Role of Testing Professionals in Building a Safe and Secure India

shinto.joseph@ldra.com

LDRA
Tool Suite
Delivering Software Quality and Security through
Test, Analysis & Requirements Traceability

Agenda

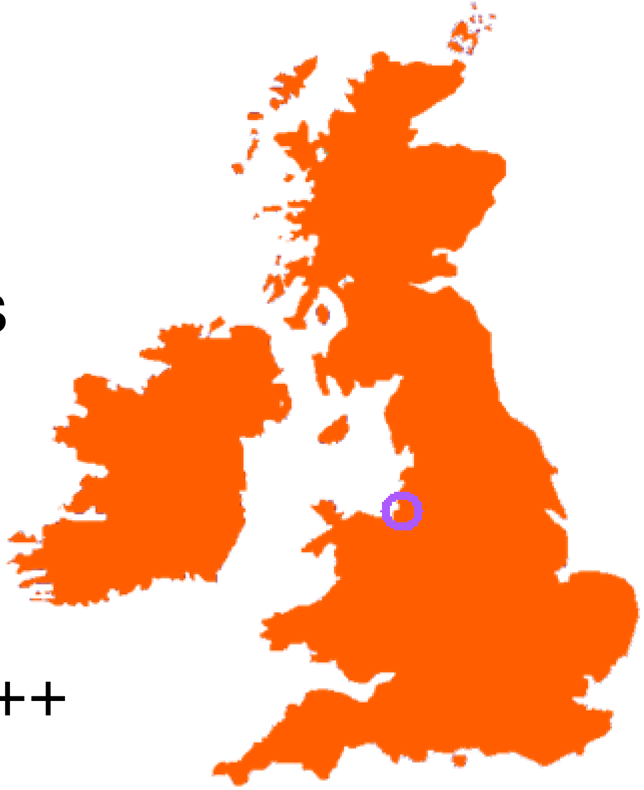
- LDRA Introduction
- Global Safety Critical Standards
- Safety in Indian Context - A Critical Review
- Way Forward
- Questions & Answers

LDRA INTRODUCTION

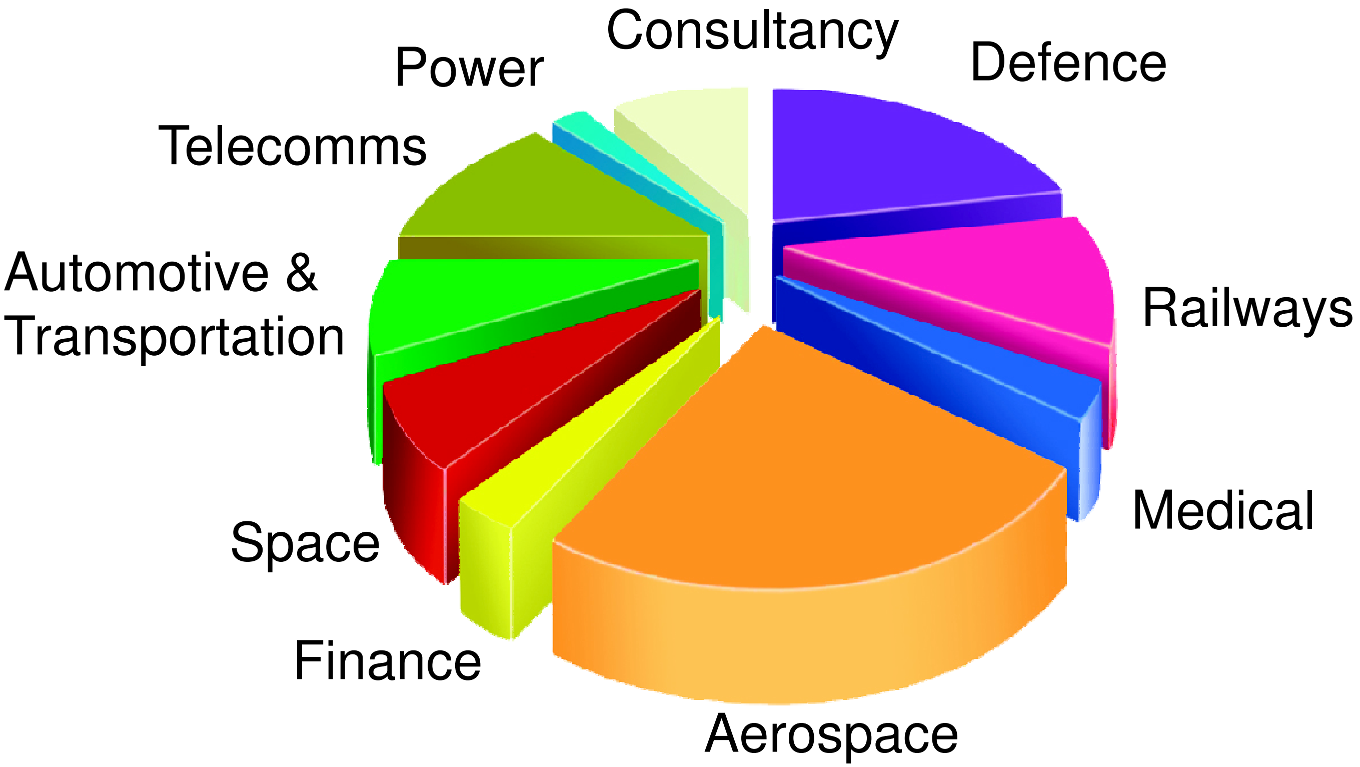
Delivering Software Quality and Security through
Test, Analysis & Requirements Traceability

LDRA Ltd

- Liverpool Data Research Associates
- Founded 1975
- Provider of Test Tools & Solutions
- Metrics Pioneer
- Consultancy, Support, Training
- Active participation in standards such as DO-178B/C, MISRA C/C++



Customer Profile



- Used by companies where the software must work correctly and where the cost of failure is very high

GLOBAL SAFETY CRITICAL STANDARDS

LDRA
Tool Suite
Delivering Software Quality and Security through
Test, Analysis & Requirements Traceability

Why Certify?

