Suresh Wadhwani
IBM Software, Rational

How to achieve compliance with IEC 62304 for medical device software development

- IEC 62304 Overview
- Standards Landscape
- Key elements of IEC 62304
- IBM Rational solution
- Recommendation
- Conclusion

IEC 62304 Overview

- *IEC 62304:2006 Medical device software – Software life cycle processes*
- Software use should not cause any unacceptable risk with respect to safety and effectiveness of the device
- Focused on software development and **maintenance** processes for medical devices but does not specify the methodologies, artifacts or life cycle models themselves
- Derived from ISO/IEC 12207, a general standard for software processes
- Adoption
  - FDA Consensus Standard since September 2008
  - FDA regards complying with IEC62304 as fulfilling “Software Development Environment Description” section of the *Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices*
  - Normative standard in Europe for conformance marking
- Standard available for purchase from ISO website (~$225 USD)

IEC 62304 Structure

Set of interrelated or interacting activities that transforms inputs into outputs

Set of interrelated or interacting tasks

Single piece of work that needs to be done and results in a deliverable

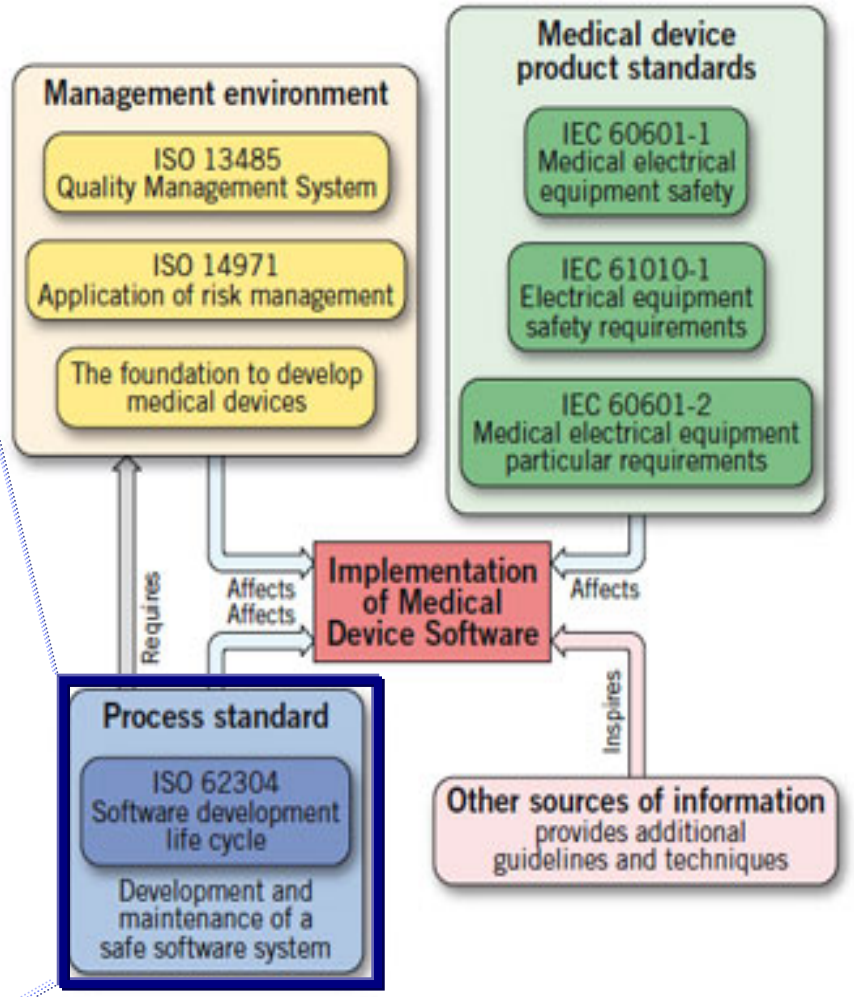
What IEC 62304 does not do

Does not cover validation and final release of a medical device

- Does not specify an organizational structure
  - You can do have a hierarchical, matrix, or mixed organization
- Does not specify the content of the documentation to be developed
  - You need to show traceability through all the artifacts but not in some set format
- Does not prescribe a specific lifecycle model
  - Waterfall, Iterative, Evolutionary, … it is all up to you

Standards Landscape

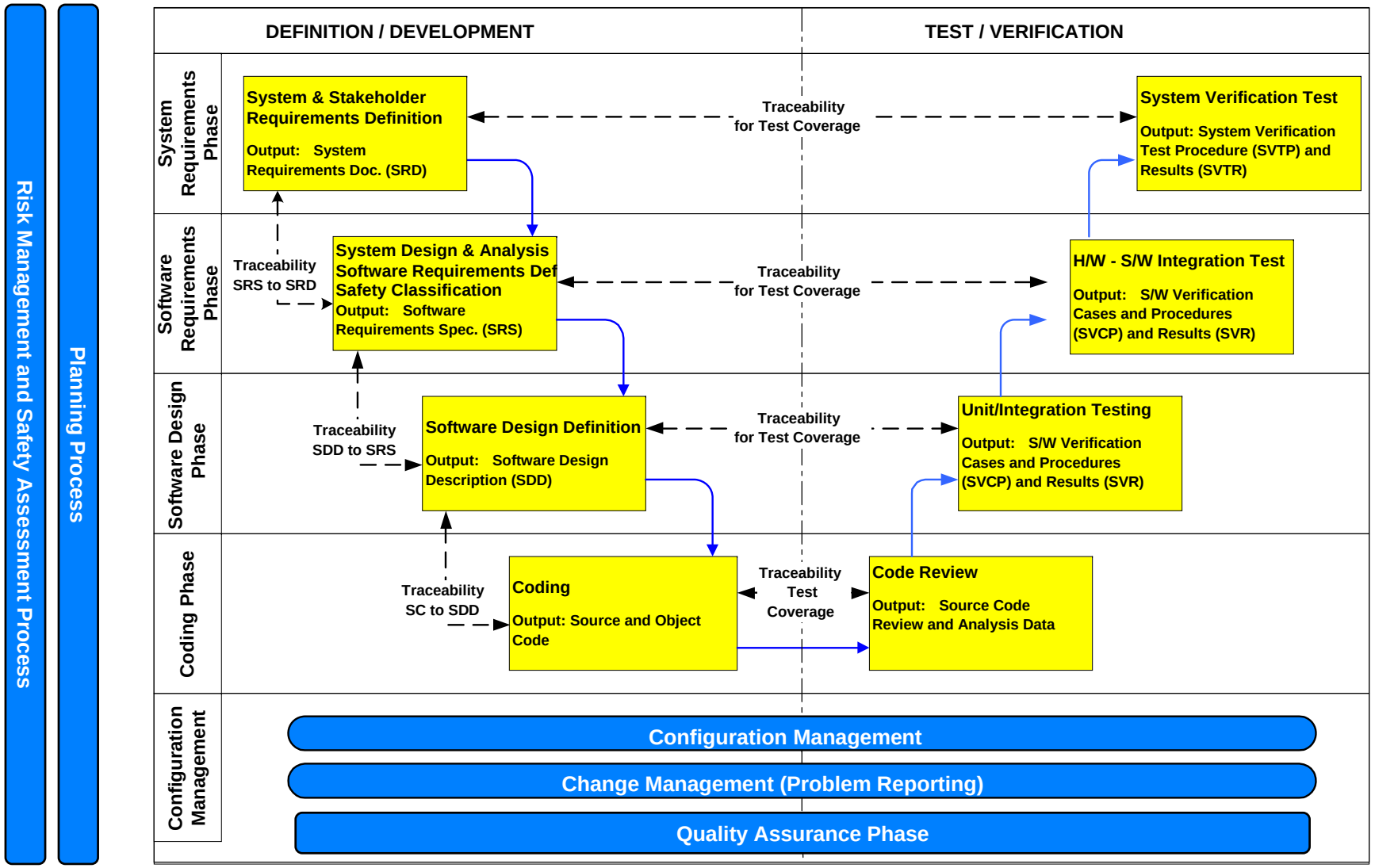
- Quality management system
- RISK MANAGEMENT
- Software safety classification
- Software development PROCESS
  - Software development planning
  - Software requirements analysis
  - Software ARCHITECTURAL design
  - Software detailed design
  - SOFTWARE UNIT implementation and verification
  - Software integration and integration testing
  - SOFTWARE SYSTEM testing
  - Software release
- Software maintenance PROCESS
- Software RISK MANAGEMENT PROCESS
- Software configuration management PROCESS
- Software problem resolution PROCESS



