International Council on Systems Engineering
A better world through a systems approach

Digital Safety Analysis for Small Modular Nuclear Reactors (SMRs)

Ron Claghorn, Idaho National Laboratory (USA)
Peter Suyderhoud, Idaho National Laboratory (USA)

There's never been a better time to be an engineer

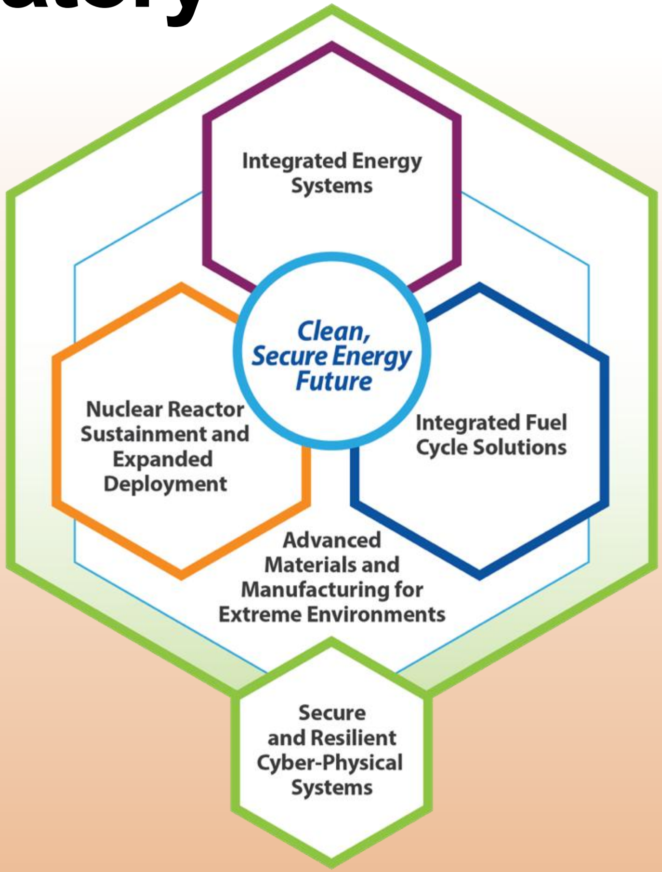
Before Digital Tools	Now
The System Engineering perspective is based on systems thinking. Systems thinking is a unique perspective on reality—a perspective that sharpens our awareness of wholes and how the parts within those wholes interrelate. When a system is considered as a combination of system elements, systems thinking acknowledges the primacy of the whole (system) and the primacy of the relation of the interrelationships of the system elements to the whole. Systems thinking occurs through discovery, learning, diagnosis, and dialog that lead to sensing, modeling, and talking about the real-world to better understand, define, and work with systems. A systems thinker knows how systems fit into the larger context of day-to-day life, how they behave, and how to manage them. [INCOSE]	A Systems Engineer is a generalist: • Develops and maintains the system concept start to finish. • Coordinates the work of engineering disciplines. • Steps in when a technical resource such as 3D modeling is missing.

Today’s Agenda

- INL’s Digital Transformation Mission (Peter)
- What is a Small Modular Reactor (SMR)?
- The typical licensing process
- Human Systems Integration (HSI) to make a better license application
- An elegant system
  - Design verification & system validation
  - Traversable structure
  - Dynamic views
  - Automatic Configuration Management
  - Transformation to Probability Risk Assessment (PRA)

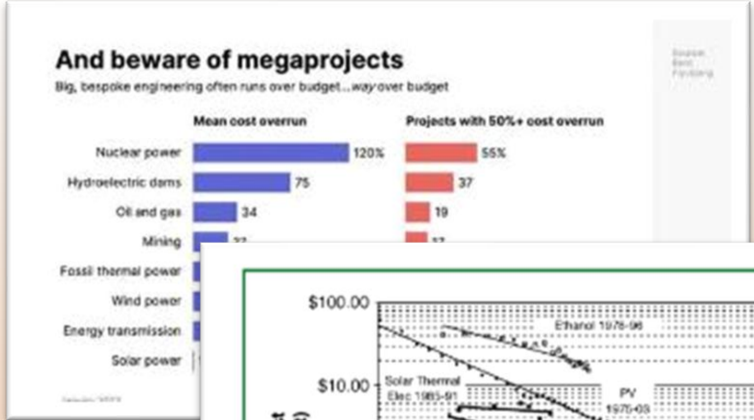
Idaho National Laboratory

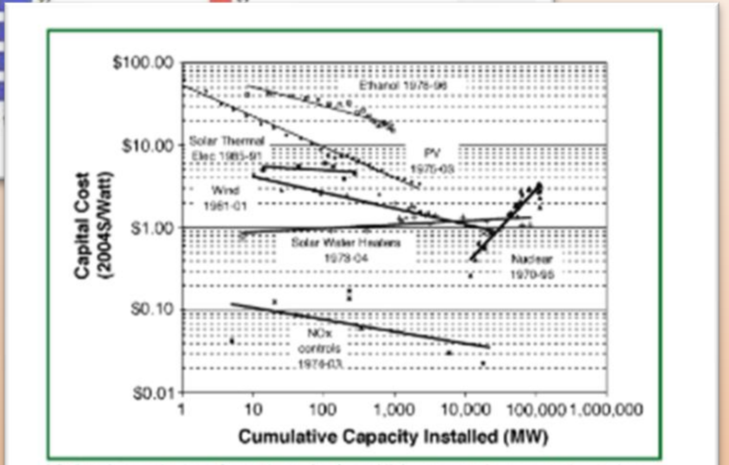
- Innovation for a secure and resilient clean energy future
- INL's five strategic science & technology initiatives work together to advance our mission.
- The nation's nuclear energy laboratory



Digital Transformation at Idaho National Laboratory

- WHY? Nuclear power has a historical cost overrun of 120% with poor schedule performance
- Vogtle Units 3 & 4
- Initial $14B, final > $30B (+$17B)
- Initial 2026, final 2024 (+8 yrs)
- DE technologies and techniques demonstrated in other industries (defense, aerospace, etc.) have historically shown the ability to save around 15-20% on project cost & schedule based on statistics from DoD and commercial construction
- **DE is a risk reduction capability for nuclear, enabling projects to complete closer to budget and schedule than current trends**





Via Interim monitoring of cost dynamics for publicly supported energy technologies - ScienceDirect

Digital Transformation Process

1. Transform the way Organizations / Projects Generate Data

- Model-Based Engineering
- Systems Engineering
- Model-Based Systems Eng.
- Simulation

→

2. Transform the way Organizations / Projects Store and Connect Data

- Digital Threads
- Data Warehouses
- Product Lifecycle Management
- Configuration Management

→

3. Transform the way Organizations / Projects Use and Automate Data

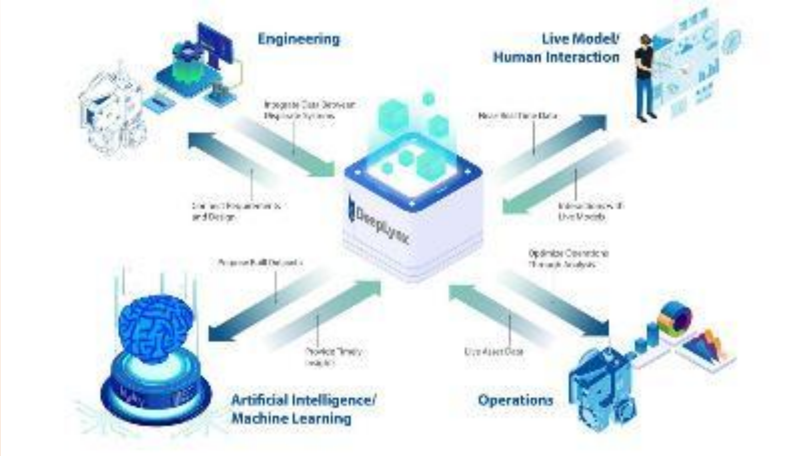
- Data Pipelines
- Data Analysis
- Artificial Intelligence

Computing Infrastructure, Cloud Hosting, Authentication, etc.

Culture and Workforce Adoption

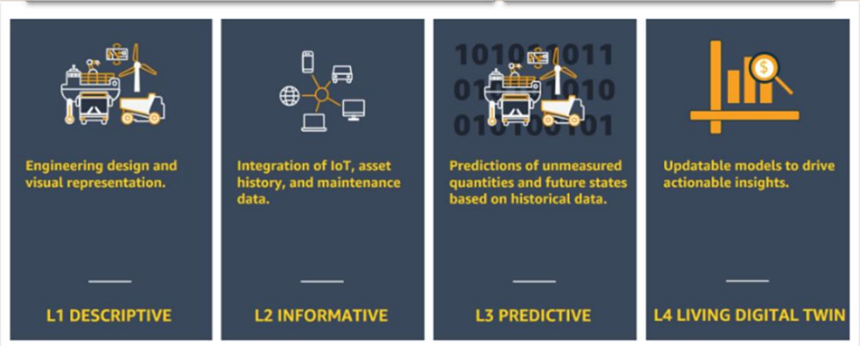
Digital Ecosystems

- **Interconnected** software data exchange used to enable digital engineering and digital twinning systems
- **Connects** data to other digital definitions created later in the development process
- Maintains system **integrity** across lifecycle
- Standardized ontologies to store and relate information
- Suite of software adapters using open-source directed acyclic graph (DAGs) technology



Digital Twins

- Digital Twins represent the merging of integrated and connected data, sensors and instrumentation, artificial intelligence, and online monitoring into a single cohesive unit.
- What is different than a traditional simulation?
- Integration of real-time data
- Dynamic model update (AI/ML integration)
- Real-time operator visualization
- Accurate predictions with fused (integrated) data
- Ability to enable autonomous control
- Distributed across computing platforms



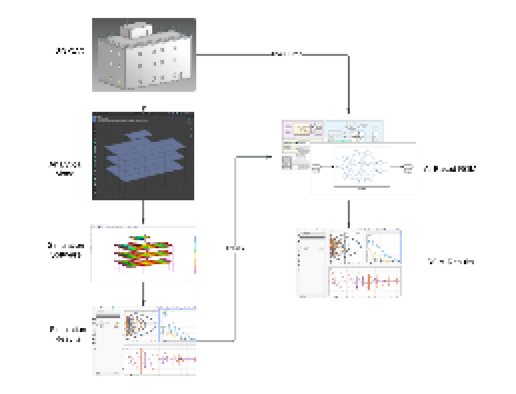
DT Levels framework adapted from: Verdantix, Five Digital Twin Strategies For Industrial Facilities, 2019.

