2023
Annual INCOSE
international workshop
HYBRID EVENT
Torrance, CA, USA
January 28 - 31, 2023

INCOSE RWG
Pre-IW2023 Sessions

Standards and Regulations Compliance

Lou Wheatcraft, Senior Consultant, Wheatland Consulting
Wheatland.consulting@gmail.com

Needs and Requirements Manual (NRM)

- The NRM (originally NRVVLM) is the RWG flagship product, V1.1 released in May 2022
- Content in the NRM aligns with and provides further elaboration of the concepts and activities contained in the INCOSE SE Handbook version 5 material.
- Material in this presentation is taken from the sections that deal with standards and regulation compliance.

Contents

- Drivers and Constraints
- Lifecycle Concepts and Needs Definition
- Transforming Needs Dealing with Relevant Standards and Regulations into Design Input Requirements
- System Verification and System Validation
- Documenting the Evidence of Compliance
- Obtaining Approval.

Drivers and Constraints

- Drivers and constraints are things outside the project's control that constrain or drive the solution space.
- Compliance is mandatory - failing to show compliance, will result in the system failing system validation, qualification, certification, acceptance, and approval for use.
- Drivers and constraints represent a major source of needs and requirements that drive and constrain the lifecycle concepts analysis and maturation activities as well as the solution space available to the design team.
- **Standards and Regulations are a major source of drivers and constraints.**
  - Showing compliance can represent a substantial portion of product development activities, cost, and schedule.
  - The SOI must be verified to show compliance with the applicable requirements within the standards and regulations
  - The SOI must be validated to show compliance with the needs that invoke the relevant standards and regulations.
  - Organizations must show evidence they have developed the SOI per the relevant standards and regulations.
- Organizations may define internal organizational standards based on lessons learned and best practices to ensure quality products are developed by the organization and establish a "brand".

Standards and Regulations

- Standards and regulations can contain requirements related to:
  - Regulatory compliance (e.g., medical devices, pharmaceuticals, aviation, ground transportation, consumer products);
  - Safety, Security, Resilience (e.g., addressing prevention of harm, loss, misuse; and recovery from loss);
  - Production processes, parts, and workmanship (e.g., soldering, crimping, coding);
  - Development, risk, quality management processes, configuration management project management, systems engineering (e.g., medical devices, pharmaceuticals, transportation, and space systems);
  - Design approaches of certain types of systems (e.g., petroleum extrication, distribution, and processing; medical devices; transportation systems);
  - Specified methods for test, verification, validation, acceptance, certification, and qualification of certain types of systems (e.g., medical devices, pharmaceuticals, safety critical systems, automotive, petroleum, human crewed space systems).
  - Compatibility/Interoperability (e.g., interactions between systems, communication protocols, APIs, ICDs, connectors.

Applicability

- There are standards and regulations that apply to:
  - Processes and methods used by an organization to develop products;
  - All levels of the system architecture and lifecycle stages of products being developed;
  - Showing compliance – system verification, system validation, production verification.
- In some cases, the standards and regulations on the product are written at the design input level of abstraction, stating what needs to be done and why, but not how.
  - The how is left up to the design, test, and manufacturing organizations.
- In other cases, the standards and regulations address specific design “how” implementation type requirements for the design, testing, or manufacturing.
- In the medical device and pharmaceutical world, regulations concerning system validation are of critical importance for approval for release for public use (e.g., animal versus human testing, staged approach to human testing)
  - Clinical trials for certain classes of medical devices and pharmaceuticals

Relevancy

- Projects must make sure they comply with all "**relevant**" industry standards and standards and regulations mandated by the customer and government regulatory agencies.
- "**Relevant**" is highlighted, in that it is important that an organization *only address* standards and regulations and portions of those standards and regulations *that apply* to the the types of products developed by the organization.
- A key mistake is invoking a generic list of standards and regulations on a project without specifically identifying which apply or which portions apply.
- The project will have to show compliance through system verification and system validation activities with each requirement invoked by a standard and regulation.
  - Only those requirements within standards and regulations that are **relevant** to the specific SOI should be invoked by the project to reduce development time and cost.
- Organizations must identify all **relevant** the standards and regulations for each country in which the device is to be marketed.

Rationale must be defined for each standard and regulation, making it clear why that standard and regulation is relevant and why the cost of compliance is acceptable.

Compliance Stakeholders

- Often the organization will have an internal “compliance” or “quality” group responsible for ensuring the relevant standards and regulations are identified, managed, and clearly complied with by all projects within the organization.
- This group will work with each project team within the organizations throughout the development lifecycle activities to help ensure compliance.
- This compliance group will also interact with the external regulatory agencies to make sure:
  - The intent of the standards and regulations are being met.
  - The objective evidence needed to show compliance (system verification and system validation) is clearly defined and concepts for compliance defined, and
  - Data needed for certification, qualification, and acceptance is properly recorded in the **Approval Packages** and submitted to the regulatory agency’s **Approving Authority** in accordance with the requirements defined by the agency.
  - For systems being developed for a customer, the objective evidence and data needed for certification, qualification, and acceptance will be supplied to the customer per the activities and deliverables defined in the SOW or SA.

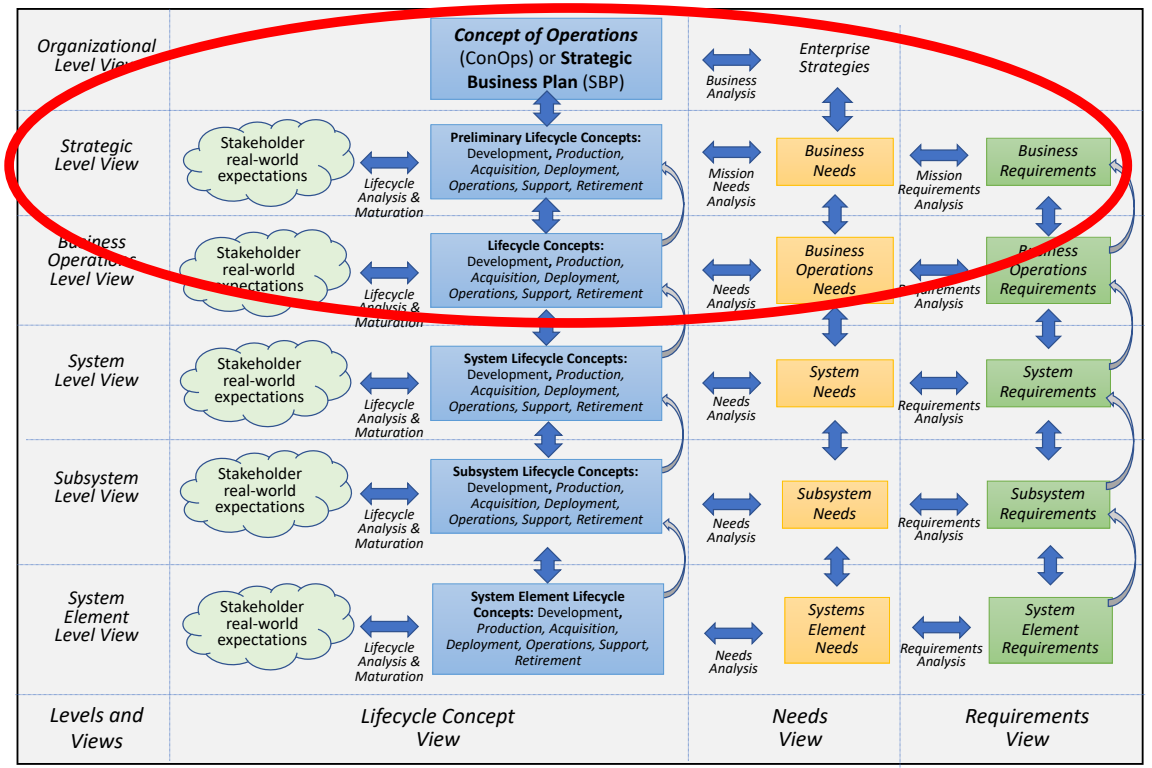
Identification of Relevant Standards and Regulations

As part of an Organization's overall ConOps, product line and services to be provided are identified .

Based on this, relevant standards and regulations are identified.

For these standards and regulations, lifecycle concepts, needs, and requirements are defined that apply to all products and services supplied by the organization.

The compliance stakeholders exist at the business and business operations levels of the organization.



Consequences of Failing to Show Compliance

- Failing to identify **relevant** standards and regulations early in the development lifecycle can result in missing needs and requirements dealing with relevant standards and regulations adding **risk of non-compliance**.
  - How can the SOI be expected to meet security or safety needs and requirements if they were not identified, lifecycle concepts developed concerning compliance, and included in the SOI's integrated sets of needs and resulting sets of design input requirements?
- Failing to show compliance (failed system verification and system validation), will result in the system failing qualification, certification, and approval for use, resulting in the developed SOI being rejected by the customer or regulatory agency.
- If this happens, the result will be costly changes, expensive rework, and schedule slips.
  - In some cases, failing to meet all **relevant** standards and regulations could lead to bankruptcy and loss of millions of dollars.

Compliance Risk

- Failing to **properly** show compliance with standards and regulations is a major source of risk for a project.
  - For example, in 2017, the FDA conducted 17,487 audits worldwide, and issued 5045 letters of non-compliance.
  - To minimize compliance risk, organizations must research and understand:
    - Which standards and regulations are **relevant**, and
    - The requirements for certification, qualification, and acceptance that must be met, and the data and form of the data required by the **approving authorities** and regulatory agencies to show compliance.
- To avoid **compliance risk**, even if not explicitly stated by the customers or other stakeholders, the organization must be aware of and research all relevant standards and regulations applicable to their product line.
  - Failure to address relevant standards and regulations can result in:
    - System rejection by the customers or regulating agencies even if they did not explicitly identify the relevant standards and regulations to which the project must comply.

Developing Products For a Customer

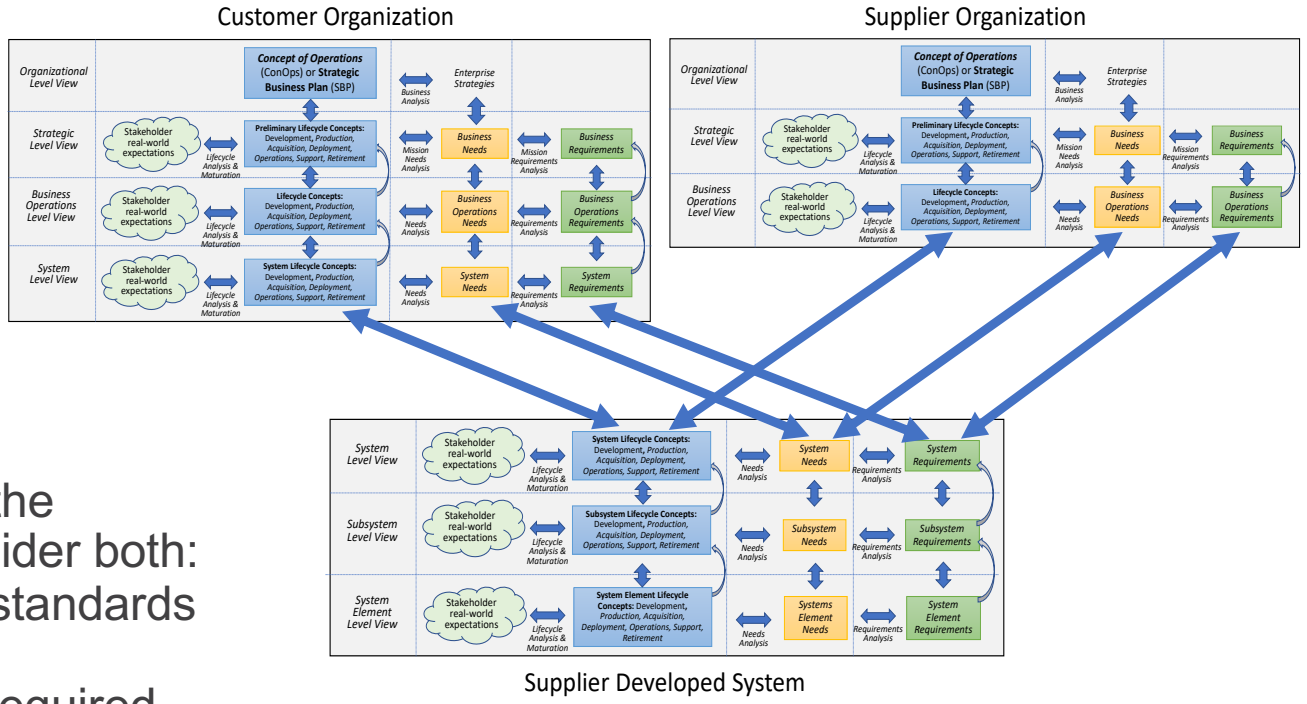
- If a project is developing a SOI for an external customer, that customer will frequently specify which standards and regulations apply in the customer-owned system requirements and SOW.
- The project will have to derive specific needs and requirements that meet the intent of the requirements in these documents AND will have to provide evidence, thru system verification and system validation, that their SOI is compliant with those standards and regulations.
  - This compliance will be part of the project's customer's or regulatory qualification and acceptance activities.
- Even if not explicitly stated by the customer, awareness of, researching, showing compliance the relevant standards and regulations is crucial to avoid compliance risk.