Source: European Medical Device & Technology, June 2010

Note: ISO 14971 is a Normative standard for Risk Management Process

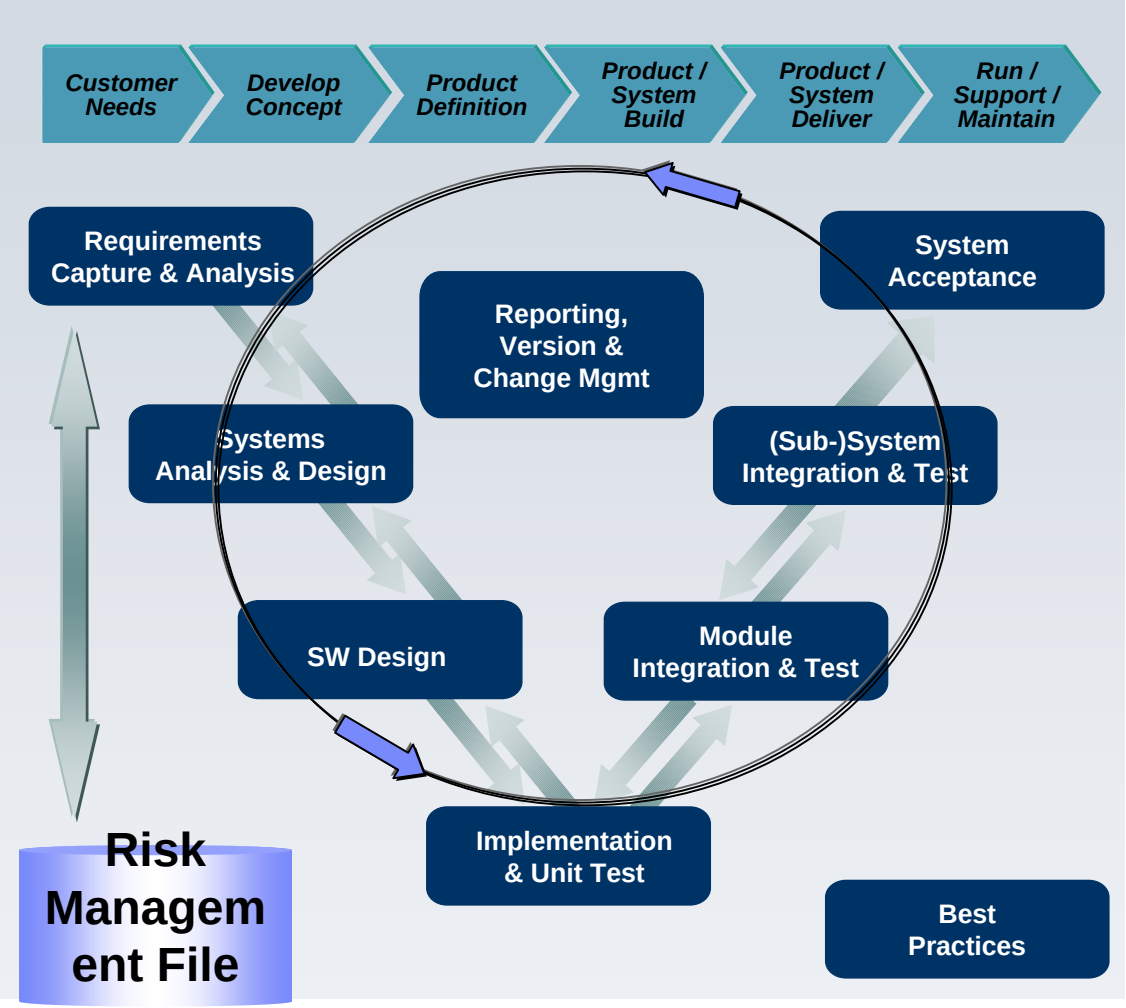
IEC 62304 Software Development Lifecycle - Model



IEC 62304 Software Risk Management - Process

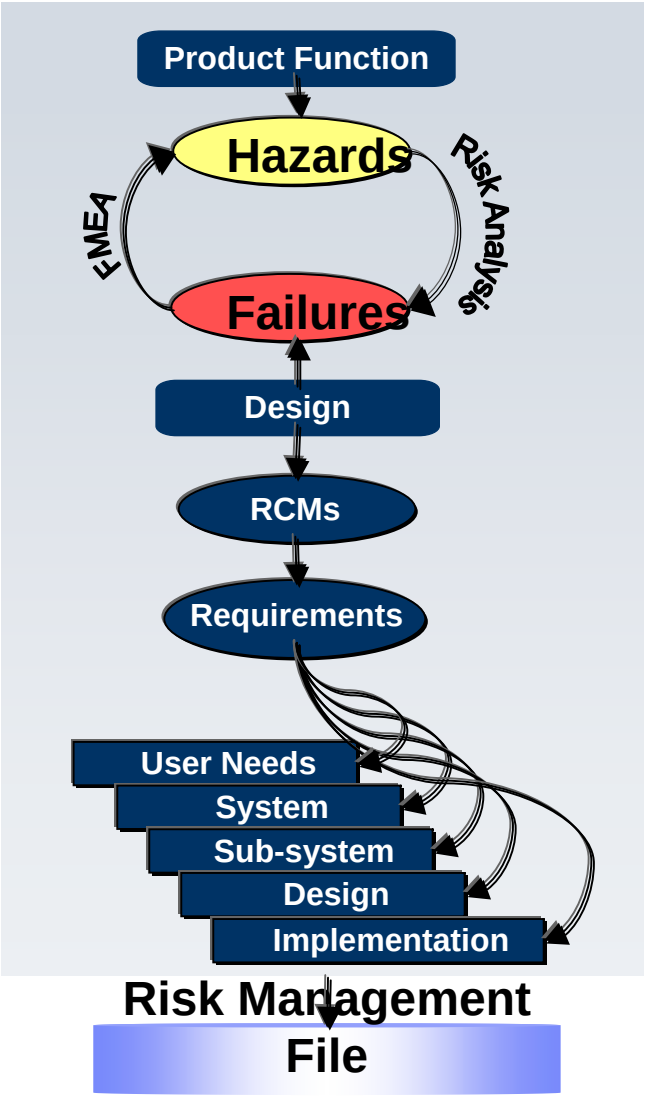
Analysis of software contributing to hazardous situations