Extended Reality (XR)

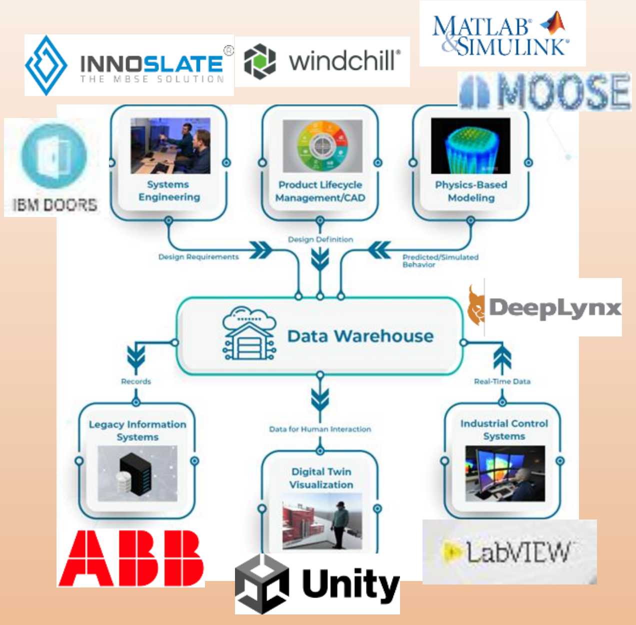
- A graph and source of information is nice, but humans are visual – we need a better way to consume data
- Extended reality (XR)
  - Virtual reality (VR)
  - Augmented reality (AR)
  - Mixed reality (MR)
- Centering information on models facilitates understanding
- Engineers can interact with visualization – inspect, change, delete, etc.

Some INL Case Studies

Seismic Analysis Automation



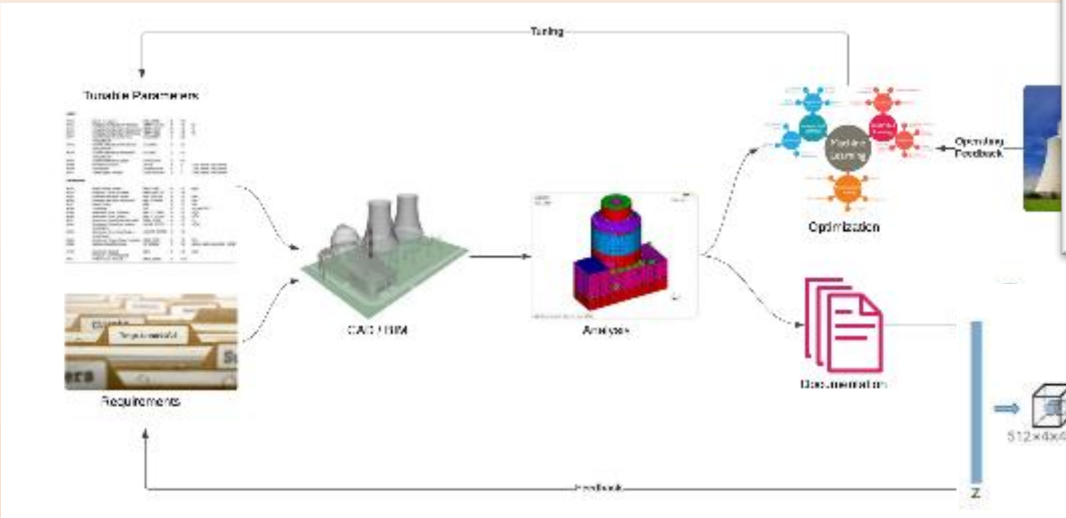
NRIC Digital Engineering Ecosystem

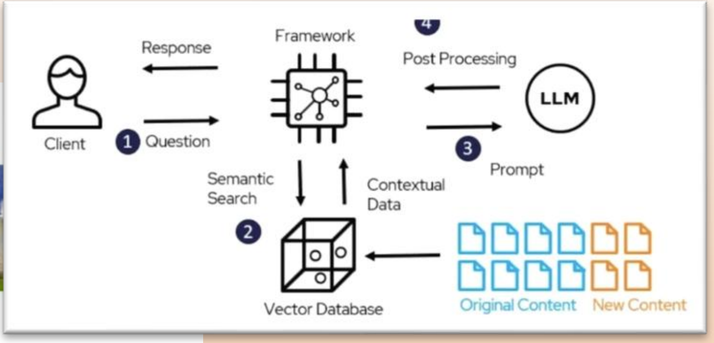


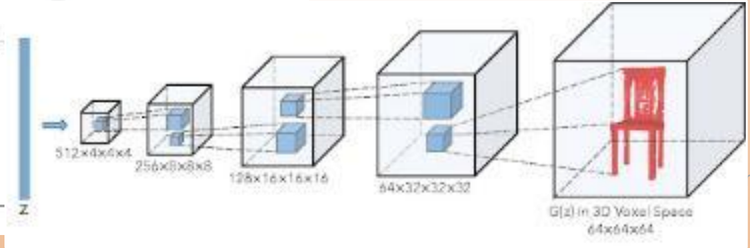
AGN-201 University Reactor Digital Twin

Artificial Intelligence

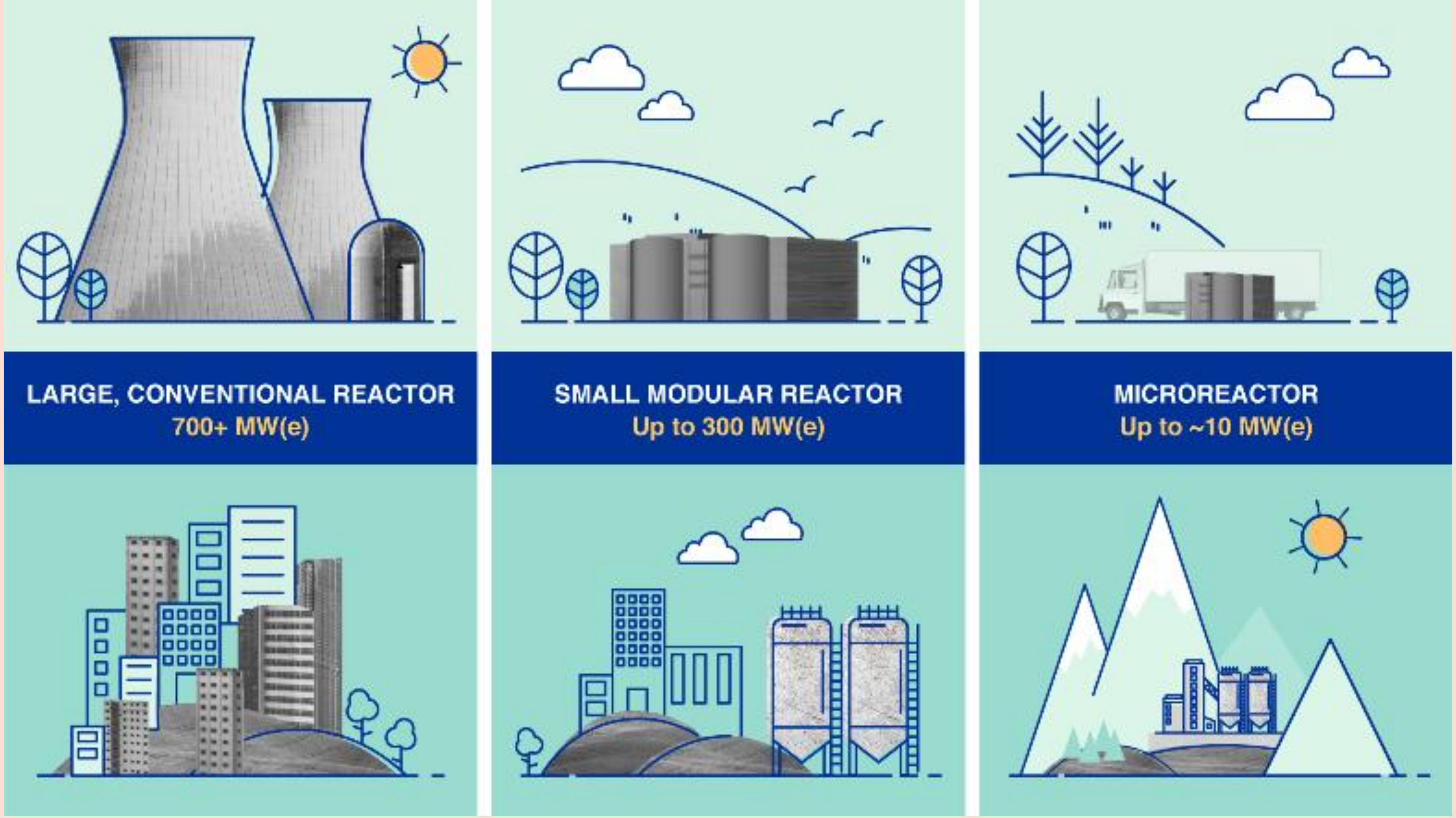
Engineering and systems have become more complicated – AI can help us manage this complexity by accelerating / augmenting traditional systems engineering processes







Small Modular Reactors (SMRs)



