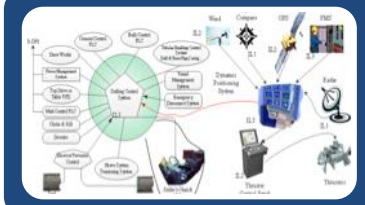
ABS Group

Technologies and IT Trends

Operational Cybersecurity on Offshore Assets

Agenda

Software Integrity



Complexity of Systems

Industry Standards and Committee Initiatives

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

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 |

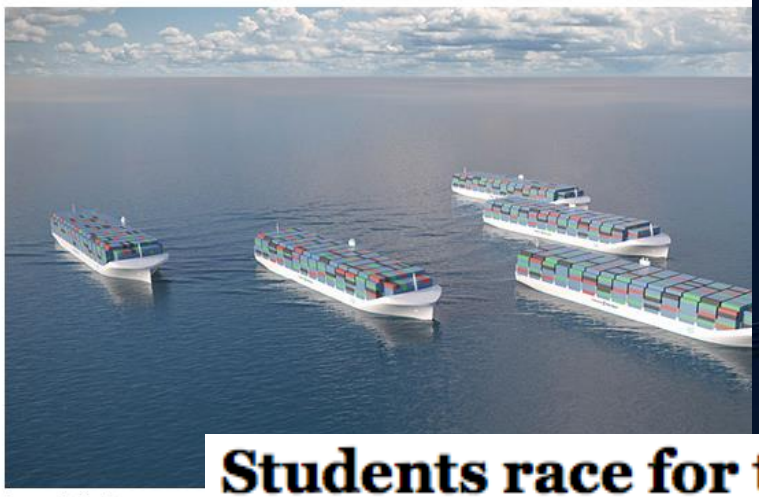
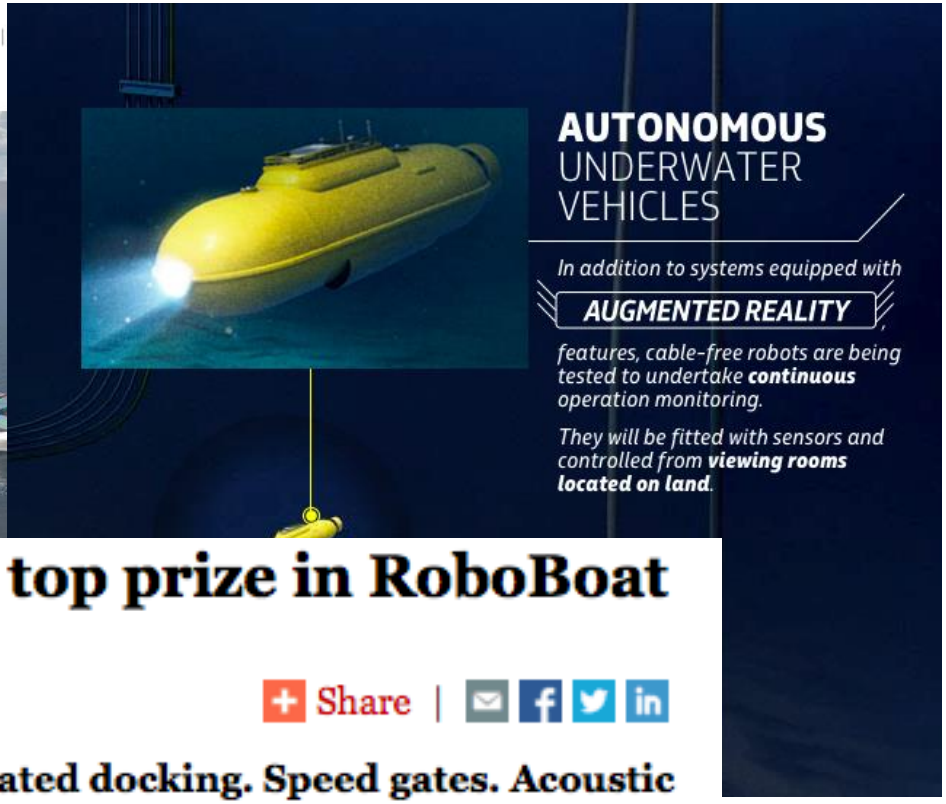