- Software risk management in addition to ISO 14971 (see also IEC 80002 for specifics)
- Adds RISK CONTROL measures to Requirements
- Includes software to control MEDICAL DEVICE RISKS
- Allows for Design Risk Management (Bottoms Up)
- Complements Functional Risk Management (Top Down)
- Risk Management applied recursively throughout product lifecycle
- Documentation – various tools, safety assurance cases



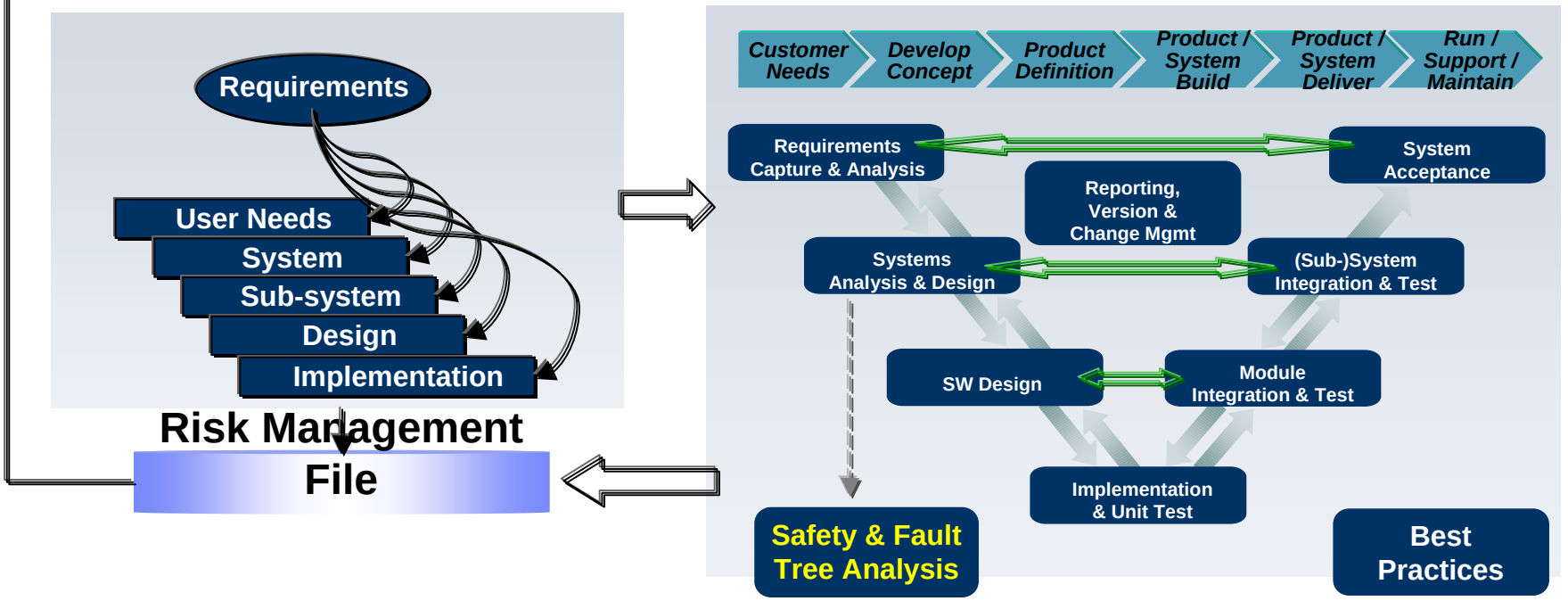
IEC 62304 Risk Management - Approach

- Anticipate possible failures of the system
  - Define control measures
    - Inherently safe
    - Preventive
    - Corrective
    - Informative
- Systematic risk analysis is to anticipate failures
  - Top-down: Function analysis - ISO 14971, FTA
    - **Hazard Analysis**
  - Bottom-up: Design/ Process Analysis – FMEA
    - **Failure Modes and Effects Analysis**
- Each failure leads to risk control (RCM) measures
- Each RCM leads to requirements implemented in product hardware, software or documentation
- Risk Management File documents traceably risk to control measure, to verification of control measure
- Risk Management Activities continue after release



IEC 62304 Risk Management – Traceability, Verification

Document TRACEABILITY of software HAZARDS
From hazardous situation to the SOFTWARE ITEM
From SOFTWARE ITEM to the specific software cause
From the software cause to RISK CONTROL measure
From RISK CONTROL measure to VERIFICATION of RISK CONTROL measure



62304 Safety Classifications

"The software safety classes shall initially be assigned based on severity as follows:

Class A: No injury or damage to health is *possible*

Class B: Non-SERIOUS INJURY is possible

Class C: Death or SERIOUS INJURY is possible"

