SAFEWELL

Focus on Lifecycle Risk Management of Automation Systems used in Commercial Diving Vessels

Briefing to the Bergen International Diving Seminar – November 2021

Ed Gardyne C.Eng MinstMC© Safewell Solutions Ltd™

"Illustrations by Matt Chinworth. First published by AtlasObscura.com."

Topic Coverage

- Background
- The Importance of this Topic
- Timeline of activity since the first DSAP audit in 2008
- What is the objective?
- What is a PLC and how are they applied in DSV's?
- Managing the Invisible Risks (IMCA, IOGP, IEC61508, E-Stops)
- Key Industry Lessons Learned (FMECA, OEM Audit, Proof Testing)
- Trends and Improvements
- Q & A

Background

Provision of Safety and Commercially Critical Risk Management Solutions

- ✓ **Based in Scotland**
- ✓ **Clients Worldwide**
- ✓ **35+ Years' PLC / Automation / Industrial Multi Sector Experience**
- ✓ **Focus on 'Invisible Risk' Management**
  - **Commercial Diving Vessels**
  - **Diving Gas Analysis (Mass Spec)**
  - **Breathing & Process Air Systems**
  - **Part of Shell UK SME team**

Our Clients

Examples of our clients who TRUST our solutions.

KAEFER
BAE SYSTEMS
TechnipFMC
HELIX ENERGY SOLUTIONS
cnooc
REPSOL SINOPEC
REVER OFFSHORE
BAKER HUGHES a GE company
wood.
MEGARME Rope access Specialists
TEKFEN CONSTRUCTION
Weatherford
KREUZ SUBSEA
STORK A Fluor Company
bp
SOCAR
cape
gsk
subsea 7
EnerMech Safer • Smarter • Solutions
sapura energy
TotalEnergies
dana PETROLEUM
ALTRAD
FairfieldEnergy

safewellsolutions.co.uk

The Importance of this Topic – Where is the Focus?

- Education to Create Awareness of Impact of Automation (PLC's) on Dive Systems.
- Focus on the "Invisible" Risks when Using PLC's and programmable devices – Improve quality of FMECA and safety assessment at design stage and validate the mitigations.
- Generate a Clear Mind set for Effective Systematic Life Cycle Management of PLC's.
- Tune all this into the existing DSV assurance and audit cycles e.g. proof testing of safety instrumented functions, maintenance of control systems, software management.
- Stimulate Open Discussion of the Issues – Operator / Dive System Owner / OEM.
- Demystify and remove the Fear Factor and Silo Mentality - The people in the industry typically have the technical capability and risk reduction culture to deal with this task.

Safety Assurance of Automated Dive Vessels – 2008 – 2021 Key Milestones

- 2008 - DSV Bibby Topaz - First Dive Control System Assurance for Shell UK
- 2009 - DSV Seven Atlantic – First Dive Control System Assurance during New Build
- 2012 - IOGP Diving Operation Sub Committee Start Work on the DSAP RP468
- 2013 - DSV Skandi Arctic Port Diving Bell Uncontrolled Descent Incident
- 2014 – Meeting with DNV in Oslo to determine their perspective
- 2015 - Final Draft of DSAP RP468 Submitted for Approval
- 2015 - IMCA Diving Systems PLC Seminar Amsterdam
- 2016 - DSAP RP468 Approved and Published by IOGP
- 2016 – Commenced PLC DSAP for DSVi Group of Operators
- 2018 – 10 Years of Automated DSV Assurance for Shell UK
- 2020 - Automated Dive System Assurance Activity expanding Globally US, SEA,
- 2021- Work Continues. Now also looking at assurance of automated ROV LARS

SAFEWELL

DSAP Assurance	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
Rever Topaz	✓										✓			✓
Deep Discoverer													✓	✓
Seven Atlantic		✓				✓	✓		✓	✓	✓	✓	✓	✓
Seven Havila - Falcon					✓		✓		✓		✓	✓		✓
Seawell														✓
Helix Well Enhancer				✓				✓		✓	✓	✓		✓
Boka Sapphire				✓										
Boka Polaris							✓	✓	✓		✓	✓	✓	✓
Skandi (Deep) Arctic							✓			✓			✓	✓
Seven Kestrel										✓	✓		✓	✓
Technip Deep Explorer										✓	✓	✓		✓
Khankendi (BP)											✓			
Sapura Constructor											✓			
Southern Star												✓	✓	
Seven Eagle											✓		✓	
EDT Protea											✓			
Posh Mallard													✓	✓
Kelly Ann												✓	✓	✓
Kreuze Challenger										✓	✓			
Seven Pegasus												✓		✓
Boka Atlantis												✓	✓	✓
Da Vinci												✓	✓	
Normand Reach ROV											✓			
Milestones														
Skandi Arctic Bell Drop						✓								
IOGP RP468 Developed					✓	✓	✓	✓						
IOGP RP468 Published									✓					
IMCA PLC Seminar								✓						
Shell Team	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
DSVi Team									✓	✓	✓	✓	✓	✓

The Assurance Audit Risk Reduction Objectives

When conducting these dive system PLC safety audits, we are looking at two main types of risk:

Random hardware failures – these failures can be assessed in terms of failure effects and criticality (FMECA) and can be quantified to an extent. A review of the type and safety integrity of the PLC hardware and safety components used in the dive control system design and development provides an indication of the potential for hardware failure and allows predictions of lifecycle performance.

