Introduction and Motivation

Main Topic
- Methods and tools used in development Rolls-Royce DP control systems

Background – Rolls-Royce
- Total system provider
- Joystick positioning systems since the 1970’s
- Market introduction of DP range in 2004

Policy: Design systems for maximum safety – beyond class rules
Concepts of Dependability

DEPENDABILITY
  -- Attributes
  - Availability
  - Reliability
  - Safety
  - Confidentiality
  - Integrity
  - Maintainability

DEPENDABILITY
  -- Means
  - Fault Prevention
  - Fault Tolerance
  - Fault Removal
  - Fault Forecasting

DEPENDABILITY
  -- Threats
  - Faults
  - Errors
  - Failures
Product lifecycle

Product lifecycle:
- Activities
- Stages
- Phases

System dependability is function of product lifecycle activities
Project Execution Process

Project Gates

Product/Service Development
- Concept Review
- Preliminary Design Review
- Critical Design Review
- Product Release Review
- Pre-service Review
- In-service Review

Internal Project
- Prospect Pursuit
- Project Launch
- Close-out Review
- Close-down Review

Business Gates
- Bid/No Bid
- Tender Approval
- Proposal (Contract) Acceptance
- Takeover by Customer

Stages
- Preliminary Business Case Stage 1
- Business Case Stage 2
- Execution Stage 3
- In-Service Support Stage 4
- Serial Production Stage 5
- Disposal Stage 6

Capability Acquisition Process
DP Dependability
DP System Definition:
- Power system
- Thruster system
- **DP control system**
- Sensor system
- Position reference system
DP Dependability

DP system attributes
- Availability
- Reliability
- Safety
- Confidentiality
- Integrity
- Maintainability
- Security
- Usability
- Performance
- Functionality
- Cost

DP system requirements
- Statutory & regulatory
- Classification
- Customers
- Rolls-Royce
- Suppliers

DP dependability

Fault prevention

Fault tolerance

Fault removal

Fault forecasting

DP system threats
- Faults
- Errors
- Failures
- Environment condition

DP operation tolerance
- Operation states
- Failure modes
- Time margins
- Consequences

DP system attributes

Quality assurance
- Design rules
- Specifications
- Shielding
- Standardization
- Processes
- Tools

Human interaction
- Instructions
- Guidelines
- Training
- Design for usability

Error handling
- Hardware
- System SW
- DP application

Redundancy
- Work-by
- Online / standby
- System architecture

Verification
- Code analysis
- Hardware, unit and system testing

Maintenance
- Corrective
- Preventive
- On-line repair
- Off-line repair
- Testing

Evaluation
- FTA
- FMECA
- Reliability assessment

Operator support
- What-if analysis
- Environment condition forecast
- Health monitoring
DP Threats and Operation Tolerance
DP System Threats

Faults

Random faults
Natural / physical cause
Statistic models

Systematic faults
Human cause
Design/software
No statistic model

Errors/Failures
Failure modes

Fail-stop
Permanent or transient

Erratic behaviour

DP system failure
Drift-off
Drive-off

activation
causation
propagation
DP Operation Tolerance
DP Operation Tolerance

DP control system failure
sustained failure

normal
safe

hazard
safe

breakdown
unsafe

shutdown
safe

restart

successful recovery

obtain safe vessel operation

no safe vessel operation or shutdown fails

DP control system repair

failure of safety / emergency mechanisms

damage
unsafe
DP Operation Tolerance – DP Failure

costs (damages + losses)

1. $T_{grace}$
2. $T_{homax}$
3. $T_{shut}$
4. $T_{damage}$

- vessel/equipment is damaged
- safety/emergency takeover
- shutdown time
Redundancy Solutions
DP Redundancy

Control System Redundancy
How?

plant input

plant output
Alternative Redundancy Concepts

Online / standby

- plant input
- error detection
- online
- state transfer
- standby
- error detection
- switch
- plant output

Multiple work-by

- plant input
- input synchronization
- work-by
- work-by
- work-by
- work-by
- voter
- plant output
Online / Standby Concept

**Properties**
- Online unit in control
- State transfer to standby unit
- Switch control to standby when online fails
- Switching based on error detection

Smooth transfer:
- Hot standby: Equal states, $T_{\text{recovery}} = 0$
- Warm standby: $\approx$ equal states, $T_{\text{grace}} > T_{\text{recovery}} \geq 0$
- Cold standby: Unit startup needed, $T_{\text{recovery}} > T_{\text{homax}}$

**Cons**
- Undetected errors
- Reliability of switch
- Integrity of state transfer
- Error propagation
- Hot / warm standby

**Pros**
- Possibility for SW / system diversity
- Increased tolerance to systematic faults
Multiple Work-by Concept

Properties

- Equal input to all work-by units
- Work-by units work in parallel
- Units produce equal output
- Error detection and masking by voting
- Control output by majority voting

