IBM Software

Innovate2012

The Premier Event for Software and Systems Innovation

Next NOW!

Managing Complex Systems Engineering – A Nuclear Perspective

Paul Fechtelkotter

WW Segment Leader, Energy and Utilities

IBM Rational

Agenda for Today

Issues facing the Nuclear Industry

Lessons learned and customer examples

Summary

Nuclear power projects are complex and sensitive to cost and schedule …… but have a history of large cost/ schedule over-runs

Factor	Sensitivity	Lifecycle average cost/kWh (relative to base case)
Construction cost	25% under budget	81%
	10% under budget	92%
	25% over budget	120%
	50% over budget	139%
Construction timeline	1 year under plan	94%
	1 year over plan	109%
	2 years over plan	116%
Time to ramp up to steady-state service factor	1 year earlier than plan	98%
	1 year later than plan	103%
	2 years later than plan	107%

Figure 3: Impact of Key Construction and Start-up Variables on Nuclear Power Economics[8]

"From this model we see that total construction cost is arguably *the key factor, and that even a modest cost over-run (10-15%) could erase the cost advantage over competing fuel sources that a business case would have indicated."*

Site/Supplier	Timeline		Budget		Reasons cited
	Original	Current	Original	Current	
Olkiluoto, Finland (new) ***Areva***	2009	2012	€3 Bn	€4.5 Bn	• Unrealistic forecast (5 years) • New technology (EPR) • Contractor experience • Execution flaws (e.g., welds, coolant pipes) • Lack of capable resources
…ng, …nada (refurb) ***AECL***	2001/02	2003/04	$1.1B	$3 – 4 B	• Project management capability • Complexity
Lungmen, Taiwan (new) ***GE***	2009/10	2011/12	$6.8 B	$7.9B	• Component delivery / installation • Political factors (approvals)

Figure 4: Nuclear Project Cost / Schedule Over-run Examples

Cost over runs continue to climb

* Source: Power Gen 2010: 'CAN UTILITIES DELIVER NUCLEAR CONSTRUCTION PROJECTS ON-TIME AND ON-BUDGET? Authors: Kish Khemani and Neal Walters with AT KEARNEY.

Operational plants are facing increasing regulatory challenges

- Compliance efforts are manually-intensive and time consuming
- Cost of outages can run into millions of $US per day

NRC To Investigate Safety Valve Incident At Shearon Harris Plant.

The Raleigh (NC) News & Observer (5/7, Murawski) reports, "The Nuclear Regulatory
Commission has launched a special inspection to figure out why a pair of sa
failed to close last month at the Shearon Harris nuclear plant when the Wak
was shut down for refueling." Four "NRC inspectors will spend the week revi

Lawmaker: San Onofre won't restart until safety operations are assured: Southern California Edison officials won't restart the San Onofre
clear plant in California until the safe operation of the plant is assured,
p. Dana Rohrabacher, R-Calif., said after touring the facility. The plant
s been offline since January because of steam-generator problems.
ey all have families near the plant, so they're not going ... to do anything
out the public at risk," Rohrabacher said.
n Jose Mercury News (Calif.)/City News Service (free registration) (5/4)

NRC: Concrete concern is an issue for N.H. plant relicensing

NextEra Energy's bid to extend the operating license of its Seabrook nuclear plant in New Hampshire hinges on the company's handling of concrete degradation at the facility, said Chris Miller, the Nuclear Regulatory Commission's director of reactor safety. The company needs to pinpoint the cause of the concrete degradation and establish a corrective a

Dominion shareholders defeat safety-review plan

Dominion Resources' shareholders defeated New York Co
proposal for the company to reassess its nuclear-safety pra
more than 2 million shares in the company, said that last ye
the East Coast prompted the shutdown of the company's N
Virginia, and federal regulators later determined that the inc

Swiss nuclear plants clear EU-ordered stress tests

All of Switzerland's nuclear plants have passed European Union-mandated stress tests for such facilities. The plants had shown "high safety margins and strong robustness" and

Japan nuclear plant is susceptible to accident, official says

Chubu Electric Power's idled Hamaoka nuclear plant in Shizuoka, Japan is at risk of a major nuclear accident, said Shizuoka Gov. Heita Kawakatsu. Chubu Electric's safety measures for the plant are "inadequate," Kawakatsu said, adding that he will not permit its restart until the utility resolves the used-fuel-disposal issue.

The Wall Street Journal/Dow Jones Newswires (4/25)

The tight coupling and complex interactions in nuclear plants makes them prone to “systems risk”