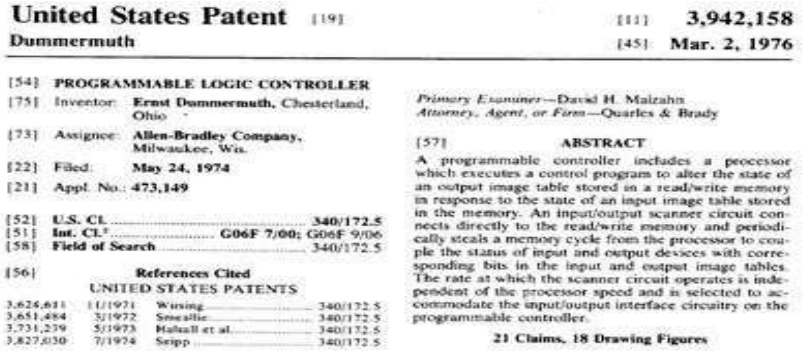
Systematic failures – these are unrelated to specific hardware (PLC) component failures and are potential risks arising from gaps in the systems, skills and disciplines applied during the complete lifecycle from initial concept through to lifecycle management of change. Such failures are unique to a system, the people involved and the system environment.

Both of these areas of risk must be assessed to ensure that the level of risk reduction is ALARP.

But Firstly a Quick Reminder…. What is a PLC?

Programmable Logic Controller

- In 1968 General Motors in the US wrote a specification for a programmable controller to replace large unwieldy relay logic panels.
- Not New Technology - PLC First Patent was released in 1974.



United States Patent [19]
Dummermuth

[11] **3,942,158**
[45] **Mar. 2, 1976**

[54] **PROGRAMMABLE LOGIC CONTROLLER**

[75] Inventor: **Ernst Dummermuth**, Chesterland, Ohio

[73] Assignee: **Allen-Bradley Company**, Milwaukee, Wis.

[22] Filed: **May 24, 1974**

[21] Appl. No.: **473,149**

[52] U.S. Cl. 340/172.5
[51] Int. Cl.² G06F 7/00; G06F 9/06
[58] Field of Search 340/172.5

[56] **References Cited**
UNITED STATES PATENTS

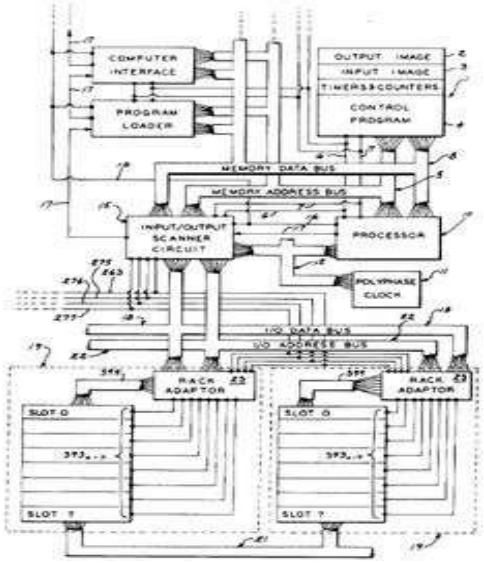
3,624,611	11/1971	Wirsing	340/172.5
3,651,484	3/1972	Smeallie	340/172.5
3,731,279	5/1973	Halsall et al.	340/172.5
3,827,030	7/1974	Seipp	340/172.5

Primary Examiner—David H. Malzahn
Attorney, Agent, or Firm—Quarles & Brady

[57] **ABSTRACT**

A programmable controller includes a processor which executes a control program to alter the state of an output image table stored in a read/write memory in response to the state of an input image table stored in the memory. An input/output scanner circuit connects directly to the read/write memory and periodically steals a memory cycle from the processor to compile the status of input and output devices with corresponding bits in the input and output image tables. The rate at which the scanner circuit operates is independent of the processor speed and is selected to accommodate the input/output interface circuitry on the programmable controller.

