Software Safety and Certification

presented to

IEEE Spring Switchgear Committee Meeting
Luncheon Seminar
4 May, 2004

by

Howard Cox
Underwriters Laboratories

Copyright © 2004 Underwriters Laboratories, Inc.

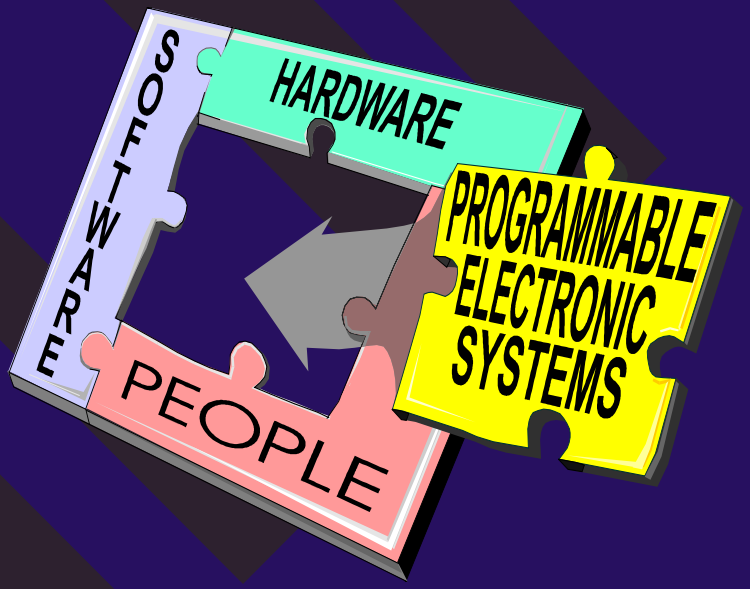
What we will cover...

- Functional Safety Concepts
  - from IEC 61508
- The Second Edition of UL 1998
  - The Standard for Software in Programmable Components
- UL's Software Certification Process

Copyright © 2004 Underwriters Laboratories, Inc.

Functional Safety Standards

- UL 1998
- IEC 61508
- UL 991
- IEC 60730-1
- UL End-product Standards



Copyright © 2004 Underwriters Laboratories, Inc.

What is Functional Safety?

IEC 61508-4

3.1.9 functional safety:

part of the overall safety relating to the EUC and the EUC control system which depends on the correct functioning of the E/E/PE safety-related systems, other technology safety-related systems and external risk reduction facilities

EUC = Equipment Under Control
E/E/PE - Electrical/Electronic/Programmable Electronic

Copyright © 2004 Underwriters Laboratories, Inc.

What is Functional Safety?

ANSI/UL 1998 Second Edition
2.45 safety-related functions:

Control, protection and monitoring functions that are intended to reduce the risk of fire, electric shock, or injury to persons.

Copyright © 2004 Underwriters Laboratories, Inc.

Role of E/E/PE Safety-related Systems

A safety-related system both:

- implements the required safety functions necessary to achieve a safe state for the equipment under control or to maintain a safe state for the equipment under control; and,

- is intended to achieve, on its own or with other E/E/PE safety-related systems, other technology safety-related systems or external risk reduction facilities, the necessary safety integrity for the required safety functions.

Copyright © 2004 Underwriters Laboratories, Inc.

Functional Safety of Programmable Systems

- Safety functions were carried out by electro-mechanical or solid state devices
- Programmable Electronics then began to replace the use of hard-wired systems
- It was proven that testing alone was not sufficient for achieving safety
- Engineering consensus defined a need for new design and assessment methodologies

Copyright © 2004 Underwriters Laboratories, Inc.

System Safety & Software Safety

- Draws from IEC 61508 and other recognized standards, such as IEC 60730-1 and ANSI/UL 1998
- Design safety into the entire system
- Software is a subsystem
- Addresses all design and development phases

Copyright © 2004 Underwriters Laboratories, Inc.