Image: Rolls-Royce

Source: Petrobras



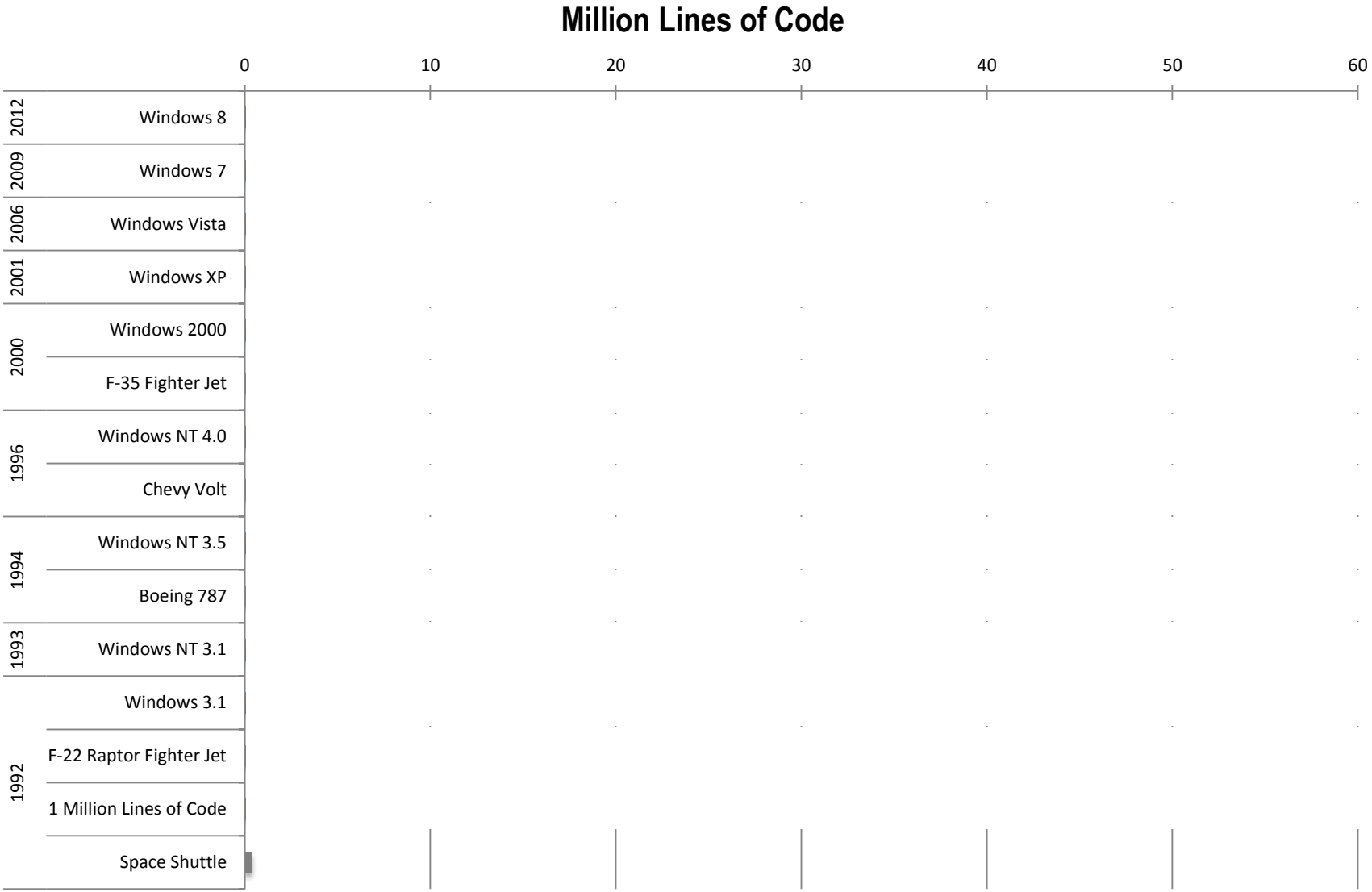
Students race for top prize in RoboBoat Competition