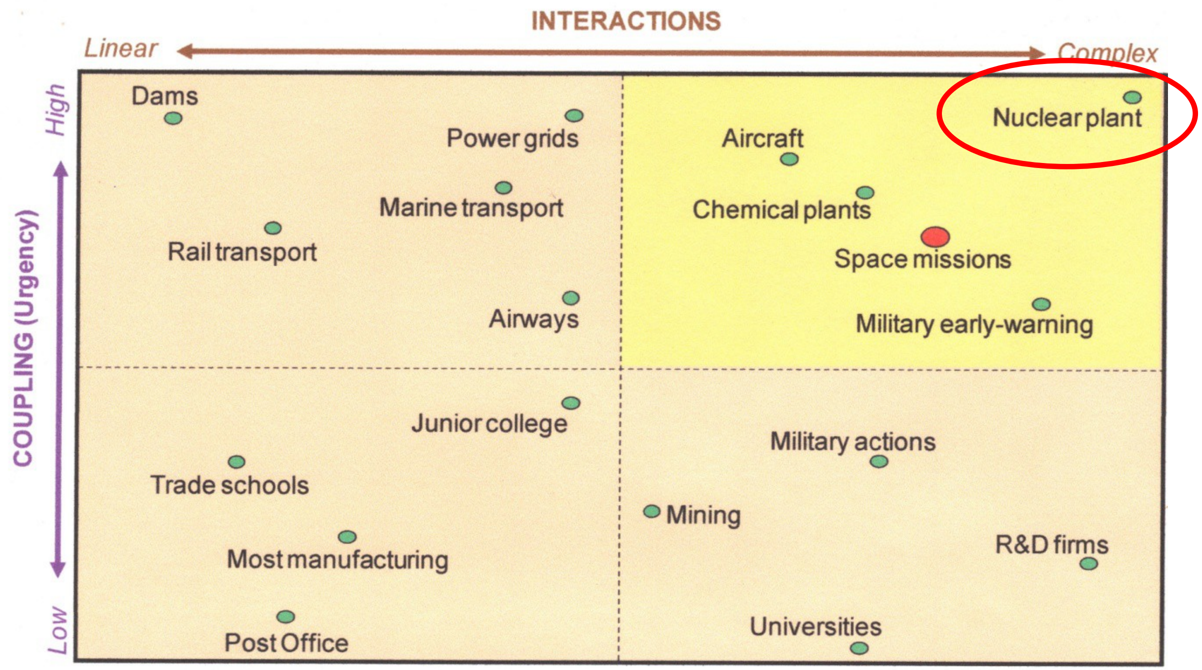


Figure 9. Systems that must manage complex interactions and high coupling are more prone to accidents. Space missions are among these high-risk systems.

The growth in complexity leads to growth in risk.

Operators need to take a systematic approach to managing the risk.

Source: Final Report: NASA Study on Flight Software Complexity, Commissioned by the NASA Office of Chief Engineer, Technical Excellence Program, Adam West, Program Manager (2009)

Combination and permutation formula illustrates the complexity

$$\frac{n!}{r!(n-r)!} = \binom{n}{r}$$

where ***n*** is the number of things to choose from, and you choose ***r*** of them
(No repetition, order doesn't matter)

$$\frac{n!}{(n-r)!}$$

where ***n*** is the number of things to choose from, and you choose ***r*** of them
(No repetition, order matters)

	Combination
	242519269720337000000000
	2.E+23
	Permutation
	3761767332187390000000000000000000000000000000000
	4.E+48
100	n
25	r

Additional challenges are being driven by the transition to digital Instrumentation and Controls (I&C)

Diversity and defense-in-depth and protection against common-cause failures

Self-diagnostics within a digital I&C platform

Communications between safety and non-safety channels

Highly-integrated control rooms

Qualification of safety system platforms

Software verification and validation (V&V)

Software quality

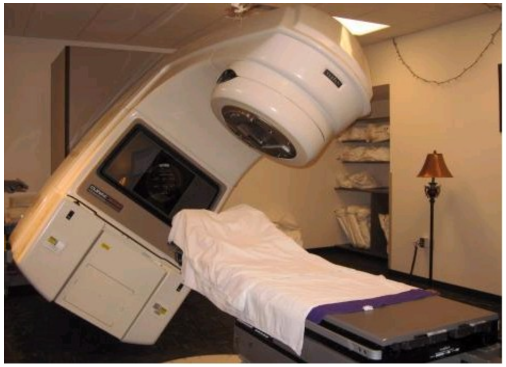
Cyber security

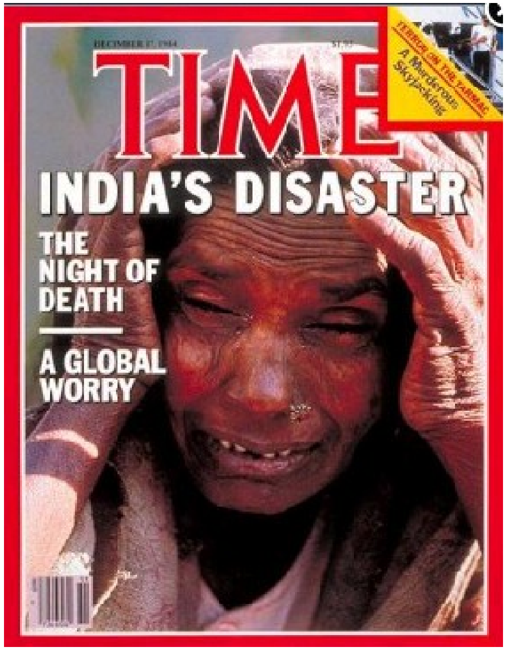
Configuration management

Probabilistic Risk Assessment (PRA) for digital systems

10 of the top issues to avoid as energy systems modernize throughout the life cycle.