Class C – 100% of 62304 activities apply

Class B – 93%

Class A – 43%

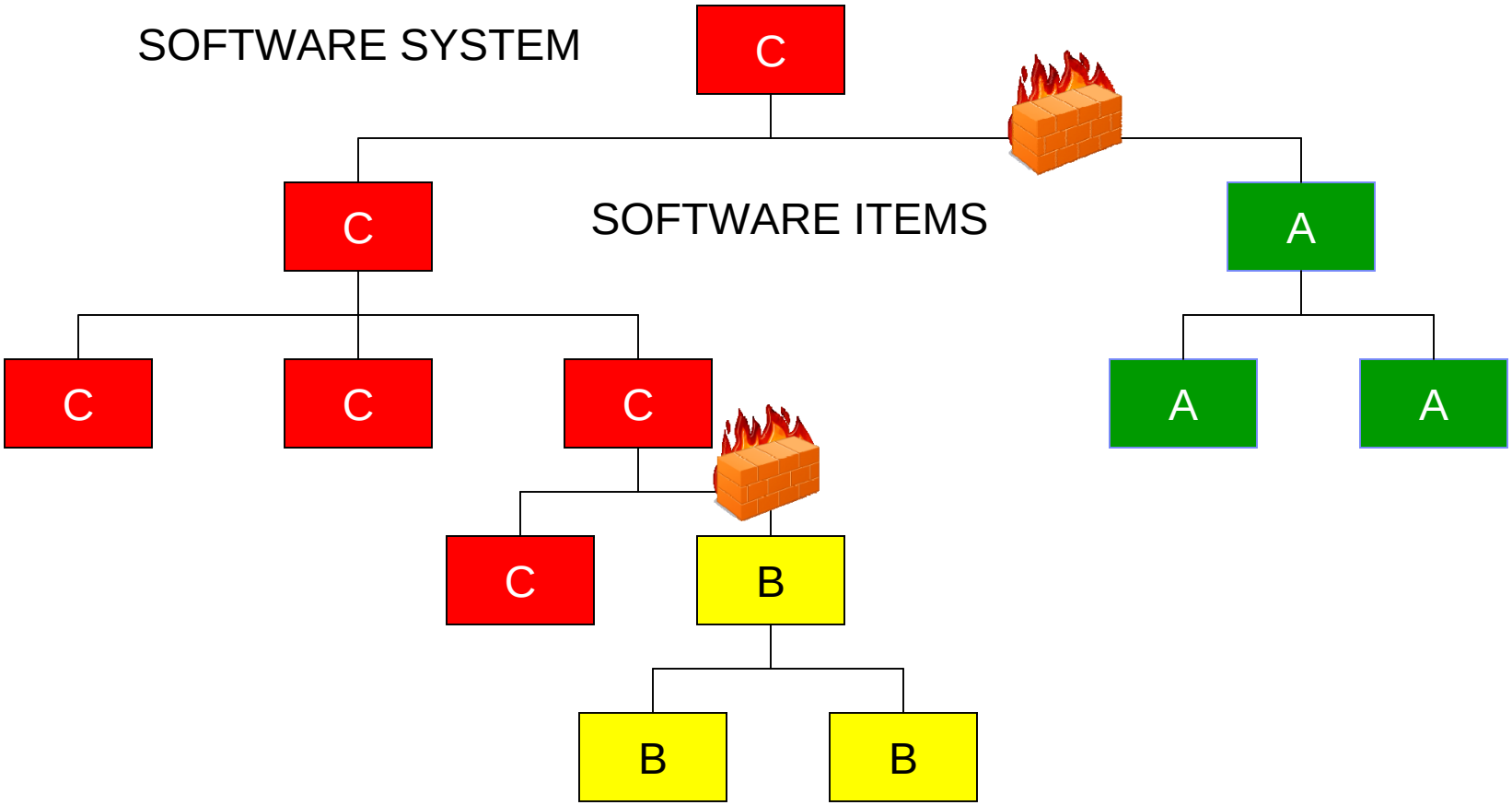
62304: Software Systems, Items, & Safety Classifications

- Software Systems are comprised of Software Items
- Software Systems are assigned a Safety Classification
- Software Items inherit the Safety Classification of the System

“ If the HAZARD could arise from the failure of the SOFTWARE SYSTEM to behave as specified, the probability of such failure shall be assumed to be 100%”

- Higher classification applies unless there is a documented rationale in a Risk Management file to justify lower safety class for software items

Segregation of Software Items



Safety, risk, and risk management process

- Safety is freedom from unacceptable risk.
- Safety is not security!
  - Security is protection of information and data so that unauthorized people or systems cannot read or modify them , and so that authorized people or systems are not denied access to them.

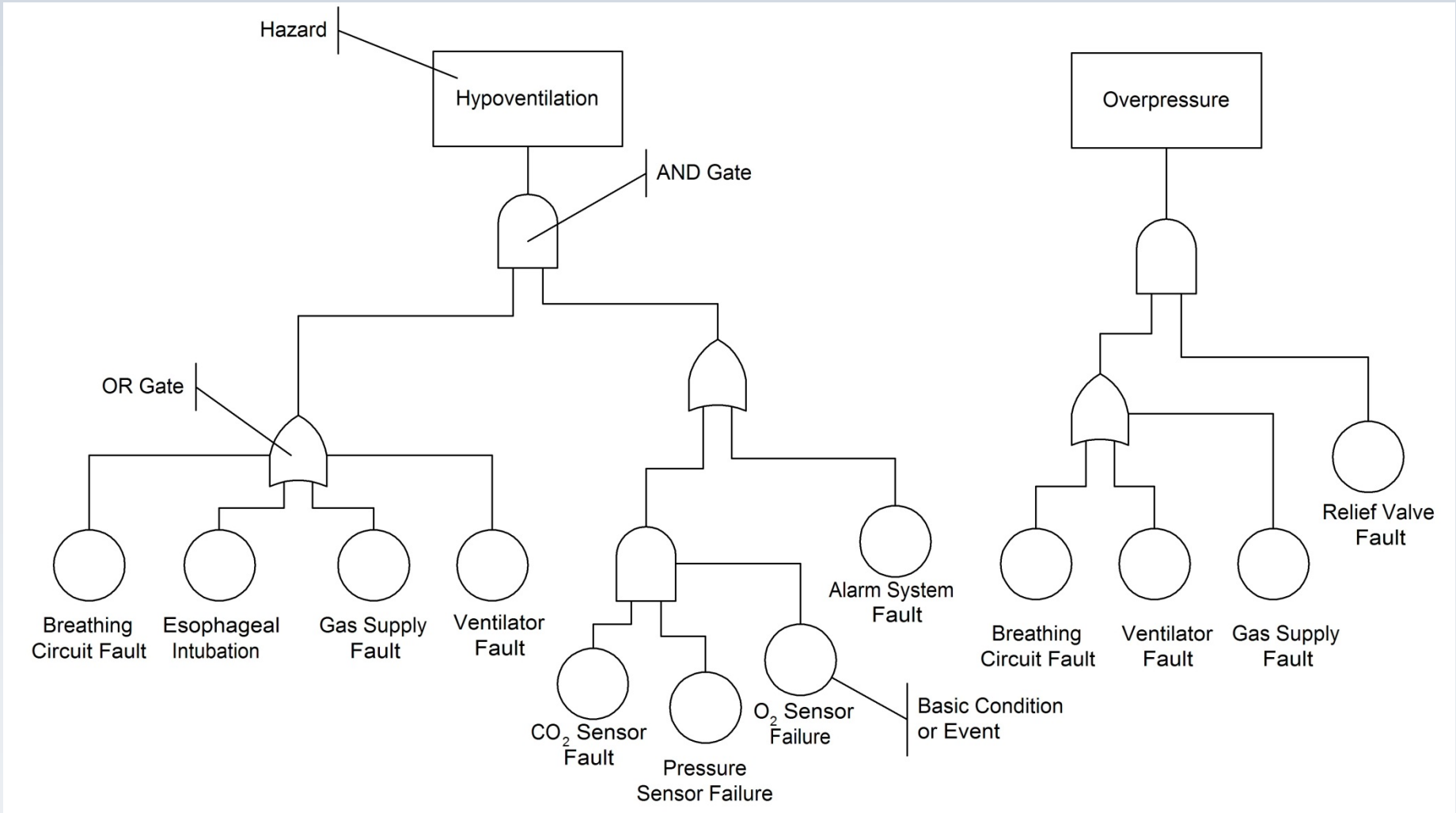
- Risk is a product of severity and probability of occurrence
- Software Risk Management Process:
  - identify software items that could contribute to a hazardous situation
  - identify causes of contribution to a hazardous situation
  - define risk control measures
  - verify risk control measures
  - Document traceability:
    - Hazardous situation to software item to specific software cause to risk control measure to verification of risk control measure