Published 30 July 2014

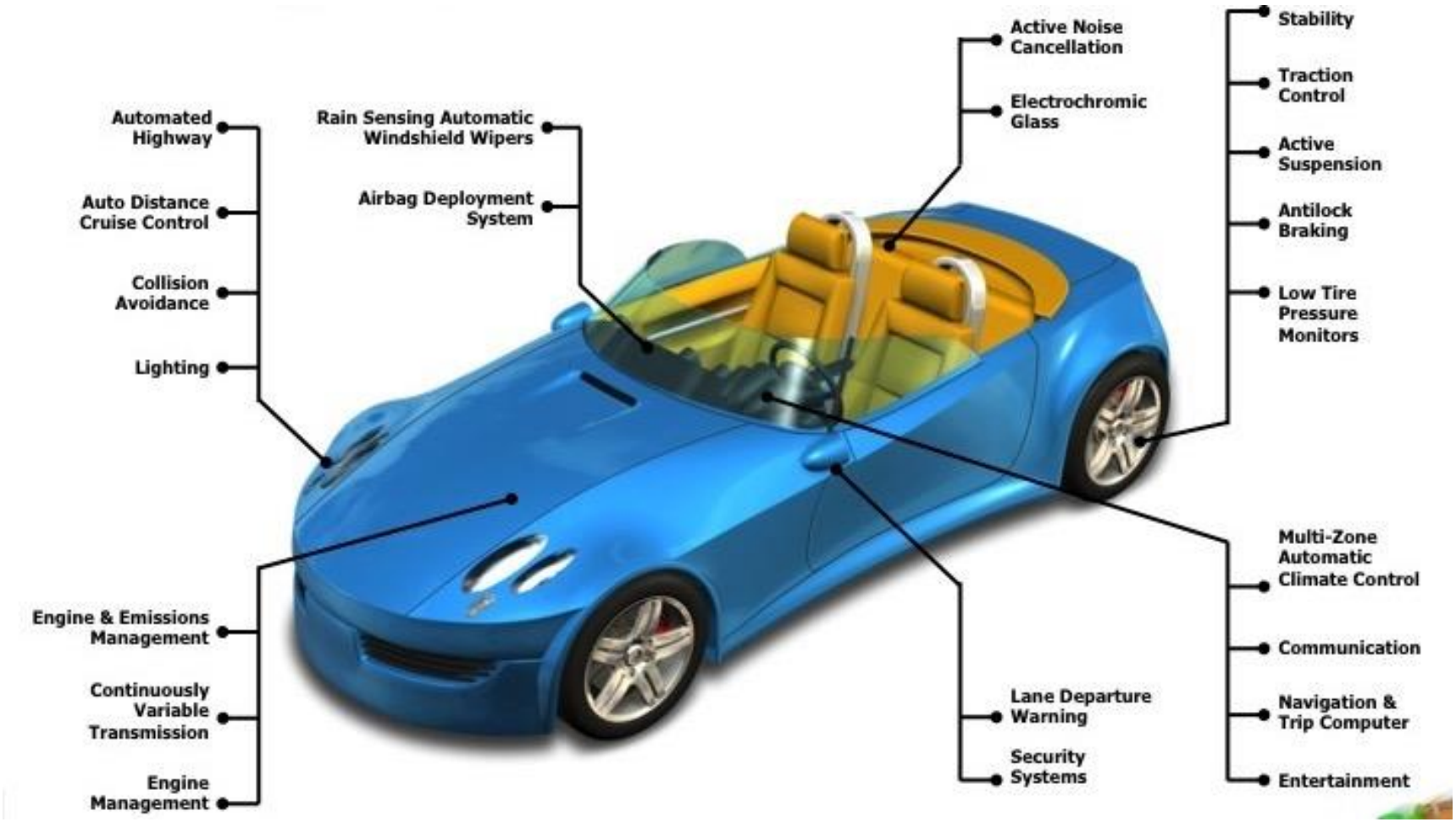
Share |

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,

