

Why an INCOSE Systems Approach is Needed

Dick Kitterman
Northrop Grumman Corporation
2611 Jefferson Davis Highway, Suite 700
Arlington, VA 22202

A Position for the Panel: Myriad Multiplying Risk Management Standards
“*Converging Toward Best Practice*” or “*A Maze of Docs to Trap Us?*”

Sixteenth Annual International Symposium of the
International Council On Systems Engineering (INCOSE)
8 - 14 July 2006

Copyright © 2006 by Dick Kitterman. Published and used by INCOSE with permission.

- I am going to focus on risk management as treated in ISO standards: 12207, 15288, 16085.
- ISO standards follow the same path that other standards do: 90% focus on the process, 10% focus on everything else. My three specific examples are:
 - ISO/IEC 12207—Amendment 1: 2002 defines a risk management sub-process in which risk management is described as a stand alone set of activities. There is no indication that one would do risk management when doing a trade study, selecting a supplier, assessing the impacts of a proposed change, or anything else. There is no wording to drive a coupling, integration, embedding into other processes.
 - ISO/IEC 15288—the process purpose is to “reduce the effects of uncertain events . . .,” which is good, because points to a reason for doing risk management. However, continuing, risk management “identifies, assesses, treats and monitors risks . . .,” which is back to a process focus and as a process isolated from other processes.
 - ISO/IEC 16085—this is still in draft, so things could change. However, there is a real step forward in the perspective because the Field of Application clause says “When used with ISO/IEC 1220:1995, this standard assumes that the other management and technical processes of ISO/IEC 12207 perform the treatment of risk. Appropriate relationships to those processes are described. Also, Annex D shows the application of risk management to the other 12207 processes. Unfortunately, this is informative, not normative, and it is not especially clear that applying risk management practices is embedded in each of the other processes, versus being applied from the outside.
- An example of the kind of risk management plan that flows from these viewpoints:
 - 50 page risk management plan

- 37 pages talk about the process of risk identification, analysis, mitigation, tracking and control
- Minimal discussion of responsibilities, metrics
- No mention of objectives, strategy, approach, customer interface/engagement, ongoing improvement

- That's WRONG!

- Before one gallops off to execute a process, one should understand why the process is being done. More specifically: what are the objectives being supported?

- At present, 100%-epsilon of risk management efforts doggedly focus on executing a risk management process as something that exists by itself in its own right, rather than as something that should be embedded in and permeated throughout a project or program as an inherent part of all the efforts of achieving that project or program's objectives.

- One must start with the objectives of whatever the risk management effort is to support, then reverse engineer down to what processes, executed where, when, by whom, will best address risks that might impede achieving the objectives.

- That reverse engineering is in fact what a systems view would bring to managing risk.

- That systems view needs to be put into the standards. The pages following illustrate some examples where risk considerations could be put into other processes.

- INCOSE has the systems view, ergo, INCOSE should be involved in bringing the systems approach to the treatment of risk management in ISO standards.

Biography

Dick Kitterman is currently risk process manager for a missile defense program. He has been responsible for systems engineering, risk management and program management functions in aviation, aerospace, and space over the past 22 years. Prior to that, Dick's experience is in program and product management in the computer peripheral and semiconductor component areas.

Mr. Kitterman has served as co-chair of the INCOSE RIMWG for over a decade, is Region V Member Board Representative and is INCOSE liaison to ISO, on the working group that is responsible for 12207 and 15288 (the software and systems engineering standards, respectively).

Area for Risk Management Engagement	Rationale	Steps to Take
System requirements definition and analysis	It is necessary to understand which requirements have uncertainties, either ambiguities in statement or uncertainty of successful execution and then evaluate the uncertainties to see where they may pose a risk to successful realization of the requirement.	<ul style="list-style-type: none"> • Develop a set of descriptions of the factors and levels that would describe higher or lower requirements risk (e.g., complexity, ambiguity, inconsistency, uncertainty, specific technical/quality/environmental/ etc. hurdles, and so on). • Work with systems engineering to incorporate the descriptions and steps to analyze and handle risks as an inherent part of each stage of requirements decomposition and allocation. • Work with systems engineering to ensure that these steps are written into their processes and any other relevant documents. • Provide training and support on an ongoing basis as required and agreed upon.
System requirements change management	Each time a change to a requirement is proposed, the change should be evaluated to see if new uncertainties and risks are being introduced.	<ul style="list-style-type: none"> • Work with systems engineering and the change management function to ensure that assessments are made of the risks associated with each proposed requirements change at a level appropriate to the scope of the change. • Ensure that doing the assessments and making use of the results in requirements change decisions are written into the change management process and any other relevant documents. • Work with the systems engineering and change management functions to ensure that these steps are written into their processes and any other relevant documents. • Provide training and support on an ongoing basis as required and agreed upon.
System architectural and design trade studies	As the decisions are made to allocate requirements to specific instantiating entities, explicit assessment should be made of the risks of that instantiation versus other alternatives	<ul style="list-style-type: none"> • Work with systems engineering to ensure that risks are identified, analyzed and handled at each stage of architecture definition and inherently in each design trade study. • Work with systems engineering to ensure that these steps are written into their processes and any other relevant documents. • Provide training and support on an ongoing basis as required and agreed upon. • See Case Study 1
System interface analysis	It is necessary to understand which interface properties have uncertainties, either ambiguities in statement or uncertainty of successful execution and then evaluate the uncertainties to see where they may pose a risk to successful realization of the interface.	<ul style="list-style-type: none"> • Work with systems engineering to ensure that risks are identified, analyzed and handled as an inherent part of each stage of interface definition and IRD/ICD development. It may be useful to use a template like the one for requirements risk. • Work with systems engineering to ensure that these steps are written into their processes and any other relevant documents. • Provide training and support on an ongoing basis as required and agreed upon.

