

An Industry view of Dependability

John Davies, BAE Systems Insyte



Overview

- Types of Systems we deal with
- Why do we need Integrity
- Influences on Dependability
- Specifying Dependability
 - Availability
 - Safety and Security
- Issues
 - Use of COTS
 - Sub-Contracts
 - Approach to Delivering Dependability

Types of System – with regard to Integrity

- ‘Standard’
 - Radars
 - Command Systems
 - Information Systems
 - Communication Systems
 - Planning Systems
 - Training Systems

 - All software intensive
 - All integrated into Systems of Systems to provide Capability
 - Apply ‘standard’ methods
 - Can include COTS
-
- ‘High Integrity’
 - Weapon Control,
 - Torpedoes

Why?

- Safety
 - Legal Responsibility
 - Reputation
 - Customer Requirement
 - Cost and delivery
-
- Level of Dependability linked to System Purpose

Influences on Dependability

- Architecture
 - Provides main dependability properties
- Components
 - Provide main functionality
 - Contain Faults – reduce dependability
- Processes
 - Reduce Faults – increase dependability

Faults -> Errors ~ Failures

- Faults – latent
 - Errors occur when defects activated
 - Failures occur if errors not handled
- Historically most found at System Integration and Test
 - manifest as errors
- Some get into delivered product
- Major cause of extra work

Faults -> Errors ~ Failures

- Processes are is the major method of avoiding/removing them
 - Main effect from CMM Level 2 processes
 - Applied across all projects (normally Level 3)

<i>Process Area</i>	<i>Category</i>
Configuration Management	Support
Measurement and Analysis	Support
Project Monitoring and Control	Project Management
Project Planning	Project Management
Process and Product Quality Assurance	Support
Requirements Management	Engineering
Supplier Agreement Management	Project Management

Unexpected Errors

- Found in Service
- Unexpected use
 - Often new use of new interface/interoperation
 - Exercises existing system in new way
 - Causes faults to be revealed
- Operator Actions
 - Examples
 - UKADGE – UK Air Defence Ground Environment
 - Ptarmigan – Army Battlefield Communications
 - C3D Sentry – Airbourn Early Warning

Specifying Dependability

- Traditionally deal with Availability, Reliability, Maintainability
- Standard /Boiler Plate Values
 - The Availability shall be greater than 99.999%
 - The Mean Time Between Failure shall be > 100 days
 - The Mean Time To Repair shall be < 1 hour
- Need is to identify realistic values
 - Use Cases to identify real requirements
- Have established methods to calculate for hardware
- Problems with applying to Software
 - Integrated systems
 - Systems of Systems
- Need to use Error Detection and Recovery so Faults do not cause Failures

Safety and Security

- All Systems need Safety and Security Cases
 - Standard process
 - Follow Certification Authority Guides
 - Identified threats
 - Proposed solution
 - minimise foot print
 - Present solution to authority
 - Get approval
 - Implement Solution
 - Present to Authority
 - Authority testing
 - Recommend for certification
- Main issue is projects not realising Safety and Security need addressing as part of the solution

Use of COTS

- Some systems have > 30 COTS Packages
- Design system based on COTS
- Issues
 - COTS 'Warranty'???
 - No published QoS
 - Dependability of COTS product not known
 - Depends on use
 - Dependencies between COTS and versions of COTS
 - How to express/measure/model dependability of system composed of COTS
- Approach
 - Use experience of product/supplier
 - Reputation
 - Get COTS in early to test out

Sub-Contracts

- Issues
 - Specification of Dependability
 - Assess process maturity of suppliers
 - Use CMMI for assessment
 - Assess maturity of Product
 - Current use
 - Development of current product
 - New development
 - Integration into Prime System
 - Responsibility
- Approach
 - Early Trials and Integration
 - Design Reviews
 - Testing
- Configuration

Accountability

- Legal Responsibility
 - Managing Director
 - Chief Engineer
 - System Design Authority
 - Chartered Engineers where possible
- Design Certificates
 - Internal process to ensure
 - Required processes are followed
 - Required evidence is obtained/maintained
 - Design Reviews are held
 - Actions are completed
 - Requirements are met
 - Certification obtained
 - Limitations of use are stated
 - System and all Design Information is under Configuration Control
- Limitations on use
 - Define use of product as delivered
 - Provided to the Customer

Summary

- Types of Systems we deal with
- Why do we need Integrity
- Influences on Dependability
- Specifying Dependability
 - Availability
 - Safety and Security
- Issues
 - Use of COTS
 - Sub-Contracts
 - Approach to Delivering Dependability

BAE Systems Integrated System Technologies (Insyte) Limited
Victory Point
Lyon Way, Frimley, Camberley
Surrey, GU16 7EX
United Kingdom
Telephone +44 (0) 1276 603000
Fax +44 (0) 1276 603001

email insyte@baesystems.com
www.baesystems.com/insyte