- When ever the cost of failure is very high
  - Risk of death or injury
  - High cost of repair
  - High cost of product recall

- What software needs to be certified?
  - Aircraft
  - Nuclear Power Stations
  - Trains
  - Cars
  - Medical Devices
  - Industrial Plants

Leading Safety Critical Standards

- Avionics : DO-178B / DO-178C

- Industrial : IEC 61508

– Railway	:	CENELEC EN 50128
– Nuclear	:	IEC 61513
– Automotive	:	ISO/DIS 26262
– Medical	:	IEC 62304
– Process	:	IEC 61511

DO-178B / DO-178C

LDRA
Tool Suite
Delivering Software Quality and Security through
Test, Analysis & Requirements Traceability

DO-178B

- Ensures that Avionics software performs intended functionality with an appropriate level of confidence as far as safety is concerned
- Describes the following processes:
  - Planning
  - Development
  - Verification
  - Configuration Management
  - Quality Assurance

Safety Integrity Levels

SIL	Failure Impact	Description
A	Catastrophic	Failure conditions which would prevent continued safe flight and landing
B	Hazardous	Failure conditions which would reduce the capability of the aircraft or the ability of the crew to cope with adverse operating conditions and could lead to occupants suffering serious or potentially fatal injuries to a small number of those occupants
C	Major	Failure conditions which would reduce the capability of the aircraft or the ability of the crew to cope with adverse operating conditions
D	Minor	Failure conditions which would not significantly reduce aircraft safety
E	No Effect	Failure conditions which do not affect the operational capability of the aircraft or increase crew workload

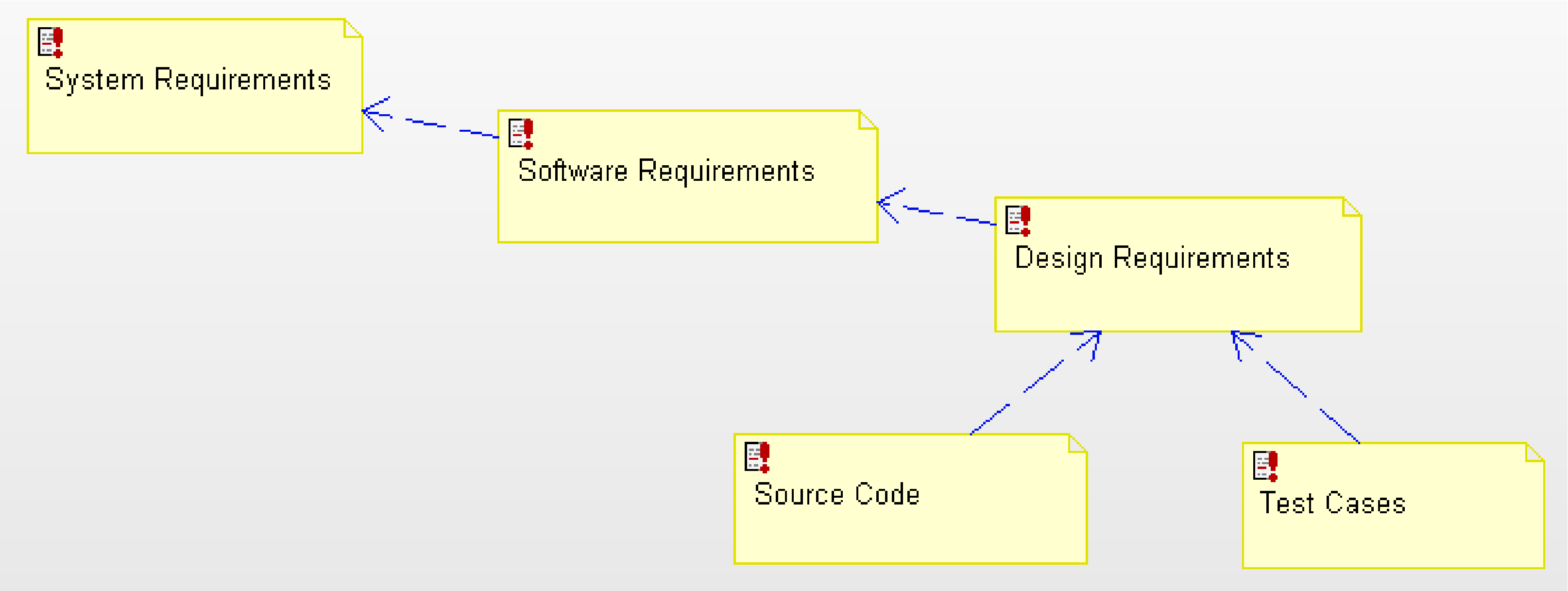
Objectives

SIL	Objectives	Objectives that must be verified with independence	Probability of failure per operating hour*
A	66	25	10^{-9}
B	65	14	10^{-7}
C	57	-	10^{-5}
D	28	-	10^{-3}
E	-	-	N/A

* FAA System Safety Handbook, Chapter 3: Principles of System Safety; December 30, 2000

Requirements Traceability

- Traceability
  - Requirements Traceability refers to the ability to link system requirements to software requirements, and then from software requirements to design requirements and then to source code and the associated test cases

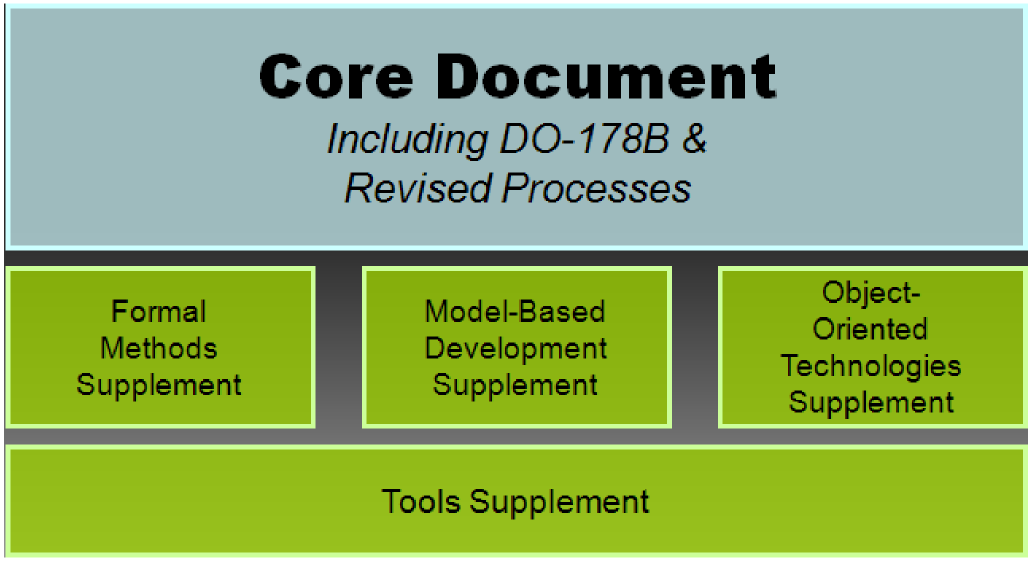


Avoid the Requirement Gap

- Process must be “right weight”
  - Not too heavy, not too light
  - Help rather than hinder
  - No bias to particular disciplines or phases
- Focus on requirements
  - Don’t ignore them once construction begins
  - Implement what the stakeholder wants
- Manage requirements
  - Continually refine
  - Apply quality criteria
- Trace requirements