The Pace of Automation

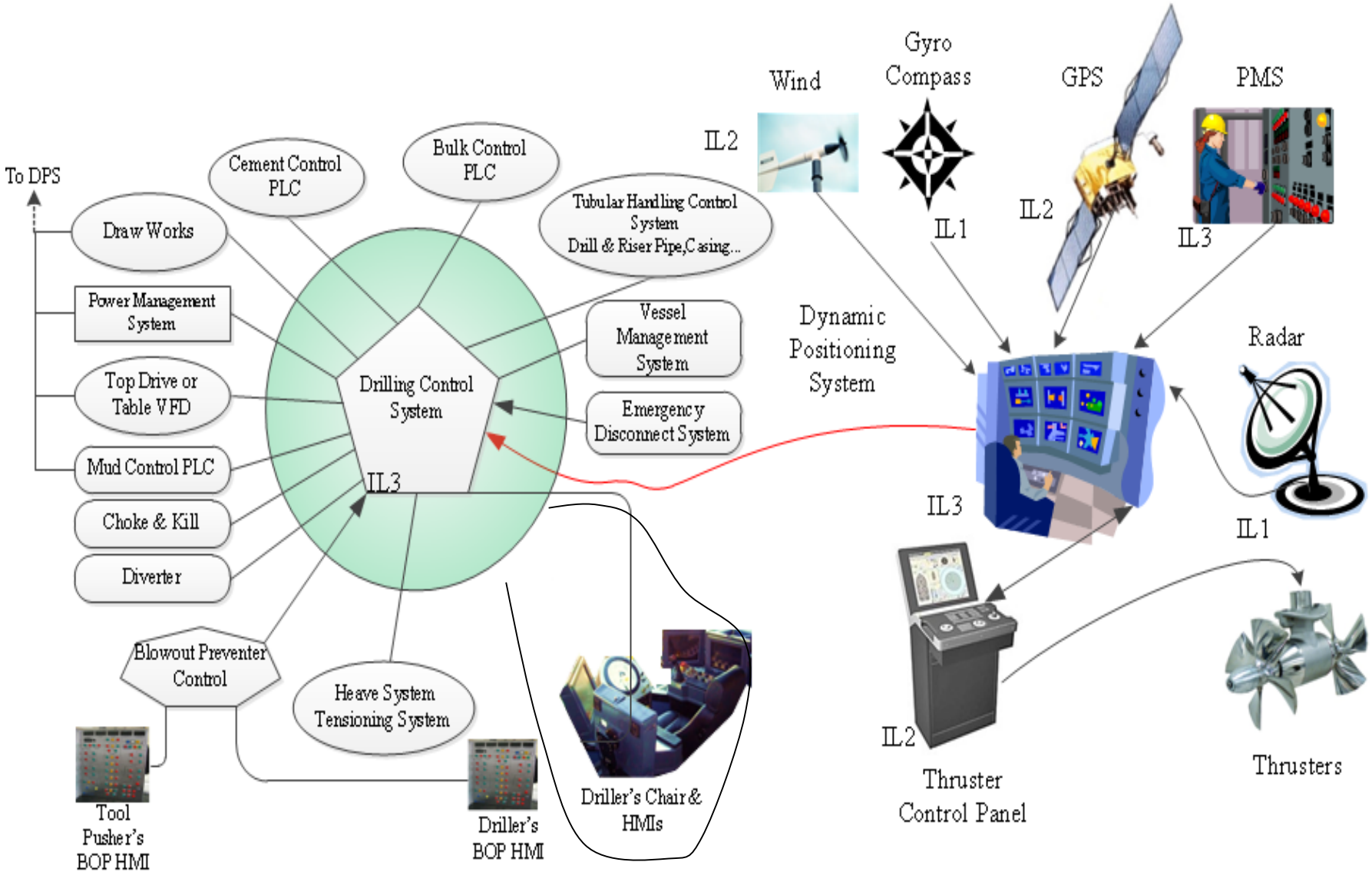


Typical New Car Automation