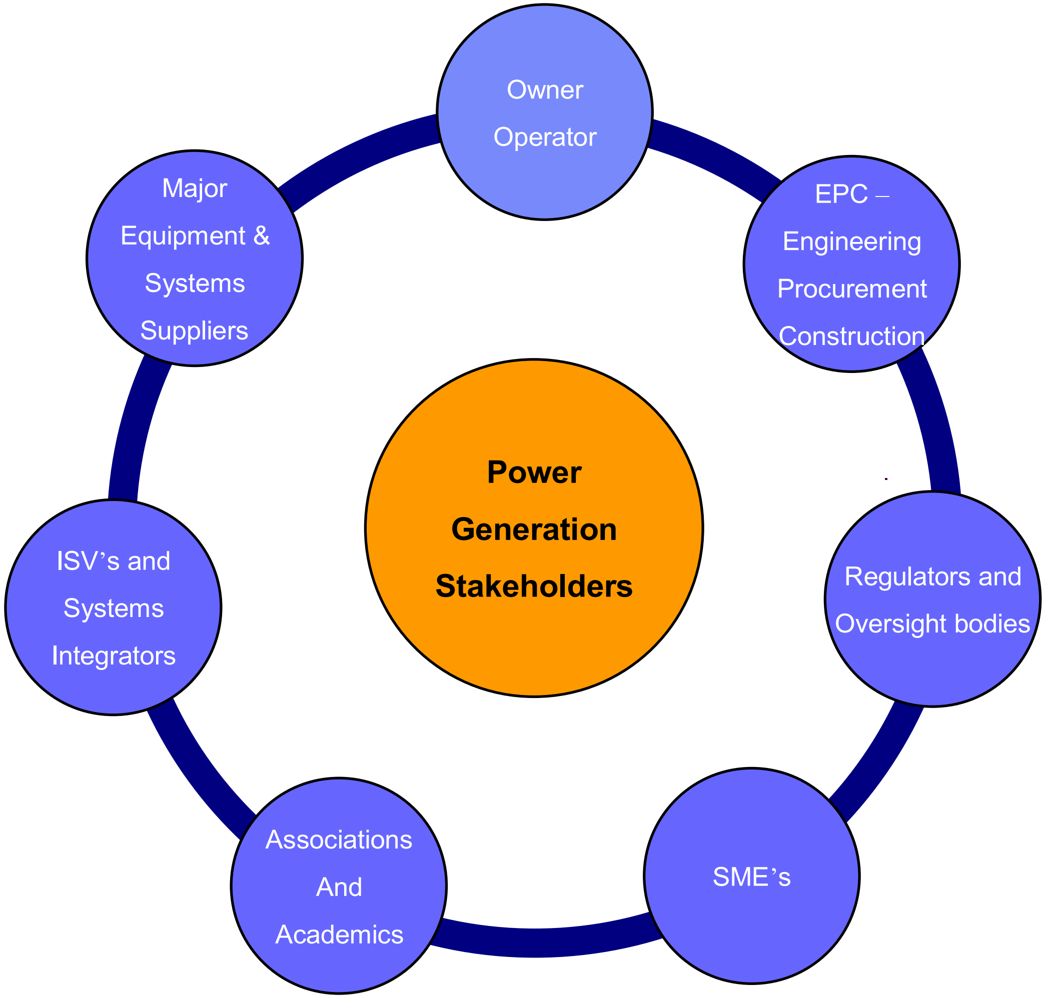
1. **Requirements grow and change at rates in excess of 1 percent per calendar month.**
2. Few applications include greater than 80 percent of user requirements in the first release.
3. Some requirements are dangerous or "toxic" and should not be included.
4. Some applications are overstuffed with extraneous features no one asked for.
5. Most software applications are riddled with security vulnerabilities.
6. **Errors in requirements and design cause many high-severity bugs.**
7. Effective methods such as requirement and design inspections are seldom used.
8. Standard, reusable requirements and designs are not widely available.
9. Mining legacy applications for "lost" business requirements seldom occurs.
10. **The volume of paper documents may be too large for human understanding.**





Software Engineering Best Practices: Lessons from Successful Projects in the Top Companies by Capers Jones

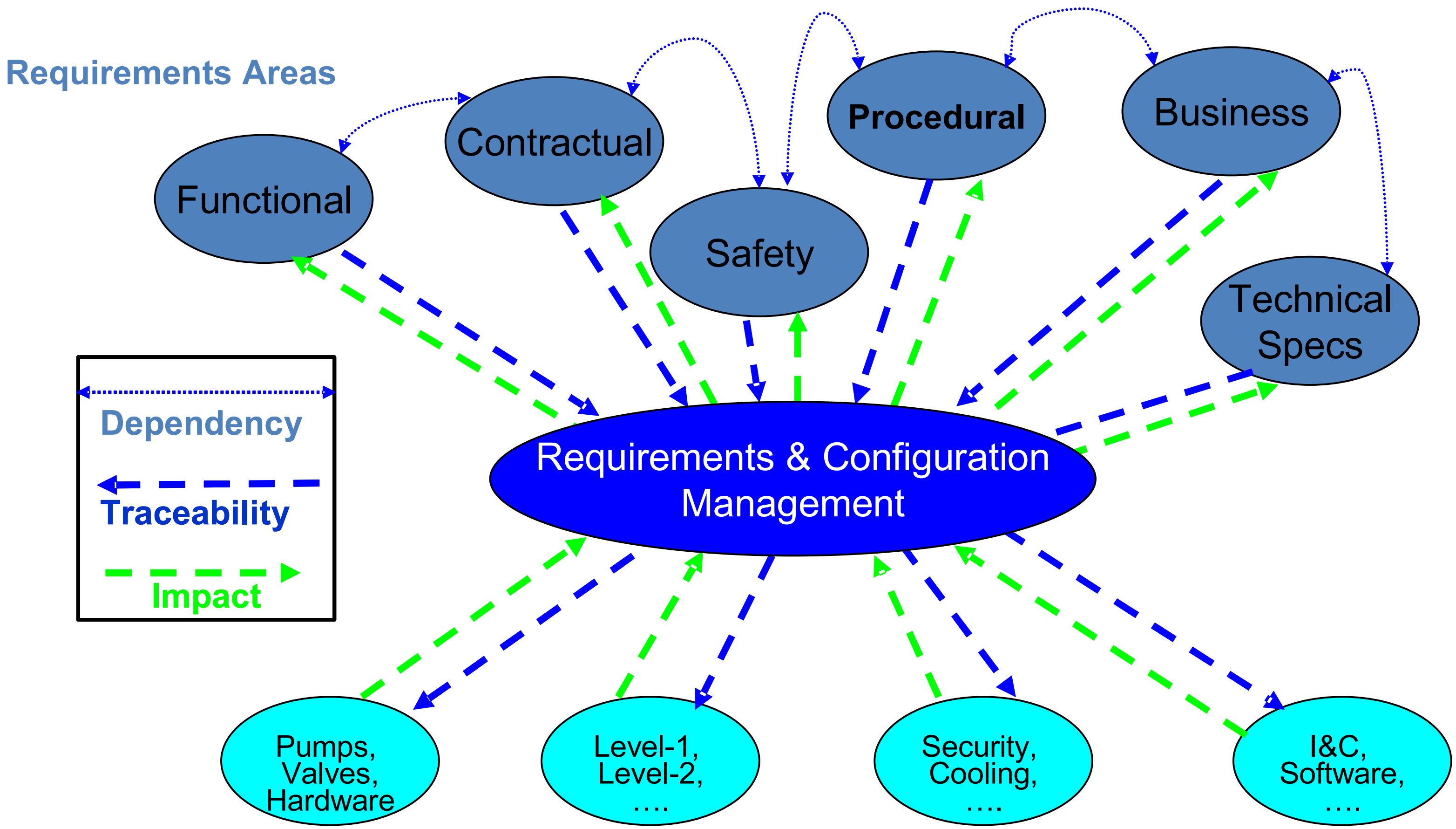
We have seen value in implementing a better collaboration platform across the ecosystem