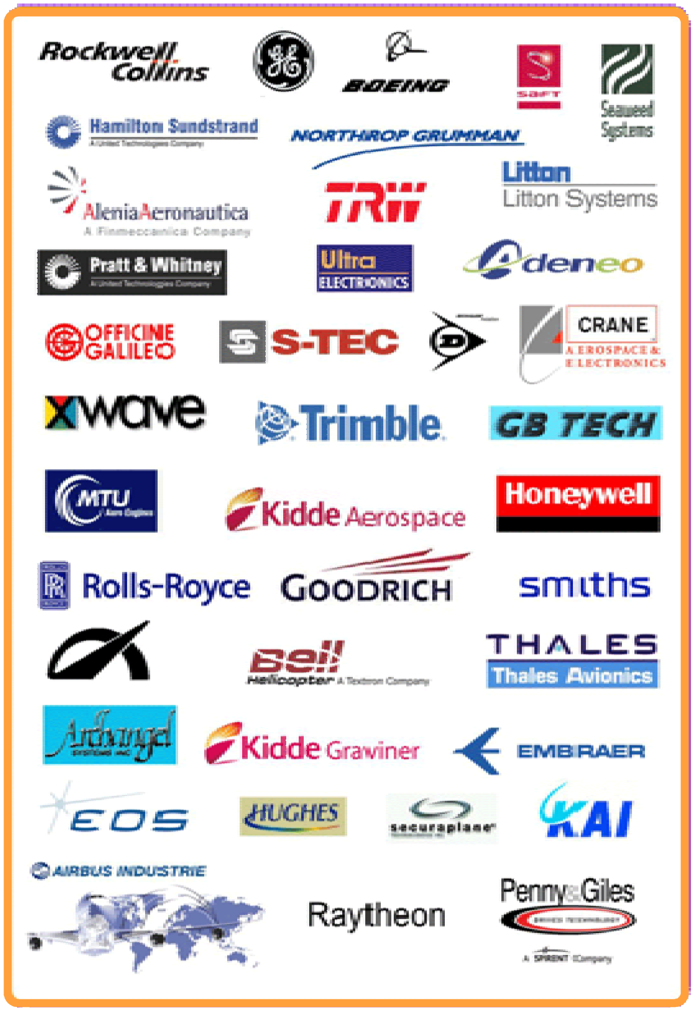
DO-178C

- Updated version of DO-178B
  - Support for Formal Methods
  - Support for Model Based Development
  - Support for Object Oriented Technologies


Core Document
Including DO-178B &
Revised Processes
Formal Methods Supplement
Model-Based Development Supplement
Object-Oriented Technologies Supplement
Tools Supplement

  - More complete Requirements Tracing
  - Security

LDRA in the Air



Lockheed Martin F-35 Lightning II (JSF)

© Lockheed Martin

Boeing 787

© Boeing

Eurofighter Typhoon

© Eurofighter

Airbus A380

© Airbus

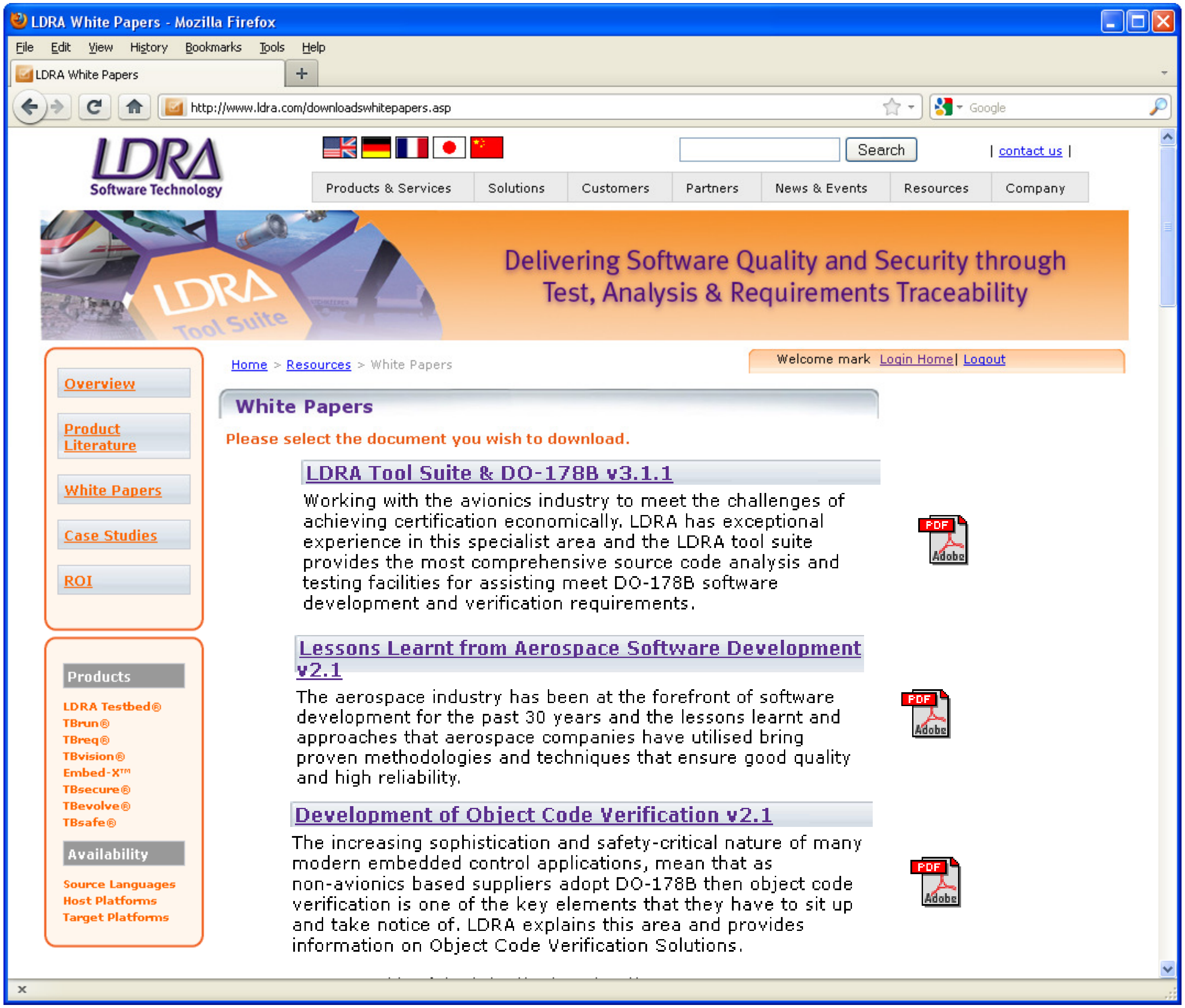
Digital Automatic Flight Control for Eclipse 500™ jetSystem supplied by S-TEC