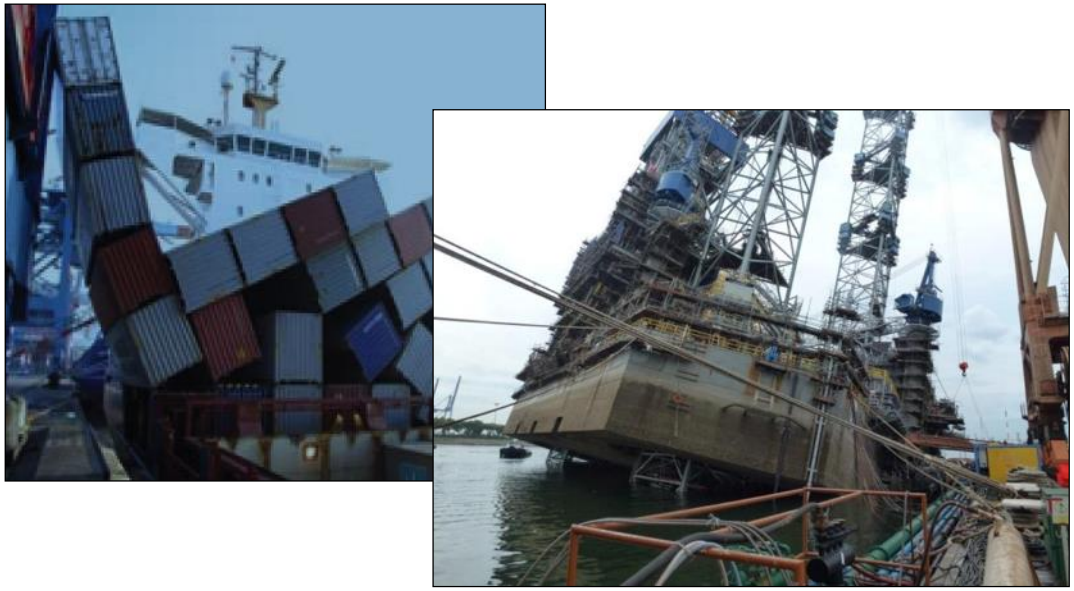
Source: John Blyler, http://www.chipestimate.com/blogs/IPInsider/?p=92

