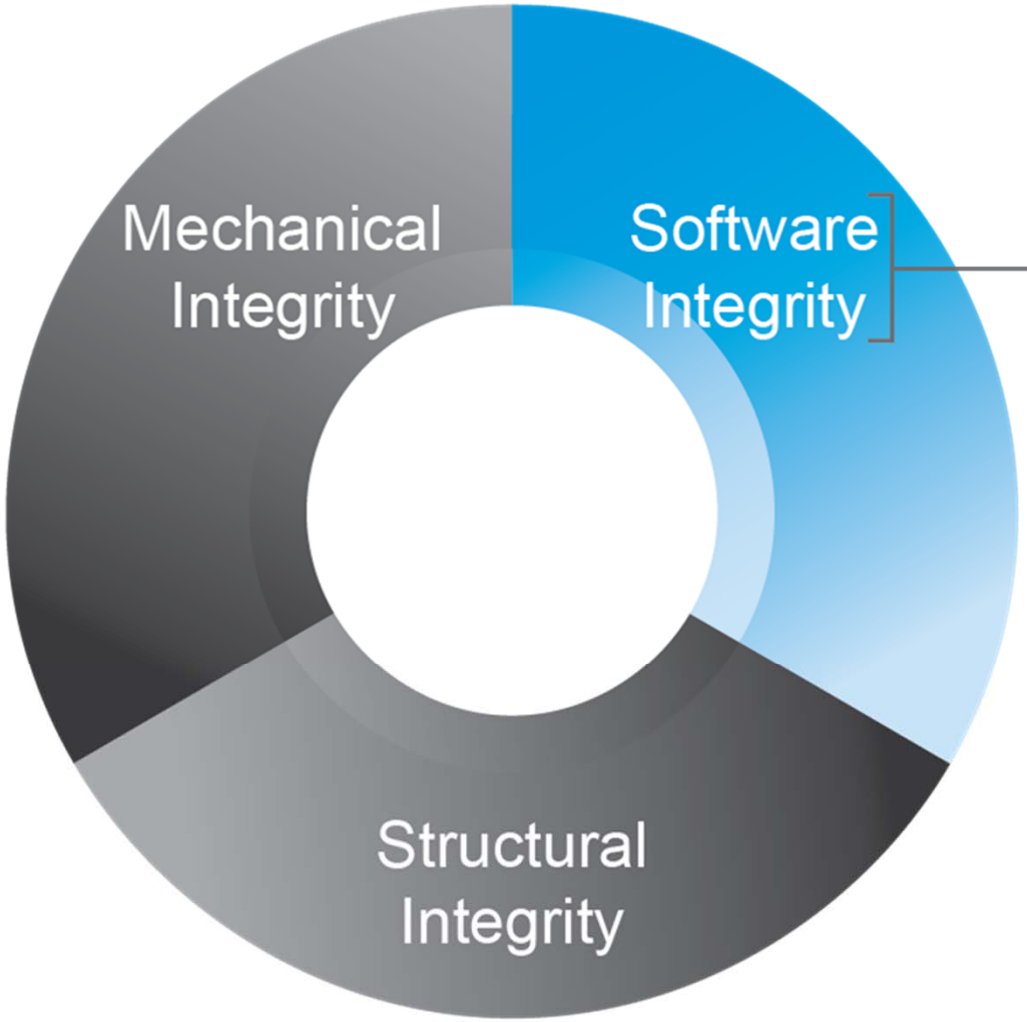
Complexity of Systems



Industry Standards and Committee Initiatives

Case Study - Risk Assessment of an Ultra-Deepwater Oil Drilling Rig

Software Integrity



Software Quality Engineering

Verification & Validation

Cybersecurity

The Future of Offshore Automation