© Eclipse Aviation

Auto Pilot Software for SJ30-2 twin engine jet supplied by Honeywell

© Sino Swearingen

LDRA White Papers



White Papers

Please select the document you wish to download.

LDRA Tool Suite & DO-178B v3.1.1

Working with the avionics industry to meet the challenges of achieving certification economically. LDRA has exceptional experience in this specialist area and the LDRA tool suite provides the most comprehensive source code analysis and testing facilities for assisting meet DO-178B software development and verification requirements.

Lessons Learnt from Aerospace Software Development v2.1

The aerospace industry has been at the forefront of software development for the past 30 years and the lessons learnt and approaches that aerospace companies have utilised bring proven methodologies and techniques that ensure good quality and high reliability.

Development of Object Code Verification v2.1

The increasing sophistication and safety-critical nature of many modern embedded control applications, mean that as non-avionics based suppliers adopt DO-178B then object code verification is one of the key elements that they have to sit up and take notice of. LDRA explains this area and provides information on Object Code Verification Solutions.

IEC 61508

LDRA
Tool Suite
Delivering Software Quality and Security through
Test, Analysis & Requirements Traceability

IEC 61508

- Generic Industrial Standard that is also a basis for Industrial specific standards such as:

– Railway	:	CENELEC EN 50128
– Nuclear	:	IEC 61513/68808
– Automotive	:	ISO/DIS 26262
– Medical	:	IEC 62304
– Process	:	IEC 61511

- Risk based approach
  - Safety Integrity Levels

- Latest version: IEC 61508:2010

Safety Integrity Levels

- SIL level 1 to 4
- A risk assessment would generally be done for every software project to understand the required safety level
- The higher the safety level, then the more rigor the process needs to be and the more thorough testing will be necessary
- Each SIL effectively reduces the risk by a factor of 10
- SIL level 3 is the highest level that can be achieved with a single component, level 4 requires hardware redundancy of level 3 components

Functional Safety Assessment

Minimum Level of Independence	Safety Integrity Level			
	1	2	3	4
Independent Person	HR	HR	NR	NR
Independent Department	-	HR	HR	NR
Independent Organization	-	-	HR	HR

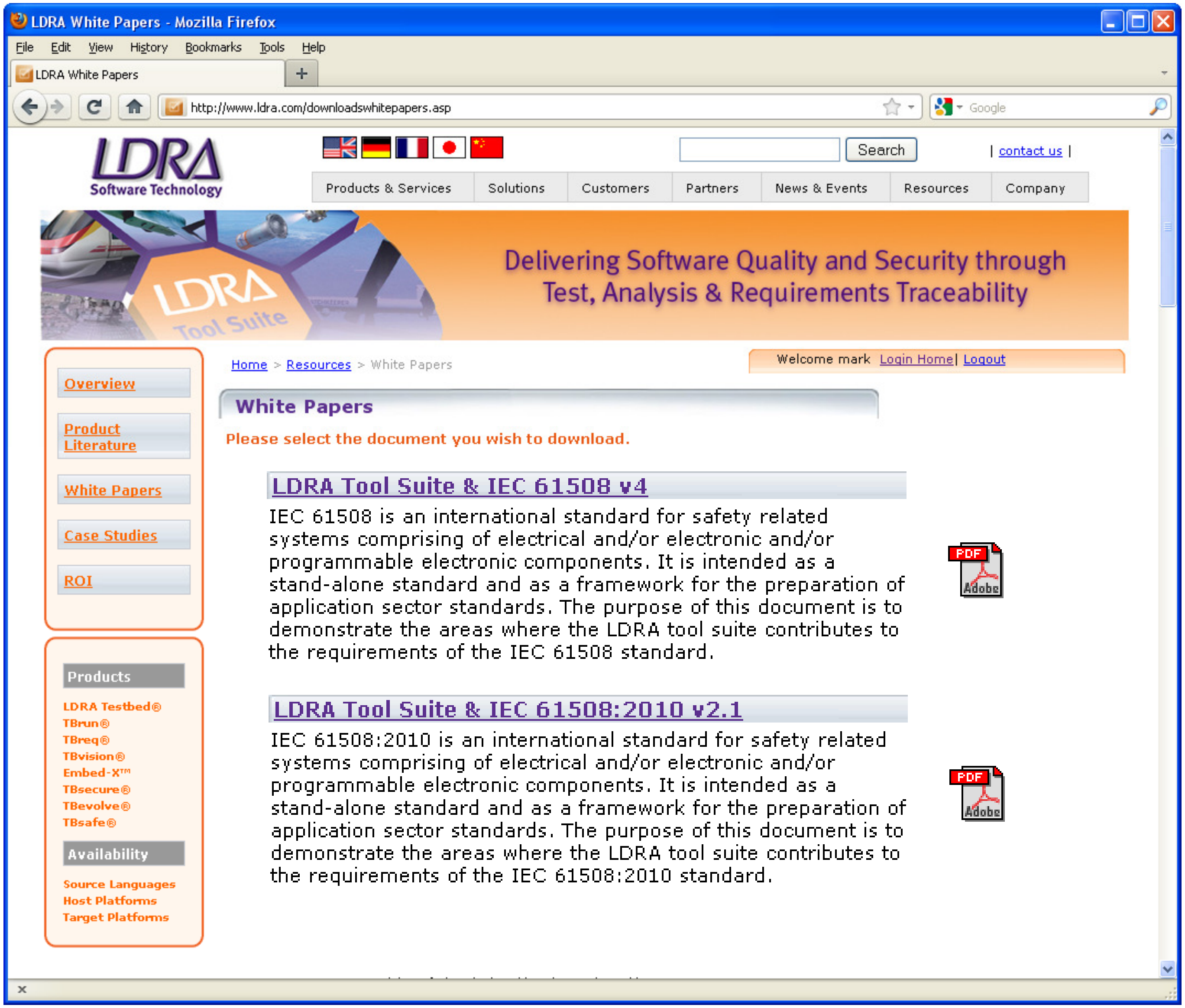
Table 2: Assessment independence level for E/E/PE and software life cycle activities