Hazard and Fault Tree Analysis

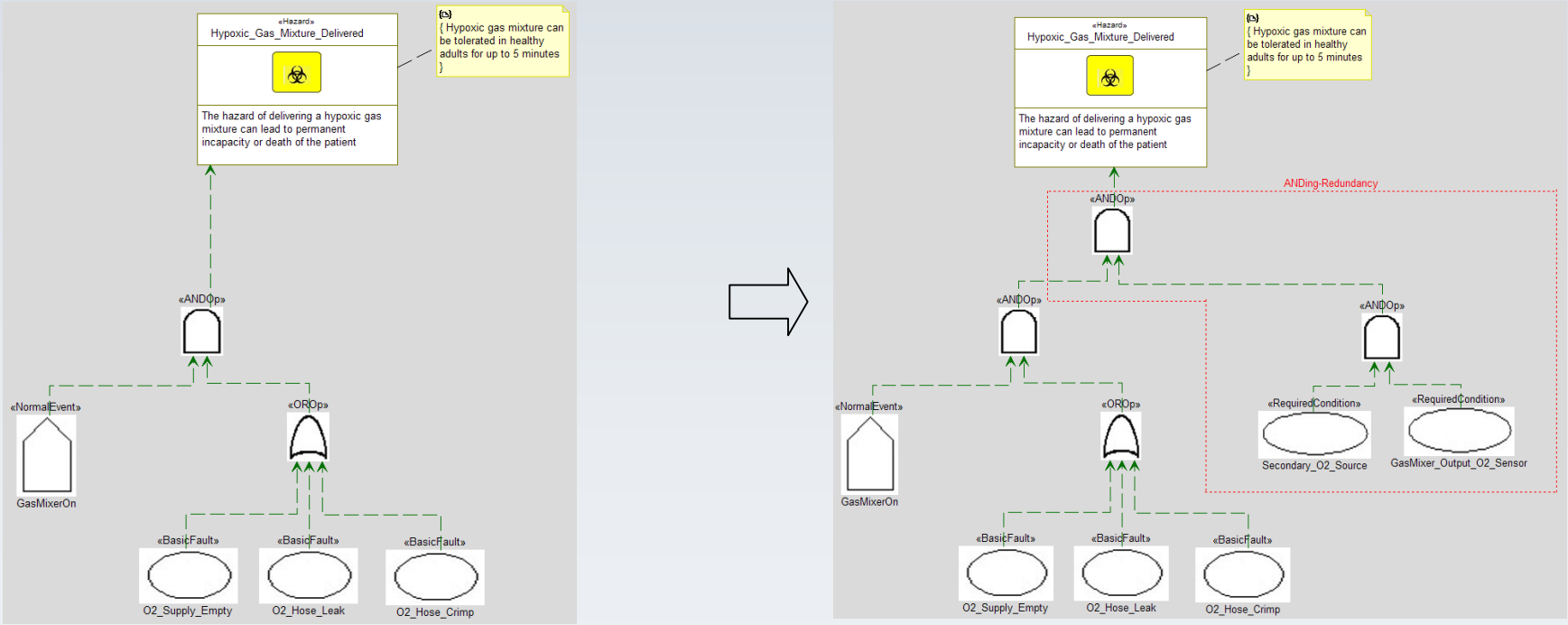
- Fault Tree Analysis determines what combinations of conditions or events are necessary for a hazard condition to occur

- Fault Tree Analysis allows the developer to identify, control and lower the risk to an acceptable level
  - This is critical in the IEC 62304 standard