System Safety & Software Safety:
Scope & Applicability

- IEC 61508 not intended for application to *Low Complexity Systems*
- IEC 61508 applies to systems including:
  - Emergency shut-down systems, gas- and oil- fired BMS's, dynamic positioning systems, signaling systems, etc…
  - PLCs, embedded controllers, firmware, PGAs, ASICs, and other configurable PEs

Copyright © 2004 Underwriters Laboratories, Inc.

System Safety & Software Safety:

Scope & Applicability

- Intended for systems utilizing PE
- Addresses system protection layers and devices (LOPA) analysis
- Addresses ALARP principle

Copyright © 2004 Underwriters Laboratories, Inc.

System Safety: Approach

- Presents minimum set of processes, techniques, and methods for a safety life cycle
- provides uniform recommendations including a hazard identification methodology
- aids in management, technical aspects and generation of safety plans

Copyright © 2004 Underwriters Laboratories, Inc.

System Safety: Structure

- Introduction/Background
- Management of Functional Safety
- Safety Life Cycle Overview
- Safety Life Cycle Phases
- Safety File
- Independent Assessment

Copyright © 2004 Underwriters Laboratories, Inc.

Safety Introduction

- Introductory report for the industry
- Basic system/software safety concepts
- Discusses need to address functional safety
- Describes benefits of implementing a system/software safety program

Copyright © 2004 Underwriters Laboratories, Inc.

Software Safety: Structure

- Software Safety Plan Framework
- Documents
- Software Safety Activities
- Information on Methods and Techniques
- References

Copyright © 2004 Underwriters Laboratories, Inc.

Software Safety: Approach

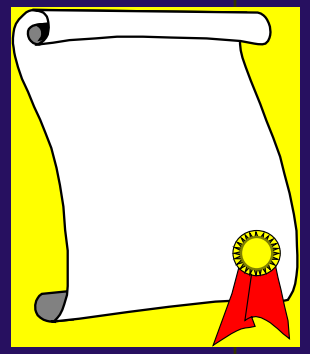
- Hazards identified associated with System Safety
- Risk analysis to determine what is to be controlled and to what degree
- Control determined in accordance with Safety Integrity Level Criteria (SIL)

Copyright © 2004 Underwriters Laboratories, Inc.

Safety File

"Proof of Safety"

"A documented body of evidence that provides a convincing and valid argument that a system is adequately safe for a given application in a given environment."



Copyright © 2004 Underwriters Laboratories, Inc.

Safety File

- Written documentation and supporting engineering data that demonstrate:
  - satisfaction of specific safety requirements of the system
  - justification of engineering and management approaches to safety issues
  - conformance to recognized standards

Copyright © 2004 Underwriters Laboratories, Inc.

Independent Assessment

- Guidance for determining the completeness and suitability of the safety evidence and justifications

Copyright © 2004 Underwriters Laboratories, Inc.

Safety Framework Guidance

- Supplements the safety framework reports
- Provides additional information to users
- Help in applying the safety framework
- Describes methodologies
- Gives examples and references

Copyright © 2004 Underwriters Laboratories, Inc.

UL 1998 Preface

- UL 1998 Requirements are to be referenced by:
  - product safety and performance requirements in a regulation, directive, or a purchasing specification
- Risks that must be considered are identified by:
  - safety and performance standards
  - purchasers
  - users

Copyright © 2004 Underwriters Laboratories, Inc.

UL 1998 Preface (cont.)

- UL 1998 avoids the specification of testing protocols and tools:
  - diversity of software functions results in a diversity of test harness
- UL 1998 instead indicates test objectives and criteria
- Benefits of this Meta-Level Approach:
  - maximum flexibility in optimizing test solutions to meet safety objectives

Copyright © 2004 Underwriters Laboratories, Inc.

2. Definitions of Terms Used

- IEEE Std. 610.12-1990

  The IEEE Standard Glossary of Software Engineering Terminology

- IEC 61508

  Functional safety : safety-related systems.

  Part 4 : Definitions and Abbreviations of Terms

Copyright © 2004 Underwriters Laboratories, Inc.

Definitions

Non-Networked Embedded Software

Embedded software that executes on a single microprocessor/microcontroller or on multiple microprocessors/ microcontrollers residing in the same physical system.

