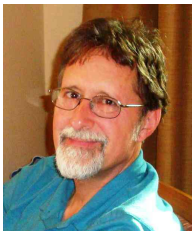
**Mr Paul Walters,**
**Assistant Chief Engineer, American Bureau of Shipping, USA**



## Short Curriculum Vitae (C.V.)

Paul Walters PE is an Assistant Chief Engineer at ABS and is the Integrated Software Quality Management (ISQM) Team Lead. He is the principal author of the ISQM Guide and leads a team of naval software engineers implementing software quality to various control systems installed aboard marine, drilling and production assets. Paul's group updated the Systems Verification Guide, ABS' Hardware-Inthe-Loop Notation, to align with the ISQM Guide requirements. He developed the ISQM-Conformity Program as an additional offering within ABS' Type Approval to improve supplier software quality.
Paul learned the ISQM process early in his career and has followed the software development process in many successful projects. Paul has 30 years' experience in the process control industries, programming and integrating control systems as well as instrument selection, power generation and advanced process control. He is fluent in 16 programming languages and is a registered Professional Engineer in the United States, where he worked in refineries and chemical plants before joining ABS.

## "Cyber Security challenges related to Offshore Oil_Gas & Sea Transport"

A cyber-safe software control system must be built on well-engineered software to which cybersecurity processes and principles are applied. While this approach helps to create a solid foundation, evolution exposes a software system to patches and updates that can contain software defects and functional nadequacies or errors. Requirements that fail to clearly and accurately communicate the desired functionality negatively affect the system during initial build as well as during systems evolution. Following rigorous software quality development principles, however, tends to reduce the risk of defects and functionality errors. In today's highly integrated systems, a fielded software defect in a single piece of equipment can cascade into multiple failures that can significantly impact the asset's mission.
With complex systems, today's owners and crews experience even greater challenges during the control system's operational lifetime. Software updates associated with maintenance processes too often lack sufficiently clear and detailed documentation to adequately support the decision to upgrade or not. One safeguard against maintenance-associated software errors is a thorough Software Management of Change (SMoC) process that requires the supplier to provide a detailed description of the purpose of the update, all interfaced register changes, a pre-installation test report, a post installation test plan, and a final test report.
The integrity of control systems also can be compromised by cybersecurity breaches. The corruptivepotential of a breach can be experienced through a number of well-known threats, such as unprotected ports (network and USB), unauthorized use of USB memory sticks, out of date virus protection applications, and nonexistent or poorly executed SMoC processes, to name just a few. Over time, the risk to system integrity presented by corruption vectors having origins in Internet connectivity, inadequate cybersecurity protections, and weak management of change processes increases. The presentation outlines some solutions and recommended best practices addressing these challenges.

Please contact: Paul R. Walters PE
pwalters@eagle.org
Office: +1.281.877.1539

Mobile: +1.832.331.1539