Change in one area ripples across the other areas

All participants must be synchronized during the plant's life, from conception to decommissioning

Effective, comprehensive, and well-integrated requirements management is often chosen as a place to start



The relationships become difficult to manage as well as the change - a solid and integrated platform is needed

Effective requirements management is a foundational element that needs to needs to be addressed from project conception

Virtual Plant | Construction | Physical Plant

Year 0

New Build
Opportunity assessment

Licensing
Licence application, import and management

Requirements
Detailed specs, planning work execution

Engaging Suppliers
Issue RFX

Concept Evaluation
Process Simulation

Year 2

Contract Management
Issuing contracts to EPC's. Managing deliverables

Design Vault/CM
Capture 3D data from EPC. Library part reuse

Document Mgt
Capture and associate project data (eg safety case)

Construction Planning
Plan and execute the build process

Year 4

Commissioning
Manage process of commissioning

Handover
Efficient handover of rich information
ERP Integration

Maintenance Planning
Document maintenance procedures

Configuration Management
Requirements, Design and Plant alignment

Year 6

Maintenance
Simulate changes to procedure. Process Optimisation

Asset Knowledge Management
Complementing EAM to support decision making through the lifecycle

Cl…
Impact analysis
Design Basis and Part Equivacy

Year 15

Regulation change
Maintaining a valid configuration

License Maintenance
Keeping the license up to date

Performance Reporting
System…

…extension
Benefit of 3D

Year 45++

Decommissioning Equipment Design
Working within regulations

Plant view
Decommission by Area

Process Planning
Simulate the de-construction

…site from nuclear regulations

Decisions made here can have impacts for up to 100 years

Requirements Management (RM)

Text-based approaches introduce risk into the system and project but that is the norm today.

Advanced step

Method	Requirements Completeness	Requirements Defects per Function Point
Dynamic Modeling	97%	0.10
Quality Functional Deployment	96%	0.25
Requirements Inspections	95%	0.10
Use Cases	80%	0.80
Energy Legacy Applications	70%	0.20
Prototyping	62%	0.55
Information Requirements Gathering	**57%**	**1.00**
Normal Text Documents	**50%**	**1.10**

Interim step

Standard procedure today

Requirements Methods (Capers 2010)

Nuclear customers are moving forward with this approach

国家核电 SNPTC 国核自仪系统工程有限公司
STATE NUCLEAR POWER AUTOMATION SYSTEM ENGINEERING COMPANY

Rolls-Royce

GE Energy

British Energy
PART OF EDF ENERGY

TVO

FPL
Florida Power and Light

POSIVA

SKB
Svensk Kärnbränslehantering AB

GE-Hitachi Nuclear Energy

HITACHI

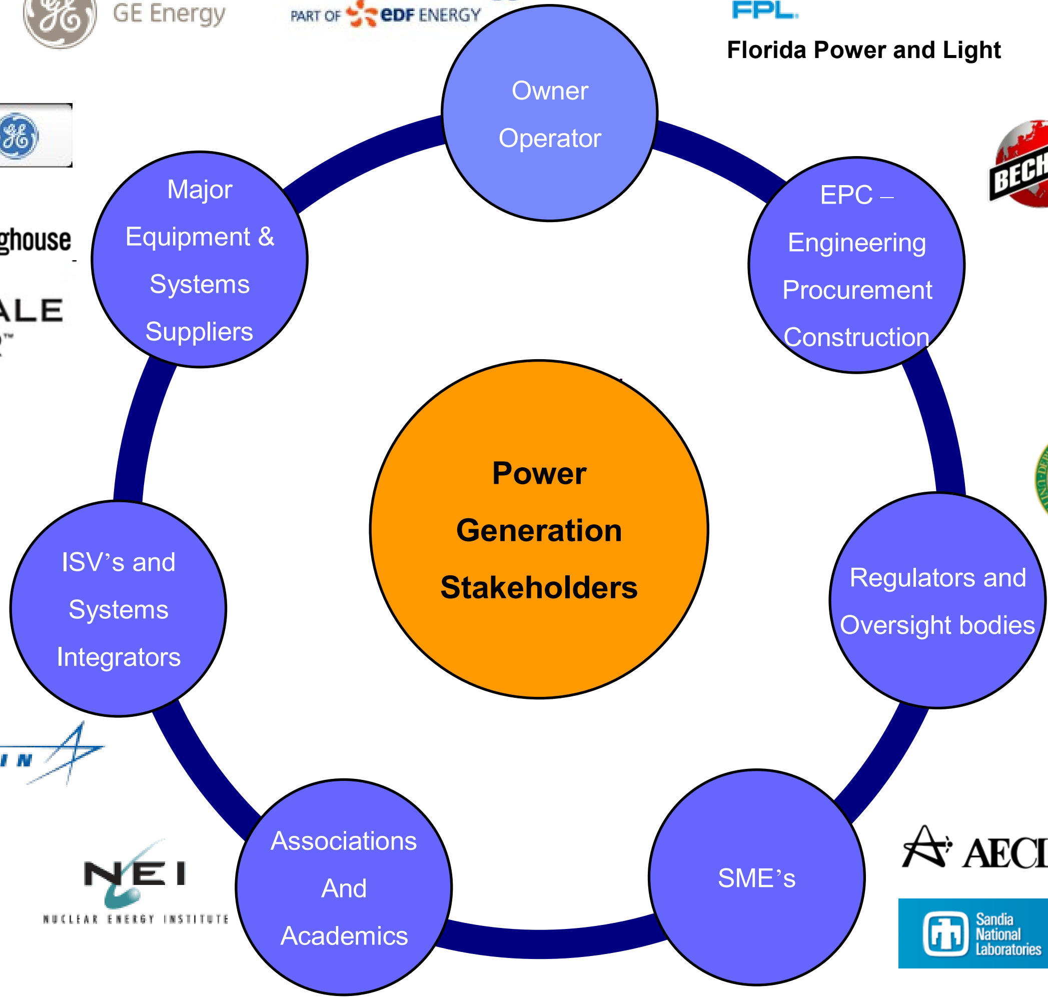
BECHTEL

Shaw a world of Solutions

SIEMENS

Westinghouse

NuScale Power



US Department of Energy (DOE)