Developing Products For a Customer

Organizations define business and business operations requirements concerning standards and regulations to which all project's within the organization must show compliance.

For the cases where there is a customer/supplier relationship, the supplier project team must consider both:

- their organization's required standards and regulations, as well as
- the customer organization's required standards and regulations as defined in the SOW or SA.



Developing Products For a Customer

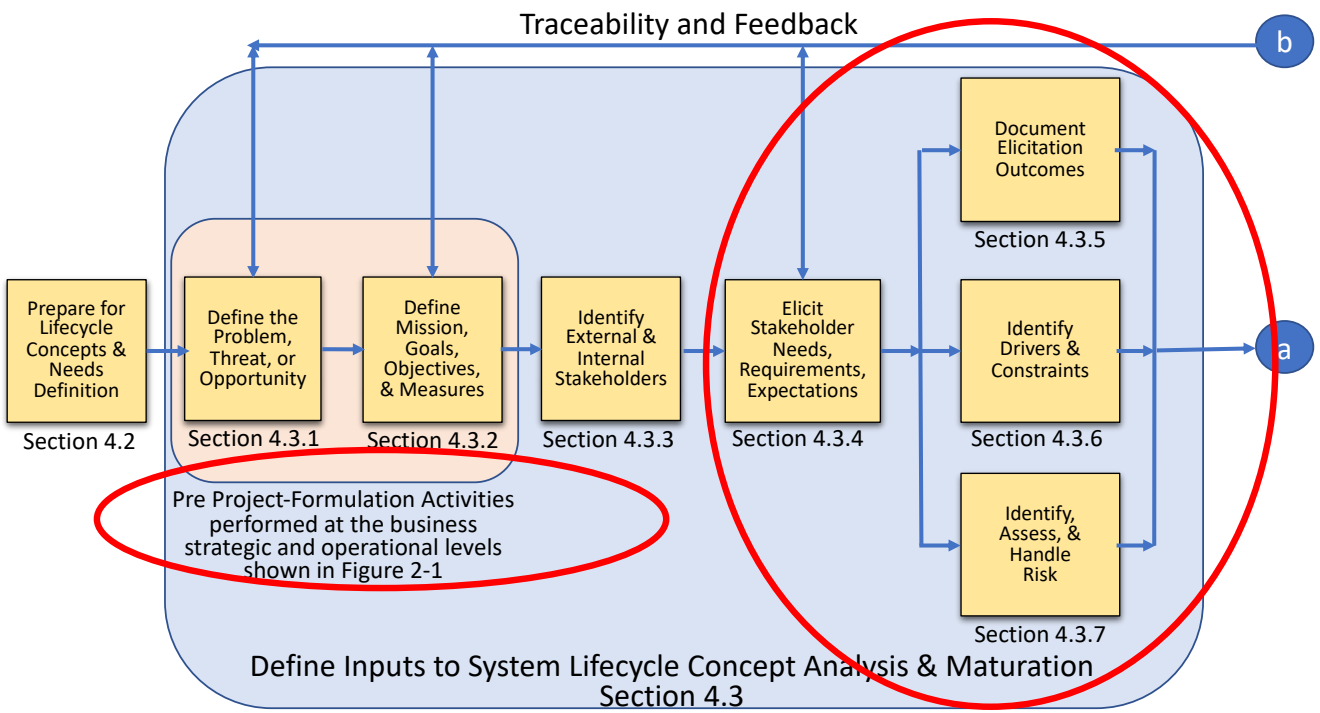
- For standards and regulations required by a customer or regulatory agency, organizations may be able to do an “equivalency check”.
  - Rather than meeting the specific customer or regulatory standard or regulation requirements, the supplier may be able to show that their internal standards meet the intent of the customer or regulatory agency required standards and regulations, and are thus equivalent.
  - This approach is based on whether the customer or regulatory agency allows an equivalency assessment - in some cases they may accept a supplier's existing processes and methods to reduce cost or time to delivery.
  - An example of this is use of a European soldering standard on a contract that specifies a standard released in the United States or the other way around.
  - Another example is the project already has in place a quality management system and design controls that address the standards and regulations applicable to the specific products being developed.

Developing Products For a Customer

- For projects developing an SOI for a customer, specific requirements for activities and contract deliverables concerning compliance with standards and regulations need to be defined in the SOW or SA, making these deliverables contractually binding.
- The SOW should also make it clear what role the customer and supplier will have in the system verification, system validation, and production verification activities.
  - In some cases, the supplier is responsible for the verification that the SOI meets the design input requirements and the associated acceptance artifacts
  - In other cases, the customer assumes responsibility for validating the SOI meets their needs and the associated the validation artifacts and obtaining approval for use from the regulatory agencies.
    - The customer may require supplier support in these activities.
  - For a more detailed discussion where there is a customer/supplier relationship and how system verification and system validation are handled, see the NRM Section 13.

Lifecycle Concept and Needs Definition

Lifecycle Concept and Needs Definition



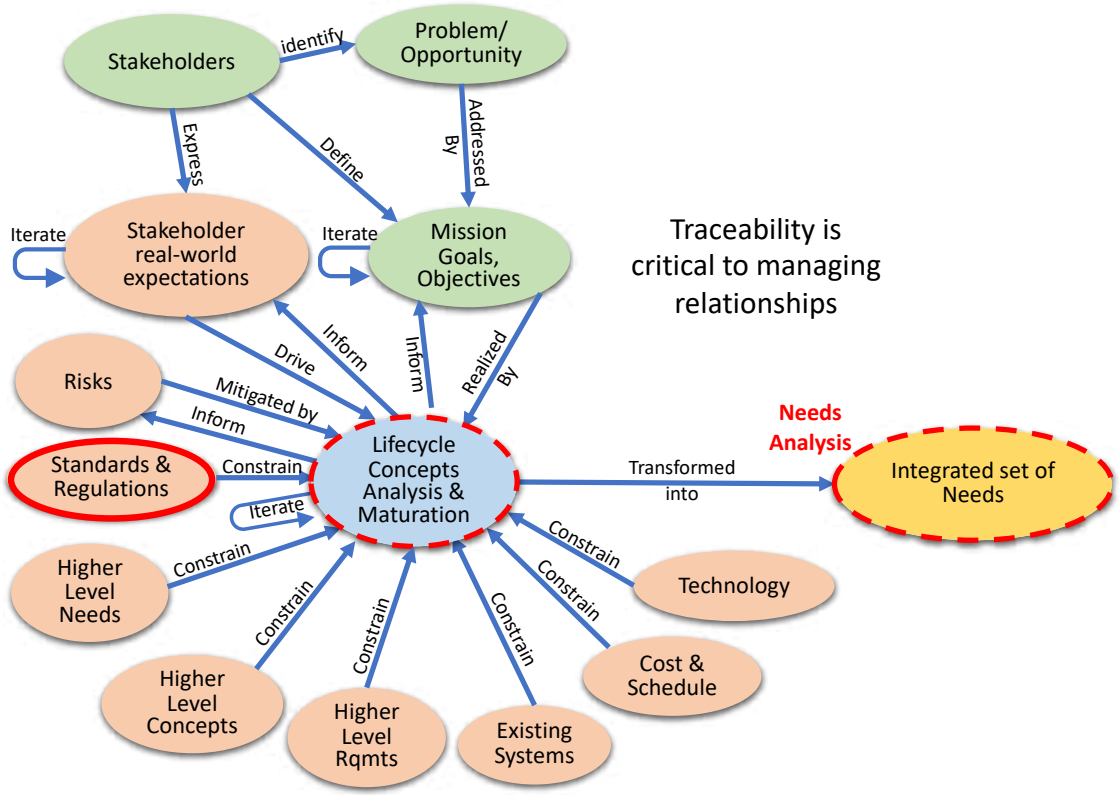
At the system (project) level, the identification of relevant standards and regulations comes from several sources:

- Higher- level organizational business requirements
- Customer SOW or SA
- Elicitation activities for system level stakeholders
- Project's research to identify drivers and constraints

Lifecycle Concept and Needs Definition

Once identified, the relevant standards and regulations are inputs into the lifecycle concepts analysis and maturation activities.

Based on these activities feasible lifecycle concepts are defined from which an integrated set of needs is defined and baselined that address the relevant standards and regulations.

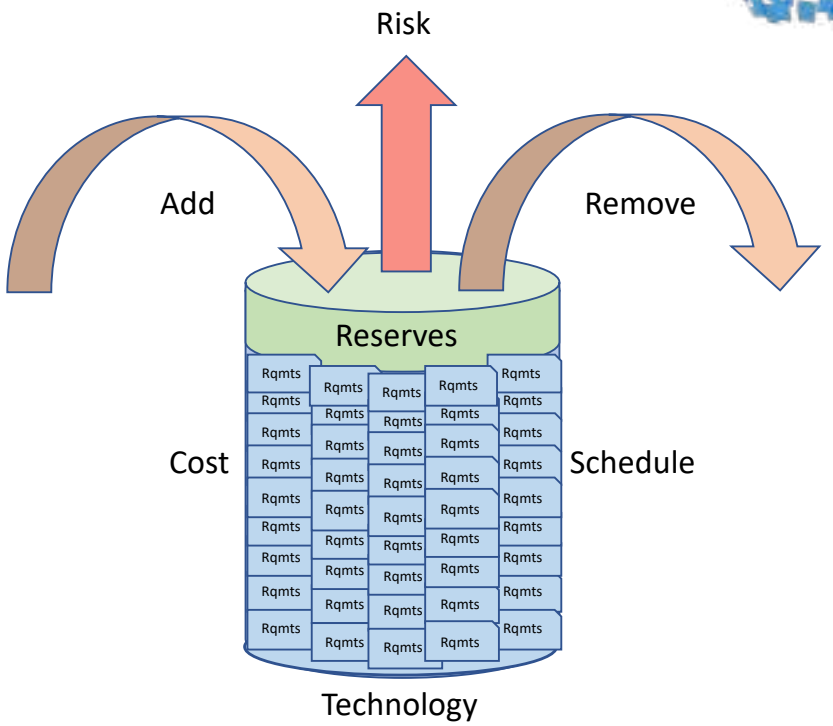


Lifecycle Concept and Needs Definition

- The Project team must do an analysis of each relevant standard and regulation
  - Which apply to the project's processes and methods?
  - Which apply to the SOI? Design input or design output?
  - Which apply to system verification and validation that will result in objective evidence of compliance?
  - Which apply to qualification, certification, and acceptance?
- In each case, the project must develop concepts for how they will comply with the applicable requirements within the relevant standards and regulations as well as how they will provide evidence of compliance.
- These concepts include determining the methods, tools, data, and information needed to document, manage, and provide the required evidence that will be included in the **Approval Packages** submitted to the **Approving Authorities**.
  - To be successful, these concepts must be defined at the beginning of the project.
  - In a data-centric practice of SE, concepts developed at the business and business operations levels and associated tools and processes can be leveraged at the project level, e.g.,
    - Business level requirements tailored to the enterprise that meet the intent of the standards and regulations are recorded and managed within a tool that supports libraries and reuse.