21 Claims, 18 Drawing Figures



Modern PLC uses modular building blocks to integrate a system

PLC

SAFETY CONTROLLER

SAFETY RELAY

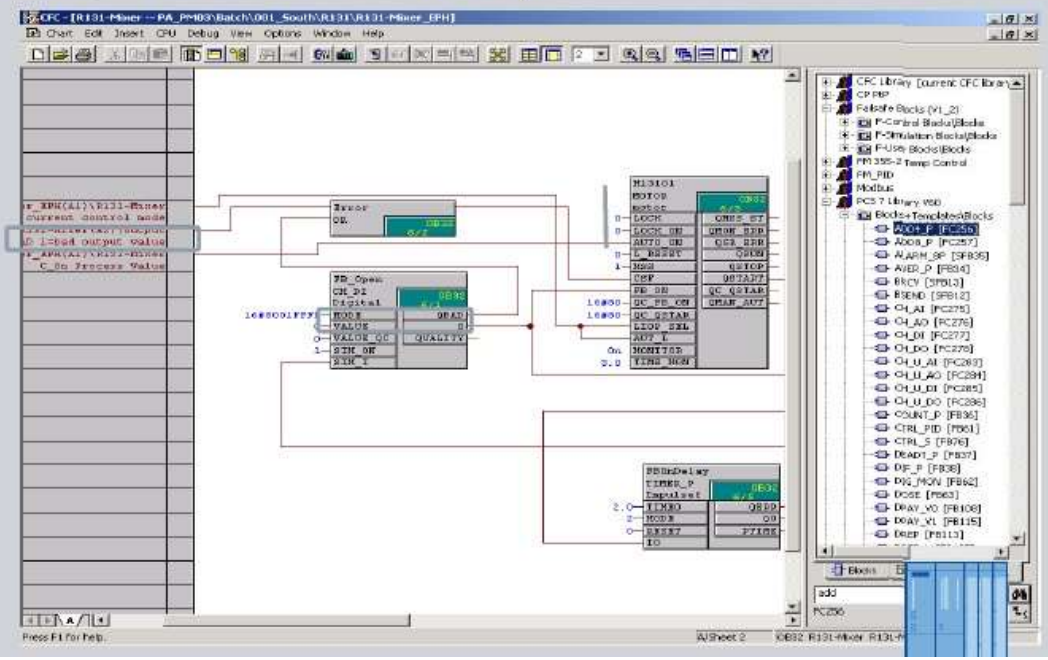
With Ethernet switches built automation systems can now be easily networked with business IT systems so there is a need to assess the Cybersecurity threat.

Electric drives, safety controllers, safety relays, smart actuators are also programmable / configurable devices and their software configurations must be carefully managed during lifecycle It's easy to forget these devices – they are not standard PLC's

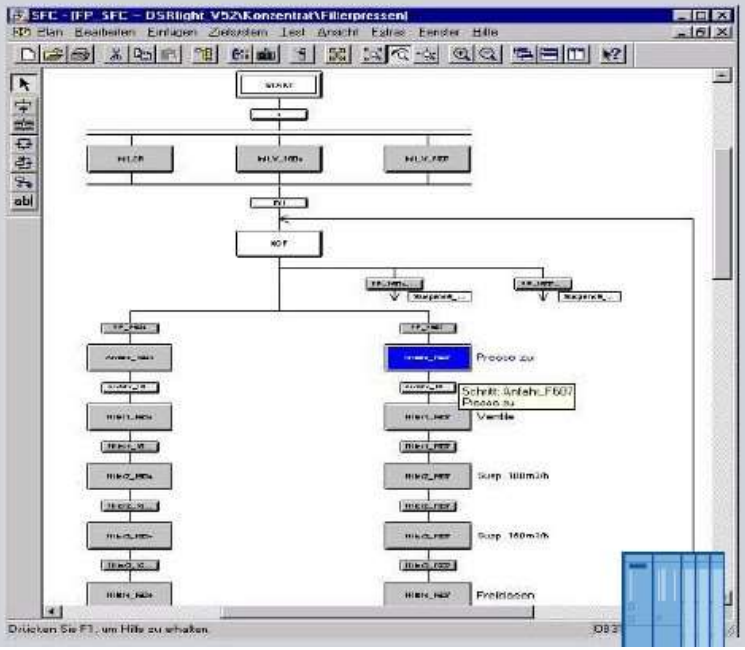
SAFEWELL

PLC's and Devices Programmed using High Level Languages

CFC (Continuous Function Chart)