- Bumpless transfer / reconfiguration, $T_{\text{recovery}} = 0$ sec

Cons

- Reliability of input synchronization
- Reliability of voter
- SW diversity not possible
- SW potential common mode failure

Pros

- Errors detected by voting
- Bumpless transfer
- Multiple redundancy
Refined Triple **Controller** Redundancy

**Triple Controller Redundancy – TCR**

- Triple work-by
- Error handling
- Graceful degrade
- Online repair
- Input synchronization
- Distributed voting – 2oo3
- Bumpless transfer for all DP control functions
- Fire separation (DP 3)
Online / Standby System Redundancy

TCR and online/standby

- Triple main system
- Single alternate system
- Online / standby scheme
- State transfer monitoring
- Manual selection
- No dependencies
- SW / system diversity
- Systematic faults tolerance
- Limited bumpless transfer
System Configurations
DP class 2

Bridge

Sensor Groups

Integrated Work Stations

Control Cabinets

Propulsion and Thruster Devices

DPC A  DPC C  DPC B

Icon DP

Dual DP LAN

Dual R&T LAN

Poscon Joystick

PC
DNV DYNPOS-ER Notation
DP class 3

- Sensor Groups
- Integrated Work Stations
- Control Cabinets
- Propulsion and Thruster Devices
- Main Bridge
- Emergency Bridge
- Icon DP Main
- Icon DP Alternate
- Dual DP LAN
- Dual P&T LAN
- DPC A
- DPC C
- DPC B
- DPC D
Design for Usability
Control System Levels

- DP Main Control System
- DP Emergency Control System
- Independent Joystick Control System
- Remote Thruster Control
- Emergency Thruster Control
- Local Thruster Control

- DP Main Control System
- DP Alternate Control System / Independent Joystick Control System
- Remote Thruster Control
- Emergency Thruster Control
- Local Thruster Control

Reduced complexity
Integrated Workstation – DP and P&T

- Common joystick for DP Main and DP Alternate
- DP Main display
- DP Alternate and P&T display
- System selection
- Alarm mute
- Common command transfer
System Design and Architecture
System Software Layers

Application Software
- Application specific component

Application Framework
- Process scheduling
- Message handling
- Data routing
- Controller redundancy
- Clock sync
- Network redundancy
- UDP IO
- GUI Comm
- Serial interface
- CAN

Operating system
- Realtime scheduling
- Memory protection
- Network stack
System Decomposition

DP Main = Triple DP = DP AC|B = DP Online

DP Alternate = Single DP (Independent Joystick) = DP Hot Standby
Error Propagation

- fault in component
- error in component
- component failure
- fault in superior component
- error / failure in adjacent component

causation, activation, propagation
DP Dependencies – Data Links

DP Controllers - Sensor Groups

DP LAN Switches

P&T cabinets

DP Operator Stations

Links:
- Ethernet
- Serial
DP Dependencies – Power Cabling

- DP Controllers
- PSUs 24 VDC
- UPS’s 220 VAC
- Sensor groups
- DP LAN Switches
- DP Operator Stations

Hardwired connections.
System Level Error Handling

Components

- Processing units (Controllers, OS computers)
- Transmission links (LAN, CAN bus, serial links)
- IO units (AI / AO / DI / DO)
- Power supplies

Techniques

- Voltage, frequency, battery, short circuit monitoring
- Coding, masking, retransmission, overwriting
- Voting of redundant processor units
- Software exception and error handling on different levels
Application Level Error Detection

- Interface check
- Device specific checks
- Range check
- Frozen signal check
- Wildpoint check

- Step check
- High variance check
- High dynamics
- Voting reject
- Differ reject
Evaluation and Verification
Assessment

Design aspects
- Parallel groups
- Online repair

Assessment
- Reliability
- Availability
- Safety

Related aspect
Design for maintainability; ability to undergo repair and modifications.
Reliability with No Repair

Reliability distributions single $R_1(t)$, dual $R_2(t)$, triple $R_3(t)$

Cases

- single
- dual
- triple

$MTTF_{sys}$
System Evaluation and Verification

FMECA framework
- System design evaluation
- System test and verification
- Probabilistic approach
- Risk assessment according to GQP 2.63 and IMO

Compliance with IMO, IMCA and DNV guidelines
System Evaluation and Verification

**ESV in office / at factory**

- Input
  - DP Control System
  - ESV Simulator
- Output

**ESV at sea**

- Input
  - DP Control System
  - Vessel
- Output

- ESV Simulator

Graphs:
- Out of range
- Freeze
- Wild point & replacement
- Step
- High dynamics
- High standard deviation
Summary
Summary

Threats
- Random faults
- Systematic faults
- Fire & flooding
- Human fault (~time limits)

Means
- Triple redundant system
- Distributed voting
- Online/standby systems
- Unified workstations

Attributes
- Reliability
- Availability
- Usability
- Safety

General solution  DP1→DP2→DP2.5→DP3

Rolls-Royce
Thank you for your attention!