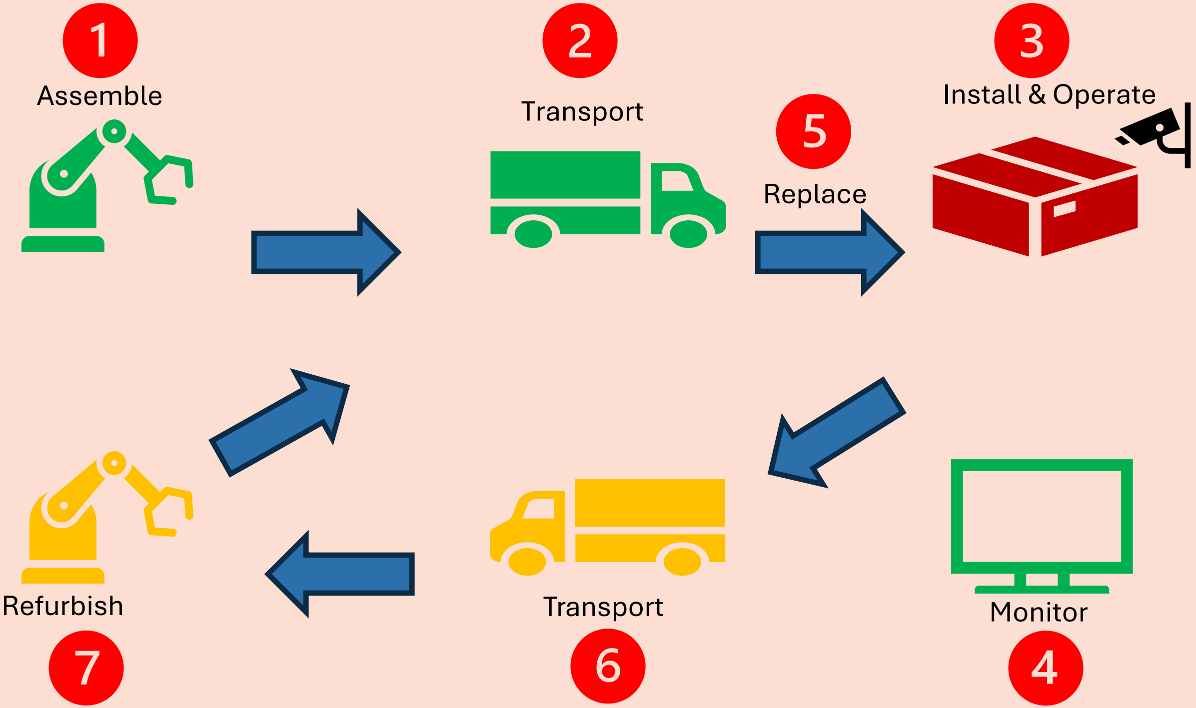
Source: A. Vargas/IAEA 2024

Advantages of SMRs/Microreactors

Much smaller and simpler than traditional nuclear power reactors.

- Minimum site preparation
- Standard, commercial components
- Flexible operation
- Enhanced safety
- Refueling (every 2-10 years)
- Operational lifetime: 5 –20 years.

SMR Lifecycle



Mass Production

According to Copenhagen Atomics, thorium molten salt breeder reactors can be mass manufactured on assembly lines with an expected output of minimum 1 reactor per day (per assembly line).

https://www.copenhagenatomics.com/about/

Image generated by Microsoft Designer

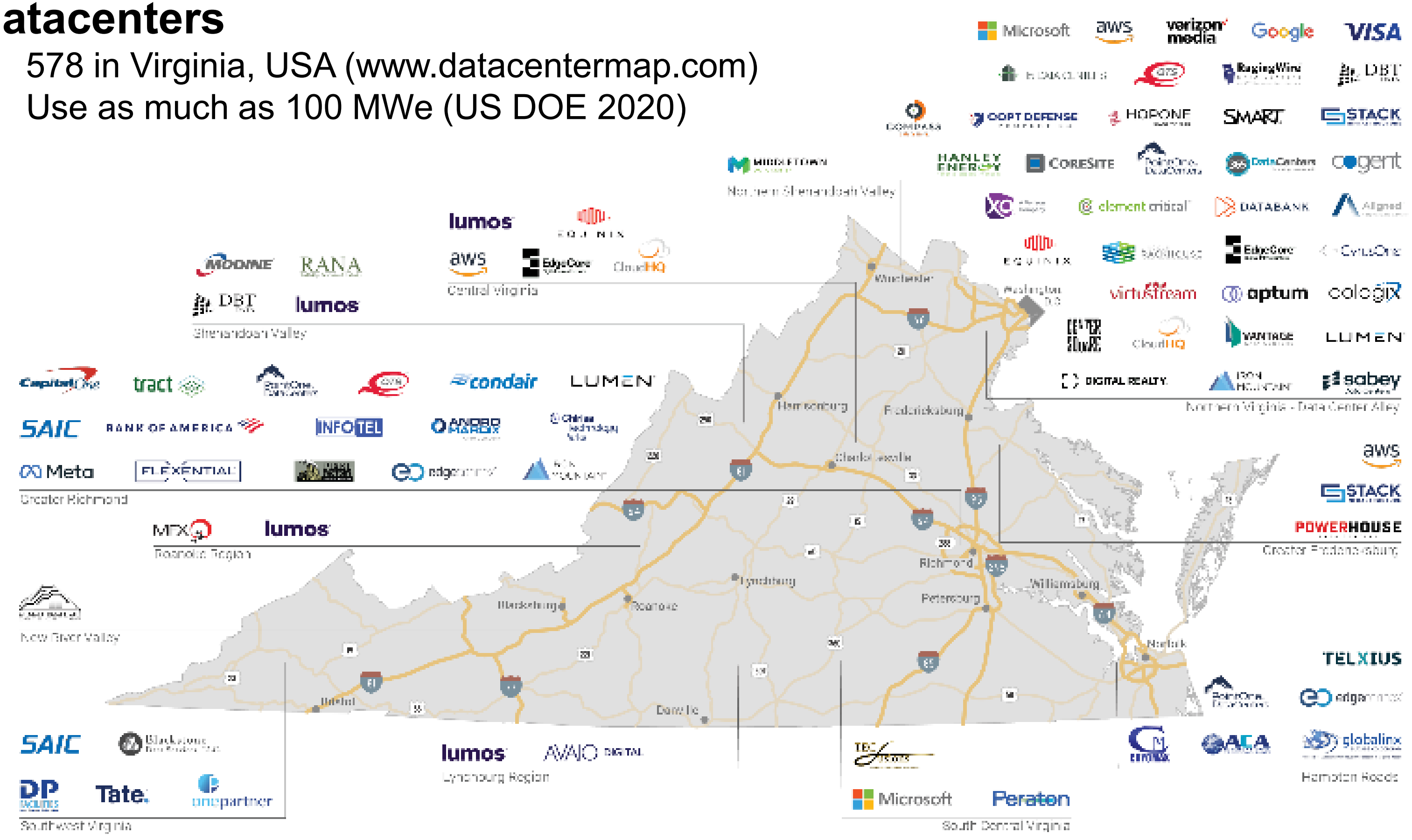
Modular Deployment

https://www.copenhagenatomics.com: Conceptual visualization of a 1GW power plant.

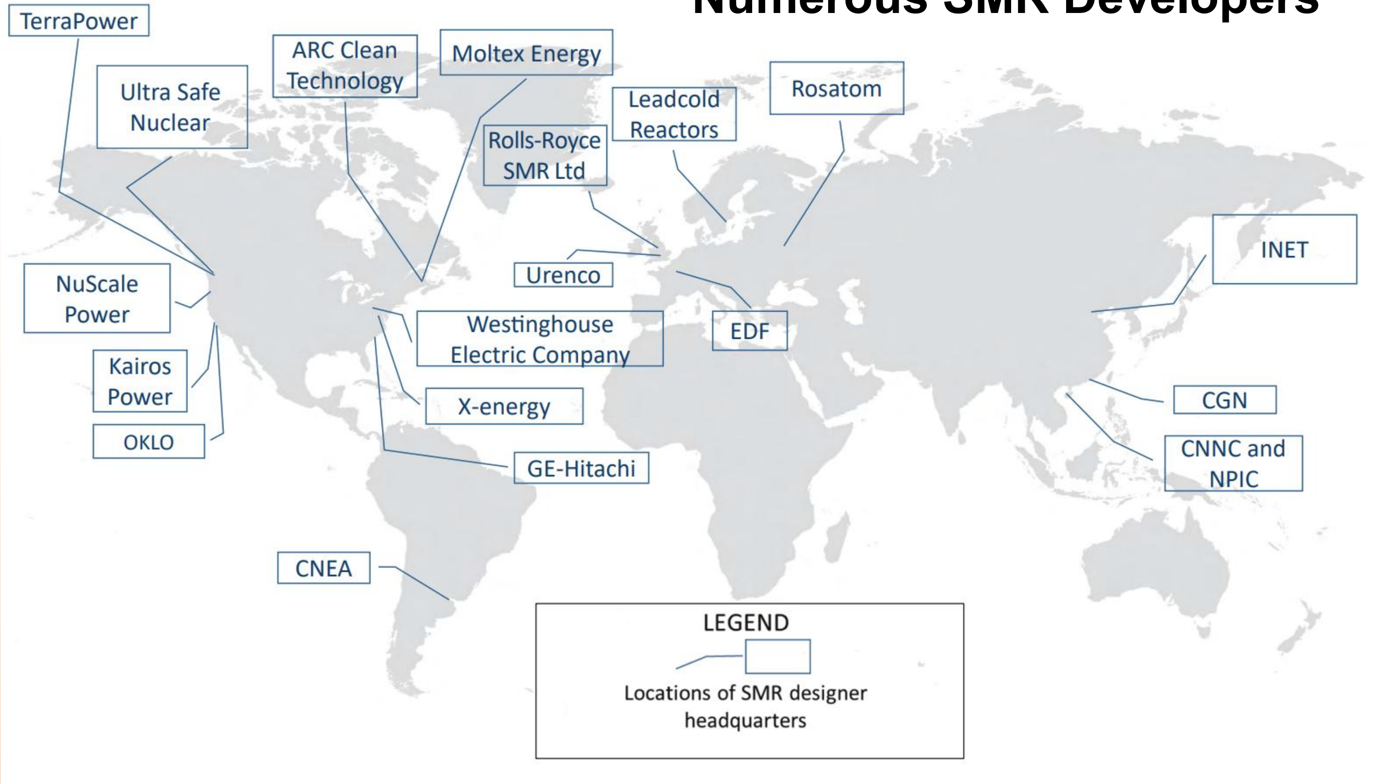
INCOSE

Datacenters

- 578 in Virginia, USA (www.datacentermap.com)
- Use as much as 100 MWe (US DOE 2020)



Numerous SMR Developers



Source: The NEA Small Modular Reactor Dashboard (2023). The list changes rather rapidly.