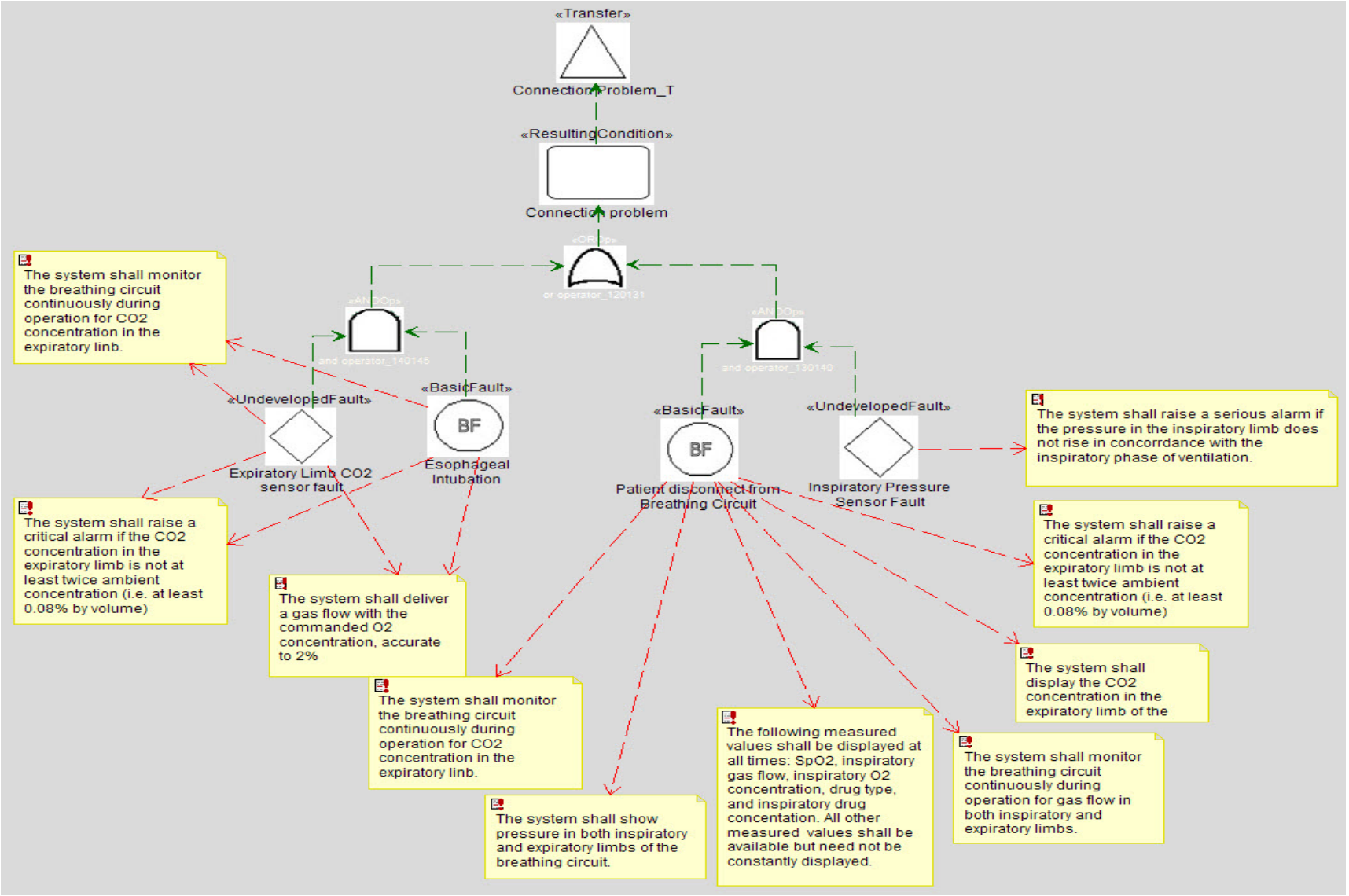
Example Fault Tree Analysis



Design Redundancy for Safety



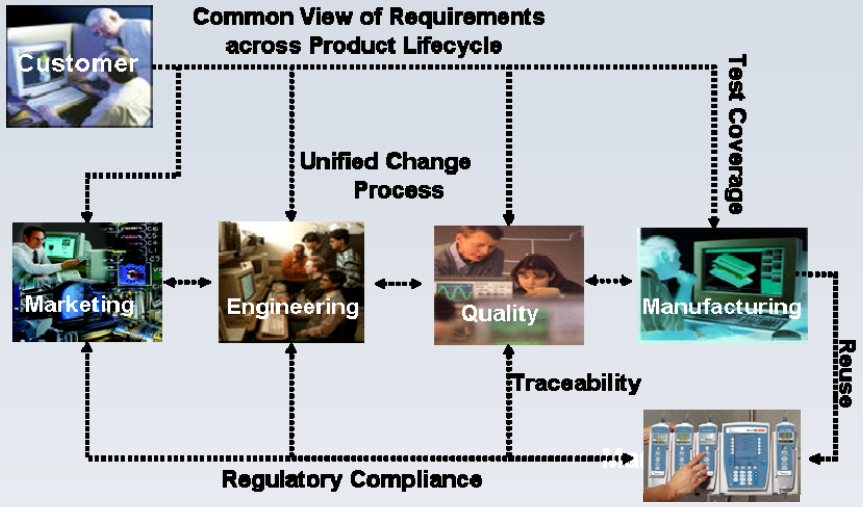
Connecting FTA to Requirements (TraceToReq)



Manage Requirements across the Product Lifecycle

Capture, define, analyze, and manage requirements

- Improves visibility and collaboration
  - Accurate documentation for regulatory audits and reviews
- Supports FDA CFR21 Part 11 compliant electronic signatures
- Integrates with:
  - Portfolio management
  - Modeling
  - change management
  - Quality management solutions

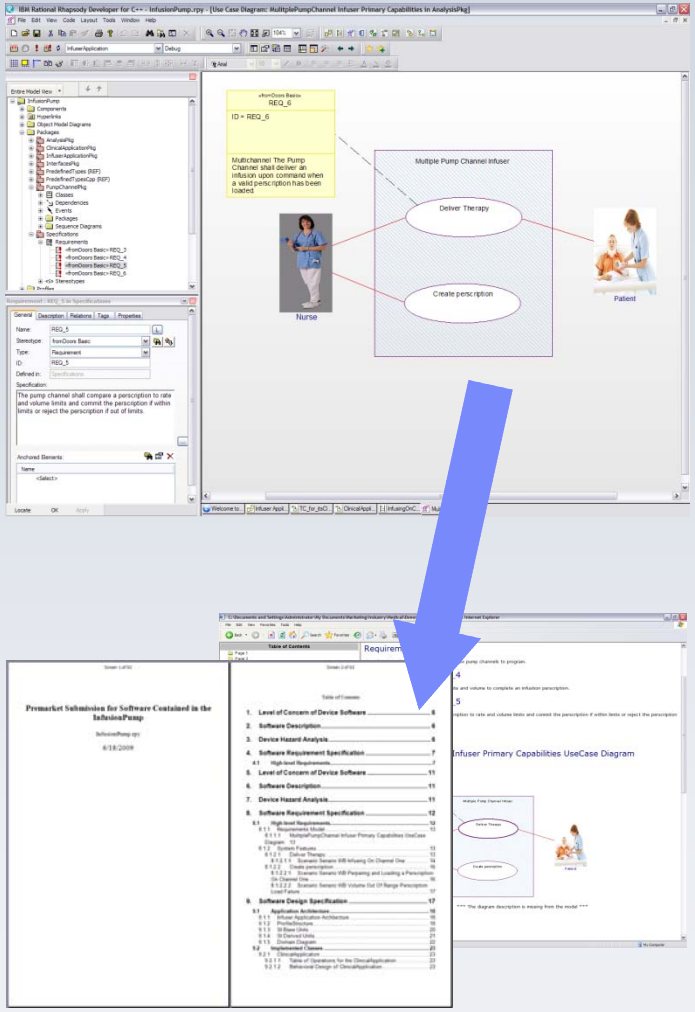


Show link to IEC sections

Develop Systems and Software in a Model-Driven way

Visually develop complex systems using a structured approach

- Traceability from requirements -> implementation
- **Automate FDA documentation** submission
- Visual modeling manages complexity
- Generates production quality code
- Reduce testing time with model-driven testing
- Leverage existing code for documentation



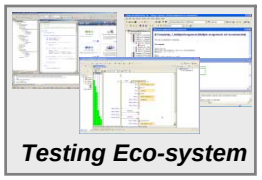
Show link to IEC sections

Manage Change for Good Manufacturing Practice (GMP)