Programmable Components

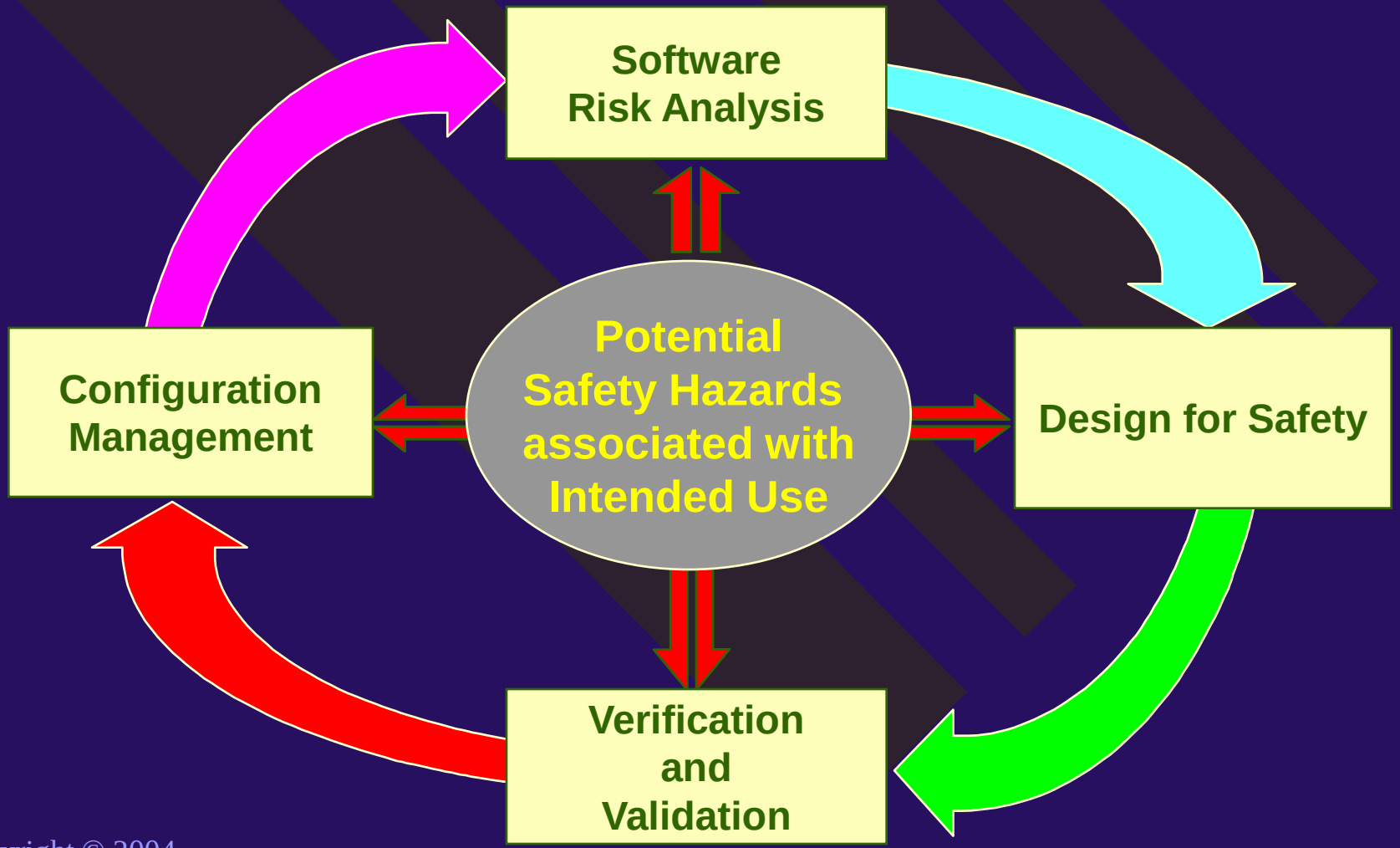
Microelectronic hardware that can be programmed in the design center, the factory, or in the field.