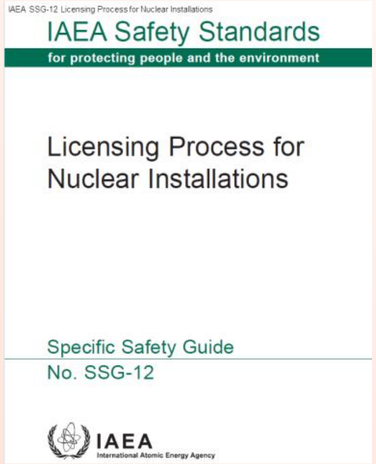
Traditional Licensing Processes

The IAEA identifies a multi-step process and 32 examples of documents to be submitted to the regulatory body. The regulatory body must review the documentation to assess the safety of the proposed nuclear installation. *Source: IAEA SSG-12, Licensing Process for Nuclear Installations.*

The licensing process usually takes years of submittals and feedback. *Source: https://www.nuclearinnovationalliance.org*

Image generated by Microsoft Designer

International Atomic Energy Agency (IAEA) SSG-12 Licensing Process for Nuclear Installations



"alternative approaches do exist, especially for countries with experience in nuclear power where several similar nuclear installations have already been built and are proven."

Proposal for an Alternative Licensing Process

Design an application review process that is repeatable, objective, and comprehensive.

Case Study: Digital Documented Safety Analysis (DgDSA)

The Documented Safety Analysis (DSA) is a US Department of Energy (USDOE) that requires the review and approval of numerous documents. It includes an in-depth description of hazards, safe boundaries, and hazard controls.

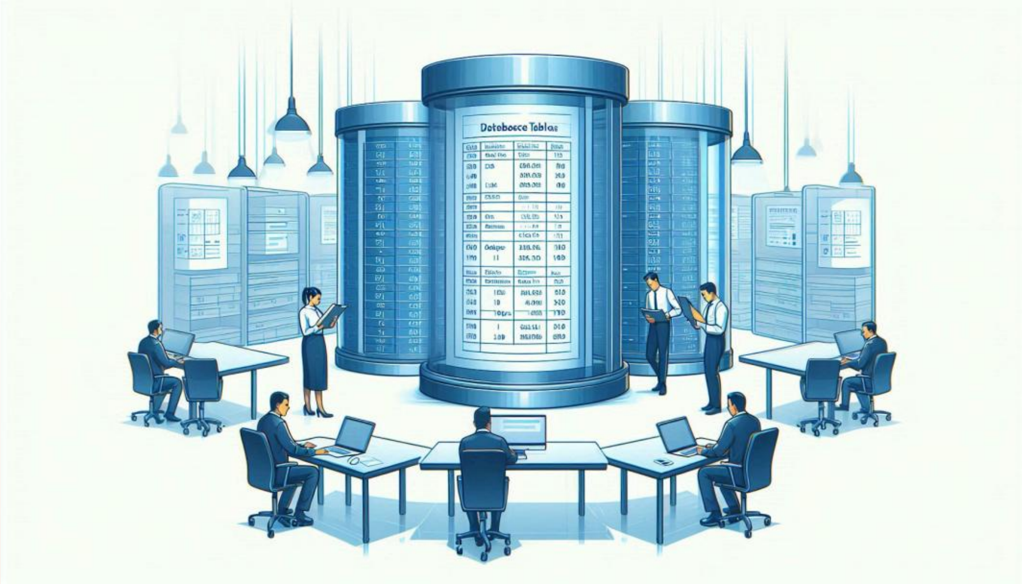


Image generated by Microsoft Designer

Idaho National Laboratory (INL) Motivation

Multiple Test Beds Hosting Multiple Microreactors Each Requiring a Documented Safety Analysis

DOME Test Bed

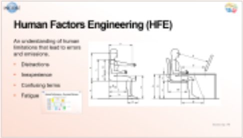
DOME: Demonstration of Operational Microreactor Experiments

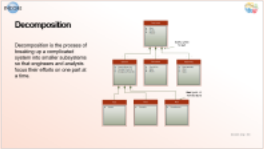
LOTUS Test Bed

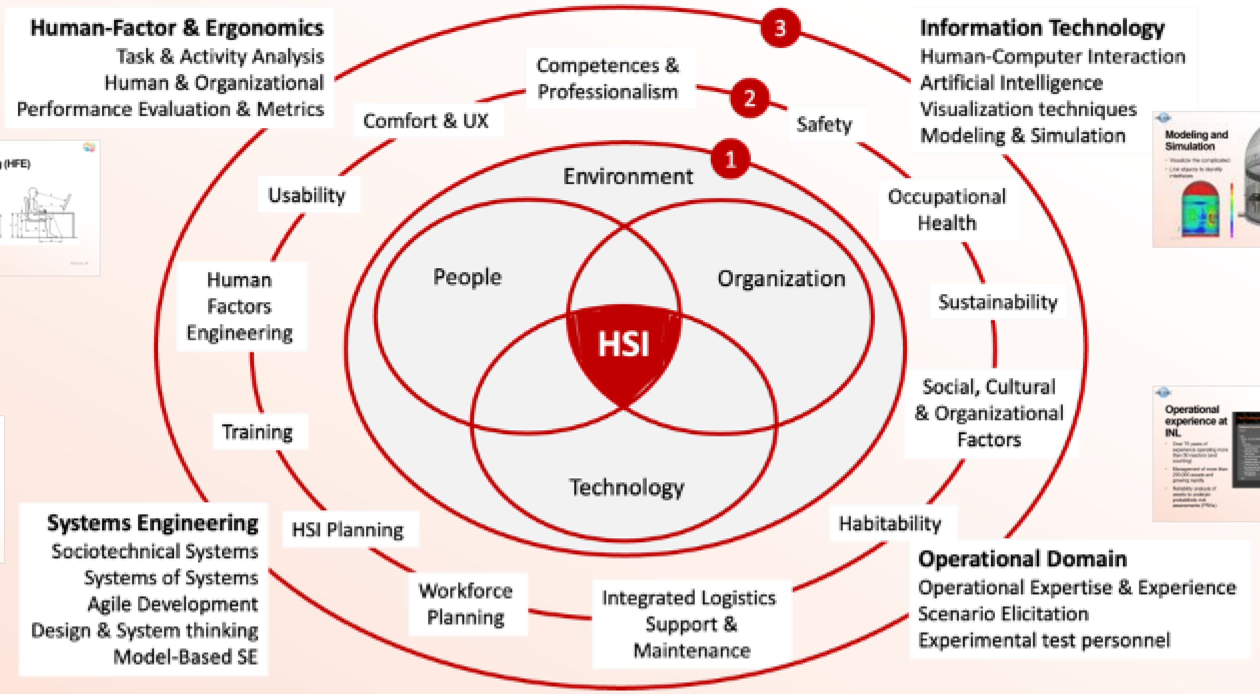
LOTUS: Laboratory for Operation and Testing in the United States

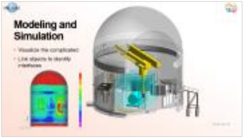
See INL/RPT-23-72206, Recommendations to Improve NRC Licensing

Study human performance to make a better license application









Source: INCOSE The Human Systems Integration (HSI) Primer

Bad practices that diminish human performance

Based on a review of recent (but highly redacted) submittals to the US Nuclear Regulatory Commission (USNRC)* and author reviews of developer documents

*https://www.nrc.gov/reactors/new-reactors/advanced/who-were-working-with/pre-application-activities.html

- Use of non-standard abbreviations and terms
- Unnecessary words
- Paragraphs with multiple topics
- Misidentified performers
- Unnecessary complexity
- Incomplete

Non-standard abbreviations and terms

INCOSE *Guide for Writing Requirements* (GWR) is also applicable to technical writing

Characteristics and Rules in the GWR

C11 – Consistent: Use a consistent language (that is, the same words are used throughout the set to mean the same thing).

R37 – Acronyms: Consistent with other artifacts developed across the lifecycle.

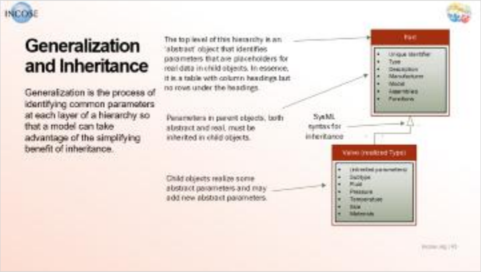
Confusing: "Ice cream scoop" (for a pump outlet)

Example Standards: NRC Glossary for reactors and OmniClass® for host facilities.

Solution: Load database with standard terms and abbreviations and use macros to flag non-standard items.

Unnecessary words

Refer to best practices from software code, database structures, and construction specifications



Examples:

- A passive voice adds auxiliary (helper) words.
- Duplicate words such as “The System shall” when the entire section is about the System.
- Duplicate requirements among various documents

Solution:

- **Active Voice**: Start directives with a verb
- **Generalize**: Sort information into a hierarchy and present in a tree view.
- **Inherit**: Don’t copy general information into containers of specific information.

Paragraphs with multiple topics

The INCOSE *Guide for Writing Requirements* (GWR) is also applicable to technical writing.

Common English Syntax is also applicable to technical writing. For example, *Topic Sentences That Make the Purpose Clear*

https://www.yourdictionary.com/articles/topic-sentences-purpose

Characteristics and Rules in the GWR

C5 – Singular: (A paragraph) should state a single capability, characteristic, constraint, or quality factor.

R1 – Structured Statements: Conform to a standard pattern (such as paragraphs that begin with a topic sentence).

Solution: Parse paragraphs into single topics and paste two or three words at the beginning of each paragraph to identify the topic.

Parse paragraphs into single topics

Before

The reactor core is enclosed within a canister filled with an inert gas just above atmospheric pressure to protect reactor components from oxidation while enhancing heat transfer. The core design consists of graphite blocks with repeated, segmented, hexagonal unit cells oriented horizontally along the length of the core. The unit cells contain channels for fuel, burnable absorbers, alkali metal heat pipes, and shutdown rods.