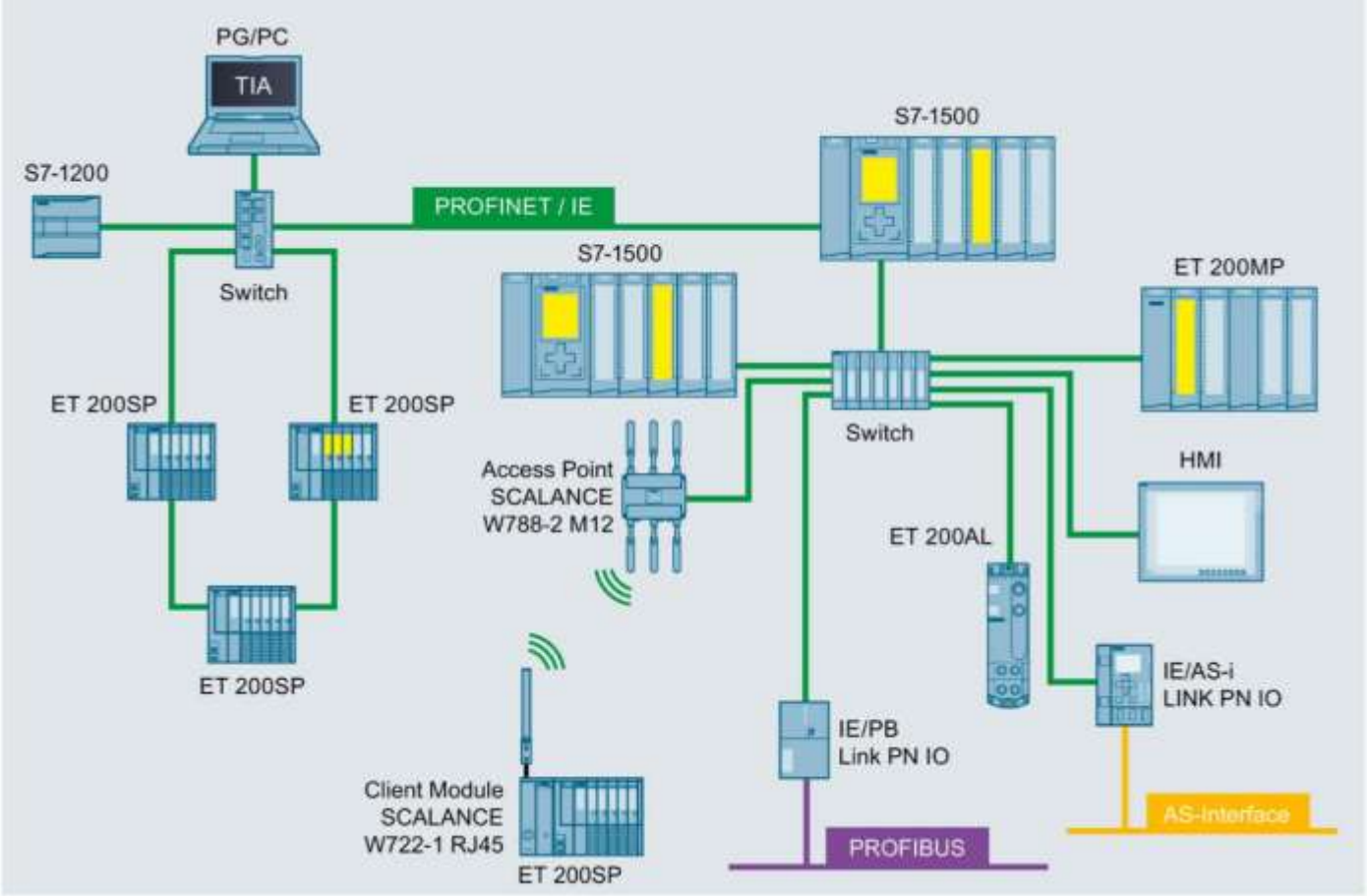


SFC (Sequential Function Chart)



SAFEWELL

Modern Dive (PLC) Control System Architectures can be complex



PROCESS AUTOMATION UBIQUITOUS, PERVASIVE, DISRUPTIVE?

e.g. Impact on Offshore Drilling Industry – When Automation changed things in the 80's and 90's

The Way It Was –
Hydraulic - Pneumatic

The Way It is Now – The Drill floor is automated using Programmable Systems

COMMERCIAL DIVING INDUSTRY

- Modern DSV's designs may include many PLC's and other programmable devices

- Systems are complex and more difficult to audit unless you have the necessary knowledge and experience

EXTENT OF AUTOMATION ON DIVE VESSELS

- Bell launch and recovery systems
- Bell Utilities
- Compression / Decompression
- Oxygen Concentration Control
- CO2 Monitoring / Scrubbing
- Humidity & Temperature Monitoring
- Environmental Monitoring
- Data Logging
- Warnings / Alarms
- HPU Control- Emergency Stops
- ROV, DP
- Cranes, Pipe Lay
- Intelligent Drives, Instruments

SAFEWELL

BENEFITS OF DIVE SYSTEM AUTOMATION

- Safer, more reliable Diving Operations using automation system (PLC) hardware and software to implement risk mitigation and maintain safety critical systems in a fail safe state
- Providing advanced tools to manage complex tasks e.g. LARS operations, running several chamber depth profiles simultaneously. More accurate and linear decompression from saturation.
- Providing sophisticated instantaneous oversight over complex operations and automating emergency responses e.g. Oxygen Shut In, Emergency Shut In, Low O2, High O2, Depth Rate of Change, High CO2
- Capturing system diagnostic data for analysis and improvement – intelligent warning and alarms
- Reducing (but not eliminating) human error during repetitive work tasks which may arise from tiredness or temporary lack of focus