(E/E/PE) : Electrical / Electronic / Programmable Electronic systems

IEC 61508

- The IEC 61508 Guidelines are primarily process oriented, and includes guidelines for the Verification and Validation (V&V) elements of that process
- The complete IEC 61508 standard comprises of 7 parts of which Part 3 defines the software requirements and sets out the safety lifecycle for software, including validation and verification, and makes recommendations regarding tools and methods which are appropriate for each SIL
- The standard requires that a number of V&V activities shall be performed, including:
  - Verification of code
  - Software module testing
  - Software integration testing

LDRA White Papers



White Papers

Please select the document you wish to download.

LDRA Tool Suite & IEC 61508 v4

IEC 61508 is an international standard for safety related systems comprising of electrical and/or electronic and/or programmable electronic components. It is intended as a stand-alone standard and as a framework for the preparation of application sector standards. The purpose of this document is to demonstrate the areas where the LDRA tool suite contributes to the requirements of the IEC 61508 standard.

LDRA Tool Suite & IEC 61508:2010 v2.1

IEC 61508:2010 is an international standard for safety related systems comprising of electrical and/or electronic and/or programmable electronic components. It is intended as a stand-alone standard and as a framework for the preparation of application sector standards. The purpose of this document is to demonstrate the areas where the LDRA tool suite contributes to the requirements of the IEC 61508:2010 standard.

ISO/DIS 26262 (ISO 26262)

LDRA
Tool Suite
Delivering Software Quality and Security through
Test, Analysis & Requirements Traceability

Expensive Recalls

2007

- Volvo recalls 18,000 cars after Euro NCAP found side-impact airbags deployed too late in minor collisions

2008

- Mercedes-Benz recalled 11 different models to fix a software problem affecting fuel gauge readings and the speedometer

2009-2011

- Toyota recalled over 9 million vehicles due to a number of problems, some of which were software problems for example: Hybrid anti-lock brake software

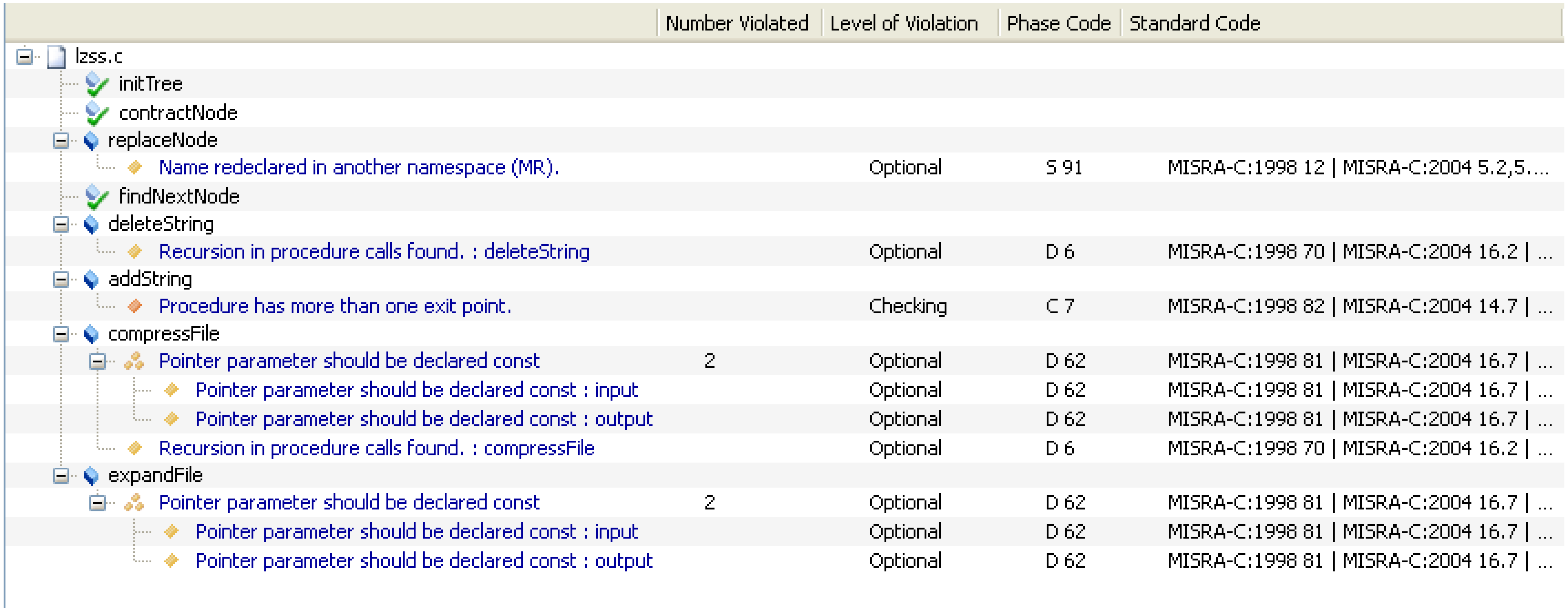
2011

- General Motors recalled more than 10000 Cadillac and Buick vehicles due to a software glitch in the climate control system

ISO 26262

- Draft International Standard
- Adaptation of the IEC 61508 generic standard
- Adapted for high volume production
- Some commonality with the DO-178B standard
- Safety is already a significant factor in the development of automobile systems
- With the ever increasing use of Electrical / Electronic / Programmable Electronic systems (E/E/PE) in areas such as driver assistance, braking and steering systems, and safety systems, this significance is set to increase