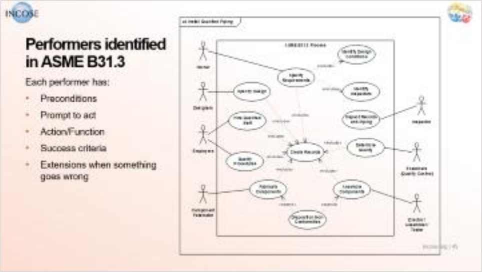
After

Reactor Enclosure: A canister filled with an inert gas encloses the reactor core. The system maintains the gas above atmospheric pressure to protect reactor components from oxidation while enhancing heat transfer.

Core Configuration: The core consists of graphite blocks with repeated, segmented, hexagonal unit cells oriented horizontally along the length of the core.

Unit Cell Content: Unit cells contain channels for fuel, burnable absorbers, alkali metal heat pipes, and shutdown rods.

Misidentified performer



Most codes and standards direct a human to perform something.

Yet, many functions, requirements, and descriptions written by engineers misidentify the system as the performer.

Incorrect: "The system shall comply with ASME B31.3."

Solution: Use case diagrams and associated tables clarify who or what is the performer: specifiers, designers, contractors, crafts, software, hardware, etc.

Unnecessary Complexity

Problem: Focusing on codes and standards rather than functions

Result: Amorphous, incomplete set of requirements.

Solution: Focus on functions first. What must the system do? Then for each function, identify the performance requirements.

An elegant solution

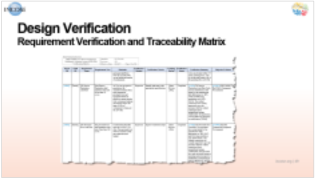
A simplification of NASA/TP–20205003644

Author's Definition: A data-based application that is so well structured that it only takes simple queries to derive an enormous amount of useful information.

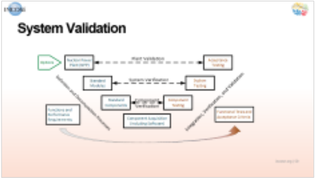
Design Verification & System Validation

ISO/IEC/IEEE 15288
as cited in the INCOSE
Systems Engineering
Handbook

Design Verification is comparing design outputs to design requirements to verify compliance.



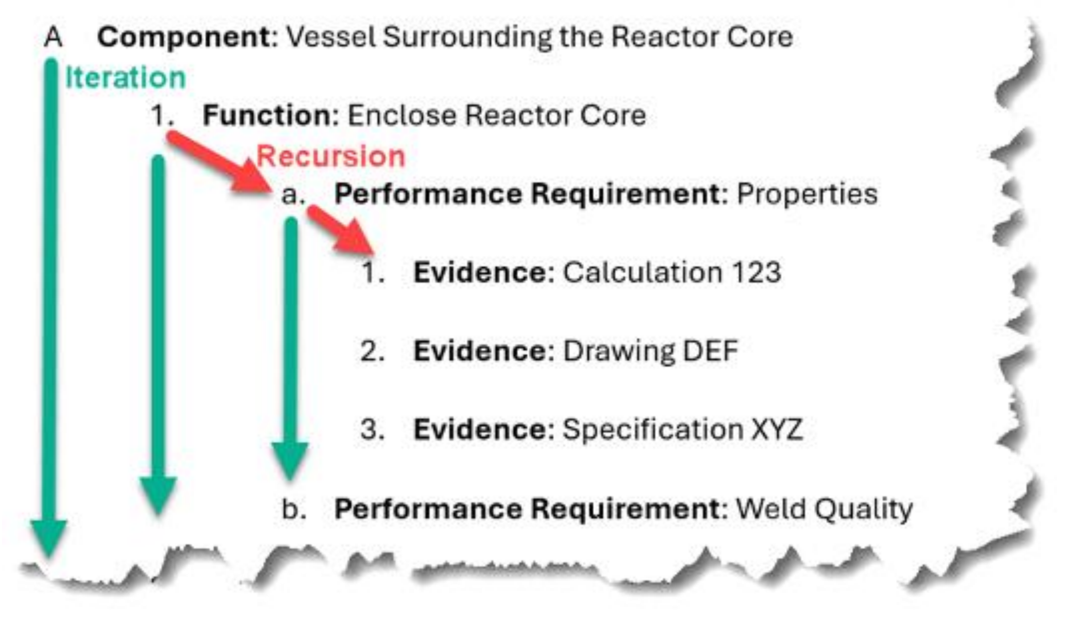
System Validation is the objective evidence that the system, when in use, fulfils its business or mission objectives and stakeholder requirements, achieving its intended use in its intended operational environment



Traversable Structure

Verify

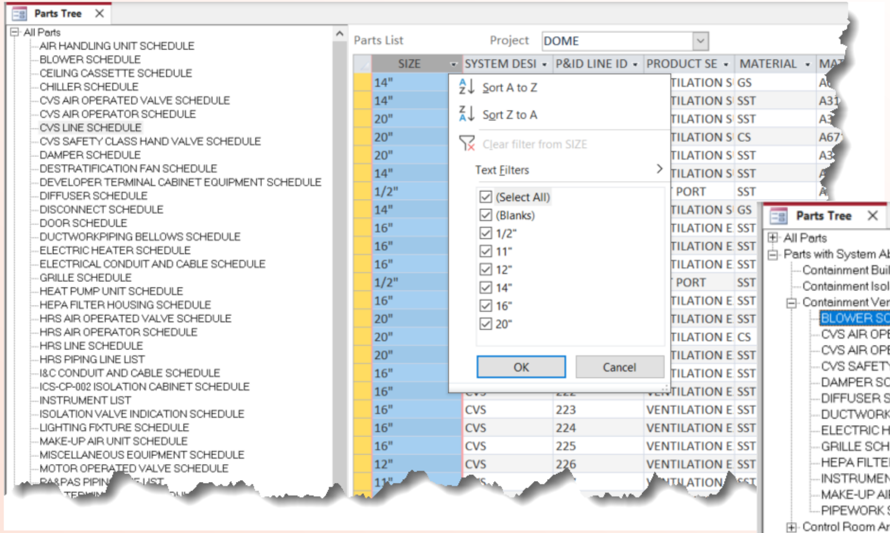
- Decomposition
- Every component has a function
- Every function has performance requirements
- Every requirement has objective evidence of compliance



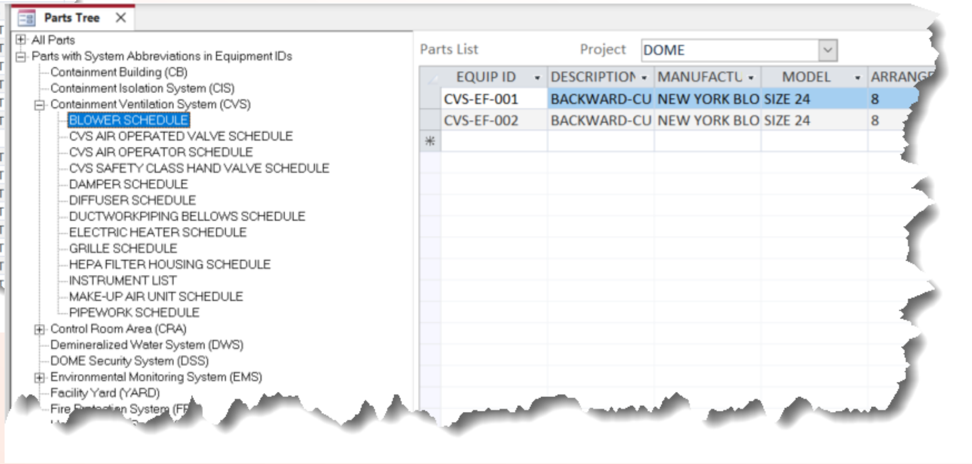
![INCOSE]

Dynamic Views

Part Hierarchy

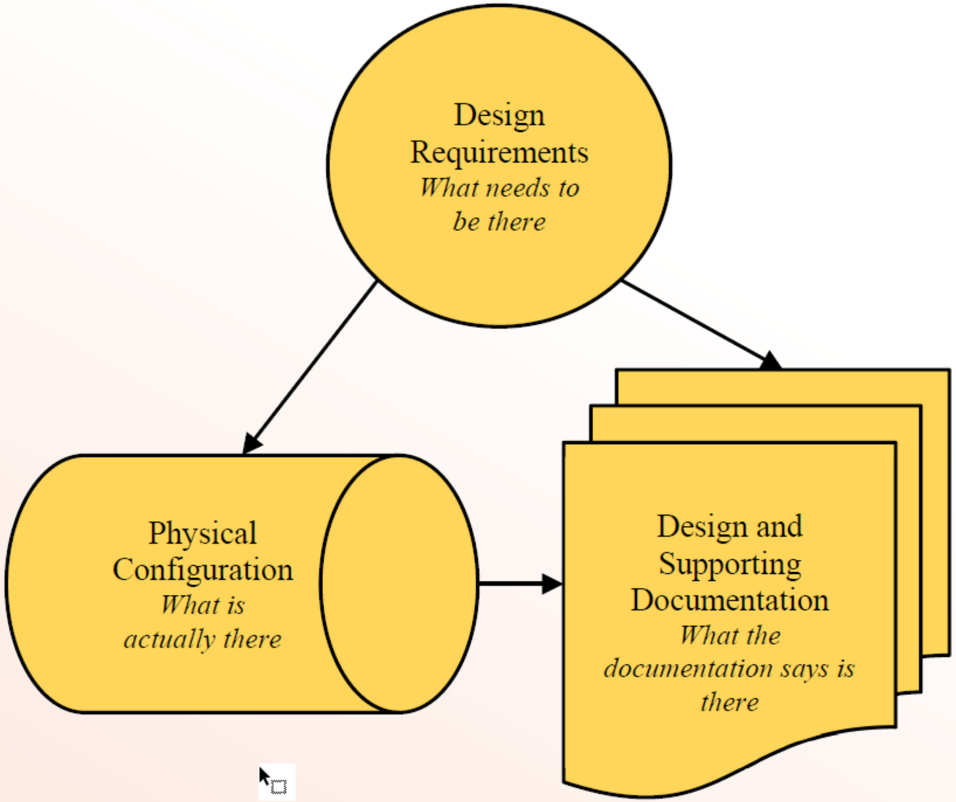


Parts in Each System



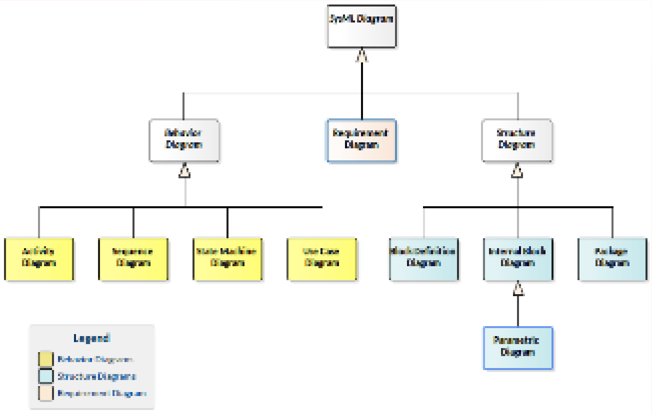
Configuration Management

Making sure that the design basis, the design, the physical system, and the operating procedures are always consistent.