Establish an integrated change process across the lifecycle

Capture customer requests & market driven enhancements

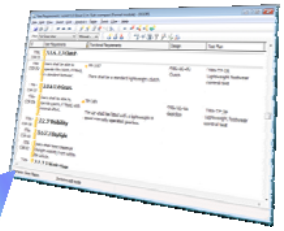
Manage Portfolio & Product Priorities



Execute Tests

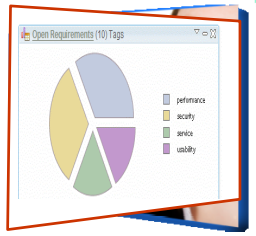
Collaboration, Process, Workflow

Capture & manage requirements

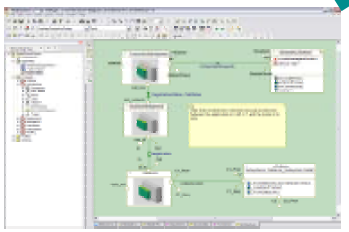


Integrated Change Management

Configuration Management



Develop Model-Driven System -> Software



Collaborate across Development Disciplines

- Software
- Electrical
- Mechanical

Integrate Suppliers

Show link to IEC sections

Automate Document Generation
Generate the right document at the right time

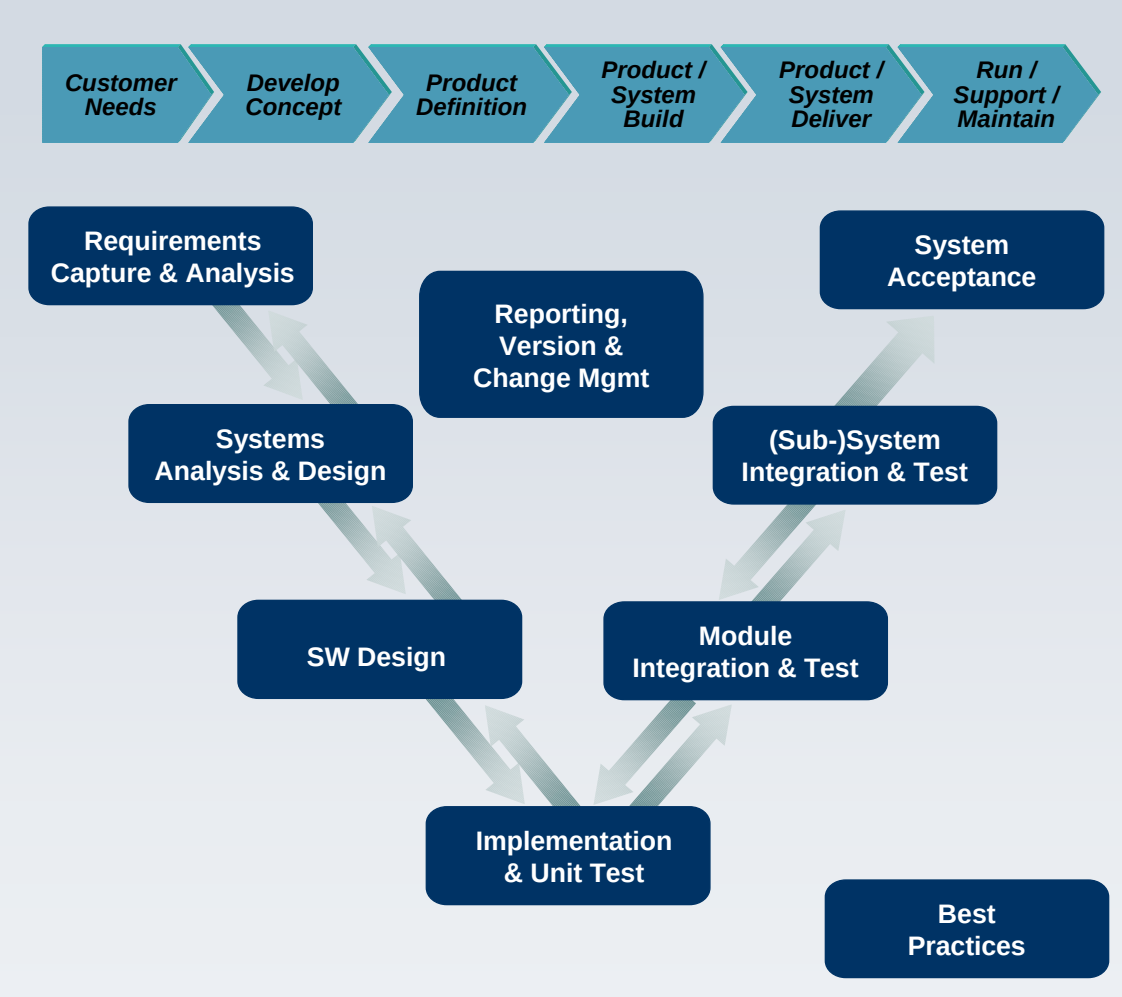
- Increase productivity by allowing engineers to focus on engineering
  - NOT formatting concerns
- Maintain accuracy through quick one-click document generation
  - Captures last minute changes from data held in different source applications
- Enhance documentation quality thru template reuse

Recommendations

- Determine compliance with IEC 62304 by performing gap analysis
  - Create a chart that maps IEC 62304 clauses and subclauses to company procedure(s)
  - The mapping chart can be a standalone document, or it can be an appendix to a company's procedure(s).
- Address open issues revealed in gap analysis
  - Establish missing processes
  - Amend deficient processes
  - Deploy appropriate software development tools that execute or enforce your processes
- Document updated software development process showing compliance with IEC 62304
  - Mapping chart should now have 100% coverage of IEC 62304 clauses within your processes

IBM Rational Software Platform for Systems

Full coverage of the systems engineering lifecycle



- Spans the entire systems and software lifecycle
- Integrates complex systems, embedded software and IT to create innovative products
- Achieves end-to-end traceability
- Provides proof of compliance

Waters Corporation

Testing equipment for medical, pharmaceutical and food products

What's smart?

- Efficient systems for verifying the purity of drugs, food products and water resources
- Highly accurate blood tests with greater precision for healthcare diagnosis

Smarter business outcomes

- Innovation to enable significant advancements in healthcare delivery, environmental management, food safety, and water quality
- Increased quality and throughput of the assays performed with cost effective technology

How Rational enables smarter products

- Full traceability with an integrated requirements, change, and configuration management solution
- Performance improvement through global collaboration and component-based development

"After about 15 minutes of spending with the auditor, he was just blown away on how effective the Rational tools were in terms of addressing all of his audit questions."

Customer Success: Safe Ventilation – at rest and on the move

Hamilton Medical AG and IBM partner EVOCEAN GmbH

What's smart?

- Intelligent ventilation for intensive care
- Innovative cockpit display, ease of use
- Frees medical staff, improves patient outcome, reduces cost

Smarter business outcomes:

- Earlier error recognition, using modeling approach with code generation
- Consistent documentation with direct association between design and code
- Improved collaboration

How Rational Rhapsody helps:

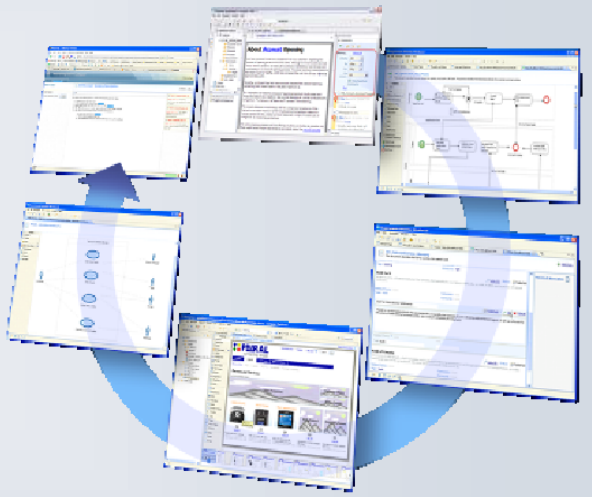
- Proven embedded and real-time track record
- Code generation
- Re-usable Software Plattform

"Thanks to graphical representation of processes and states and being able to execute them, we now have a significantly improved basis for discussion. It's also easier for new employees to get going - provided they have some basic understanding of UML and Rhapsody®, " Andreas Anderegg – Software Engineer

IBM Rational Solution for Medical Devices

Execute best practices and collaborate through an integrated product lifecycle solution

- Deliver medical devices that address market needs through portfolio management
- Provide clear audit trail across the development lifecycle with requirements management
- Validate designs early with model driven development
- Integrate change processes to coordinate development
- Automate document generation for compliance
- Drive quality throughout the product lifecycle



Powered by Jazz

www.ibm.com/rational/innovate

IBM Software

Innovate2011

The Premier Event for Software and Systems Innovation

Software. Everyware.