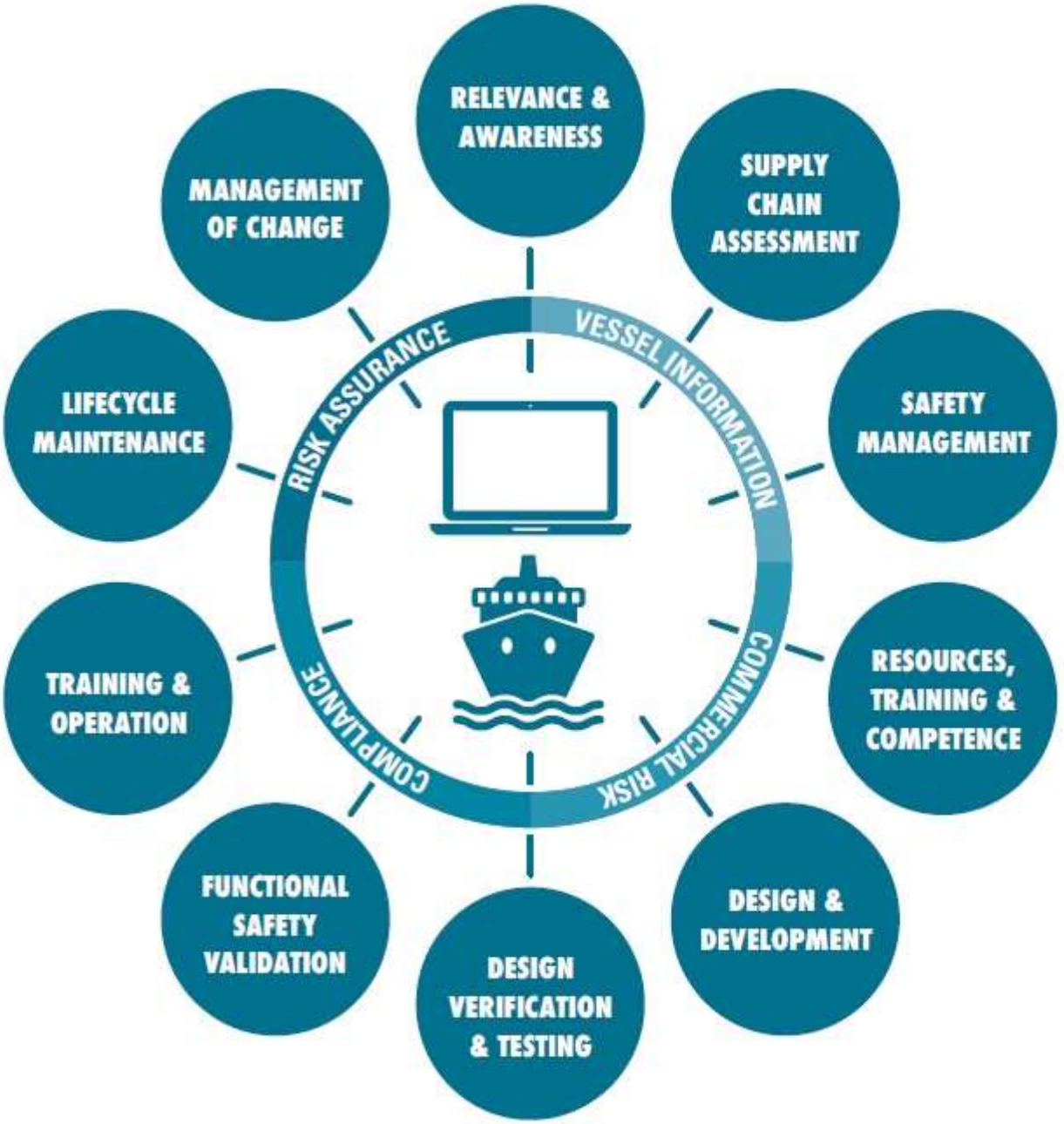
SAFEWELL

BUT THERE ARE ALSO NEW LIFECYCLE RISKS TO MANAGE!