US DOE - Waste Isolation Pilot Plant

US DOE - National Nuclear Security Administration

US Nuclear Regulatory Commission (NRC)

EDF

BECHTEL

LOCKHEED MARTIN

All Russian Scientific Institute

SRNL
SAVANNAH RIVER NATIONAL LABORATORY
We Put Science To Work

AECL

INL Idaho National Laboratory

NEI
NUCLEAR ENERGY INSTITUTE

Sandia National Laboratories

Oak Ridge National Laboratory

Los Alamos National Laboratory EST. 1943

Customer example

A REQUIREMENTS MANAGEMENT SYSTEM FOR A SPENT NUCLEAR FUEL REPOSITORY

Svensk Kärnbränslehantering AB

Lena Morén and Åsa Olson, SKB
Swedish Nuclear Fuel and Waste Management Co, Box 250 SE-101 24 Stockholm
Lena.Moren@skb.se

The operation and construction of a final repository facility and repository for spent nuclear fuel is regulated in Swedish laws. To support the development of a repository design in conformity to the regulations SKB has developed a requirements management system (RMS). The RMS shall make the basis and motive for the design traceable, facilitate system development, understanding and decision making.

In the RMS the requirements and other design premises are organized in a hierarchy. Each level in the hierarchy can be regarded as a specification. The highest level specifies the problem to be solved and the principles to be applied in the design, and the lowest level the design of individual components.

The higher level requirements are based on laws and regulations and generally accepted safety and radiation protection principles. The lower level design premises are based on results from the assessments of the operational and long-term safety and technology development. The formulation of concise requirement texts requires both system understanding and, since the requirements constitute specifications, choice of design alternative. The development initiates cooperation between groups and supports system understanding.

Customer example

SKB
Kärnbränslehantering AB

Design premises	Sources and level of detail	Example
Level 1: Stakeholder requirements		
Requirements expressing basic requirements and principles for the design.	Laws and regulations Stakeholder demands Problem to be solved and principles to be applied in the design	The post-closure safety of the final repository shall be based on several barrier functions that are maintained through a system of passive barriers.
Levels 2 and 3: System and sub-system requirements		
Requirements expressing the functions the repository and repository facility shall have to conform to the objectives and principles.	Laws and regulations The KBS-3 method The spent nuclear fuel The KBS-3 repository and repository facility	The final repository shall contain the spent nuclear fuel and isolate it from the environment at the surface.
Requirements expressing the functions the barriers and technical systems shall have for the repository and facility to maintain their functions.	Laws and regulations The KBS-3 method The spent nuclear fuel The engineered and natural barriers The technical systems	The canister shall sustain the containment and withstand the mechanical loads that are expected to occur in the final repository.
Levels 4 and 5: Design requirements and reference design		
Requirements expressing the properties and parameters to be designed and the terms they shall fulfil.	The required functions and results from the safety assessment, research and development	The compression yield strength and the dimensions of the insert shall be such that the copper shell remains tight with respect to the largest expected isostatic load.
Other premises for the design Premises for the design from: - the safety assessment, - the other barriers, - the production and operation	The components of the engineered barriers and their properties The layout and properties of the underground openings The components of the technical systems	Largest isostatic load 45 MPa = max. swelling pressure + max. groundwater pressure.

Figure 1 The hierarchy of design premises in SKB's RMS with an example.