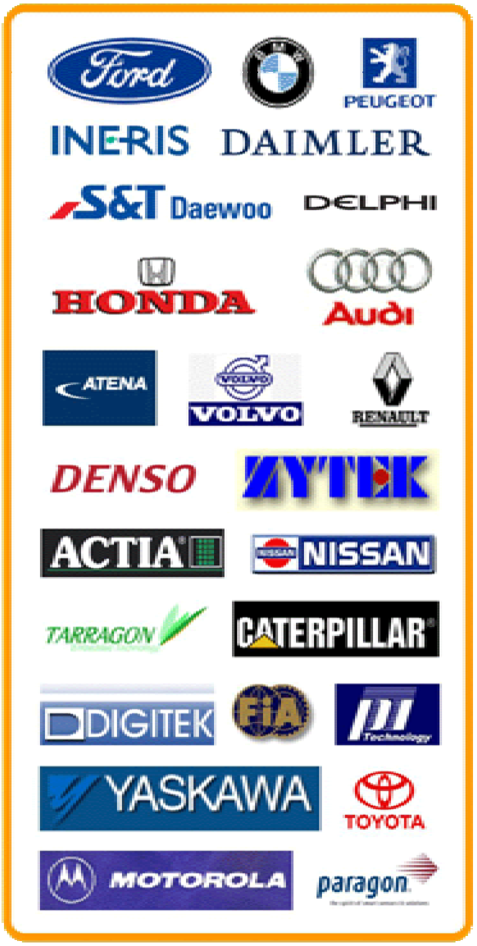
LDRA tool suite : MISRA-C:2004



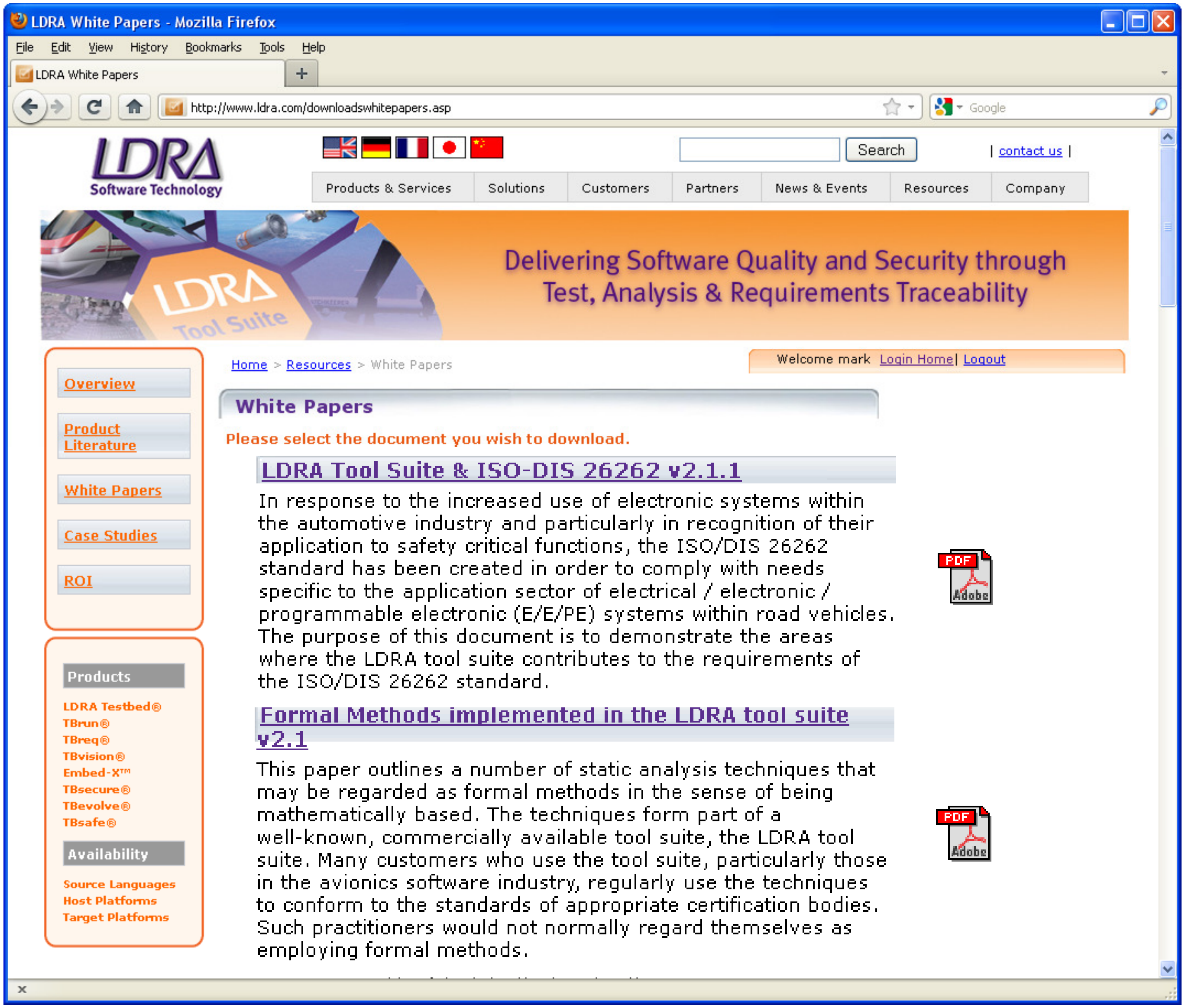
	Number Violated	Level of Violation	Phase Code	Standard Code
lzss.c				
initTree				
contractNode				
replaceNode				
Name redeclared in another namespace (MR).		Optional	S 91	MISRA-C:1998 12 | MISRA-C:2004 5.2,5....
findNextNode				
deleteString				
Recursion in procedure calls found. : deleteString		Optional	D 6	MISRA-C:1998 70 | MISRA-C:2004 16.2 | ...
addString				
Procedure has more than one exit point.		Checking	C 7	MISRA-C:1998 82 | MISRA-C:2004 14.7 | ...
compressFile				
Pointer parameter should be declared const	2	Optional	D 62	MISRA-C:1998 81 | MISRA-C:2004 16.7 | ...
Pointer parameter should be declared const : input		Optional	D 62	MISRA-C:1998 81 | MISRA-C:2004 16.7 | ...
Pointer parameter should be declared const : output		Optional	D 62	MISRA-C:1998 81 | MISRA-C:2004 16.7 | ...
Recursion in procedure calls found. : compressFile		Optional	D 6	MISRA-C:1998 70 | MISRA-C:2004 16.2 | ...
expandFile				
Pointer parameter should be declared const	2	Optional	D 62	MISRA-C:1998 81 | MISRA-C:2004 16.7 | ...
Pointer parameter should be declared const : input		Optional	D 62	MISRA-C:1998 81 | MISRA-C:2004 16.7 | ...
Pointer parameter should be declared const : output		Optional	D 62	MISRA-C:1998 81 | MISRA-C:2004 16.7 | ...