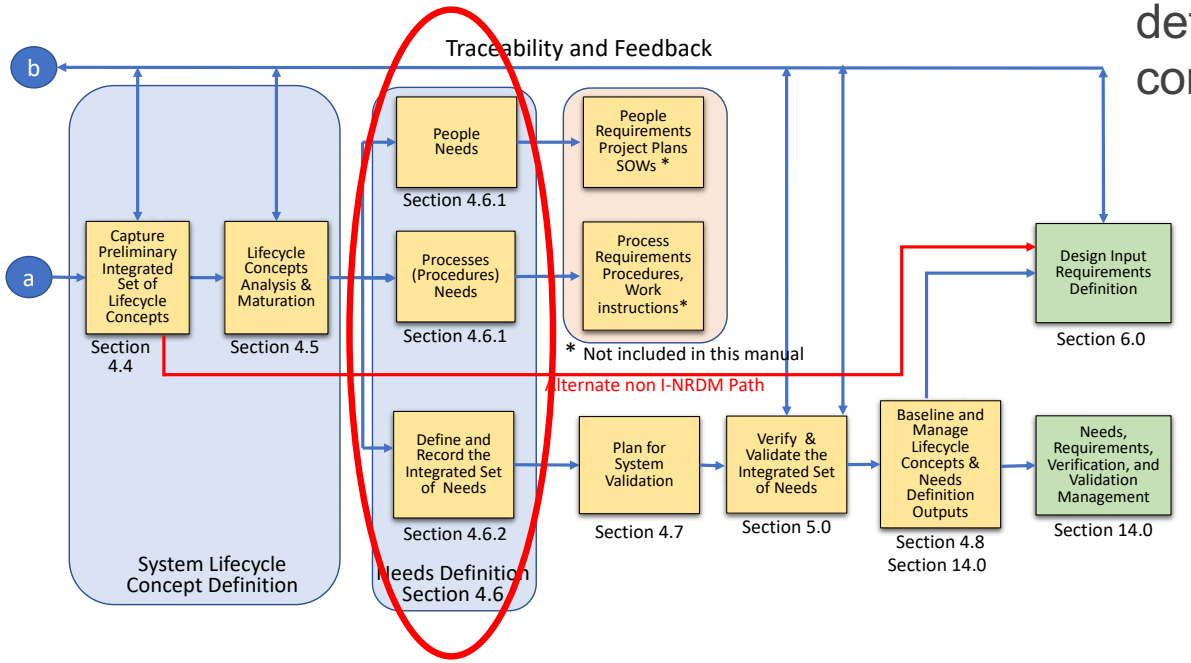
Feasibility

- A key consideration when assessing standards and regulations is the feasibility of compliance within program constraints.
- Assessment of feasibility is part of the lifecycle concepts and needs definition activities - before defining the design input requirements.
- The baselined integrated set of needs (defines scope) must individually and as a set be feasible.
  - Feasibility in terms of implementation as well as the resources, cost, and time required to provide evidence of compliance.



Needs or Requirements Feasibility/Risk Bucket

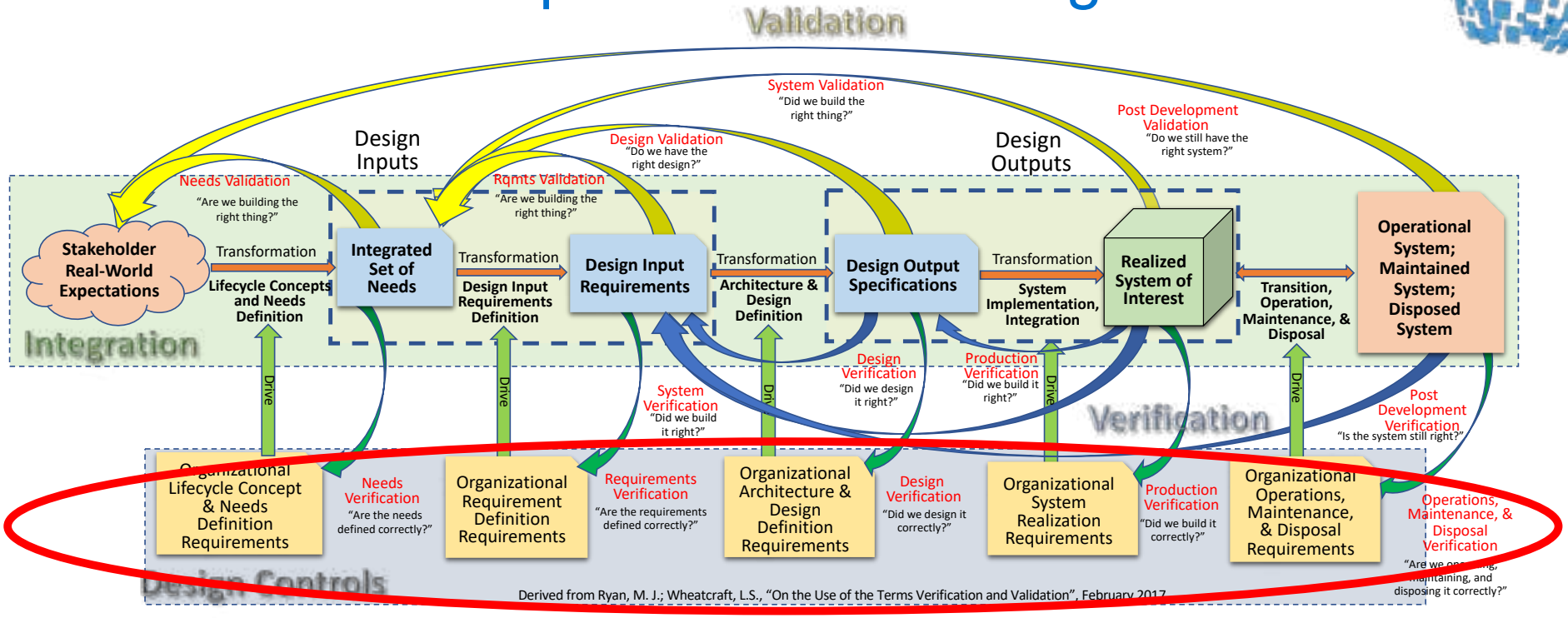
Lifecycle Concept and Needs Definition



Once lifecycle concepts have been defined, needs associated with compliance can be defined.

- **People needs** – needs on the organization that will be transformed into organizational requirements (Project plans, SOW).
- **Process needs** – transformed into process and method requirements, work instructions (design controls).
- **Product needs** to be included in the integrated set of needs and transformed into design input requirements.

Needs and Requirements vs Design Controls



Design Controls are the organizational requirements on the people developing the SOI.

Design Controls are part of an organization's Quality Management System.

There are standards and regulations dealing with design controls and the QMS.

Technical Debt

- Historically, requirements would refer to relevant standards and regulations at the document level or sections within a standard or regulation, rather than defining specific individual well-formed derived requirements tailored to the SOI being developed.
- This approach results in including poorly formed requirements in the set of design input requirements which, in turn, results in issues concerning allocation, traceability, verification, and validation as well as cost and schedule issues.
- By not defining specific design input requirements that meet the intent of the applicable requirements in the relevant standards and regulations, the project is accumulating ***technical debt***.
- ***Technical debt*** is a metaphor made up by Ward Cunningham, one of the authors of the Agile Manifesto, to describe what occurs when a project team uses a quick short-term solution that will require additional development work later to meet the needs of the stakeholders.
- From a project perspective, technical debt refers to the eventual consequences of poor project management and system engineering practices.

Technical Debt

- **Technical debt** is closely related to project and technical risk - not performing key activities early in the development lifecycle adds risk to the project due to the consequences of not doing those activities when they should have been done and addressing the consequences later - “kicking the can down the road”.
- By not doing or postponing key lifecycle development activities or making “band-aid” type fixes is like taking out a high interest loan resulting in debt for the project.
- Like all loans, the debt collector is persistent in demanding the loan be repaid along with the interest.
  - Like financial debt, **technical debt** accumulates interest on top of interest.
  - This interest represents the increased cost and time along with cost and time associated with rework that could have been avoided if the work were done at an earlier point in the project when the cost and schedule impacts of change are less before hardware is built and software coded.

Failing to adequately identify relevant standards and regulations, define concepts for compliance, and deriving specific requirements tailored to the SOI being developed, adds to the project’s technical debt.

Transforming Needs Dealing with Relevant Standards and Regulations into Design Input Requirements

General Considerations

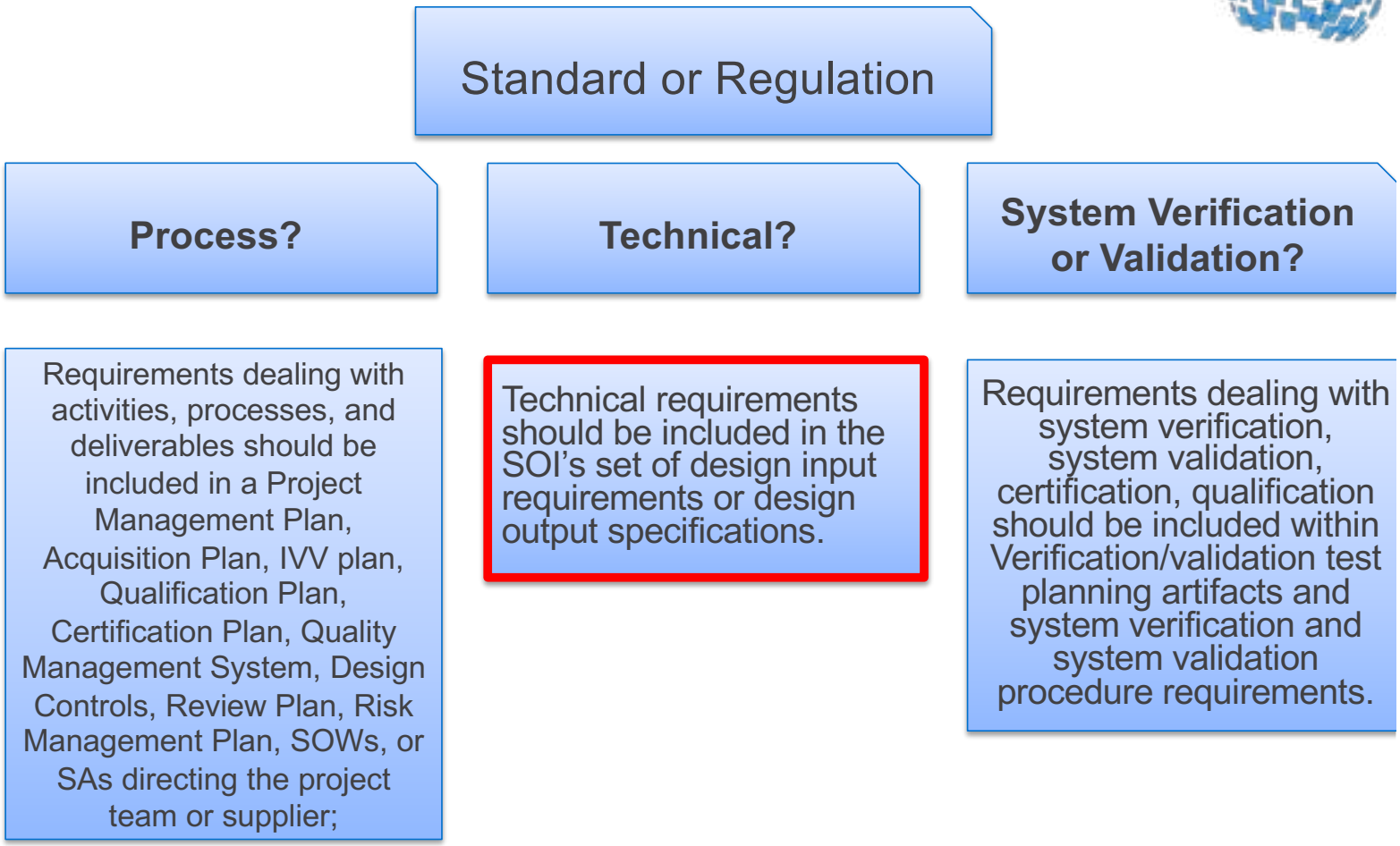
- Many standards and regulations contain at least three types of requirements:
  - Process requirements on the developer/designer;
  - Technical requirements (design input requirements as well as design output specifications) on the SOI itself, and
  - Requirements dealing with system verification and system validation activities.