Safety-Related Functions

Control, protection and monitoring functions that are intended to reduce the risk of fire, electric shock, or injury to persons.

Copyright © 2004 Underwriters Laboratories, Inc.

UL 1998 CORE REQUIREMENTS



Copyright © 2004
Underwriters
Laboratories, Inc.

3. Risk (Hazard) Analysis

Risk Analysis answers the questions....

- What is potentially harmful ?
- How could this situation arise?
- How is this risk addressed?

Copyright © 2004 Underwriters Laboratories, Inc.

HAZARD ANALYSIS TECHNIQUES

- Fault Tree Analysis (FTA)
- Failure Mode and Effects Analysis (FMEA)
- Other Equivalent Methods

Copyright © 2004 Underwriters Laboratories, Inc.

Fault Tree Analysis (FTA)

- Deductive method starting with an identified hazard (from the hazard list) and examines combinations of contributing events to this hazard by tracing the pathway into the product

Copyright © 2004 Underwriters Laboratories, Inc.

Limitations of FTA

- Originally intended for hardware
- Based on assumptions
  - Events are sequential
  - Hardware and software are discrete
  - Prior knowledge of product design

Copyright © 2004 Underwriters Laboratories, Inc.

Failure Mode and Effects Analysis (FMEA)

- Starts with an identified hazard
- Assumes a component failure mode, and predicts the local and system effects
- Assigns a mitigation method
  - Predicts the change in the local and system effects
  - Predicts a reduction in the severity of the identified hazard

Copyright © 2004 Underwriters Laboratories, Inc.

Limitations of FMEA

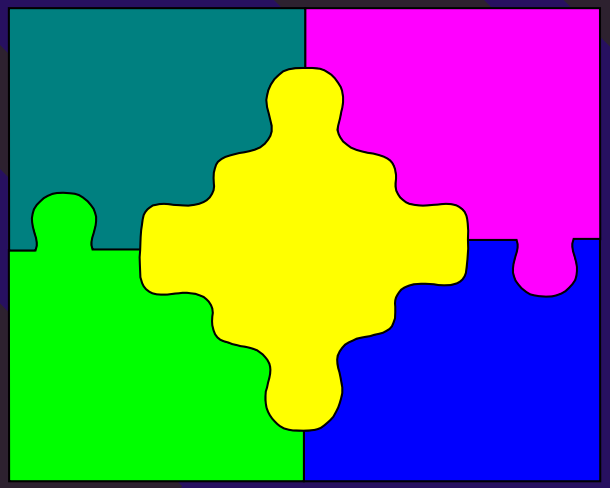
- Originally intended for hardware production and/or production process analysis
- Based on assumptions
  - Events are sequential and predictable
  - Hardware and software are discrete
  - Prior knowledge of product design or process steps
- Infinite number of possible component failures
- Each process step needs to be analyzed with separate FMEA

Copyright © 2004 Underwriters Laboratories, Inc.

LIFE-CYCLE PHASES

EXAMPLES

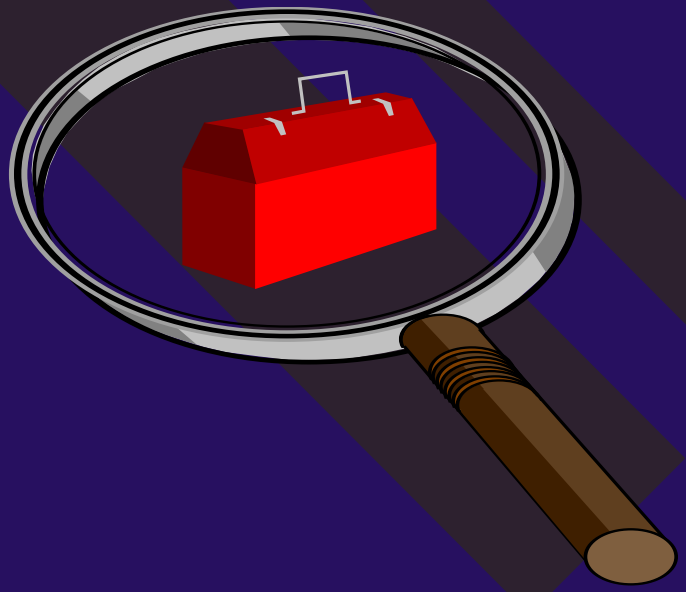
- Requirements
- Design
- Implementation
- Installation
- Operation and maintenance



Copyright © 2004 Underwriters Laboratories, Inc.