Unmanned Cargo Ships Face Industry Resistance, Are a Good Idea Anyway

By Evan Ackerman
Posted 27 Feb 2014 | 16:27 GMT

Share | Email |

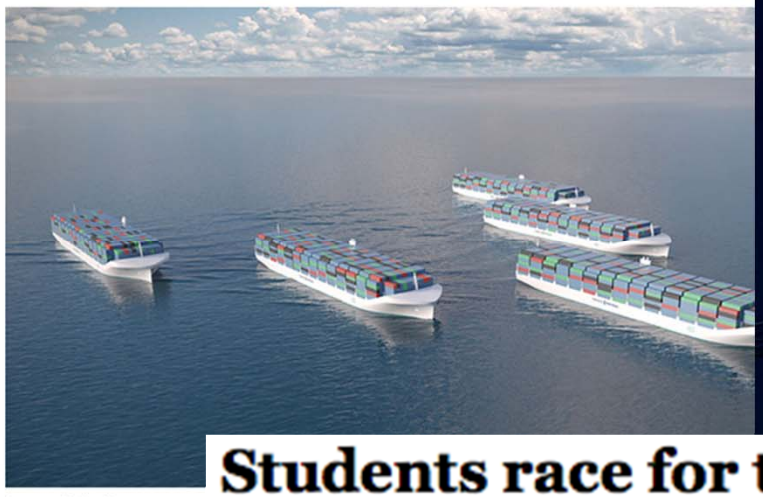


Image: Rolls-Royce

Source: Petrobras

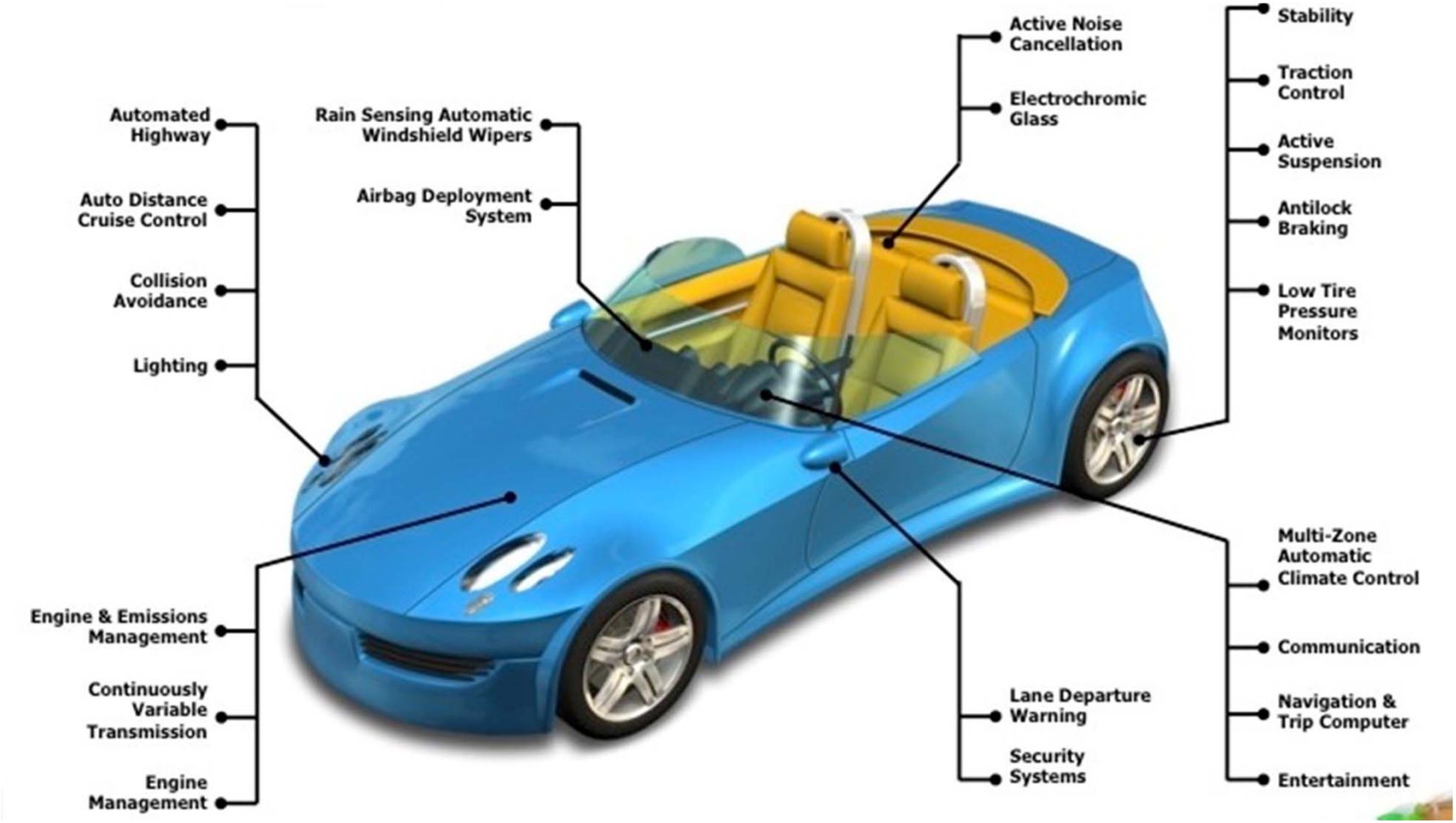
Students race for top prize in RoboBoat Competition