- Do not mix these three types of requirements in the SOI set of design input requirements.

General Considerations

The organization will need to separately document requirements within the standards and regulations based on type and applicability.

For requirements dealing with processes, the organization should define the governance and processes to be followed by all projects within the organization and show traceability of the processes to standards and regulations to which the processes are compliant.



General Considerations

- Not all standards contain requirements (shall statements).
  - The requirement is often written by the customer for the project or supplier to follow the best practices within the standard and documented in a SOW or SA.
- Some standards contain both requirements (shall statements) which are binding and will be verified; as well as goals (should statements) whose purpose is to communicate best practices that the project is encouraged to follow.

- In most cases, standards and regulations are called out by document and section number.
  - The organization will have to determine the specific version of each standard and regulation and its date that is applicable.
  - In a traditional, document-centric practice of SE, a listing of “Applicable” documents is included in the requirements document.
    - The specific version number of the standard and requirement is often included in this section rather in a need or requirement statement.

General Considerations

- Standards and regulations change overtime.
- Organizations need a policy, supported by processes, to determine how these changes will be managed for the relevant standards and regulations requirements based on their product line.
  - Not all changes will have an impact on the organization's projects and products.
  - If not impacted by the change, updates to set of design input requirements are not necessary.
- There are some changes that will have an impact, e.g., a change to a regulation (law) or a change to an interface definition document and the product will not be able to interact successfully with the other system without invoking the change to the interface requirements within its set of design input requirements.
- There may also be changes that do affect a given product, but not a critical function or its intended use in the operational environment.
  - In these cases, there should be provisions to "grandfather" the changes so current projects and products do not have to be compliant with the change, but any new versions or models of the product will have to be compliant.
- The organization must have a process that enables the organization to be knowledgeable when any standard or regulation changes as well as which projects could be impacted by those changes.
  - This capability is often contained within the organization's CM or Compliance Office.

General Considerations

- Requirements within standards and regulations are written “generically” at a level of abstraction that is applicable to a class of products, but not necessarily the specific products being developed by the organization or a specific project.
  - Because of this, there is an expectation of tailoring the requirements to apply to an organization’s specific product line.
- Requirements in many standards and regulations do not have the characteristics of well-formed requirements as defined in the INCOSE GtWR.
  - As a result, the requirement statements often contain wording that seems ambiguous or not appropriate (in terms of system verification) for the level the project is recording the requirements.
- In many cases, rationale is not defined for the requirements within a standard or regulation.

General Considerations

- There are cases where standards contain specific design implementation (mechanical design drawings) for some concern, without communicating what the actual concern is or reason for that specific implementation (rationale).
  - In these cases, the design input requirement is a design constraint that is an exception to the “avoid design implementation” within the design input requirements.
  - If possible, the project should strive to understand the reason for the design implementation and define well-formed design input requirements based on this understanding.
    - Based on this understanding, the developing organization may have discovered a more effective design solution that better meets the intent of the standard’s organization who wrote the standard.
    - More than one subsystem or system element may play a role in meeting the intent, by defining the applicable design input requirement at the appropriate level, it can be allocated to the subsystems or system elements that do have a role.
    - This is especially important when considering today’s increasingly complex, software intensive systems where many issues can be addressed by the software rather than the hardware.

General Considerations

- It is common for a standard or regulation to call out other standards or regulations that contain requirements.
  - This can be a serious issue when one document calls out another and that document calls out yet another, and so on.
- Failing to address this issue, the organization and the project teams will have lost control of their projects, because they no longer have a say if or which of these lower tier requirements apply and which they will have to show compliance.
- One way to address this issue is to consider the current set of design input requirements as “Tier 1”.
  - Any requirement in a standard or regulation invoked directly by a requirement in the Tier 1 set of design input requirements is considered a “Tier 2” requirement.
  - If that Tier 2 requirement calls out requirements in another document, those requirements are considered “Tier 3”.
- In cases like this, it is recommended the organization have a policy that says, “Any Tier 3 or lower requirements are not applicable - if any requirements within a Tier 3 or lower document do apply, they will be addressed directly within the set of Tier 1 design input requirements”.

Common issues when communicating needs and requirements for standards and regulations.

- In the past, it has been a customary practice to call out entire standards or regulations or sections a standard or regulation within a requirement statement.

  "The <SOI> shall be complaint with *all applicable ISO standards*". Or

  "The <SOI> shall be complaint with *all* requirements within FDA regulation xyz". Or

  "The <SOI> shall meet *all requirements* within OSHA regulation xyz, Section 4.5.9.11."

  - In the first example, who determines which requirements are applicable?
  - Because they are passive, to whom do they really apply (SOI or project?)
  - In the second and third examples, how certain is it that all requirements are applicable?
  - This is like kicking the can down the road and letting someone else determine which requirements are applicable or not.
- It is dangerous to call out a complete standard or regulation when only a portion of the requirements apply.
  - All requirements invoked within the set of design input requirements will have to be implemented in the design and the system verified to meet those requirements.
  - This is a real issue if contracting to a supplier who is contracted to implement all requirements in the set.

Common issues when communicating needs and requirements for standards and regulations.

- The owner of a stakeholder need or stakeholder requirement must do the analysis and determine and communicate their needs concerning which specific standards and regulations the SOI must comply.
- **The result would be separate need statements for each applicable standard or regulation and section within that standard or regulation**.
- An example resulting stakeholder need would then state:
  - "The <stakeholders> need the <SOI> to be compliant with OSHA safety regulation <xyz, section 1.2.3." and the resulting stakeholder requirement (need):
  - "The <SOI> shall be compliant with OSHA safety regulation <xyz, section 1.2.3."
- What often happens is that this stakeholder requirement is copied and pasted into the set of system design input requirements as written.
- While well-intended, this requirement statement does not have the characteristics of a well-formed requirement.
  - It is not singular, it is ambiguous, and is not verifiable.
  - Sadly, this approach is what is most commonly used!

Common issues when communicating needs and requirements for standards and regulations.

- Another common issue is adding a “shall” to a need statement and calling it a requirement:
  - “The <stakeholders> need the <SOI> to be compliant with all OSHA safety standards and regulations.”
  - This stakeholder need is communicated as a stakeholder requirement:
    - “The <SOI> shall be compliant with government safety standards and regulations.” or
    - “The <SOI> shall be compliant with all government safety standards and regulations.” or
    - “The <SOI> shall be compliant with all applicable government safety standards and regulations.”
  - Again, while well-intended, each of these statements are too vague to verify or validate the system against because each is ambiguous as to which specific standards and regulations are applicable.
  - Restating the poorly formed need as a stakeholder requirement with a “shall” does not result in a well-formed requirement.

Common issues when communicating needs and requirements for standards and regulations.

- In either case, there are multiple issues with requirements stated within standards and regulations.
  - As discussed previously, the quality of the requirements in the standard or regulation is often lacking, and their intent unclear - often there is no rationale.
  - A standard or regulation could contain hundreds of requirements, of which only a portion apply to the SOI under development.
    - Who determines, which one is applicable?
  - In some cases, requirements in one standard or regulation may be inconsistent or contradict a requirement in another similar standard or regulation.
  - Will all the requirements in the document or section invoked by the design input requirement be allocated the same way to lower-level subsystems and system elements within the system architecture? Verified the same way?
  - There are multiple “standards” organizations – sometimes they are contradictory or inconsistent – which standard should an organization be compliant?

Common issues when communicating needs and requirements for standards and regulations.

- Another key issue when calling out a standard or regulation, is the question of design and system verification.
  - Each requirement within the invoked document or section will have to be implemented in the design and the design and system verified to meet each of those requirements.
  - All the system verification attributes (Success Criteria, Strategy, and Method) would need to be defined for each of these requirements and the system verification artifacts discussed in Section 10 would have to be developed.
  - This would involve a lot of time and resources if each project within an organization did this, especially if the requirements in a standard or regulation are poorly written and the intent not clear.

Common issues when communicating needs and requirements for standards and regulations.

- For cases when the development of the SOI is contracted to a supplier, who determines which requirements are applicable and who determines the system verification attributes for each?
  - Invoking all or portions of a standard or regulation represents substantial compliance risk to both the customer and supplier.
  - If the customer does not clearly communicate the specific requirements that address the relevant standards and regulations in a contract as well as the system verification attributes, this can result in expensive contract disputes and changes.