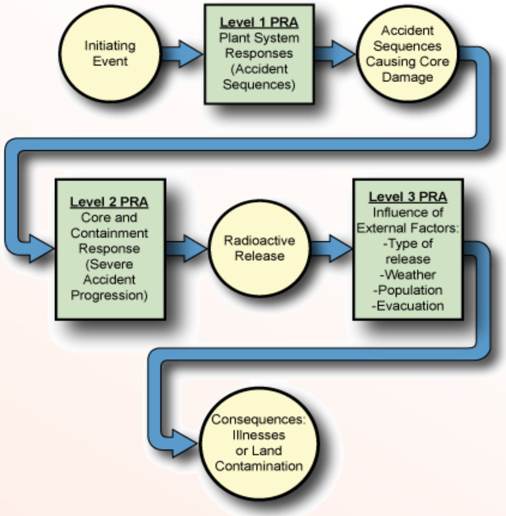


Phase 2 – Transformation of Data

Model-Based Systems Engineering



Probabilistic Risk Assessment (PRA)



Risk Analysis and Assessment Modeling Language (RAAML)

INCOSE

35th Annual INCOSE international symposium

hybrid event

Ottawa, Canada
July 26 - 31, 2025

INCOSE

Home ▸ NRC Library ▸ Basic References ▸ Glossary

Full-Text Glossary

See also NUREG-0544, "Collection of Abbreviations"

Access hatch

An airtight door system that preserves the pressure integrity of reactor, while allowing access to personnel and equipment.

Activation

The process of making a radioisotope by bombarding a stable

Active fuel length

The end-to-end dimension of fuel material within a fuel assemb element").

Activity

The rate of disintegration (transformation) or decay of radioacti activity (also known as radioactivity) are the curie (Ci) and the Measuring Radiati

MasterFormat®

A

	abatement
02 82 13	asbestos
02 80 00	hazardous materials
01 66 13	hazardous materials, procedures
02 63 00	hazardous materials, site
02 83 00	lead
02 84 00	PCB
01 42 13	abbreviations
	aboveground storage tanks
33 56 43	aviation fuel storage
33 56 13	fuel, utility
23 13 23	fuel-oil, facility
33 56 13	hydrocarbon
23 13 26	liquefied-petroleum gas, facility
09 96 13	abrasion-resistant coatings
	abrasive aggregates
03 05 00	concrete
09 60 00	flooring
32 10 00	paving
09 66 00	terrazzo flooring
40 32 10	abrasive materials piping and chutes
05 55 00	abrasive metal treads and nosings
09 60 00	abrasive safety floors
09 30 00	abrasive tile
23 64 13	absorption water chillers
26 32 00	AC generators
40 77 13	acceleration measurement
03 05 00	accelerators, concrete
00 65 19	acceptance certificate
01 71 16	acceptance of conditions
01 64 00	acceptance of products
01 23 00	acceptance procedures for rnate bi
28 16 00	interfaces
28 11 00	global applications
28 14 15	inputs and outputs
28 15 11	integrated credential readers
28 15 11	keypads
28 19 11	loading dock systems
28 18 11	metal detectors
28 17 17	mobile access identification management systems
28 13 11	mobile applications
28 14 11	network controllers
28 13 11	operating systems
28 19 13	parking garages
11 14 00	pedestrian traffic
28 19 15	perimeter
28 05 07	power sources
28 14 17	printers and encoders
28 15 19	remote devices
28 17 13	self check-in and kiosk visitor systems
28 18 17	sniffing equipment
28 13 11	software
28 12 01	system requirements
28 05 09	surge protection
28 14 00	system hardware
28 19 00	vehicle identification systems
28 17 11	visitor management systems
28 15 13	wireless key fobs
28 18 13	x-ray equipment
08 31 13	**access doors**
23 33 33	ductwork
07 72 33	roof hatches
09 69 00	access flooring
07 72 33	access hatches, roof
08 31 13	**a... panels**
08 70 79	hardware
10 28 26	hygiene and custo
12 40 00	interior decorating
12 92 43	interior landscapin
11 53 43	laboratory
10 28 23	laundry
04 05 23	masonry
12 41 00	office
32 94 00	planting
09 65 13	resilient flooring
07 72 00	roof
13 11 46	swimming pool
12 42 00	table
10 28 13	toilet
	accordion folding
08 35 13	doors
08 35 16	grilles
10 22 39	panel partitions
40 17 13	acetylene welding pipi
40 17 16	acetylene-hydrogen welding piping
	acid etching
03 35 00	concrete
08 81 00	glass
12 17 13	glass artwork
	acid-resistant
04 61 00	brick
09 96 35	coatings
09 62 35	flooring
08 81 00	glass
04 05 13	mortar
	acoustic
02 22 16	assessment
00 31 19	available informa...
09 83 16	ceiling coating
09 83 22	draperies
09 83 00	finishes
09 ...	floo...

Parse paragraphs into single topics

Before

The reactor core is enclosed within a canister filled with an inert gas just above atmospheric pressure to protect reactor components from oxidation while enhancing heat transfer. The core design consists of graphite blocks with repeated, segmented, hexagonal unit cells oriented horizontally along the length of the core. The unit cells contain channels for fuel, burnable absorbers, alkali metal heat pipes, and shutdown rods.

After

Reactor Enclosure: A canister filled with an inert gas encloses the reactor core. The system maintains the gas above atmospheric pressure to protect reactor components from oxidation while enhancing heat transfer.

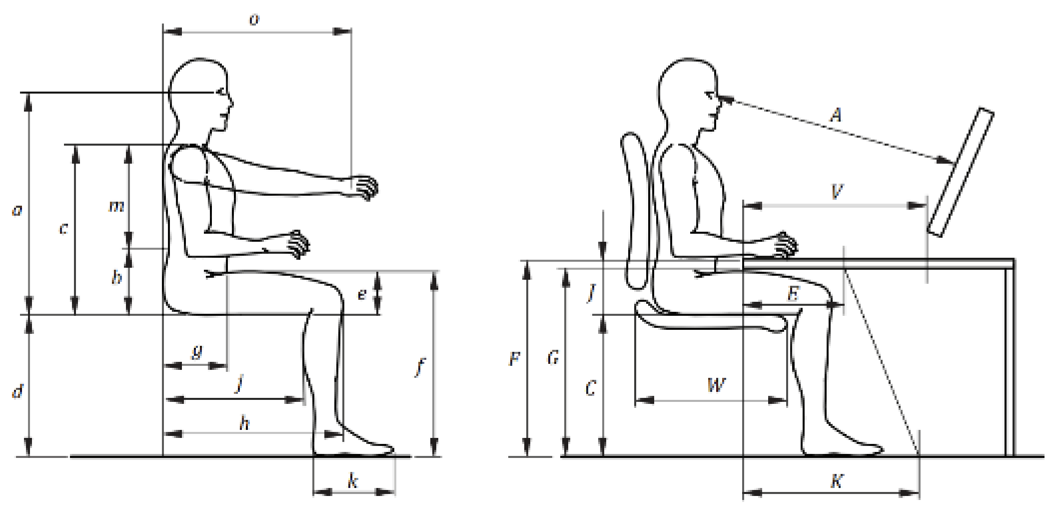
Core Configuration: The core consists of graphite blocks with repeated, segmented, hexagonal unit cells oriented horizontally along the length of the core.

Unit Cell Content: Unit cells contain channels for fuel, burnable absorbers, alkali metal heat pipes, and shutdown rods.

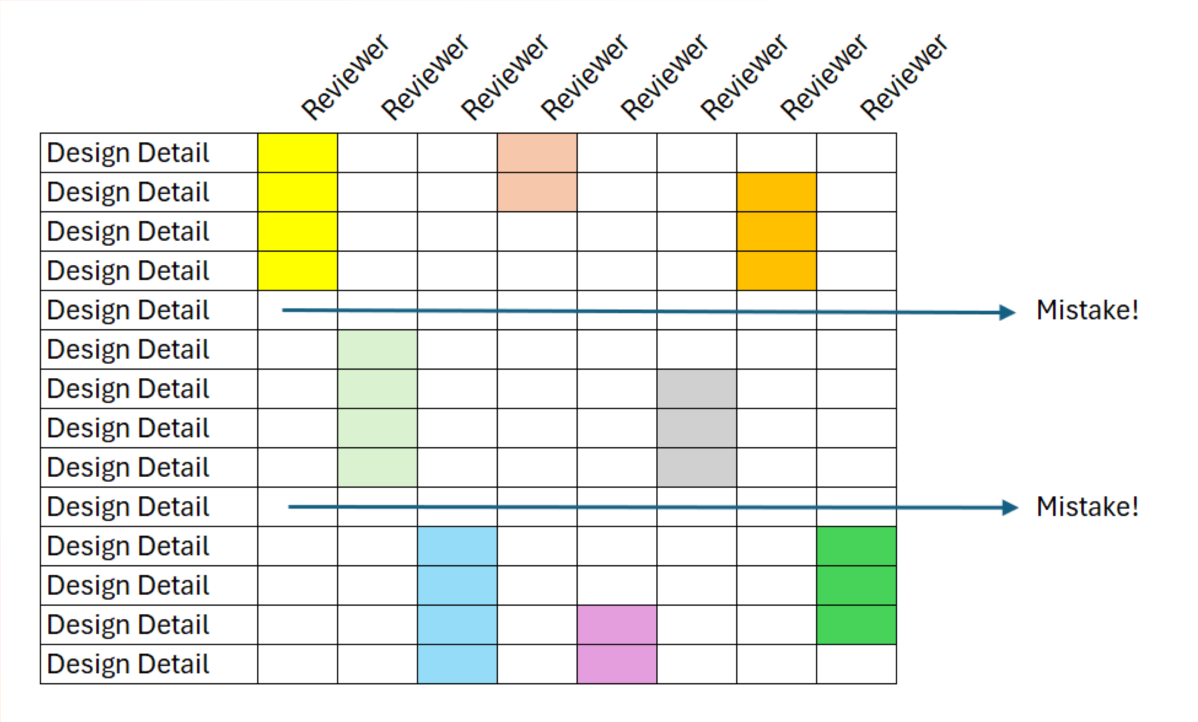
Human Factors Engineering (HFE)

An understanding of human limitations that lead to errors and omissions.