Customer example

Svensk Kärnbränslehantering AB

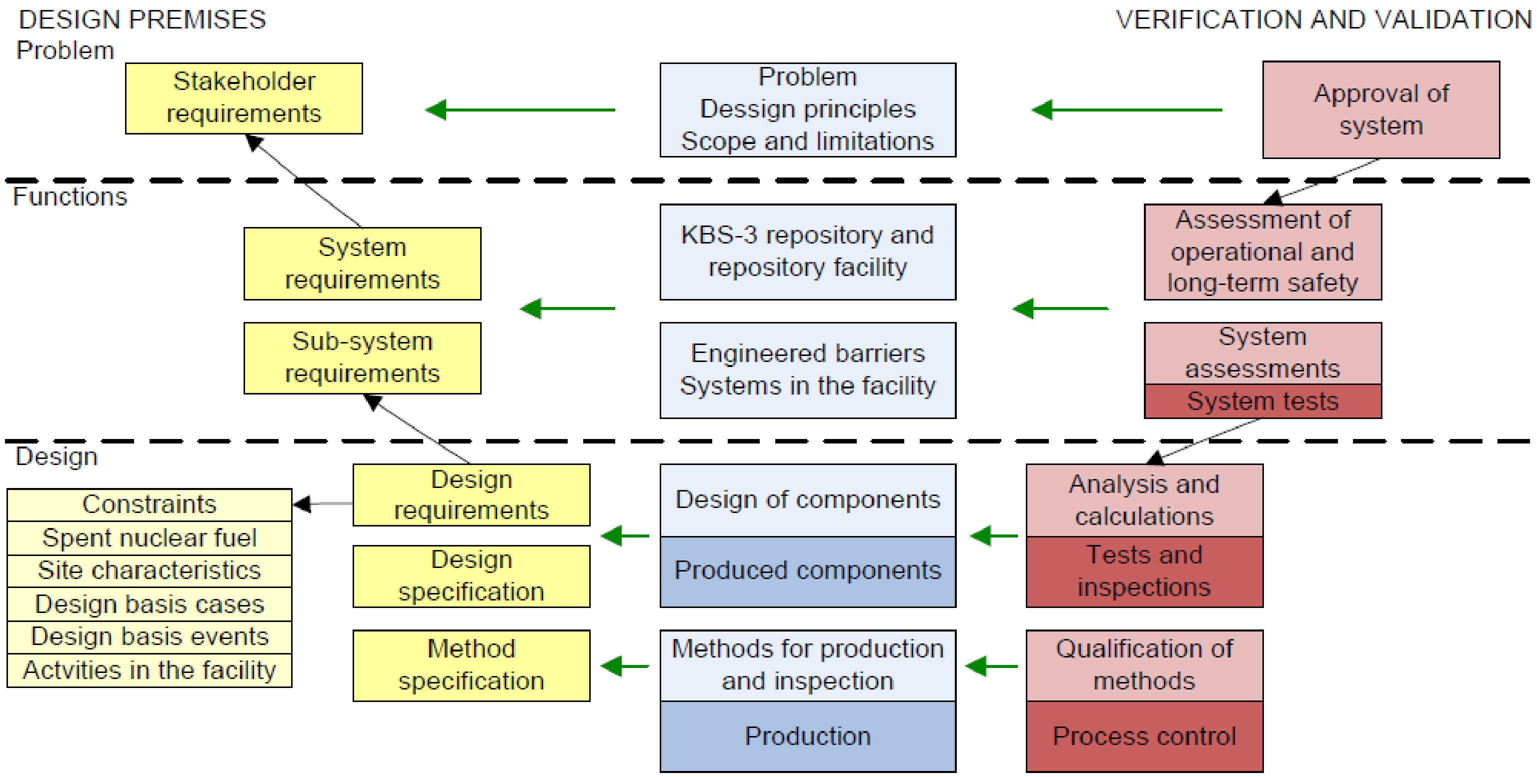


Figure 1. SKB's version of the V-model with the requirement hierarchy, the constraints, the specified issues and the verification. The black arrows illustrates links in the RMS. For the verification lighter colour illustrate design phases and darker construction and operation phases.

VAHA

Requirements Management System for the Final Disposal of the Spent Fuel

May 10, 2012

Posiva Oy
Juhani Palmu

VAHA Project - the requirements related to the geological disposal of spent nuclear fuel in Finland

POSIVA

POSIVA Juhar

VAHA Project

- VAHA – vaatimustenhallinta – requirements management
- The aim of the project is to design and implement a systematic process and an information system to manage **the requirements related to the geological disposal of spent nuclear fuel** in Finland.