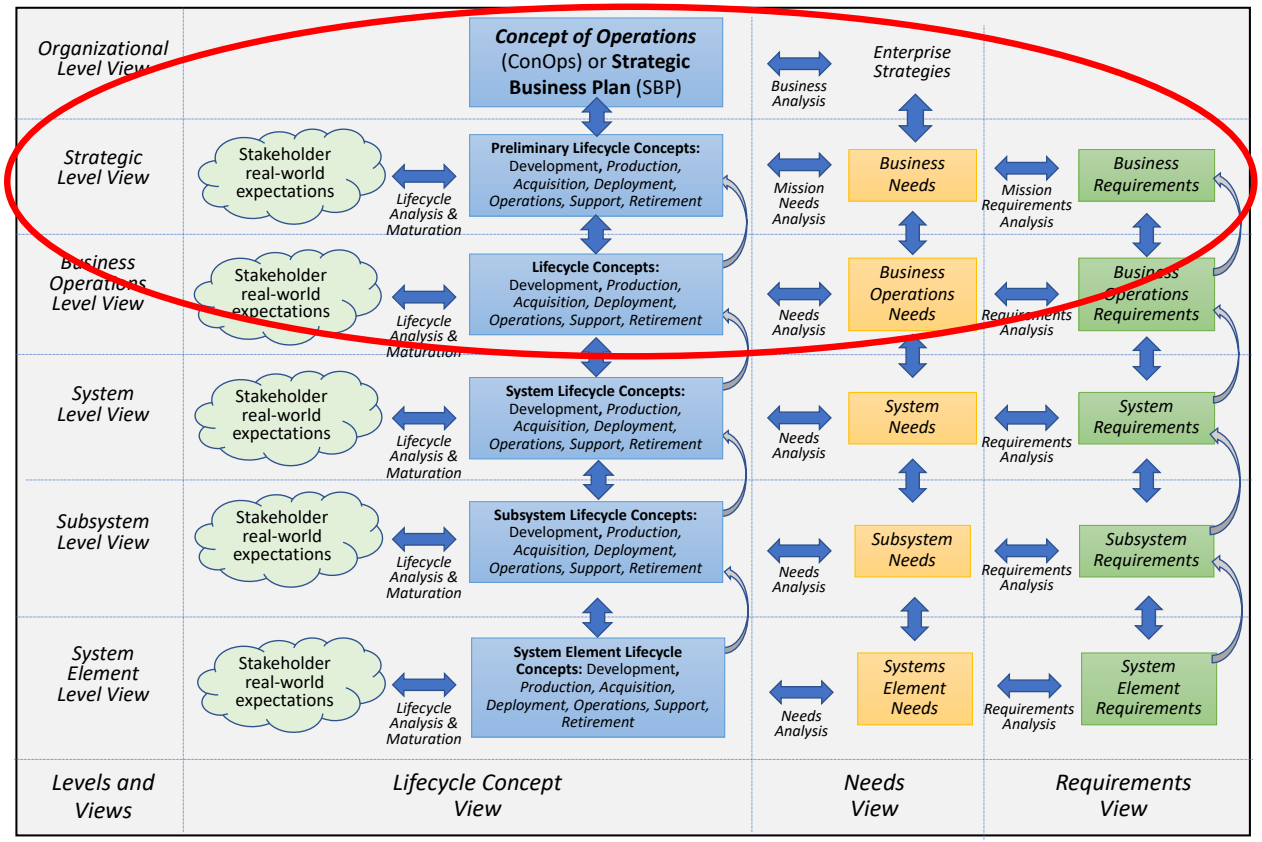
Best Practices and Guidance.

- What should happen when transforming needs dealing with standards and regulations into design input system requirements, is that the project team responsible for the transformation, must do an engineering analysis to determine:
  - Which specific requirements within the regulation sited in the need, apply to the SOI under development (vs project or process requirements);
  - Whether these requirements are design inputs for the SOI or requirements on the design team and resulting design output specifications or requirements on production; and
  - For those that apply to the SOI, determine specifically what the SOI must do to meet the intent of the applicable requirements within the standard or regulation.
- Based on that analysis, the project team would then derive specific well-formed design input requirements that when implemented by the design would result in the intent of the parent requirements within the standard or regulation referenced in the integrated set of needs to be met.
- **While this could result in a large number of requirements**, each would be well-formed making it clear what is expected to be addressed by the design and against which both the design and realized system can be verified against.

Best Practices and Guidance

At the organizational (enterprise) level of the organization, the product line and services to be provided by the organization are defined.

At the strategic and business operations levels, relevant standards and regulations are identified that apply to the products and services developed or supplied by the organization.



Best Practices and Guidance

- For each relevant standard or regulation, the organization should clearly establish which requirements within a relevant standard or regulation are applicable to the type of products or services provided by the organization.
- Ideally, the applicable requirements within these relevant standards and regulations will have been imported into the organization's toolset database in a form that will:
  - Allow the organization to create reusable libraries
  - Allow the organization to assign applicability of the standards and regulations to specific projects and systems to be developed and
  - Allow the projects to establish traces from their implementing requirements to the applicable standard or regulation requirement(s).
- This approach requires the organization to "buy" rights from the organization that "owns" these standards and regulations and get permission to include the applicable requirements in the organization's toolset.

Best Practices and Guidance

- One way to establish applicability to specific projects, products, or services is to develop an applicability matrix for each relevant standard and regulation.
  - In the applicability matrix, for a given applicable standard or regulation, sections of requirements or individual requirements are listed as a row heading.
  - Individual projects, products, and services are listed as column headings.
  - For each row, an “X” is placed in any column to which the requirement identified for that row applies. (Note in a RMT or similar tool, the “X” represents a link or trace.)
- With this approach, need statements within the integrated set of needs would invoke the columns within the organization’s applicability matrices for the SOI being developed.
  - For example: “The stakeholders need the SOI to comply with [regulation xyz] requirements as indicated in column C of [regulation xyz Project A applicability matrix.”]
  - Using this approach, the project team would then know which specific requirements in the regulation or standard that apply to their project and SOI and to which they would have to show compliance.
- This approach can also be used within a SOI.
  - The specific regulation or standard requirements applicable to the project can be allocated to lower-level subsystems and system elements using this same approach.

Best Practices and Guidance

Applicability Matrix for Standard XYZ

Standard XYZ Rqmts	Project A	Project B	Project C	Project D	Project E
Rqmt 1	X	X	X	X	X
Rqmt 2		X		X	X
Rqmt 3	X		X		X
Rqmt 4		X	X	X	
Rqmt 5	X				X
Rqmt 6	X	X	X	X	X
Rqmt 7	X	X			

Best Practices and Guidance

Applicability Matrix for Standard XYZ for Project A

Standard XYZ Rqmts	Column A Process	Column B Technical	Column C V&V
Rqmt 1	X		
Rqmt 3		X	X
Rqmt 5		X	X
Rqmt 6	X		
Rqmt 7	X		

Best Practices and Guidance

- The number of requirements invoked on a project dealing with standards and regulations can be large, taking considerable time, resources, and money to manage, implement, and show compliance.
- For process focused standards and regulations, the organization could define their own processes, methods, and development environment in response to the standards and regulations.
  - From a contracting perspective, the customer could then require the suppliers to discuss in their proposal their equivalent processes that meet the intent of the customer invoked standards and regulations dealing with processes and methods.
- For technical requirements, rather than calling out requirements contained within the standards and regulations, the organization could develop their own version of each standard or regulation tailored to the product lines developed by the organization that meet the intent of the source requirements within the standards and regulations.
  - The result is often a much smaller number of requirements that still clearly communicate the intent and expectations, but which can be implemented much more effectively.
- These sets of requirements would be placed within the organization's toolset in the form of reusable libraries, establishing traceability between their derived well-formed requirements and the applicable source requirements in the relevant standard or regulation.

Best Practices and Guidance

- Because of the general nature of requirements within standards and regulations, it is a ***bad*** *practice to copy and paste requirements* from a standard or regulation into your sets of requirements.
  - The organization's derived requirements should be well-formed having the characteristics as defined in the INCOSE GtWR or similar document that meet the intent of the source requirements within the standards and regulations.
  - Each derived requirement should have **rationale** concerning why it is needed and how it is meeting the intent of the source requirement in the standard or regulation.
- When deriving **equivalent** requirements, the organization must establish traceability between their derived requirements within the organization's libraries and the source requirements in the standards and regulations.
- They would need to collaborate with the **Approving Authorities** to define the system verification and system validation attributes for each derived requirement such that verification that the project or SOI meets that requirement would provide adequate evidence that the intent of the source requirement within the standard or regulation was met and that the project or SOI is in compliance with the source standard or regulation.

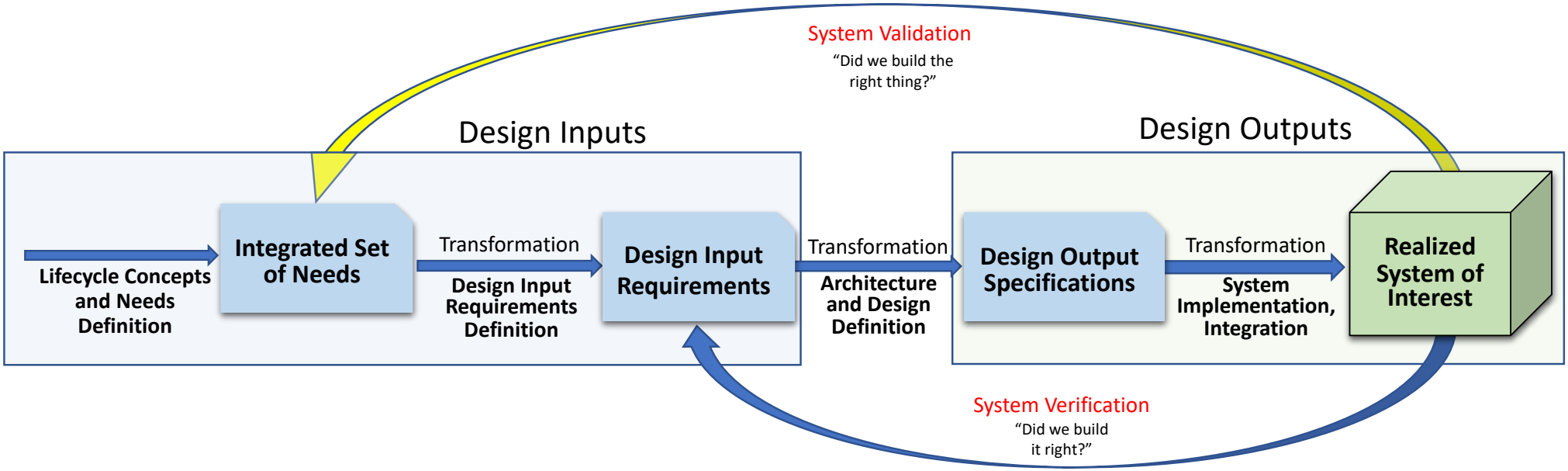
Best Practices and Guidance

- This approach is preferred from a reusability standpoint in that it would save considerable time and money not requiring individual projects to repeat these actions, over, and over.
  - Without these libraries, each project is forced to “reinvent the wheel” adding considerable cost and time to the project and risk of noncompliance.
- An added benefit, is that the RMT used to establish the libraries, can keep track of the projects that are using requirements in the library as well as how they were tailored for the specific projects.
  - If the organization sees similar tailoring by multiple projects, they can use this information to update the requirements within the library after getting approval from the Approving Authorities before doing so.
- Another added benefit is that it is easier for the organization to manage changes to standards and regulations.
  - They can better assess the applicability of a change at the organizational level.
  - They will know which projects are possibly affected by a change.
  - They can address changes in one place.

System Verification and System Validation

Note: While this presentation focus is on standards and regulation compliance, this section applied to all needs and requirements.

System Verification and System Validation



Derived from Ryan, M. J.; Wheatcraft, L.S., "On the Use of the Terms Verification and Validation", February 2017

System Verification and System Validation

- All need statements must be structured and worded such that its realization can be validated to the approving authority's satisfaction.
- Unless a need statement is written in a way that allows requirement validation, design validation, or system validation, there is no way to tell whether it has been satisfied and that the obligation has been met.
- Each need statement must include the necessary information such that validation **success criteria** can be defined, and the SOI can be validated such that **sufficient evidence** can be gathered to determine whether the **success criteria** have been met, i.e.,
  - there is no ambiguity regarding what the need statement communicates and there are no missing characteristics within the need, i.e., the need statement is Conforming (C9) and Complete (C4).
- An unvalidatable need can result in multiple, objective observers (for example, requirement writers, architects, designers, or testers) interpreting the need differently making it difficult to validate that the requirement, design, and SOI meets the need.

Each need statement dealing with standards and regulations must be validatable.