Complexity of Systems



Examples of software failures

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



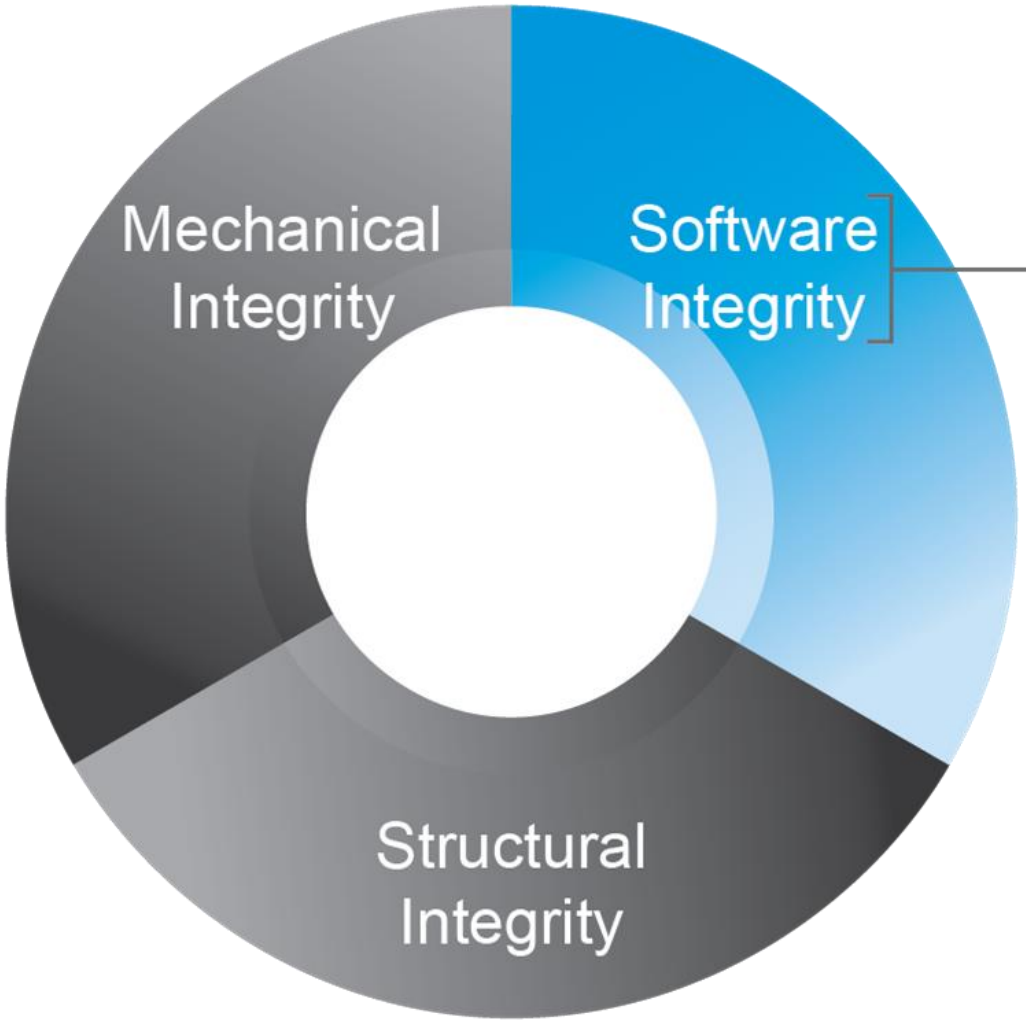
Warning to offshore industry on blocking of data communications in dynamic positioning systems