- How engaged and aware are senior management? Do they have a policy / strategy
- How well are automated PLC based dive systems failure modes and safety functions assessed at the design stage? [Level of Competence applied] and validated
- How good is the OEM FMECA and the design technical and safety specifications?
- Competency and quality assurance of designers, manufacturers, software engineers, operators, class bodies, auditors
- Hardware and Software testing and life cycle software configuration control
- Competence of Maintenance Technicians / Availability of Spares / Tools
- System Security e.g. Cybersecurity, Passwords, Ownership of Software
- Management of Change during system life cycle – who is involved
- Possible atrophy of knowledge and manual skills

SAFEWELL

This requires a recurring systematic lifecycle approach



01330 826978
INFO@SAFEWELLSOLUTIONS.COM
WWW.SAFEWELLSOLUTIONS.CO.UK

SAFEWELL

Journey to Best Practice

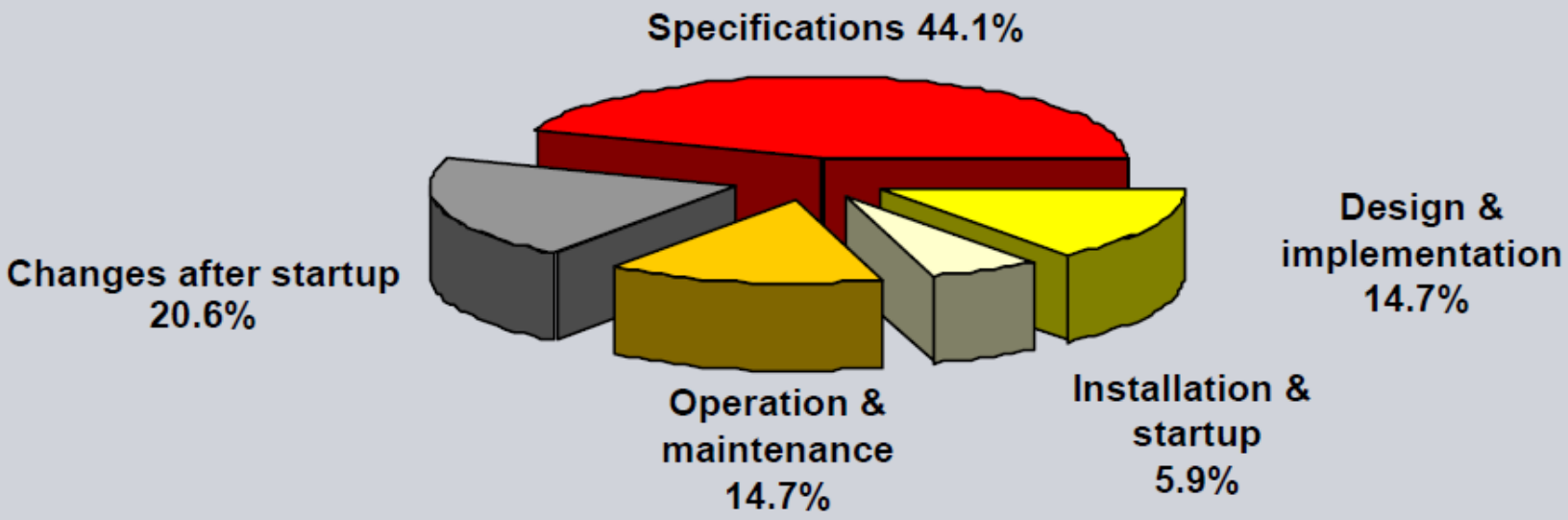
IMCA RESPONSE TO MANAGING THE RISK!

- Issued Draft Addendum to IMCA D 024 – Not Published following review
- And an Information Note on PLC's in August 2012
- Further Information Note IMCA D 30/20 Published in Dec 2020
- Quality Assurance and Quality Control of Software IMCA M 163 Rev 1 10/2019

OPERATORS RESPONSE TO MANAGING THE RISK!

- IOGP working group set up in 2013 to develop a dive vessel safety assurance audit tool DSAP for use by all operators and dive vessel owners
- Objective was to develop reliable, consistent and systematic audit approach
- Shell UK piloted the tool during DSV audits
- IOGP recommended practice for dive system assurance published in February 2016 (Report No 468).
- Safewell developed Appendix C & D used for safety assurance of automated dive systems
- This systematic audit procedure has been refined further since 2016 – Focus on Lifecycle history.

WHY A LIFECYCLE FOCUS?



Note : Based on 34 investigated incidents in the UK
Health and Safety Executive (GB): Out of Control. Why control systems go wrong and how to prevent failure. HSE Books 1995