Published 30 July 2014

Share |

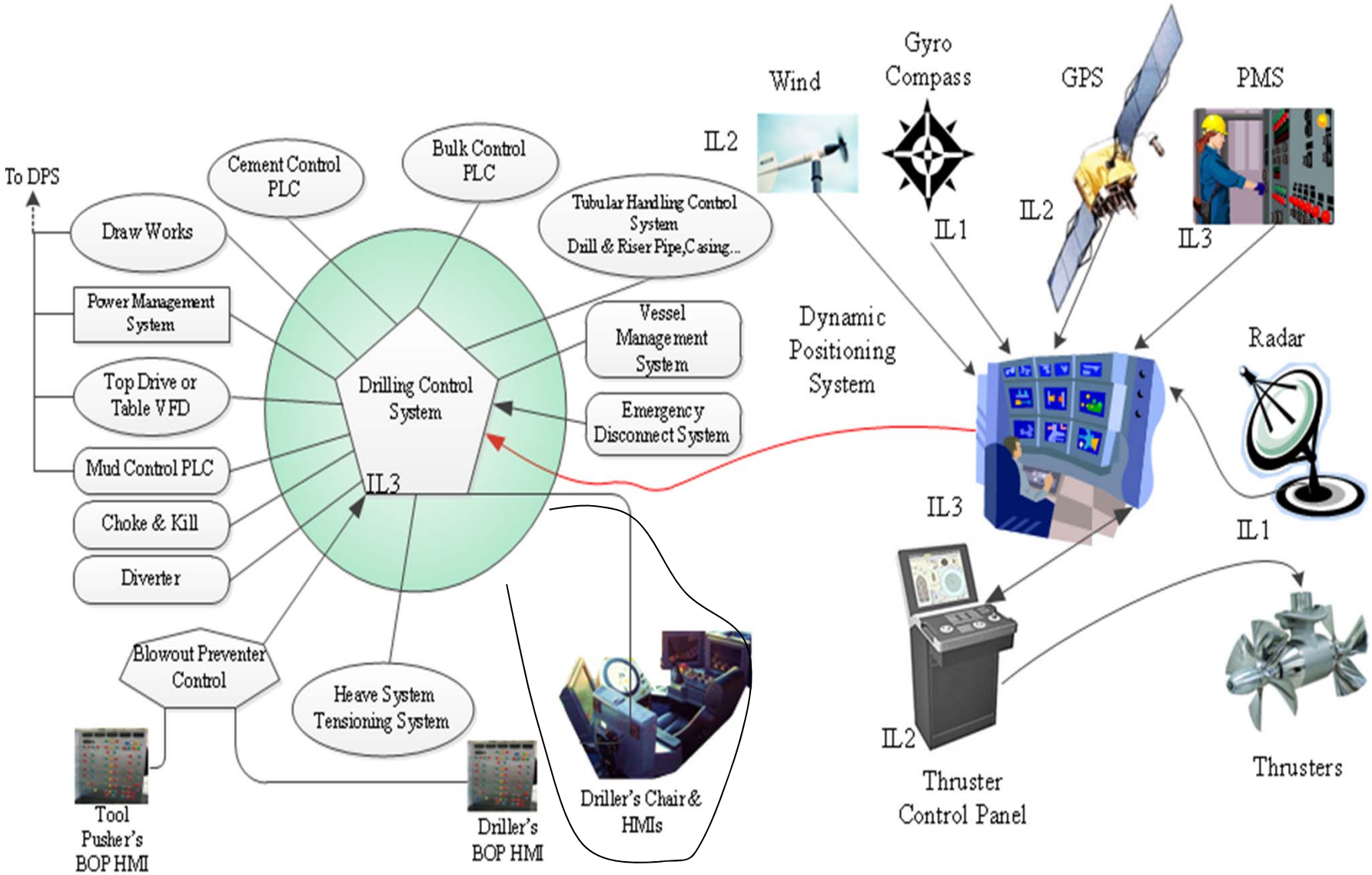
Obstacle avoidance. Automated docking. Speed gates. Acoustic beacon positioning. Underwater light identification. These are just some of the missions teams had to successfully complete to win at the 7th annual International RoboBoat Competition, held 8-13 July at the Founders Inn and Spa in Virginia Beach,