- LDRA has played an active role on the MISRA C++ committee by having committee members and the chairman as part of the committee
- LDRA is also represented on the MISRA C committee with three members of the LDRA technical team

LDRA on the Road



LDRA White Papers



White Papers

Please select the document you wish to download.

LDRA Tool Suite & ISO-DIS 26262 v2.1.1

In response to the increased use of electronic systems within the automotive industry and particularly in recognition of their application to safety critical functions, the ISO/DIS 26262 standard has been created in order to comply with needs specific to the application sector of electrical / electronic / programmable electronic (E/E/PE) systems within road vehicles. The purpose of this document is to demonstrate the areas where the LDRA tool suite contributes to the requirements of the ISO/DIS 26262 standard.

Formal Methods implemented in the LDRA tool suite v2.1

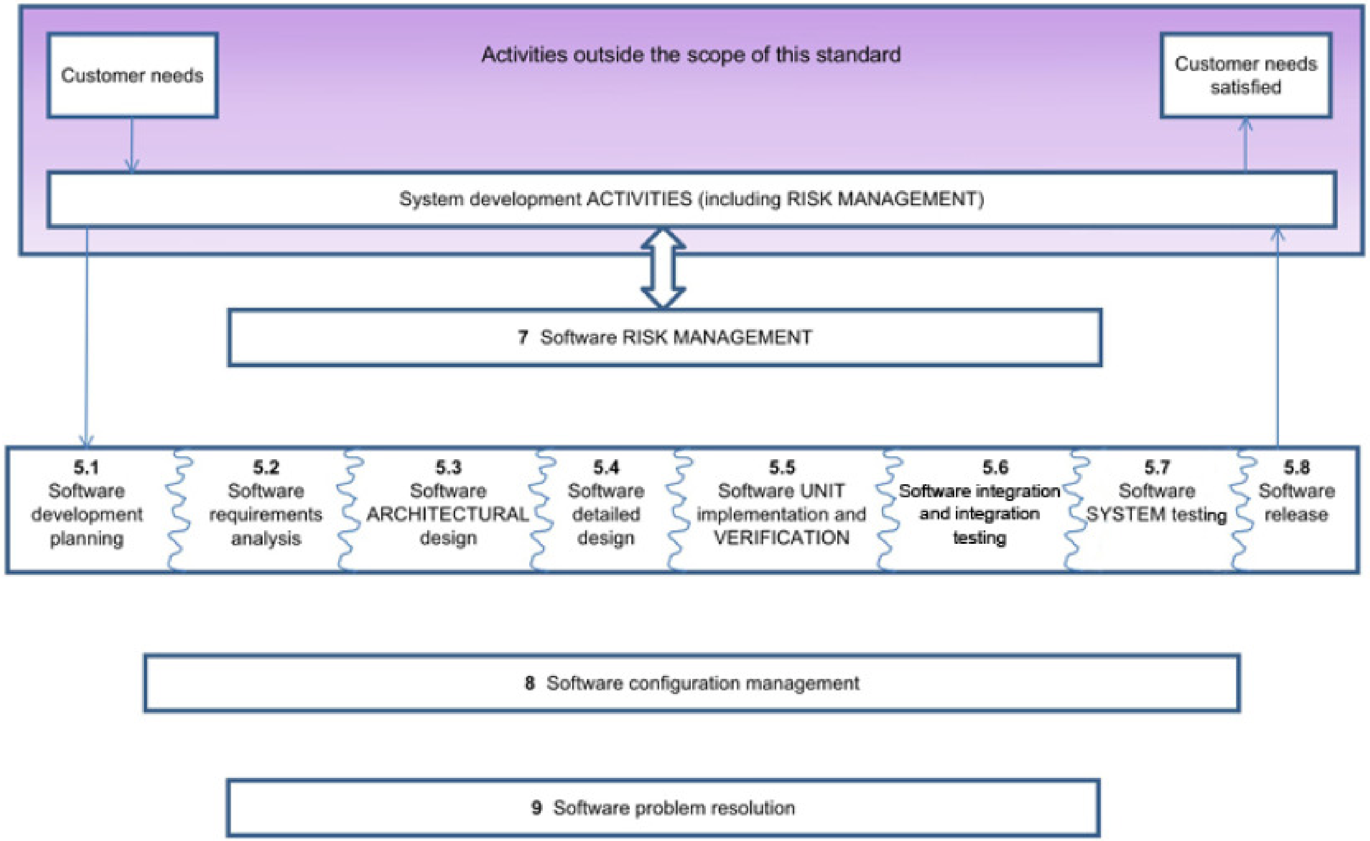
This paper outlines a number of static analysis techniques that may be regarded as formal methods in the sense of being mathematically based. The techniques form part of a well-known, commercially available tool suite, the LDRA tool suite. Many customers who use the tool suite, particularly those in the avionics software industry, regularly use the techniques to conform to the standards of appropriate certification bodies. Such practitioners would not normally regard themselves as employing formal methods.

IEC 62304

LDRA
Tool Suite
Delivering Software Quality and Security through
Test, Analysis & Requirements Traceability

IEC 62304 : Common Framework

- The set of processes, activities, and tasks described in this standard establishes a common framework for medical device software life cycle processes



Activities outside the scope of this standard

Customer needs

Customer needs satisfied

System development ACTIVITIES (including RISK MANAGEMENT)

7 Software RISK MANAGEMENT

5.1 Software development planning

5.2 Software requirements analysis

5.3 Software ARCHITECTURAL design

5.4 Software detailed design

5.5 Software UNIT implementation and VERIFICATION

5.6 Software integration and integration testing

5.7 Software SYSTEM testing

5.8 Software release

8 Software configuration management

9 Software problem resolution

IEC 62304 : Clause 5

- IEC 62304 Clause 5 details the software development process of the product. It specifically addresses:

	Process
5.1	Software development planning
5.2	Software requirements analysis
5.3	Software architectural design
5.4	Software detailed design
5.5	Software unit implementation and verification
5.6	Software integration and integration testing
5.7	Software system testing
5.8	Software release