The Rational Software Conference **June 5 – 9** Orlando, Florida

TOP 5 REASONS TO ATTEND

1. Learn the latest solutions and best practices for model based systems engineering, embedded software development, and testing
2. Hands-on technical workshops show how to apply IBM Rational system solutions to help improve design outcomes
3. Real world results and best practices from customers in A&D, Electronics, Automotive, Semiconductor, Industrial Controls
4. High-energy Exhibit Hall and IBM Solution Center featuring Innovation Labs and Business Partner Solutions
5. Network and gain insight from peers, product developers, product managers, and thought leaders

Innovate 2011 focuses on systems engineering and embedded software development on the *Modeling, Architecture and Construction track* and **new** *System Engineering track*

Profit from **Software. Everywhere.** Starting at Innovate 2011. Mark your calendar and register today!

- *Learn more at:*
- *IBM Rational software*
- *IBM Rational Software Delivery Platform*
- *Process and portfolio management*
- *Change and release management*
- *Quality management*
- *Architecture management*

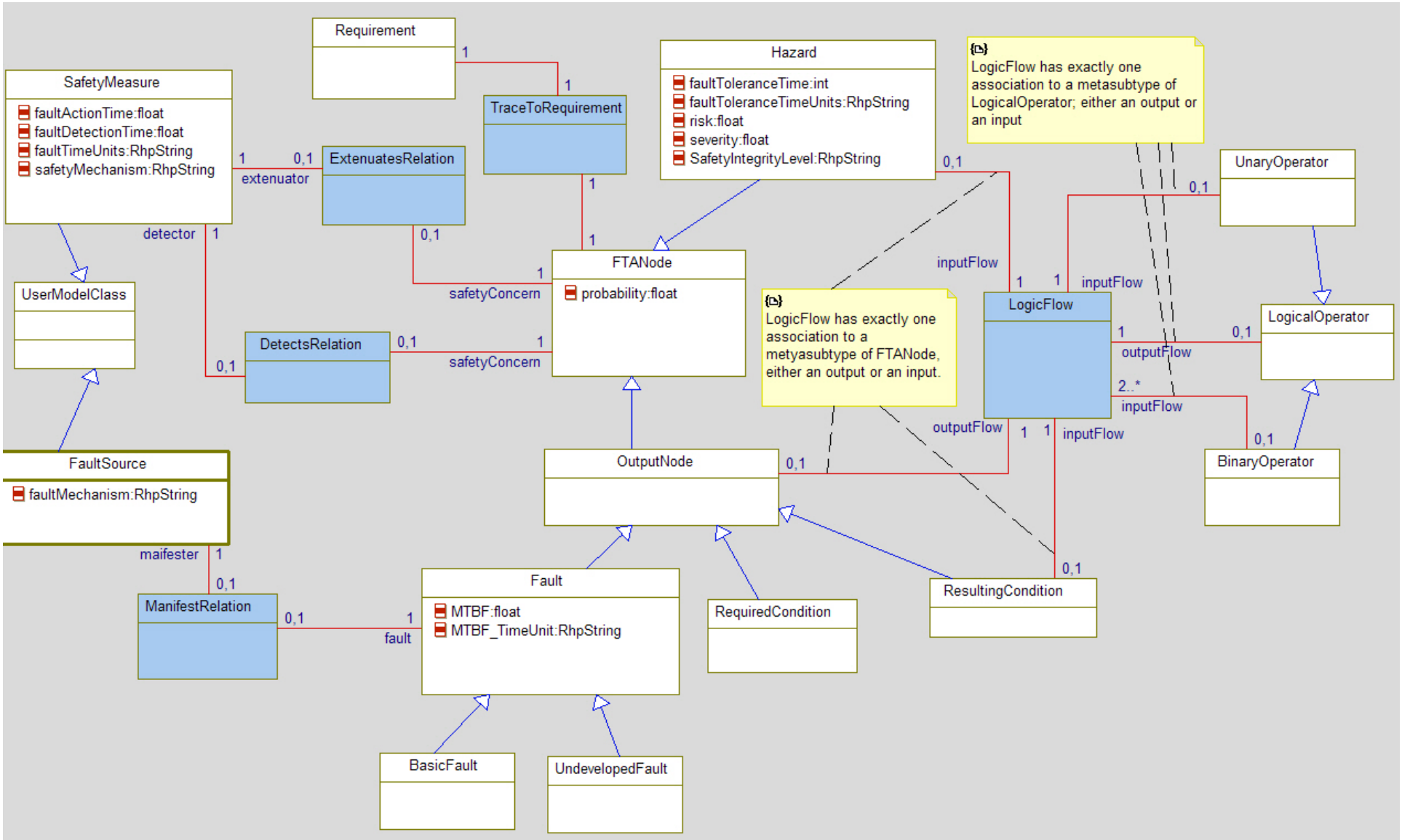
- *Rational trial downloads*
- *Leading Innovation Web site*
- *developerWorks Rational*
- *IBM Rational TV*
- *IBM Business Partners*
- *IBM Rational Case Studies*

Back-up

Safety-Related Concepts

- *Accident* is a loss of some kind, such as injury, death, or equipment damage
- *Risk* is a combination of the likelihood of an accident and its severity:
  *risk = p(a) * s(a)*
- *A Hazard* is a set of conditions and/or events that leads to an accident.
  - Hazards are predictable and therefore controllable
  - A safety-relevant system contains two kinds of hazards
    - Intrinsic hazards - due to the inherent job and operational environment of the system
    - Technology hazards - due to the addition of specific technological solutions
- A *safety control measure* is an action or mechanism to improve the safety of the system by either
  - Reducing the severity of the accident
  - Reducing the likelihood of the accident
- A fault is the nonperformance of a system or component and may be either random or systematic
- Fault Tree Analysis determines what combinations of conditions or events are necessary for a hazard condition to occur
  - Allows the developer to lower the risk of a Safety violation, critical for IEC 62304

Safety Metamodel



Fault Tree Analysis is defined in IEC 61025