5. Tool Qualification

- "5.1 Evidence of tool qualification shall be provided…"



Copyright © 2004 Underwriters Laboratories, Inc.

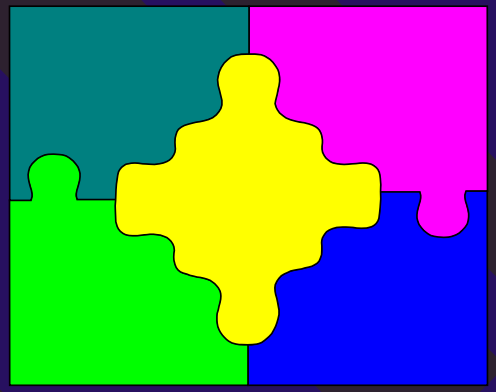
Tool Qualification Examples

- Calibration
- Errata Sheets / Bug Lists from Vendors
- Internal Verification / Audits
- Third Party Tool Certification Program

Copyright © 2004 Underwriters Laboratories, Inc.

6. Software Design

- Single point failures
- Fault detection
- System response
- Routine Priorities
- Non-terminating or non-deterministic states
- Software libraries, OS, kernels, et. al.



Copyright © 2004 Underwriters Laboratories, Inc.

Attributes of a Safety-Related Design

- Traceable to hazard analysis and requirement specifications
- Verifiable, testable, maintainable
- Well defined interfaces; sw/sw, hw/sw
- Safety-critical functions partitioned from non-safety-critical functions
- Initialization of variables to non-hazardous state
- Predictable non-hazardous system failure states

Copyright © 2004 Underwriters Laboratories, Inc.

Attributes to be Identified

- Fault-handling functions and routines
- Risk-addressed state and state transitions
- Redundant safety-related software functions
- Redundant safety-related hardware functions
- Self diagnosis routines at start-up and during run-time
- Data integrity

Copyright © 2004 Underwriters Laboratories, Inc.

7. Critical and Supervisory Sections of Software

- Requirements include
  - Partitioning
  - Addressing
  - Supervisory section
  - Software initialization

Copyright © 2004 Underwriters Laboratories, Inc.

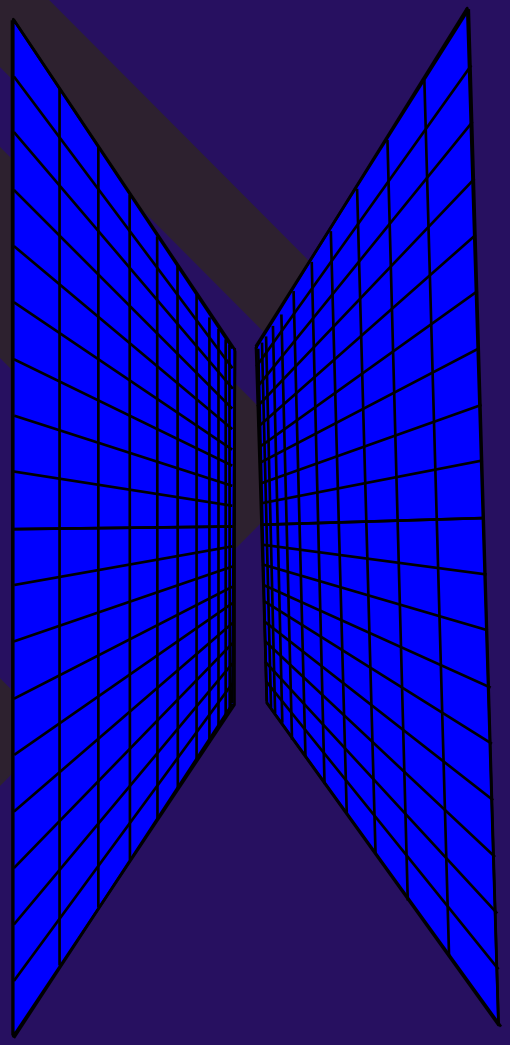
Should You Partition ?