- Distractions
- Inexperience
- Confusing terms
- Fatigue

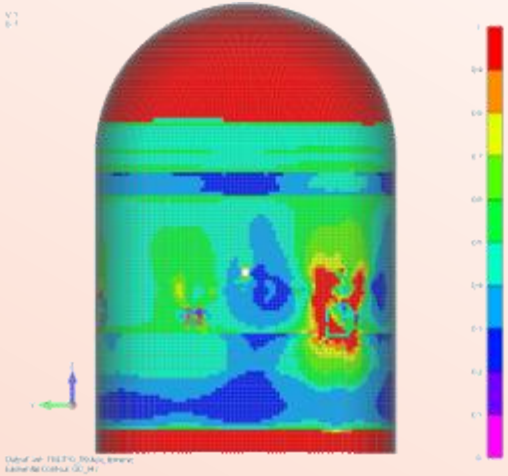


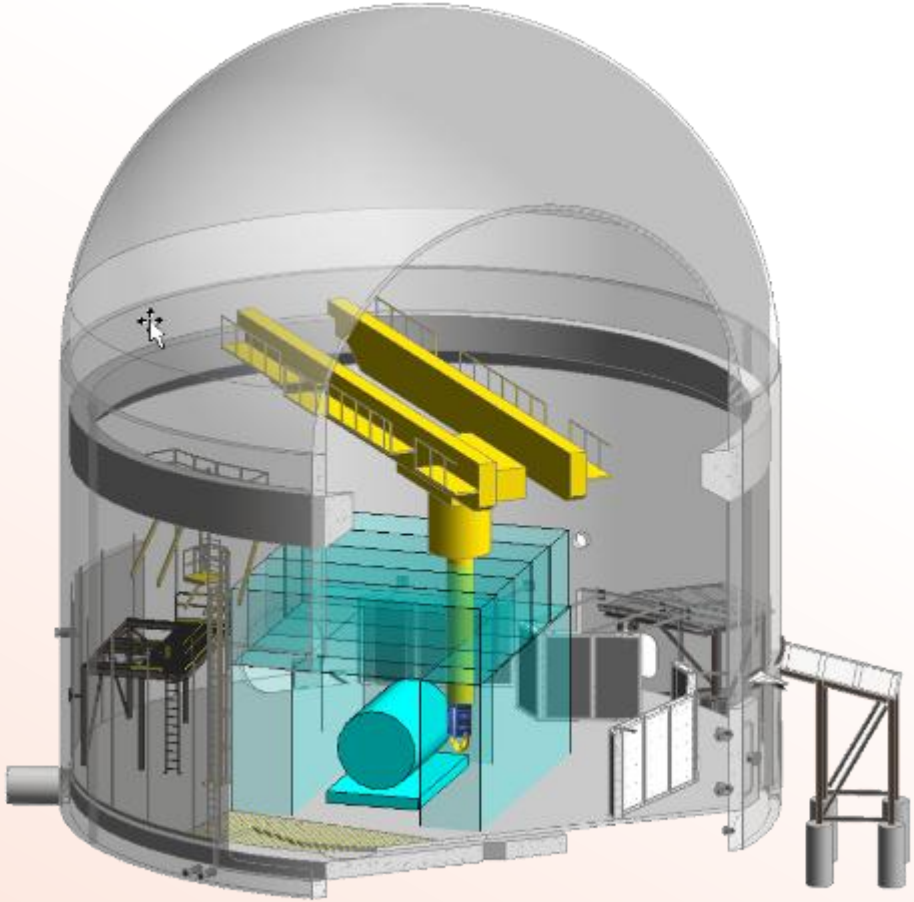
Human Performance – Document Reviews



Modeling and Simulation

- Visualize the complicated
- Link objects to identify interfaces





Generalization and Inheritance

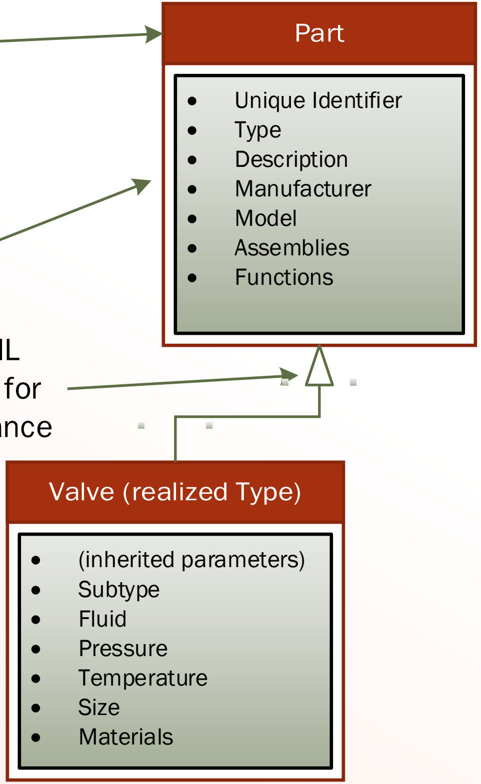
Generalization is the process of identifying common parameters at each layer of a hierarchy so that a model can take advantage of the simplifying benefit of inheritance.

The top level of this hierarchy is an ‘abstract’ object that identifies parameters that are placeholders for real data in child objects. In essence, it is a table with column headings but no rows under the headings.

Parameters in parent objects, both abstract and real, must be inherited in child objects.

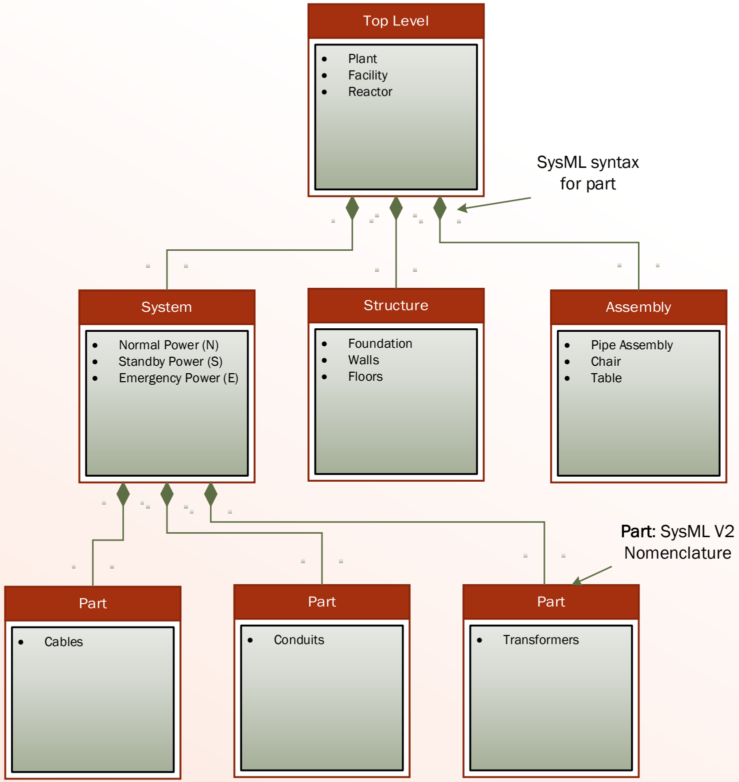
SysML syntax for inheritance

Child objects realize some abstract parameters and may add new abstract parameters.