Typical New Car Automation



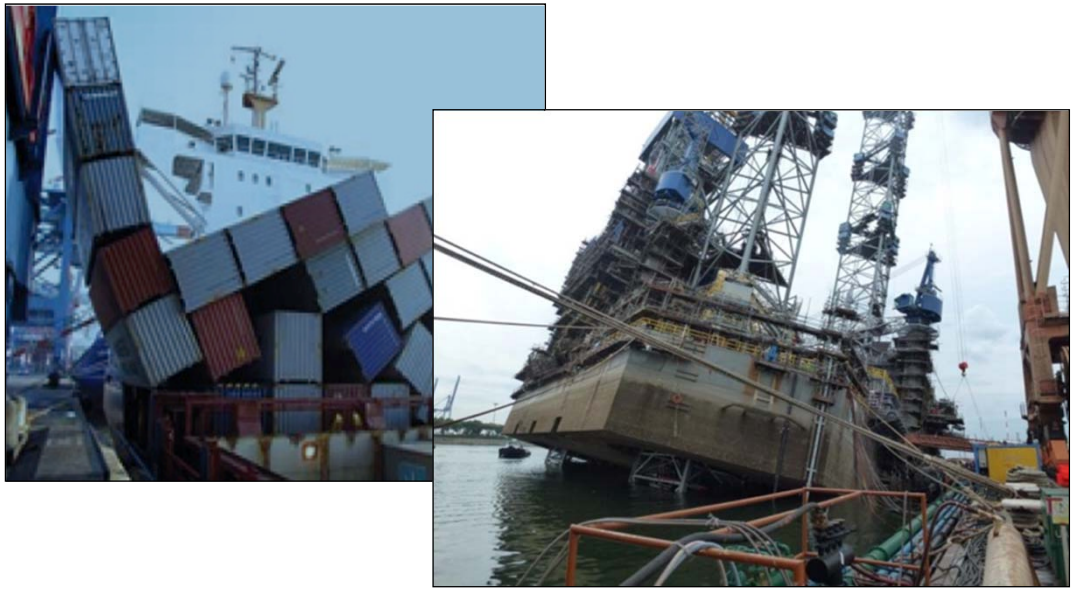
Source: John Blyler, http://www.chipestimate.com/blogs/IPInsider/?p=92

Complexity of Systems



Examples of software failures

"I need assurance that I won't have an event of high consequence caused by software." *(Operator)*



Warning to offshore industry on blocking of data communications in dynamic positioning systems

Health and Safety Executive - Safety Notice	
Department Name:	Offshore Safety Division
Bulletin No:	OSD 1-2013
Issue Date:	23 January 2013
Target Audience:	Suppliers of dynamic positioning (DP) systems, operators of offshore installations, marine classification societies, verification bodies and marine consultancies - Offshore oil and gas, Diving, Offshore, Others marine.
Key Issues:	Vessels may lose position during critical operations due to failure of their dynamic positioning system (DPS). The cause can be blocking of data communications in dynamic positioning (DP) systems dependent on data communications via a shared medium (e.g. data bus).

Earnings call, Q1 2014: *…we incurred a major downtime incident on the <rig name> due to a BOP control system problem. Resolution of this issue required more than 3 weeks of zero rate time and a loss of approximately $13 million in revenue and operating profit.*

Source: G-Captain.com, 2013; Mantelmann 2009, FastTimes 2013, Drilling Contractor Annual Report, 2014

Standards - Risk Management

- **ISO/IEC 31000-series**: Risk Management.
- **ISO/IEC 27005**: Information Security Risk Management.
- **NIST SP 800-39**: Managing Information Security Risk and its related standards (**SP 800-37** and **SP 800-30**).
- **ISACA** Risk IT Framework.