- In complex products:
  - It demonstrates design control over safety-related software, where critical components have been minimized
  - It provides a scope for conducting the software review thus reducing the costs of development and compliance
  - It allows UL to structure a practical program that is able to accommodate software updates (reduces maintenance review time)

Copyright © 2004 Underwriters Laboratories, Inc.

Safety Partitioning

- Defined interfaces between logical partitions such as modules
- Defined information flow across the interface
- Examination of shared resources, such as registers, timers, variables
- Interface exclusivity



Copyright © 2004 Underwriters Laboratories, Inc.

8. Software Measures to Address Microelectronic H/W Failure Modes

- "8.1 Measures shall be provided to detect all microelectronic hardware failure modes documented by the Risk Analysis.

★APPENDIX A - Table A2.1 provides examples of acceptable mitigation methods.

Copyright © 2004 Underwriters Laboratories, Inc.

8. Software Measures to Address Microelectronic H/W Failure Modes

Covers the following items:

- Registers
- Instruction Decoding & Execution
- Program Counter
- Addressing
- Data Paths
- Interrupt Handling and Execution
- Clock
- Timing
- Volatile Memory (DRAM)
- Non Volatile Memory (EEPROM)
- Input / Output

Copyright © 2004 Underwriters Laboratories, Inc.

9. Product Interface

- Addresses these key concepts:

  - Hardware Control
  - Power interruptions
  - Software Initialization
  - Software termination

Copyright © 2004 Underwriters Laboratories, Inc.

10. User Interface Design

- These requirements apply only to software that accepts user input
- Note - even a reset button may be considered “user interface.”

Copyright © 2004 Underwriters Laboratories, Inc.

11. Software Analysis and Testing

- Verification
- Validation
- Test

Copyright © 2004 Underwriters Laboratories, Inc.

Verification and Validation and Test

- Document
  - plan for each defined life-cycle phase
  - methods for doing and recording
  - acceptance criteria
- Tests
  - for functionality and performance
  - to challenge (stress) the system
- Validate system to
  - requirements specifications
  - intended uses
  - customer needs

Copyright © 2004 Underwriters Laboratories, Inc.

Verification Activities Include

- Reviews
  - Design reviews
  - Walkthroughs
- Prototyping
- Traceability matrices
  - Requirements specifications
  - Mitigation of identified hazards
- Testing

Copyright © 2004 Underwriters Laboratories, Inc.

Strategy for V & V Plan

For each identified hazard:

- Determine the categories of defects
- Plan to use a variety of verification methods
  - Add other verification methods to find more defects
  - Start with method most likely to find the largest population of defects

Copyright © 2004 Underwriters Laboratories, Inc.

V & V Document Control

- The V&V plan and methods may change as a consequence of the results of the V&V reviews and tests
- Changes must be under document control
- Results, even nonconforming results, must be kept

Copyright © 2004 Underwriters Laboratories, Inc.

Traceability

- Test cases are traceable to the hazard analysis
- For each identified hazard, that is traceable to the software, the logical pathway(s) is (are) subjected to adequate test coverage

Copyright © 2004 Underwriters Laboratories, Inc.

Validation of Software Requirements

IMPORTANT

- Validation is performed **before** delivery to the customer
- Validation is performed by personnel that are independent from the design team

Examples of Validation

- Functional and safety tests
- User acceptance tests
- Installation and checkout tests

Copyright © 2004 Underwriters Laboratories, Inc.

Sources of Faults

- Requirements
  - Errors in Conversion
- Design
  - Incorrect algorithms and interfaces
- Coding
  - Syntax errors, incorrect signs, endless loops
- Timing
  - Missed deadlines

Copyright © 2004 Underwriters Laboratories, Inc.