Decomposition

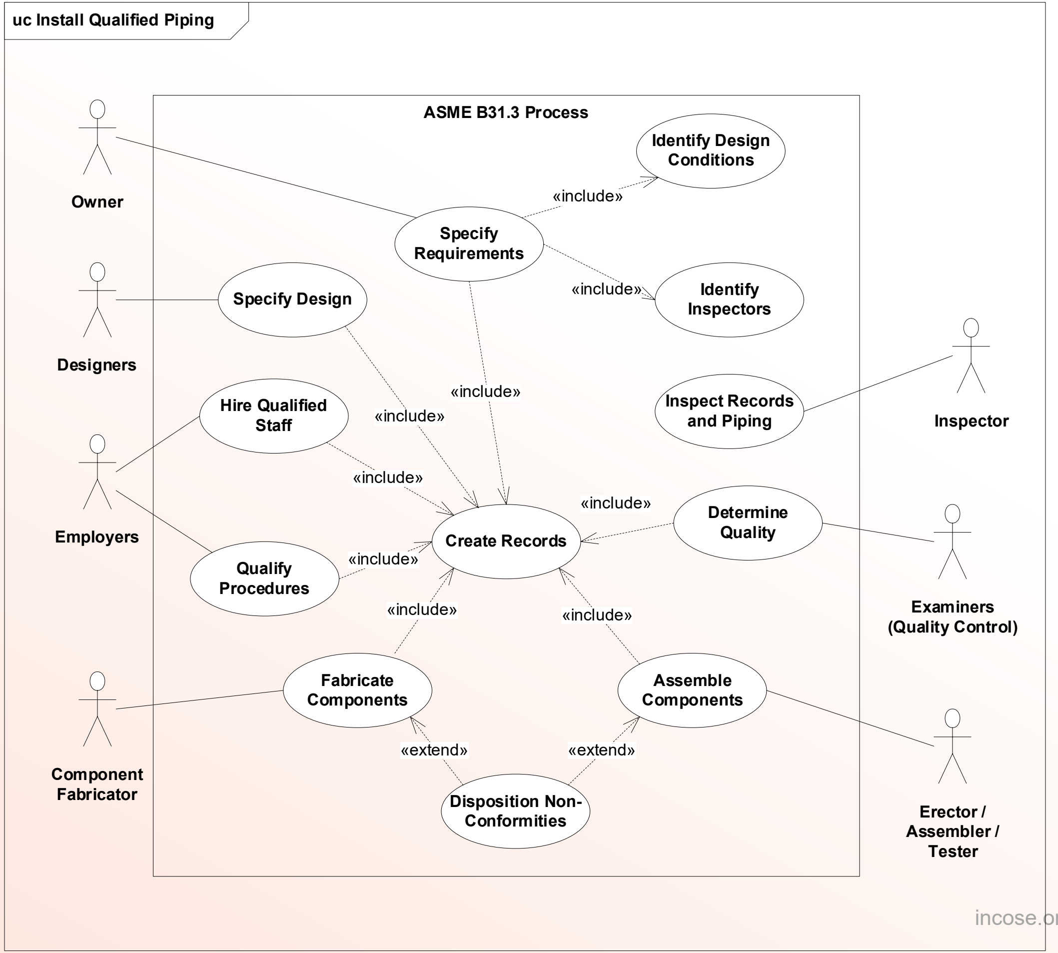
Decomposition is the process of breaking up a complicated system into smaller subsystems so that engineers and analysts focus their efforts on one part at a time.



Performers identified in ASME B31.3

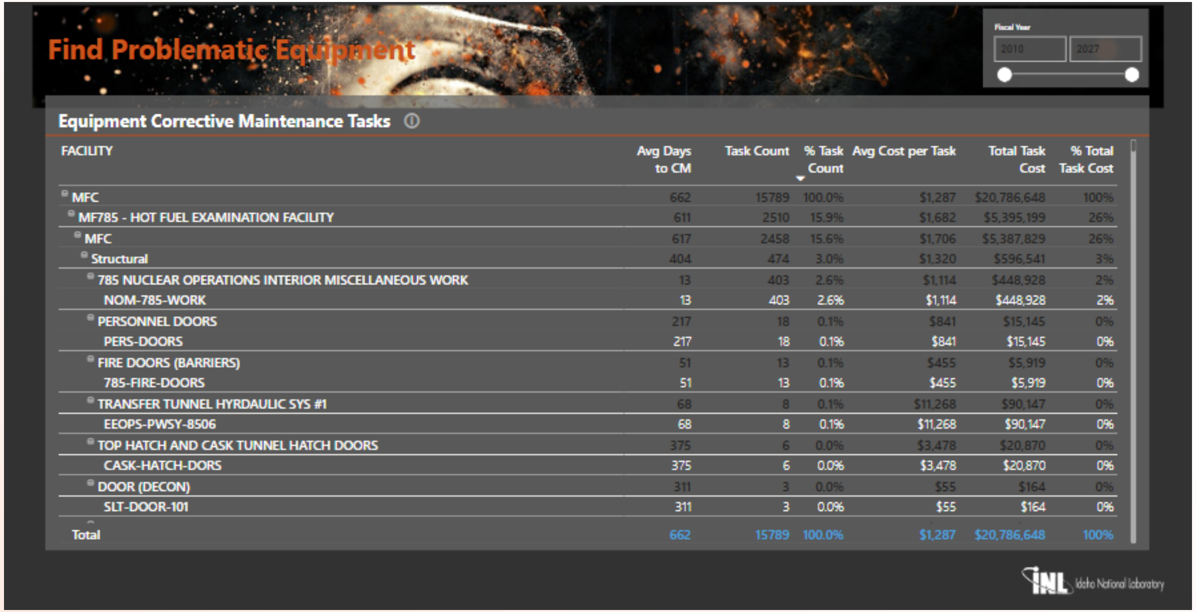
Each performer has:

- Preconditions
- Prompt to act
- Action/Function
- Success criteria
- Extensions when something goes wrong



Operational experience at INL

- Over 75 years of experience operating more than 50 reactors (and counting)
- Management of more than 200,000 assets and growing rapidly
- Reliability analysis of assets to underpin probabilistic risk assessments (PRAs)



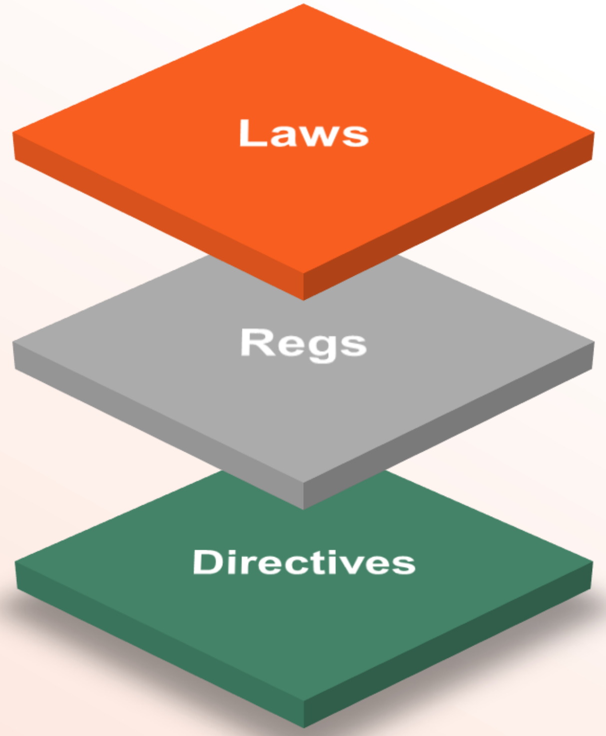
FACILITY	Avg Days to CM	Task Count	% Task Count	Avg Cost per Task	Total Task Cost	% Total Task Cost
MFC	662	15789	100.0%	$1,287	$20,786,648	100%
MF785 - HOT FUEL EXAMINATION FACILITY	611	2510	15.9%	$1,682	$5,395,199	26%
MFC	617	2458	15.6%	$1,706	$5,387,829	26%
Structural	404	474	3.0%	$1,320	$596,541	3%
785 NUCLEAR OPERATIONS INTERIOR MISCELLANEOUS WORK	13	403	2.6%	$1,114	$448,928	2%
NOM-785-WORK	13	403	2.6%	$1,114	$448,928	2%
PERSONNEL DOORS	217	18	0.1%	$841	$15,145	0%
PERS-DOORS	217	18	0.1%	$841	$15,145	0%
FIRE DOORS (BARRIERS)	51	13	0.1%	$455	$5,919	0%
785-FIRE-DOORS	51	13	0.1%	$455	$5,919	0%
TRANSFER TUNNEL HYRDAULIC SYS #1	68	8	0.1%	$11,268	$90,147	0%
EEOPS-PWSY-8506	68	8	0.1%	$11,268	$90,147	0%
TOP HATCH AND CASK TUNNEL HATCH DOORS	375	6	0.0%	$3,478	$20,870	0%
CASK-HATCH-DORS	375	6	0.0%	$3,478	$20,870	0%
DOOR (DECON)	311	3	0.0%	$55	$164	0%
SLT-DOOR-101	311	3	0.0%	$55	$164	0%
Total	662	15789	100.0%	$1,287	$20,786,648	100%

10,000 References to Codes and Standards

Laws

Regulations

Government Directives



Engineers typically select from a few codes and standards as requirements

An amorphous mess

Simplify Specifications (Functions First)

1

Before: 20 pages of codes and standards related to an analog temperature transmitter.

2

Concept of Operations:

Distributed digital control

3

After: Two pages identifying a **function**, performance, and a functional test

Design Verification

Requirement Verification and Traceability Matrix

Idaho National Laboratory

NRIC DOME Test Bed Containment Building & Isolation System (SDD-586) Verification Matrix	Identifier: RVTM-MS Revision: 001 Effective Date: DRAFT Page: 18 of 86

Parent ID	Child ID	Requirement Name	Requirement Text	Rationale	Verification Method	Verification Criteria	Verifying Person	Verification Status	Verification Summary	Objective Evidence
				permanent platforms. Note this includes FSC valves inside and outside of containment.					valves are located within 7 ft of the operating floor, with (6) of the eight within 4 ft. of the operating floor. [16130]	
[16062]	[Parent]	CB: Passive Penetration Leak Rate	Each Passive Penetration shall maintain a leak rate of less than 50 cc/sec.	At 50 cc/sec per passive penetration, the cumulative leakage from each penetration, personnel door and equipment hatch are tracked to ensure that the total containment leakage rate remains below the limit of 10% of containment volume per day (24 cfm).	Inspection	Identify leak tests in the appropriate specifications.	Mauro Oliveira [INL]	Compliant	[21478] CB: Passive Penetration Leak Rate: Each passive penetration is leak tested by the manufacturer after fabrication (re. SPC-3206) and following installation (ref. SOW-19419). The welded connections are visually inspected to provide assurance that the welded connections have insignificant leakage. Additionally, the penetration is tested following alteration or modification. [16062]	[132995] NRIC DOME Test Bed NQA-1 Equipment Procurements
[16063]	[Parent]	CB: Personnel Door Leak Rate	The personnel door shall maintain a leak rate of less than 100 cc/sec.	Containment allowable leak rate is 10%/V (24 cfm). The personnel door needs to maintain a leak rate within the total budget.	Inspection	Inspect Construction Spec	Mauro Oliveira [INL]	Compliant	[21479] CB: Personnel Door Leak Rate: The personnel door is leak tested by the manufacturer after fabrication (re. SPC-3207) and following installation (ref. SOW-19419). The welded connections are visually inspected to provide assurance that the welded connections have insignificant leakage. Additionally, the personnel door seals are tested using an operating instruction prior to establishing containment for reactor operation to verify it	[132996] Test Bed Commercial Equipment Procurements

System Validation