VAHA Project, System Structure

Level 1 - Stakeholder requirements

Level 2 - System requirements

Level 3 - Sub-system requirements

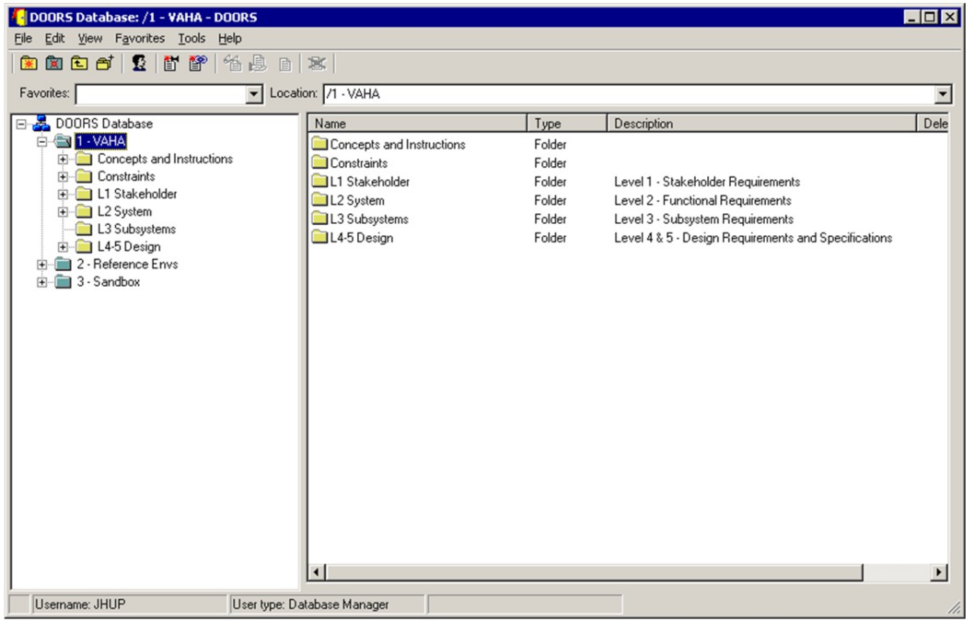
Level 4 - Design requirements

Level 5 - Design specifications

Constraints

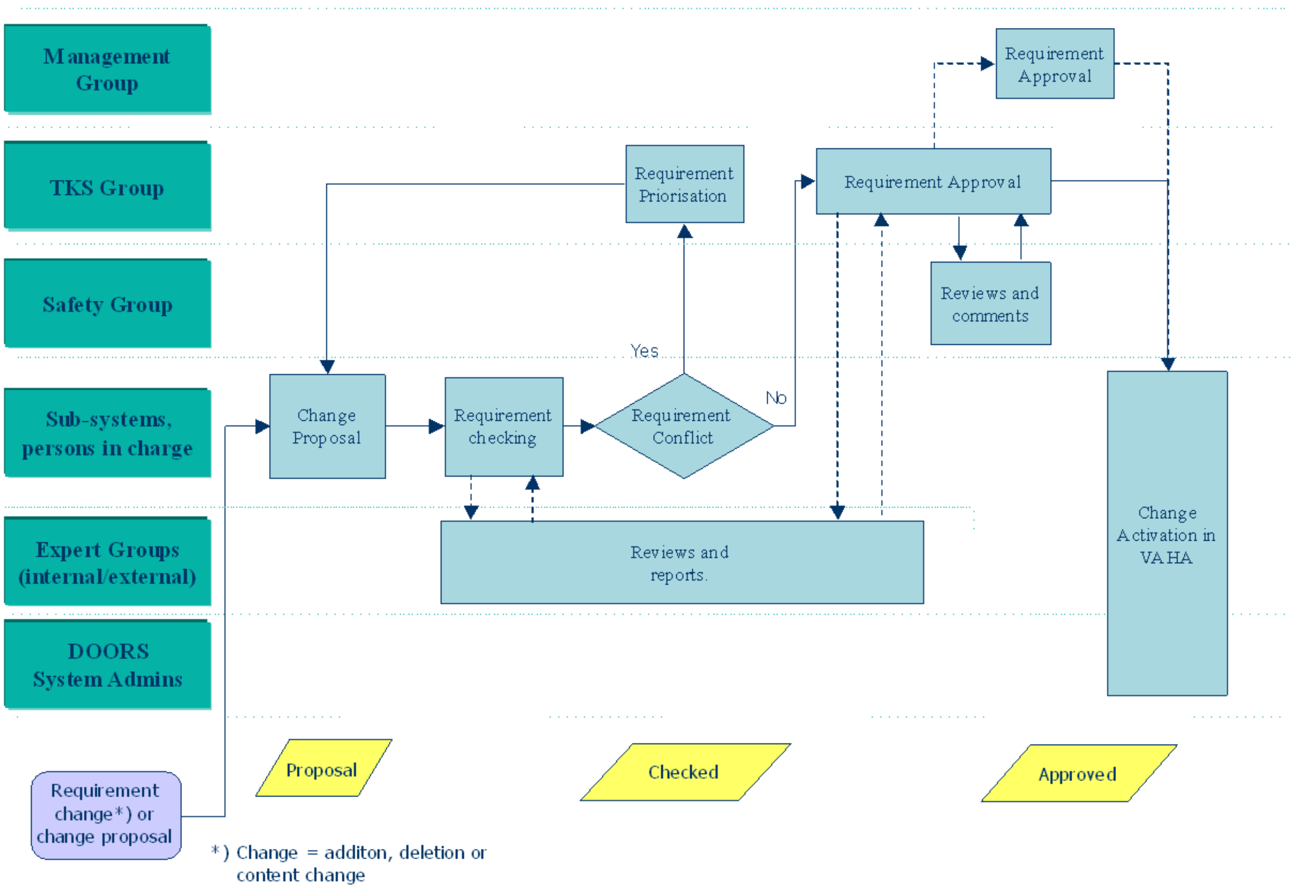
POSIVA Juhani

VAHA Project, System Structure

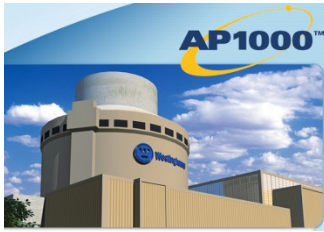


POSIVA Juhani Palmu

<u>VAHA Change Management Process</u>



Why Westinghouse Electric Company chose DOORS



The Importance of a Requirements Management Program to Westinghouse

- Customers expect their contractual requirements to be met by our products and services
- Nuclear regulatory requirements must be met by our design
- Standards & certifications must be in compliance
- Our products/services must meet these requirements before we can be paid
- "Change" happens – we use DOORS functionality to manage the change for us

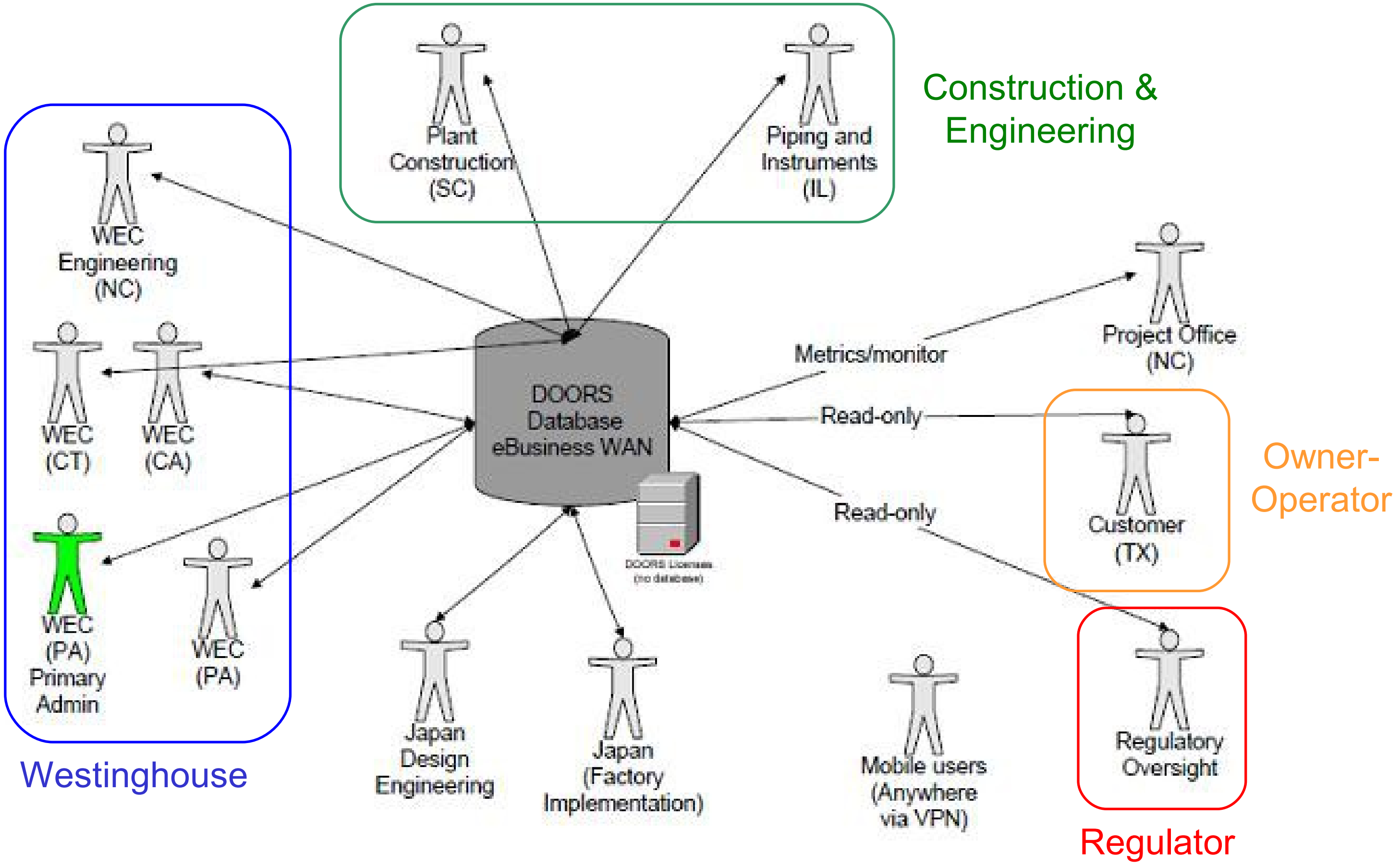
If you don't know where you are going…. how will you know when you get there?