Out of control: Why control systems go wrong and how to prevent failure

Date of publication:
2003
Series code:
HSG238

IEC61508 – USED WIDELY IN MANY SECTORS & UNDERPINS OTHER SAFETY STANDARDS

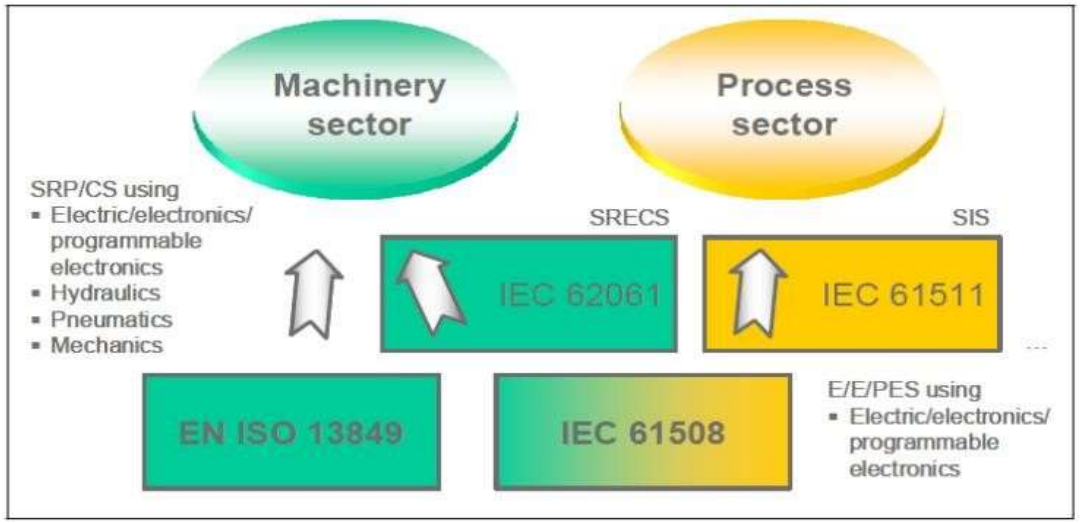
IEC Commission Electrotechnique Internationale International Electrotechnical Commission Международная Электротехническая Комиссия

IEC61508

IEC 61508 serves as the basic standard and basis for safety standardization.

It covers all areas where electrical, electronic or PLC systems are used to realize safety-related protection functions.

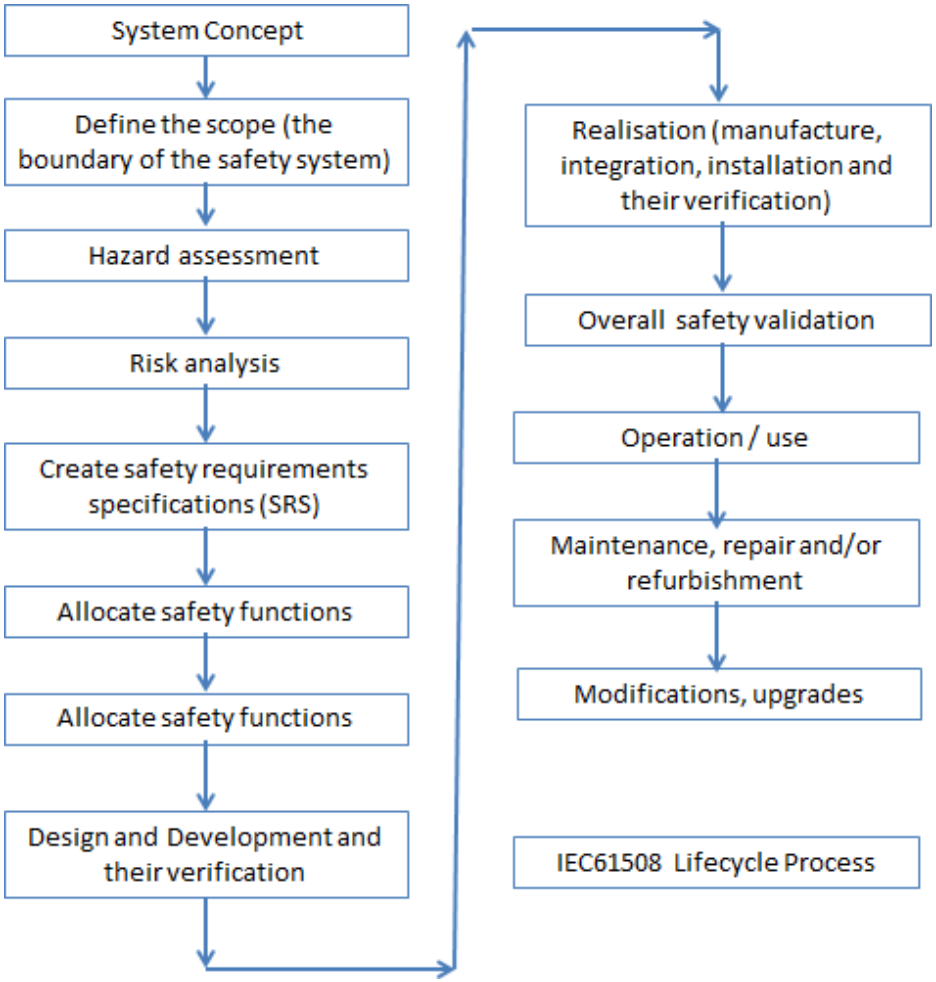
SAFETY RELATED PARTS OF A CONTROL SYSTEM