System Verification and System Validation

- All requirement statements must be structured and worded such that its realization can be verified to the approving authority's satisfaction.
- Unless a requirement statement is written in a way that allows design verification or system verification, there is no way to tell if it has been satisfied and that the obligation has been met.
- Each requirement statement must include the necessary information such that verification **success criteria** can be defined, and the SOI can be verified such that **sufficient evidence** can be gathered to assess whether the **success criteria** has been met, i.e.,
  - there is no ambiguity regarding what the requirement statement communicates and there are no missing characteristics within the requirement, i.e., the requirement is Conforming (C9) and Complete (C4).
- An unverifiable requirement can result in multiple, objective observers (for example, designers or testers) interpreting the requirement differently, making it difficult to verify the SOI meets the requirement.

Each requirement statement dealing with standards and regulations must be verifiable.

System Verification and System Validation

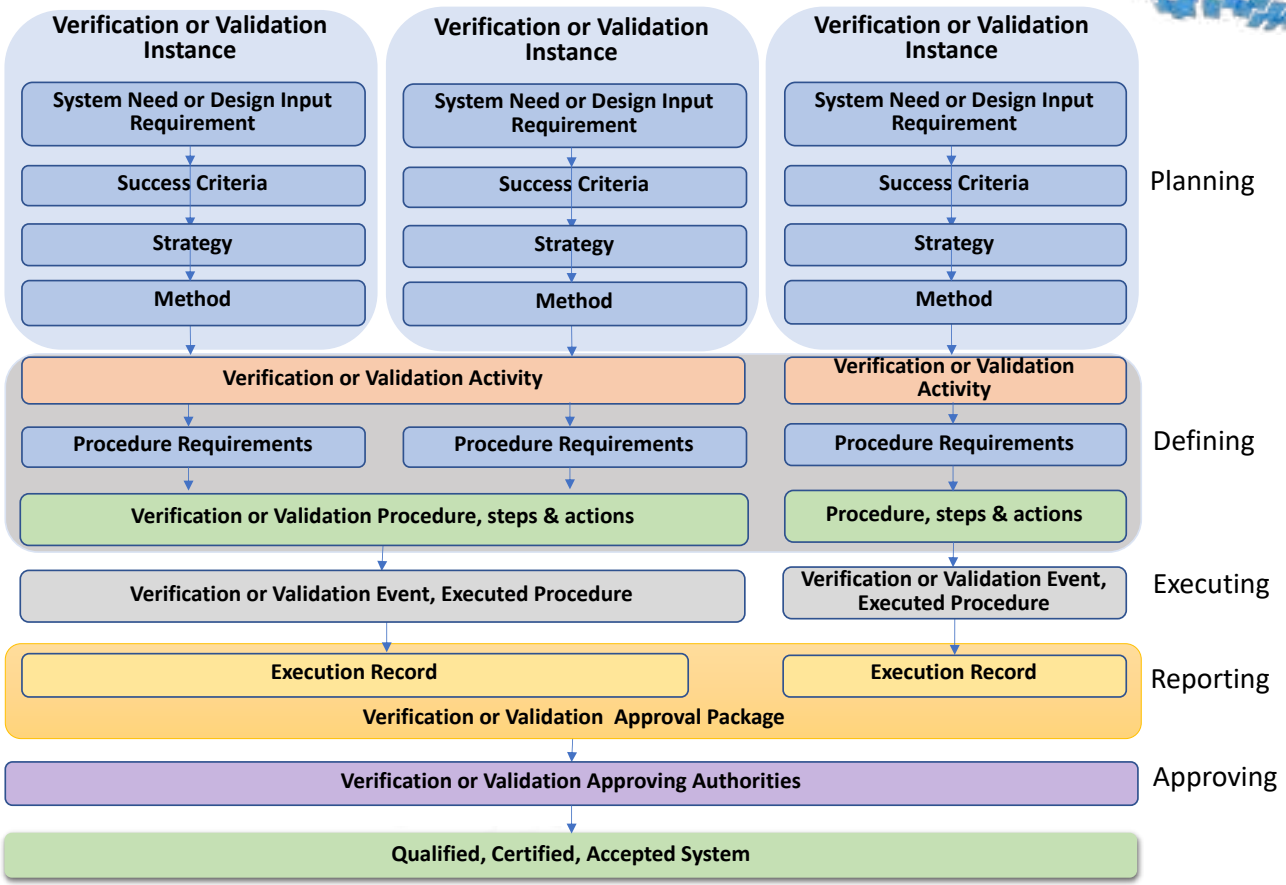
- Verifiability and validability is a necessary condition for establishing the characteristics: Appropriate (C2), Unambiguous (C3), Complete (C4), Singular (C5), Feasible (C6), Conforming (C9), Consistent (C11), and Comprehensible (C13).
  - Verifiability and validability should be addressed as the initial criterion and a basis for examining these other characteristics.
- Verifiable/validatable is about design and system verification and requirement, design, and system validation showing that
  - the requirements can be validated against the need,
  - the design can be verified/validated such that, when realized, it will result in a SOI that meets the requirement/need, and
  - the realized SOI can be verified/validated that it meets the requirement/need.
- Write each requirement and need statement in a way that allows the design or system to be verified/validated that the requirement/need has been met by one of the four standard verification/validation **methods** (inspection, analysis, demonstration, or test).
- When writing requirement or need statements, use a verification or validation point-of-view to imagine yourself performing the verification or validation activity and define what **evidence** is needed to assess whether that the need or requirement intent has been achieved as defined by the **success criteria** with the required level of confidence.

System Verification and System Validation

Each need and requirement is a verification or validation instance which requires planning.

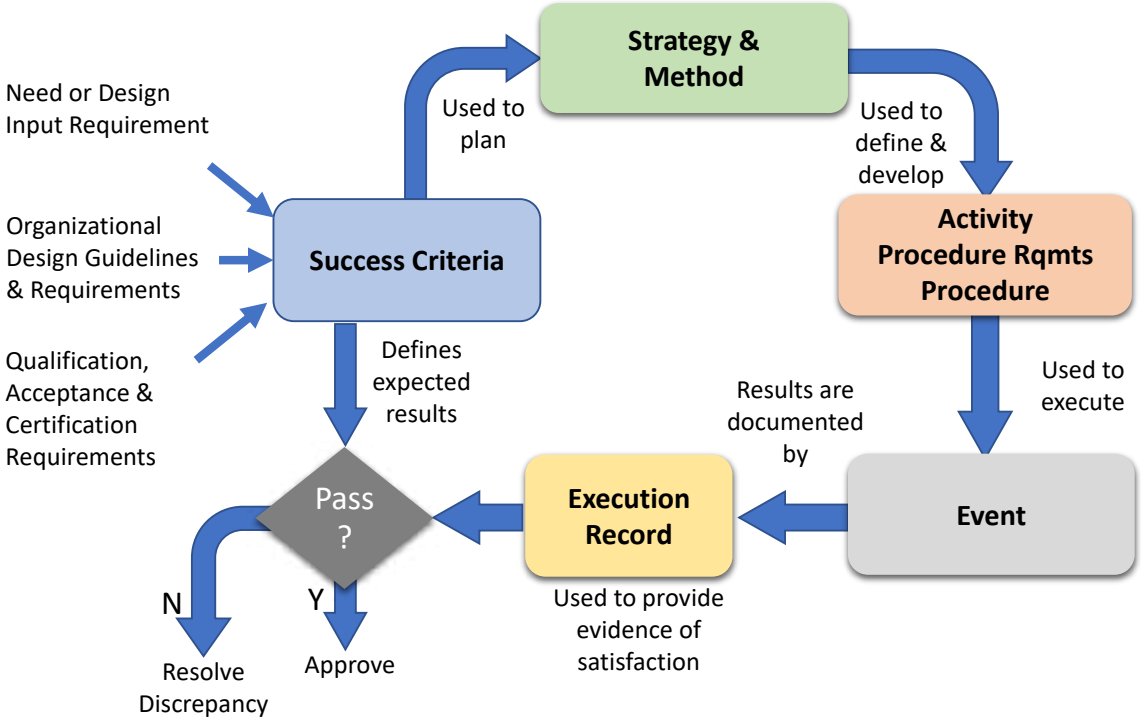
There are many artifacts that must be defined and managed formally that show evidence of compliance.

Refer to the NRM Section 10 for a detailed discussion on the development of these artifacts.



System Verification and System Validation Process Artifacts

System Verification and System Validation



Success Criteria Influence on System Verification and System Validation Planning and Implementation

- It is a recommended best practice to define the verification/validation **success criteria, strategy,** and **method** attributes when defining each need or requirement statement.
- When this is done, the quality of the requirement or need statement will improve resulting in needs and requirements that are (verifiable/validatable).

These attributes must be defined for each need and requirement dealing with standards and regulations.

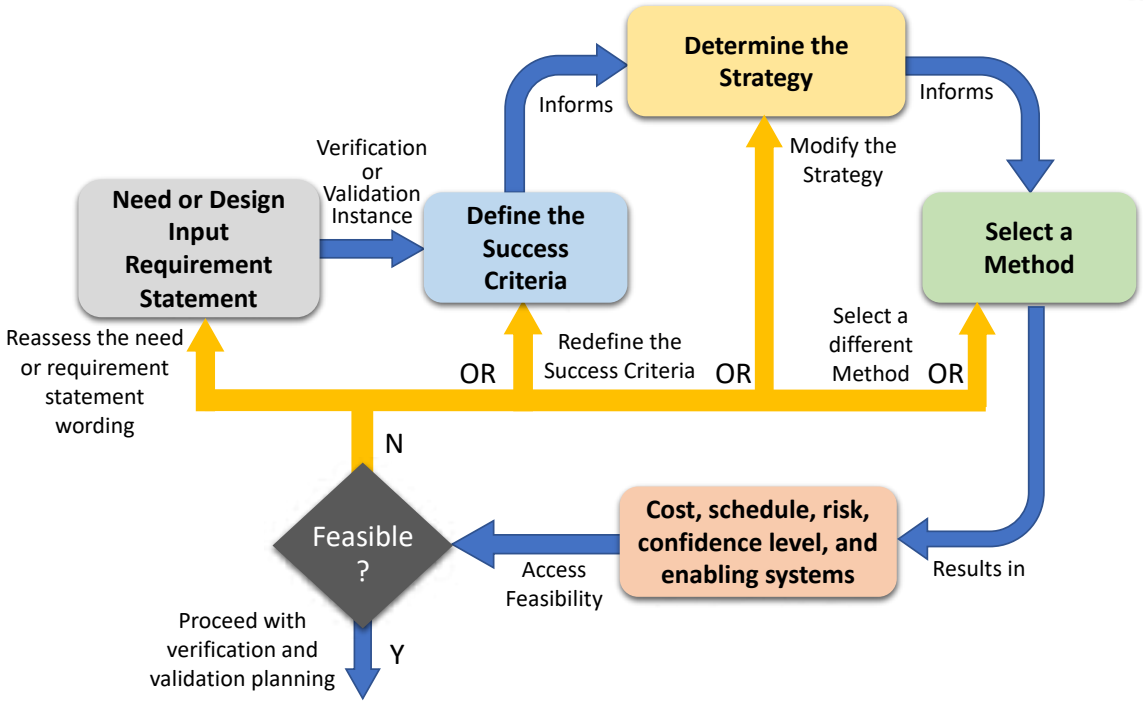
System Verification and System Validation

Each need and requirement must be written such that **success criteria** can be defined and against which evidence of compliance is based.

All other system verification and validation planning and execution are based on the defined **success criteria**.

Feasibility must be accessed before agreeing on these attributes.

The customer and supplier must agree on these attributes.



Defining the verification and validation success criteria, strategy, and method are cost, schedule, and risk decisions.

Documenting the Evidence of Compliance

Note: While this presentation focus is on standards and regulation compliance, this section applied to all needs and requirements.