Manifestation of Faults

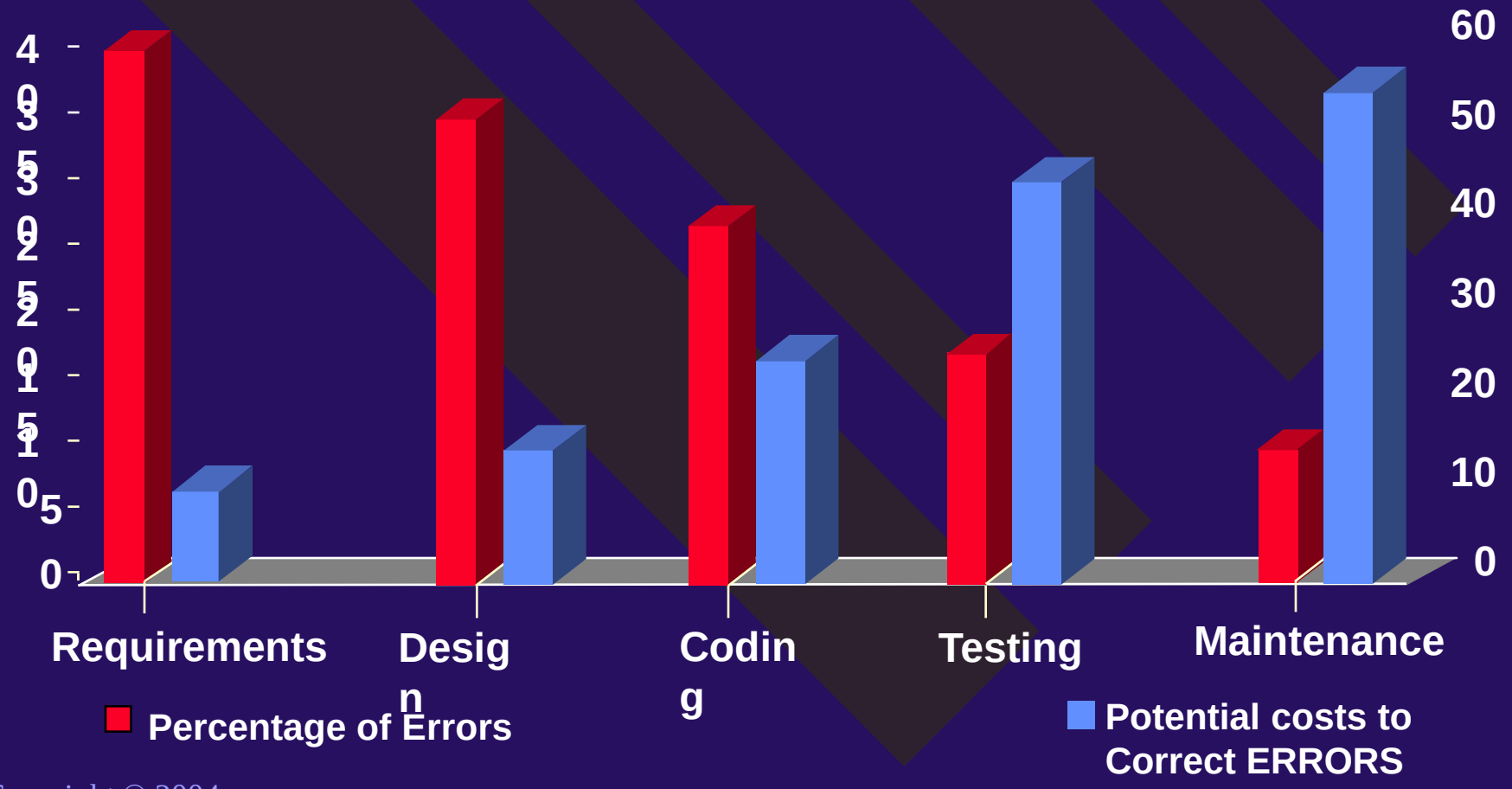
- Microelectronic Hardware
  - Not enough memory, memory overlap, memory leaks
- I/O Mismatch
- State Transition Errors
- No operation
  - Failure to perform any function at all

Copyright © 2004 Underwriters Laboratories, Inc.