IEC 62304 : Clause 6

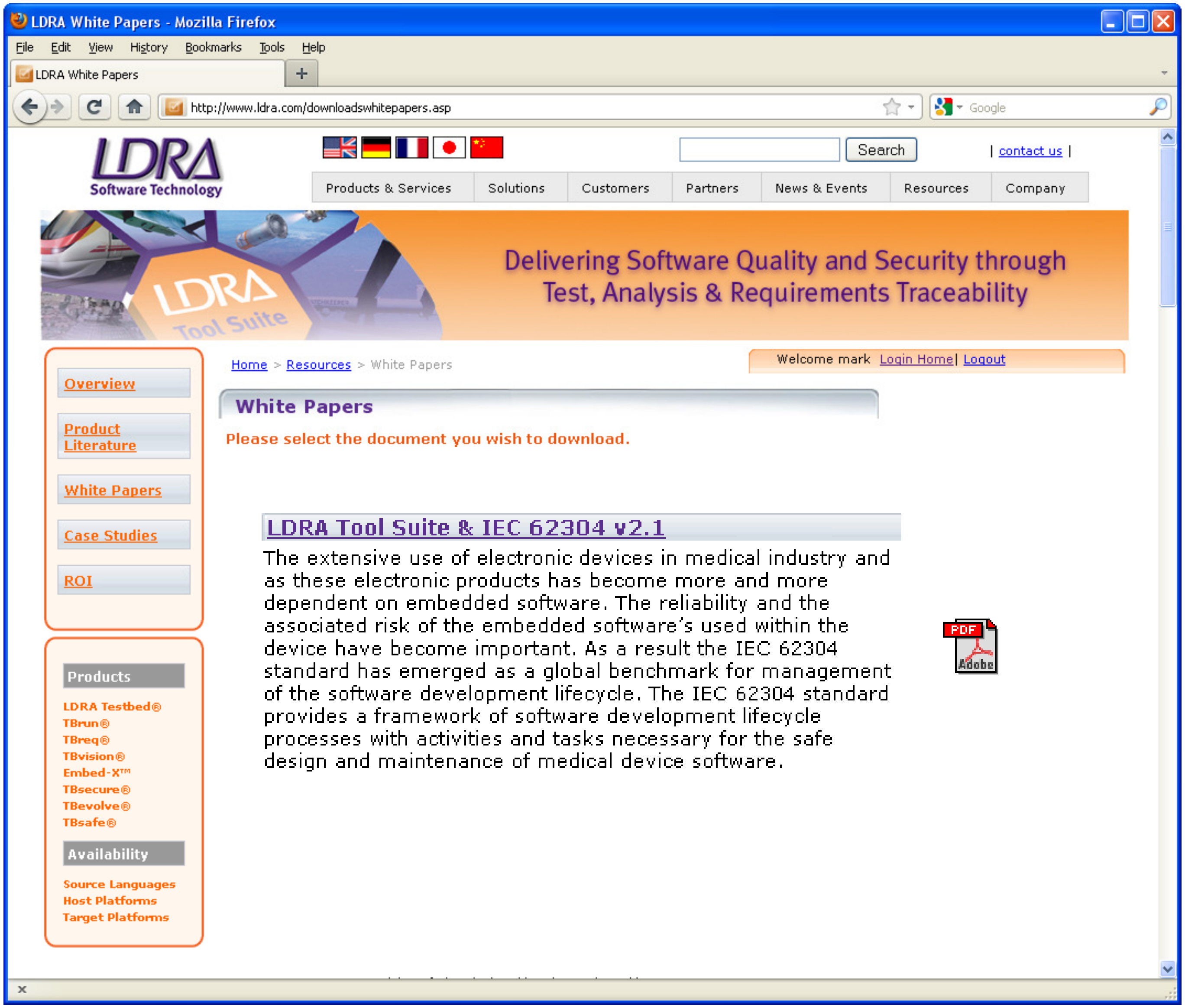
- An analysis made by FDA on 3140 medical device recalls conducted between 1992 and 1998 found:
  - 7.7% are attributable to software failures
  - Of those software related recalls, 79% were because of defects introduced during software upgrades
- IEC 62304 Clause 6 addresses the issues of software maintenance

Safety Integrity Levels

- The IEC 62304 standard expects the manufacturer to assign a safety class to the software system as a whole
- This classification is based on the potential to create a hazard that could result in an injury to the user, the patient or other people
- The software is classified into three classes:

Class	Failure Impact
A	No injury or damage to health is possible
B	Non serious injury is possible
C	Death or serious injury is possible

LDRA White Papers



Delivering Software Quality and Security through Test, Analysis & Requirements Traceability

White Papers

Please select the document you wish to download.

LDRA Tool Suite & IEC 62304 v2.1

The extensive use of electronic devices in medical industry and as these electronic products has become more and more dependent on embedded software. The reliability and the associated risk of the embedded software's used within the device have become important. As a result the IEC 62304 standard has emerged as a global benchmark for management of the software development lifecycle. The IEC 62304 standard provides a framework of software development lifecycle processes with activities and tasks necessary for the safe design and maintenance of medical device software.

IEC 60730

LDRA
Tool Suite
Delivering Software Quality and Security through
Test, Analysis & Requirements Traceability

IEC 60730

- The IEC 60730-1 Ed. 4.0 b:2010 safety standard for household appliances is designed for automatic electronic controls, to ensure safe and reliable operation
- Part 1 : General requirements
- Example Applications:
  - Cooking Products
  - Dishwashers
  - Dryers
  - Refrigerators and Freezers
  - Vacuum Cleaners
  - Washing Machines
  - Boiler and Heater Control
  - Gate Opening
  - Household Actuators
  - Motor Control
  - Lift and Elevators

IEC 60730 : Classifications

- IEC 60730 segments automatic control products into three different classifications:
  - Class A: Not intended to be relied upon for the safety of the equipment
  - Class B: To prevent unsafe operation of the controlled equipment
  - Class C: To prevent special hazards

SAFETY IN INDIAN CONTEXT

LDRA
Tool Suite
Delivering Software Quality and Security through
Test, Analysis & Requirements Traceability

Indian Scenario

- Growing Indian economy with a global ambition
- Lack of safety awareness
- Gap between local and global practices
- Role of Regulators
  - Civil Aviation – DGCA
  - Defense Avionics - CEMILAC & RCMAs
  - Nuclear - AERB
  - Rail - RDSO
  - Automotive - ARAI
  - Medical Device - ?

Way Forward

- Skill development
- Need for a healthy ecosystem, backed by long term Govt. policies encouraging domestic design, development and manufacturing
- Role of:
  - Technology vendors
  - Global players
  - Indian companies
  - Industry bodies
- Committed engineers ready to work on Indian projects

ARE WE READY?

LDRA
Tool Suite
Delivering Software Quality and Security through
Test, Analysis & Requirements Traceability

LDRA

For further information visit:

www.ldra.com

shinto.joseph@ldra.com
india@ldra.com

LDRA
Tool Suite
Delivering Software Quality and Security through
Test, Analysis & Requirements Traceability