Documenting the Evidence of Compliance

- An **Execution Record** for each **Verification or Validation Activity** is created after the completion of each **Procedure** associated with that **Activity**.
- The **Execution Record** will state the status and outcome of the **Activity** in terms of whether the results provide **sufficient evidence** that the **Success Criteria** for each system verification and system validation **Instance** were met.
- The family of **Execution Records** for the SOI are combined into **Approval Packages**.
- **Execution Records** formally document the results of the execution of the **Procedures**.
  - There will be one **Execution Record** for each **Activity**.
  - The results of the **Procedures** will be recorded in one or more forms of objective evidence.
  - This evidence can take the form of a formal report, data set, or some type of form.
  - Regardless of its form, each piece of objective evidence must be uniquely identifiable and stored in a configuration managed document or database.

Documenting the Evidence of Compliance

- The **Execution Record** should contain the following types of information:
  - A unique identifier.
    - This identifier will be used to locate and access the **Execution Record**.
    - If stored within the project's toolset, this identifier can be used as a pointer to the Execution Record.
  - Date when the **Procedure** was completed that generated the data within the Execution Record.
  - Location where the **Procedure** was executed.
  - Name of the organization responsible for the execution of the **Procedure**.
  - The Quality Control (QC) process that was used to manage the integrity of the data.
  - The name of the Quality Control person(s) that monitored the test and who signed off on the integrity of the data collected.
  - The **Success Criteria** that were to be met.
  - The **Strategy** and **Method** used to collect the data.
  - The environment and any special conditions in which the data was collected.
  - Description and form of the data collected.
  - Description of the analysis that was used to determine whether the data collected provided sufficient evidence that the **Success Criteria** was met.
  - A statement of conformance or non-conformance by the executing organization and person doing the analysis and making the pass/fail judgement.

Documenting the Evidence of Compliance

- The preparation of the **Execution Records** will often be done concurrently with the close-out activities for the **Procedure** discussed earlier.
- Once the **Execution Records** are complete, they are assembled, along with any other information needed by the **Approving Authorities**, into **Approval Packages** for submittal to the **Approving Authorities**.
- In addition to the **Execution Records**, other records included in the **Approval Packages** may include:
  - A Certificate of Conformance to the standard or regulation, often applicable to design and manufacturing processes.
  - Approved waivers, deviations, or exceptions.
  - Evidence in component end item data packages (design output specifications), such as a materials and parts list or a test report.
  - Evidence collected in build (post-production artifacts) records, such as specific inspections showing wire bundles, grounding measurements, etc.
  - Evidence that demonstrates that the design was developed in accordance with the approved design controls and system design outputs specifications (design verification and design validation).
  - Evidence that demonstrates that the device was manufactured in accordance with the approved processes and design output specifications for the system (Production verification).

Documenting the Evidence of Compliance

- As an example, for medical devices developed under the oversight of the FDA, CFR Title 21, Part 820 defines the process organizations must follow, and the set of records that must be developed, maintained, and submitted to the FDA to get a medical device approved for its intended use.
- The requirements in this regulation include key definitions for parts of the process including design inputs, design outputs, specifications, design reviews, design verification, design validation, process validation, and many other definitions.
- Concerning compliance and record keeping the regulation defines three key records and requirements for each:
  - Design History File (DHF) is a compilation of records which describes the design history of a finished device.
    - The DHF contains or references the records necessary to demonstrate that the design was developed in accordance with the approved design plan and the design input requirements.
    - The results of the design verification, including identification of the design, method(s), the date, and the individual(s) performing the verification, are documented in the DHF.

Documenting the Evidence of Compliance

- Device History Record (DHR) is a compilation of records containing the production history of a finished device.
  - Each manufacturer is required to maintain DHR's.
  - Each manufacturer is required to establish and maintain procedures to ensure that DHR's for each batch, lot, or unit are maintained to demonstrate that the device is manufactured in accordance with the DMR and the requirements of this part.
- Device Master Record (DMR) is a compilation of records containing the procedures and specifications for a finished device.
  - The DMR for each type of device includes, or refers to the location of, the following information:
    a) Device design output specifications including appropriate drawings, composition, formulation, component specifications, and software specifications.
    b) Production process specifications including the appropriate equipment specifications, production methods, production procedures, and production environment specifications.
    c) Quality assurance procedures and specifications including acceptance criteria and the quality assurance equipment to be used.
    d) Packaging and labeling specifications, including methods and processes used; and
    e) Installation, maintenance, and servicing procedures and methods.
  - The total finished design output consists of the device, its packaging and labeling, and the DMR.

Chain of Evidence of Compliance

- The project must maintain and manage records that provide a **chain of evidence of compliance** to the relevant standards and regulations.
- The **chain of evidence of compliance** could be complex, given the various levels of needs, design input requirements, the design implementation of those requirements, the design output specifications, manufacturing/coding that implemented those specifications and the system verification and system validation artifacts developed and data gathered that provides evidence of compliance.
  - There could easily be thousands of system verification and system validation **Instances** and hundreds of **Execution Records** included in the system verification or system validation **Approval Packages**, depending on the size and complexity of the SOI under development.
- Managing the **chain of evidence of compliance** is often the responsibility of the organization's internal "compliance" or "quality" group. They are responsible for:
  - CM of the sets of needs and requirements and resulting system integration, system verification and system validation artifacts.
  - Making sure the intent of the standards and regulations are being met
  - Ensuring the objective evidence needed to determine compliance and obtain certification or qualification and acceptance is properly documented and submitted to the regulatory agency in accordance with the requirements defined by the agency.

Traceability

- Many regulatory agencies, as well as customer's, will want the project to show traceability between the:
  - requirements in the relevant standards and regulations,
  - concepts to meet them, needs that communicate the which specific standards the project will be compliant with,
  - resulting design input requirements that address what the must be done to meet the needs,
  - implementing architecture and design,
  - design output specifications
  - production verification,
  - realized system, and
  - project's system verification and system validation activities that result in the objective evidence that can be used to show that the intent of the applicable requirements in the relevant standards and regulations have been met.

This traceability is fundamental to defining and maintaining the chain of evidence of compliance.

Digital treads across the lifecycle are the basis of establishing the chain of evidence of compliance.

Traceability

- Standards and regulations existing in various industries require traceability to be established across the lifecycle of the product/system. Examples include:
  - ARP4754, “Guidelines for Development of Civil Aircraft and Systems”;
    - ARP4754A Section 5.3.1.1 requires requirements dealing with safety to be “uniquely identified and **traceable**” to “ensure visibility of the safety requirements at the software and electronic hardware design level.”
  - ISO13485, “Medical devices - Quality management systems - Requirements for regulatory purposes”;
    - ISO13485 Section 7.3.2 requires organizations to document “methods to ensure **traceability** of design and development outputs to design and development inputs.”
  - ISO26262, “Road Vehicles — Functional Safety”;
    - Section 6.4.3.2 requires “Safety requirements shall be **traceable** with a reference being made to:
      a) each source of a safety requirement at the next upper hierarchical level;
      b) each derived safety requirement at the next lower hierarchical level, or to its realization in the design; and
      c) the verification specification in accordance with Section 9.4.2.

Traceability

- USC Title 21 Part 820, “Quality System Regulation” for medical devices
  - Requires developing organizations of medical devices to develop and maintain a Device History File (DHF) that “shall contain or reference the records necessary to demonstrate that the design was developed in accordance with the approved design plan and the requirements of this part.”
  - Traceability is a critical part of the DHF.
- Failure to show required traceability can lead to a product not being approved for its intended use in the marketplace.
- Historically, organizations defined and recorded the data and information associated with the various artifacts in the form of “documents”.
- As systems become more complex and regulated, the sheer volume of documentation has become overwhelming; especially in terms of configuration management, change control, completeness, correctness, and consistency.
- Because of the complexity, there are more people involved in the development of these systems spread over different geographical locations.
  - This results in many of the documents being developed and managed within silos with limited collaboration.

Chain of Evidence of Compliance

- Because of these issues, it is nearly impossible to keep all the data and information contained within the various documents in sync, current, correct, and consistent resulting in no real authoritative source of truth (ASoT).
- For highly regulated systems, the amount of documentation that must be developed, maintained, and supplied to regulators to show compliance has become overwhelming.
  - Inconsistencies in these documents can result in a system that fails system validation and that is not approved for use.
- The cost and time overhead associated with managing the large number of documents consumes a large part of development costs.
- This time overhead results in longer development times and time to market for many systems, making a company less competitive and less profitable.
- Additionally, quality suffers resulting in post system launch costs associated with increases in returns, recalls, warranty work, and company image degradation associated with negative social media comments – all of which also eat into profits.

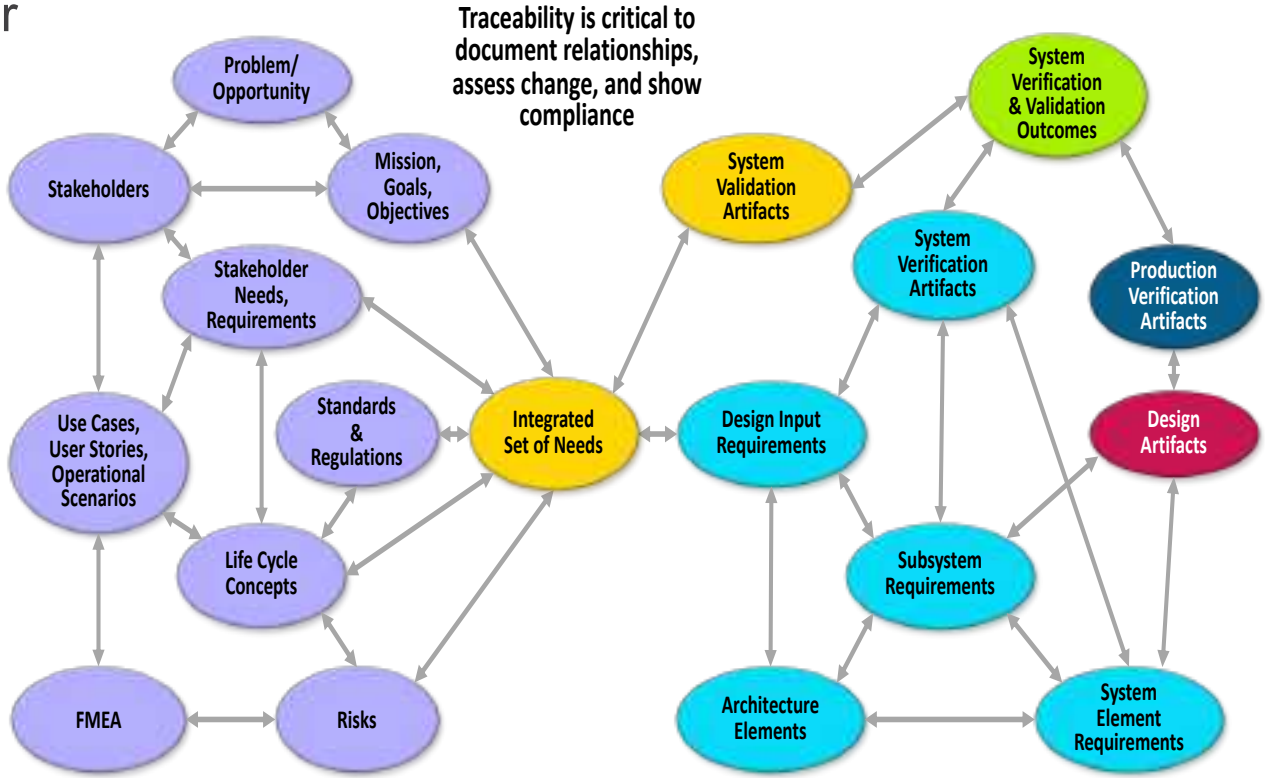
For today's increasingly complex, software intensive systems, it is very difficult to maintain traceability and the chain of evidence of compliance using a document centric practice of SE.