SOURCE of ERRORS

ERRORS FOUND EARLY ARE EASIER TO DETECT

AND LESS EXPENSIVE TO CORRECT



Copyright © 2004 Underwriters Laboratories, Inc.

13. OTS (Off The Shelf software)

- Applicable to embedded software purchased for use in the programmable system
  - Floating point library
  - CRC calculation module
  - Operating System

Copyright © 2004 Underwriters Laboratories, Inc.

14. Software Changes

- Software changes shall not introduce risks or impact previously identified risks except to reduce or eliminate them.
- Documentation should reflect all software changes
- Changes to system configuration or supervisory software also requires documentation and traceability
- Software changes are to be evaluated and determined to be in compliance with the requirements of the Standard.

Copyright © 2004 Underwriters Laboratories, Inc.

15. Identification

- Software Version Identification
  - Identifies distinct software versions when changes have been made
  - Facilitates software changes which are non-safety related
- Identification Scheme
  - Must delineate changes to safety-related code from non-safety related code
- PSCS Certificate will be issued with only the safety-related version identifier

Copyright © 2004 Underwriters Laboratories, Inc.

Client Request for Certification

- ☎ Teleconference with UL computer and product safety engineer(s) to discuss:
  - Top-level product descriptions to be provided to UL
  - Applicable U.S. and International Standards
- ✶ Typically lasts 1 -2 hours

Copyright © 2004 Underwriters Laboratories, Inc.

Follow-Up Services

- Certificated software components are audited under UL's Follow-Up Services Program
  - Microcontroller hardware manufacturer and part number
  - Other electrical/electronic components essential to software system
  - Software version identification
- This is not considered the Maintenance Review

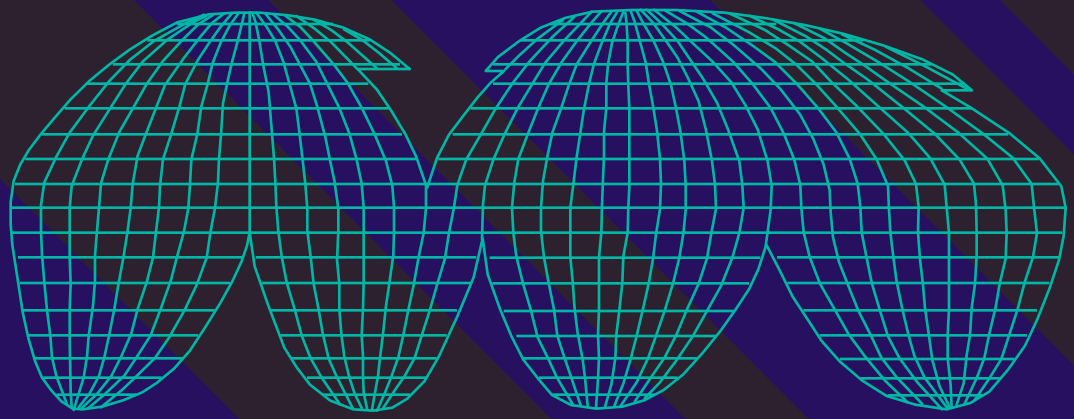
Copyright © 2004 Underwriters Laboratories, Inc.

Maintenance Reviews

- Applies to planned feature enhancements and unanticipated feature adjustments (Bug Fixes)
- Identifies functions that impact safety
- Specifies the conduct of risk analysis and re-verification
- Results in Maintenance Review Report and Certificate
- Revision of Follow-Up Services Instructions

Copyright © 2004 Underwriters Laboratories, Inc.

Additionally UL's Programmable Systems Certification Service ...



... can be coordinated through UL affiliates world wide to meet global requirements.

Copyright © 2004 Underwriters Laboratories, Inc.