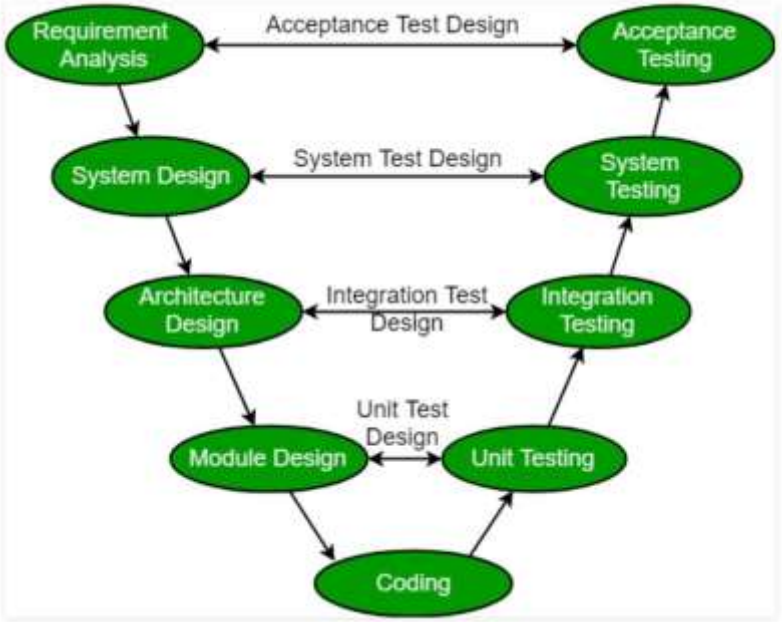
SAFETY INSTRUMENT SYSTEM

IEC61508 has a foot in either camp i.e. machinery and process

IEC61508 – LIFECYCLE MODEL SYSTEMATIC METHOD



Embed V Model



Verification: It involves static analysis technique (review) done without executing code. It is the process of evaluation of the product development phase to find whether specified requirements meet.

Validation: It involves dynamic analysis technique (functional, non-functional), testing done by executing code. Validation is the process to evaluate the software after the completion of the development phase to determine whether software meets the customer expectations and requirements.

SAFEWELL

IEC61508 – SAFETY INTEGRITY LEVEL (SIL)

Safety Integrity Level	Probability of failure on demand (PFD) per year (Low Demand mode of operation)	Risk Reduction Factor (RRF)
SIL 4	$>=10^{-5}$ to $<10^{-4}$	10000 to 100000
SIL 3	$>=10^{-4}$ to $<10^{-3}$	1000 to 10000
SIL 2	$>=10^{-3}$ to $<10^{-2}$	100 to 1000
SIL 1	$>=10^{-2}$ to $<10^{-1}$	10 to 100

SIL: A performance criterion of an SIF which describes, for example, the probability of the SIF failing in case of a process demand.

SIF = Safety Instrumented Function

Lessons Learned – Trends and Positives

- Increasing use and reliance on programmable devices embedded in dive systems
- Improved awareness and knowledge of operators and sub-sea companies involved in lifecycle safety management of automated dive systems e.g. functional safety assessments, design standards, design verification, system testing and validation
- Diving companies have developed lifecycle safety management resources, policies (supply chain), procedures (annual internal audit, security, management of change), training and competence assurance
- Development by diving companies of lifecycle maintenance and proof testing procedures to validate failure mode mitigation and emergency response
- Improved Lifecycle management of automation system software.
- The Automation hardware used to implement systems is getting safer with validated safety integrity built in.
- The manufacturing supply chains (OEM's) are now aware of the scrutiny applied to the design of automated dive systems.
- IEC61508 principles have been adopted by some OEM's in the diving sector to reduce systematic risk and is embedded in their ISO9001:2015 management systems

Lessons Learned – Trends and Positives

- The risk of using PLC's in automated dive systems is manageable
- The diving industry already has a strong safety culture and a mind set of learning and continuous improvement. It is now applying this to PLC's and programmable devices
- UK Operators and DSVi Collective are leading the way on directing lifecycle assurance of PLC systems used on dive vessels [and ROV]
- The trend among manufacturers and integrators is to provide safer PLC hardware with certified levels of safety reliability and diagnostic cover – Functional safety principles are being adopted by OEM's
- This trend extends to the use of standard 3rd party certified software safety modules so bespoke coding risk is reduced – Reliance on the software guy is reducing.
- Integration Tools provide standards based documentation for traceability and configuration management
- **It's becoming easier than ever to design safe and reliable automated dive systems.**

Thank you! We may have time for some questions but if not, contact me on;

Email: ed@safewellsolutions.com

Phone: +44(0)7917887320 / +44(0)1330 826978