Data-Centric Practice of SE

At the beginning of your project, you must choose to develop your product using a **data-centric practice of SE** which allows establishing traceability across the lifecycle activities and artifacts.

A first step is selecting your SE toolset and determining what data and information will be defined and managed within the toolset.

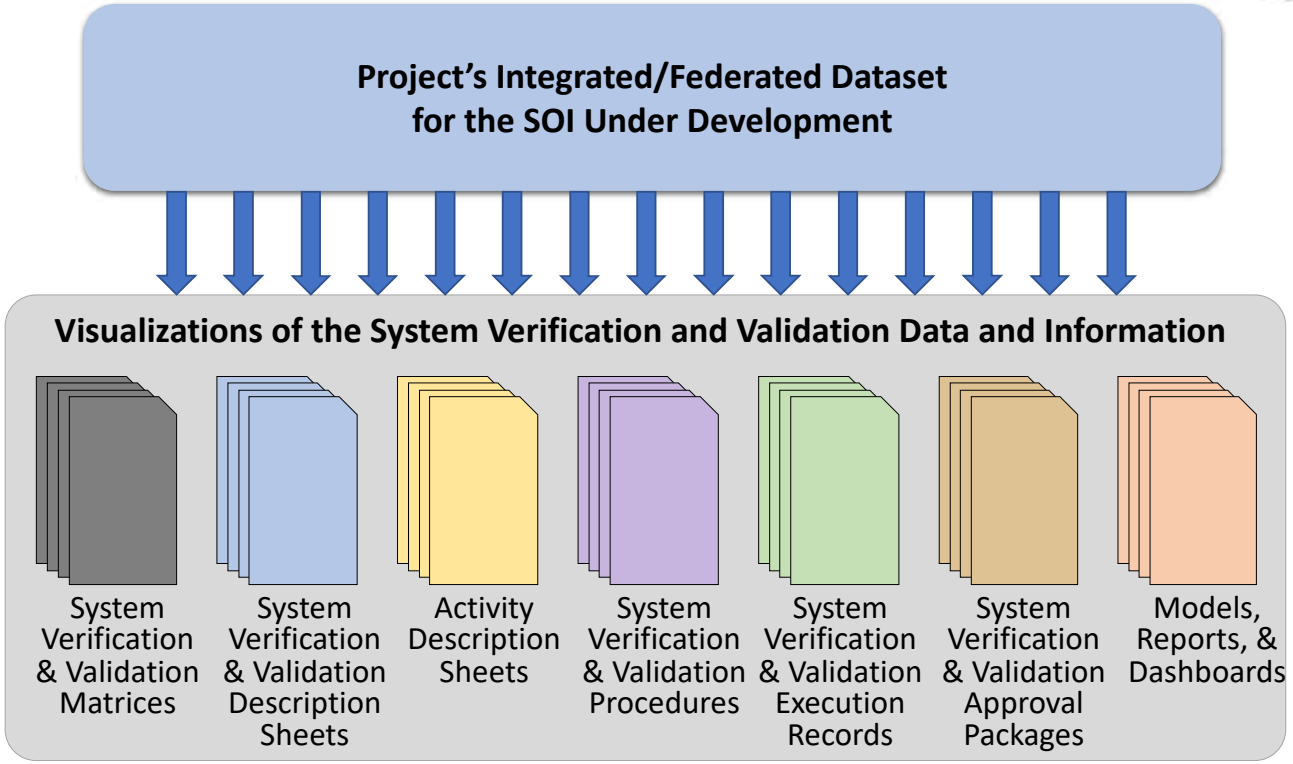
A second step is defining a traceability relationship model addressing which relationships will be established and managed via traceability.



Using an SE Toolset to Maintain the Chain of Evidence

Because of the number of system verification and system validation artifacts, it is recommended that organizations use a dedicated application to define and manage them.

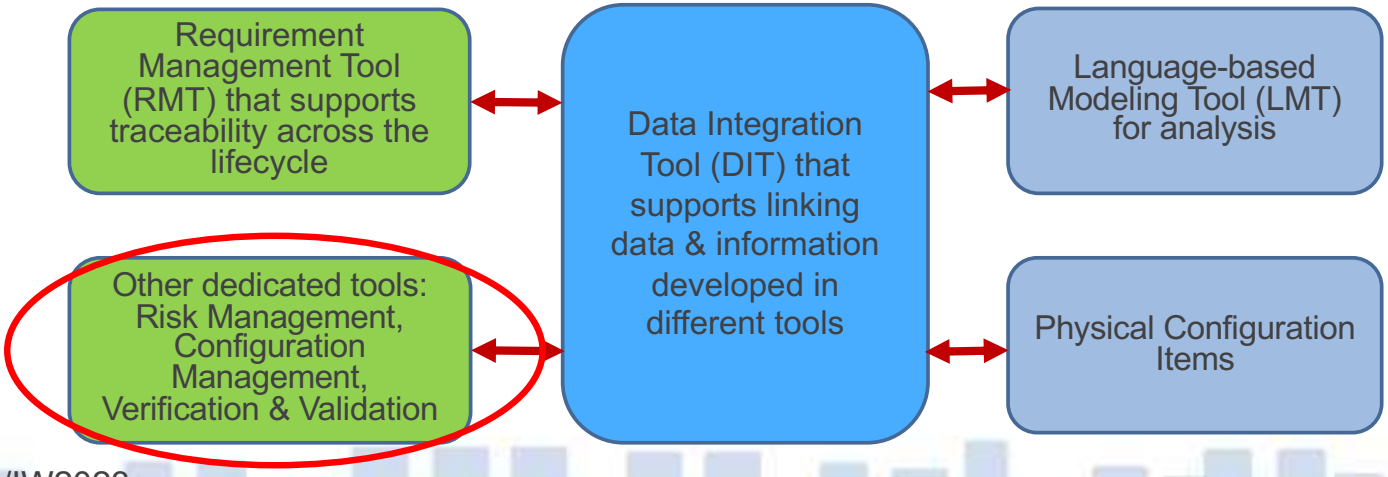
The project team must ensure there is a capability to link the data in this application to other data developed and managed within other tools in the project's toolset.



Refer to the NRM Section 10 for a detailed discussion concerning each of these artifacts.

Using An SE Toolset to Maintain the Chain of Evidence

- Using a dedicated application to manage system verification and system validation artifacts, an SE Toolset must be selected that:
  - Supports sharing and linking of data between tools.
  - Supports the development of an integrated/federated dataset that represents an authoritative source of truth (ASoT).
  - Supports digital threads (traceability) across all SE artifacts, no matter the tool used.
  - Supports change impact assessment across the lifecycle.
  - Allows the use of attributes to manage your project using dashboards and reporting.
  - See the NRM for a more detailed list of features your SE tool set should have to support a data-centric practice of SE.



Obtaining Approval

Note: While this presentation focus is on standards and regulation compliance, this section applied to all needs and requirements.

Obtaining Approval

- **Approval Packages** are submitted to the **Approving Authorities** for approval (acceptance, certification, readiness for use, or qualification).
- The **Approving Authority** is any individual, group of individuals, or organization that has the authority to approve the system for use in its operational environment by its intended users.
- The **Approving Authorities** could be a combination of internal or external customer(s), a regulatory agency, or a third-party certification organization.
- The **Approving Authorities**
  a) decide what constitutes necessary for acceptance, and
  b) determines if the SOI meets that criteria.
- The approval process should be well defined in the project's PMP, SEMP, MIVV plan, and SIVV plan.
- For regulatory agencies, the approval process is often defined as part of the regulations governing the SOI under development.
- Some organizations will conduct a formal System Acceptance Review (SAR) or Readiness for Use Review (RFUR) as part of the approval process prior to submission of the **Approval Package** to the **Approving Authority(s).**

Obtaining Approval

- Assuming a project follows the process defined by the **Approving Authorities** and successfully completed the system verification and system validation activities defined in the NRM, the risk of non-approval is low.
- Sadly, this may not be the case.
  - In the previous FDA example, one of the major reasons for non-approval was the failure to follow the required product development process and submit the required records to the **Approving Authority** - in this example the FDA.
- For many products developed for use around the world, there will be **multiple Approving Authorities**, each with different defined approval processes and associated requirements for documentation and records.
  - In this case, the project will have to be in conformance/compliance with each set of regulations and go through multiple system verification and system validation approval processes.
- For example, US DoD programs there is a Developmental Test an Evaluation (DT&E) process for system verification and Operational Test an Evaluation (OT&E) process for system validation.
  - USC Title 9 requires these processes to be conducted by different organizations.

Closing Thoughts

- **The approval process can be long, complex, and frustrating**.
- Because of this, the focus of the project must be on both the approval process requirements that define what is “necessary for approval” in addition to
  - Concepts associated with meeting the intent of the standards and regulations.
  - Concepts for validating the SOI meets its integrated set of needs associated with relevant standards and regulations.
  - Concepts for verifying the SOI meets the design input requirements associated with relevant standards and regulations.
  - Concepts for establishing and maintaining the chain of evidence of compliance
  - Concepts for how the project will obtain approval
- Both Customers and Suppliers must define the processes, methods, tools, and environment associated with the approval process at the beginning of the project.
  - These must be reflected in the budget and schedule.
  - These must be reflected in the supplier SOW or SA
    - Specific activities the supplier must accomplish or be involved in
    - Specific deliverables and their form and content.

Questions and Discussion

Lou Wheatcraft

- **Lou Wheatcraft** is a senior consultant and managing member of Wheatland Consulting, LLC. Lou is an expert in systems engineering with a focus on needs and requirements development, management, verification, & validation. Lou provides consulting and mentoring services to clients on the importance of well-formed needs & requirements helping them implement needs & requirement development and management processes, reviewing and providing comments on their needs and requirements, and helping clients write well-formed needs & requirements.
- Specialties include: Understanding and documenting the problem; defining project and product scope; defining and maturing system concepts; assessing, mitigating, and managing risk; documenting stakeholder needs; transforming needs into well formed design input requirements; allocation, budgeting, and traceability; interface management, requirement management; and verification and validation.
- Lou's goal is to help clients practice better systems engineering from a needs and requirements perspective across all life cycle stages of system/product development. Getting the needs and requirements right upfront is key to a successful project. Poor needs & requirements can triple the chances of project failure.
- Lou has over 50 years' experience in systems engineering, including 22 years in the United States Air Force. Lou has taught over 200 requirement seminars over the last 21 years. Lou supports clients from all industries involved in developing and managing systems and products including aerospace, defense, medical devices, consumer goods, transportation, and energy.
- Lou has spoken at Project Management Institute (PMI) chapter meetings and INCOSE conferences and chapter meetings. Lou has published and presented many papers concerning needs and requirement for NASA's *PM Challenge*, INCOSE, INCOSE *INSIGHT Magazine*, and *Crosstalk Magazine*. Lou is a member of INCOSE, past Chair and current Co-Chair of the INCOSE Requirements Working Group (RWG), a member of the Project Management Institute (PMI), the Software Engineering Institute (SEI), the World Futures Society, and the National Honor Society of Pi Alpha Alpha.
- Lou has a BS degree in Electrical Engineering from Oklahoma State University; an MA degree in Computer Information Systems; an MS degree in Environmental Management; and has completed the course work for an MS degree in Studies of the Future from the University of Houston – Clear Lake.