DOORS connects requirements to test cases and test results

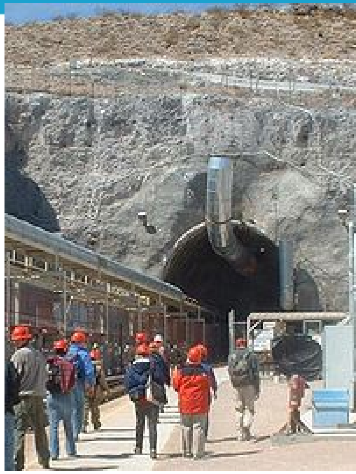
DOORS provides the ability to hold online document review process

Westinghouse's collaborative example

- Collaborating among ecosystem partners for new-build design work

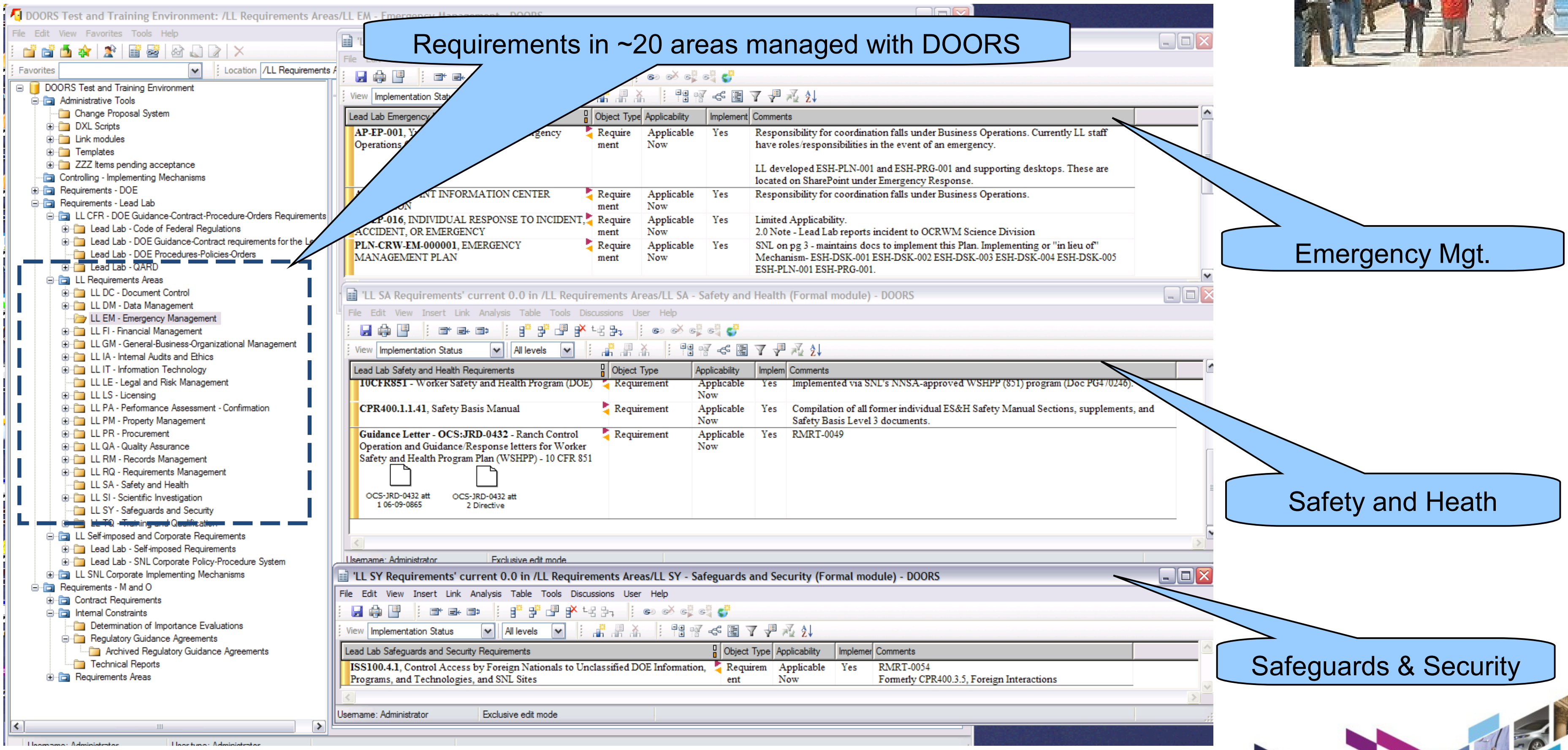


US Department of Energy (DOE) - Yucca Mountain Repository



Develop a national site for spent nuclear fuel & high-level radioactive waste storage.
Project lead by a consortium of government contractors, URS Corporation, Shaw Corporation and Areva Federal Services LLC.

The program used ***Rational's DOORS*** product to develop an extensive requirements database to track and manage an extremely broad range of program and regulatory requirements ranging from US CFRs to Contract Requirements.



Summary

- The challenges facing the nuclear community continue to rise
  - The introduction of software-based I&C is one of the key drivers
- There is a need for more effective collaboration and synchronization amongst all parties is the ecosystem
- Better collaboration is achievable through the use of existing integrated, scalable, and battle-tested IT platforms