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

Software Integrity



Software Quality Engineering

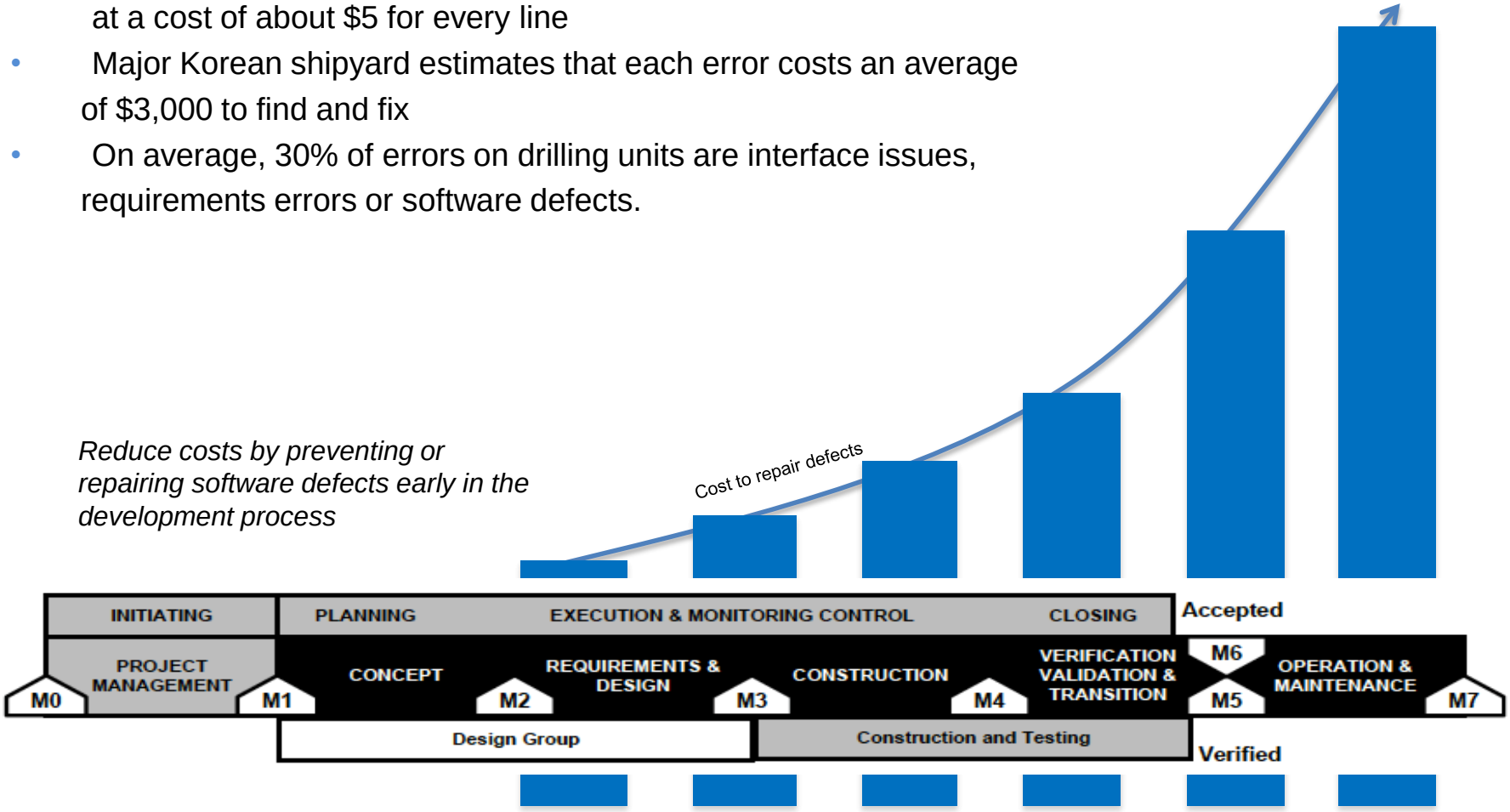
Verification & Validation

Cybersecurity

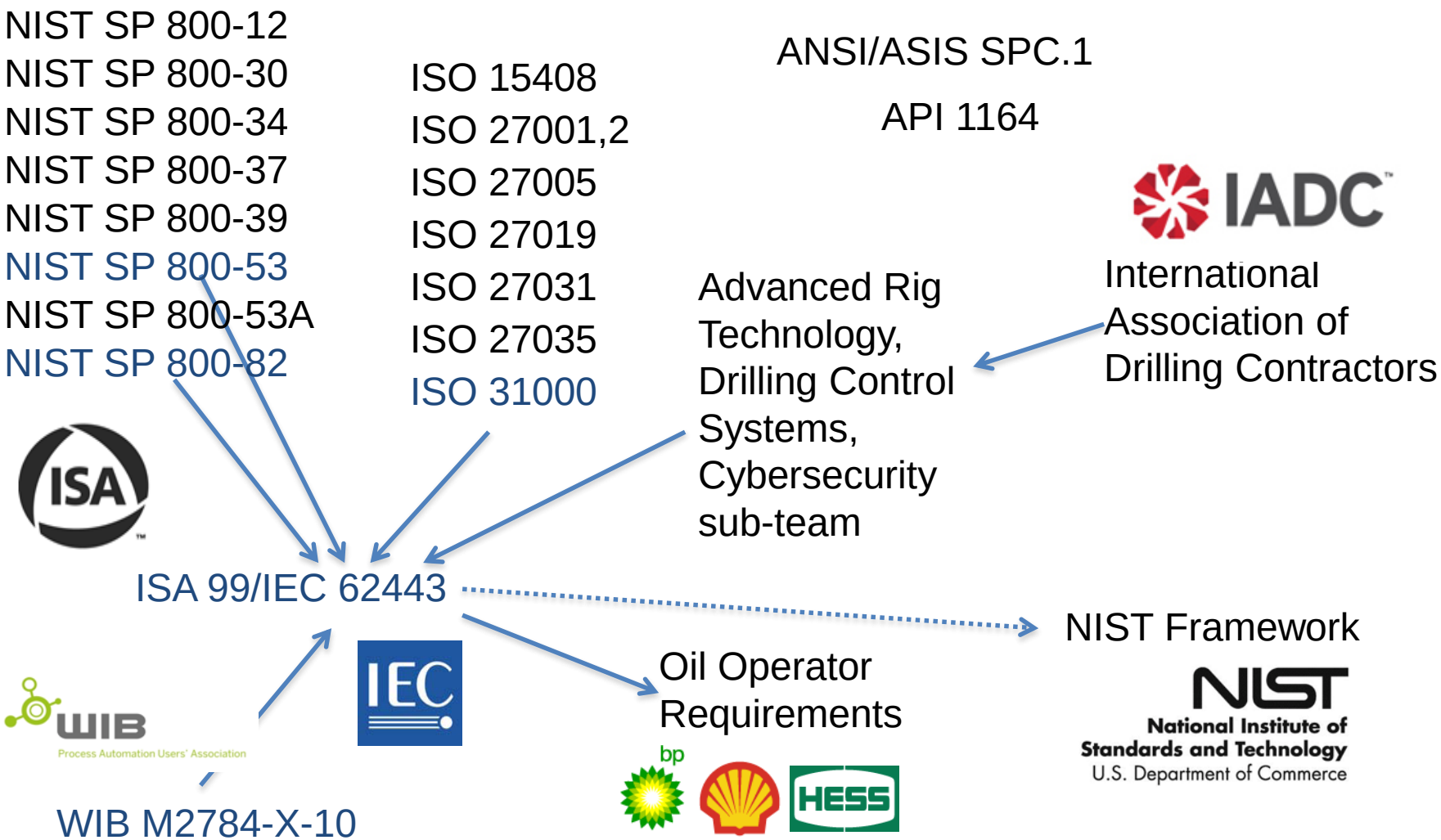
Software Repair Costs over Asset Lifecycle

- Cost of poor quality: repairs to defects in software increase exponentially through the vessel lifecycle
- Industry standard - 5 bugs per every thousand lines of code at a cost of about $5 for every line
- Major Korean shipyard estimates that each error costs an average of $3,000 to find and fix
- On average, 30% of errors on drilling units are interface issues, requirements errors or software defects.

Reduce costs by preventing or repairing software defects early in the development process



Industry Standards and Committee Initiatives



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

Observations

- Everyone is “authorized”
  - During production, and in-between wells
- Software Management of Change processes not followed
  - SMOC software was in the middle of implementation – stacks of paperwork “ready for entry”
- 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

Recommendations

- Embrace the differences between IT and OT
  - CIA vs AIC
  - Involve IT in OT
- Document your systems – connections AND data flows
- Harden your systems
  - Manage patches
  - Turn off unnecessary programs and processes
  - Authorize/authenticate applications and specific communication paths
- Do the basics
  - Control USBs, follow processes, educate users, hold OEMs accountable for quality, compartmentalize architectures…
- Prepare to respond and recover from an “event”