Source: 9th Annual API Cybersecurity Conference & Expo
November 11-12, 2014 - Houston, TX

Standards - Information Security & Assurance

- **Common Criteria/ISO 15408**: Information Technology – Security Techniques – Evaluation Criteria for IT Security.
- **ISO 27000-series**: IT-ST – Information Security Management Systems.
- **NIST SP 800-12**: An Introduction to Computer Security and security controls related standards (**SP 800-53** and **SP 800-53A**).

Source: 9th Annual API Cybersecurity Conference & Expo
November 11-12, 2014 - Houston, TX

Standards - Industrial Automated Control Systems

- **ISA 99 / IEC 62443**: Industrial Automation and Control Systems Security.
- **NIST SP 800-82**: Guide to Industrial Control Systems Security.
- **WIB M 2784-X-10**: Process Control Domain – Security Requirements for Vendors.
- **ISO 27019**: IT-ST – Information Security Management Guidelines based on ISO 27002 for process control systems specific to the energy utility industry.
- **DHS/CPNI** State Agency - Cyber Security Assessments of Industrial Control Systems.
- **API 1164**: Pipeline SCADA Security.

Source: 9th Annual API Cybersecurity Conference & Expo
November 11-12, 2014 - Houston, TX

Industry Standards and Committee Initiatives

NIST SP 800-12
NIST SP 800-30
NIST SP 800-34
NIST SP 800-37
NIST SP 800-39
NIST SP 800-53
NIST SP 800-53A
NIST SP 800-82

ISO 15408
ISO 27001,2
ISO 27005
ISO 27019
ISO 27031
ISO 27035
ISO 31000

ANSI/ASIS SPC.1

API 1164

IADC
International Association of Drilling Contractors

Advanced Rig Technology, Drilling Control Systems, Cybersecurity sub-team

ISA

ISA 99/IEC 62443

IEC

WIB
Process Automation Users' Association

WIB M2784-X-10

Oil Operator Requirements

bp

HESS

NIST Framework

NIST National Institute of Standards and Technology U.S. Department of Commerce

Case Study - MODU

Objectives:

- Start Contract
- Verify Network Compartmentalization
- Identify/eradicate unauthorized software (Anti-virus)
- Evaluate Software Management of Change
- Evaluate Remote Access

Tools:

- OEM Support Staff (where available)

  Wireshark

  Anti-Virus scanner

  Profiscan (not used)
- "Toolkits" based on specific standard of compliance (IEC 62443)
- Certified control system cybersecurity experts with asset knowledge

Work Effort:

- 2 days on shore
- 7days on Asset
- 2 Cybersecurity experts

Case Study - MODU

Call to action:

- Operator / Drilling Contractor Concerns:
  - Drilling program integrity
  - Interconnectedness "System of systems"
  - Windows XP Vulnerabilities
  - USB
  - Remote Access
  - Software Change Management
- "Wash list" of threats
  - Limited testing of sw updates
  - 0day exploits (for sale)
  - Unidentified exploits
  - Limited scope of Anti-Virus
- Out of scope
  - Disaster Recovery
  - Business Continuity

Case Study - MODU

Methodology

- Tabletop exercise to:
  - Understand asset's control network architecture
  - Review policies and procedures
    - Operational technology (OT) vs. information technology (IT)
    - Create toolkit, plan on-asset activities
- On-Asset Assessment (IEC62443, time boxed)
  - Cyber-physical
    - Cabling, physical equipment settings (dip switches…)
    - Enclosures (rooms, doors, cabinets, ports…)
  - Cyber
    - SMoC
    - Policy implementation
    - Passive network scanning
    - Remote access
    - Unauthorized software, Anti-virus scan (where applicable!)

Observations

- Everyone is “authorized”
  - During production, and in-between wells
- Cyber-physical vulnerabilities not addressed
  - Access to Barge Control BOP controls unsecured
- Robust procedures for remediation of unauthorized software did not exist for the OEM systems
  - 1 OEM introduced malware onto a USB from a business network computer
- Obsolete/irrelevant routing protocol on network
  - Novell routing protocol enabled on control system router
- Software Management of Change processes not followed
  - SMOC software was in the middle of implementation – stacks of paperwork “ready for entry”

The Pace of Automation