Area for Risk Management Engagement	Rationale	Steps to Take
System interface change management	Each time a change to an interface is proposed, the change should be evaluated to see if new uncertainties and risks are being introduced.	<ul style="list-style-type: none"> • Work with systems engineering and the change management function to ensure that assessments are made of the risks associated with each proposed interface change at a level appropriate to the scope of the change. • Ensure that doing the assessments and making use of the results in interface change decisions are written into the change management process and any other relevant documents. • Work with the systems engineering and change management functions to ensure that these steps are written into their processes and any other relevant documents. • Provide training and support on an ongoing basis as required and agreed upon.
System test definition and planning	It is necessary to understand where there are risks of being able to test a particular requirement, or related group of requirements.	<ul style="list-style-type: none"> • Work with systems engineering to ensure that risks are identified, analyzed and handled as an inherent part of each stage of test definition and planning. • Work with systems engineering to ensure that these steps are written into their processes and any other relevant documents. • Provide training and support on an ongoing basis as required and agreed upon. • See Case Study 2
System operational use planning	Operational scenarios that are not clearly defined may pose risks to successful execution, so all such scenarios need to be examined for risk.	<ul style="list-style-type: none"> • Work with systems engineering and appropriate user and support stakeholders to ensure that risks are identified, analyzed and handled, e.g., scenario modeling and analysis, as an inherent part of each stage of operational use planning. • Work with systems engineering and the other stakeholders to ensure that these steps are written into their processes and any other relevant documents. • Provide training and support on an ongoing basis as required and agreed upon • See Case Study 3
System support planning	It is necessary to determine which areas of life cycle support have uncertainties of successful execution, hence pose risks to ongoing use of the system under consideration.	<ul style="list-style-type: none"> • Work with systems engineering and appropriate user and support stakeholders to ensure that risks are identified, analyzed and handled as an inherent part of support planning. • Work with systems engineering and the other stakeholders to ensure that these steps are written into their processes and any other relevant documents. • Provide training and support on an ongoing basis as required and agreed upon • See Case Study 4
System retirement/replacement planning	It is necessary to determine the risks associated with planning to either retire or replace an in-use system, including development, transition and disposition.	<ul style="list-style-type: none"> • Work with systems engineering and appropriate user and support stakeholders to ensure that risks are identified, analyzed and handled as an inherent part of planning for system retirement, with or without replacement. • Work with systems engineering and the other stakeholders to ensure that these steps are written into their processes and any other relevant documents. • Provide training and support on an ongoing basis as required and agreed upon.

Table 1: General Overview of Embedding Risk Management within Systems Engineering Processes

ISO/IEC Process Title & Purpose	Embedding Rationale	Steps to Take
<p><u>Agreement Processes: Acquisition Process</u>—to obtain a product or service in accordance with the acquirer’s requirements</p>	<p>Risk assessments and handling are appropriate at least when establishing acquisition strategy, selecting a supplier (whether an internal organization or an external enterprise), justifying the selection, and establishing the agreement to acquire the product or service</p>	<p>Illustrating with the case of an externally obtained product of service:</p> <ul style="list-style-type: none"> • With Procurement, modify procurement procedures that address establishing strategy, etc., to explicitly state what risk management steps are to be done, when, and by whom. Include pointers to detailed risk management process documents as appropriate. • Develop metrics to evaluate value of risk management in the acquisition process. The process for internal sources is directly analogous
<p><u>Enterprise Processes: Enterprise Environment Management Process</u>—to define and maintain the policies and procedures needed for the organization’s business with respect to the scope of [15288]</p>	<p>This is a high-leverage place from which to scrutinize all policies and procedures on an ongoing, consistent basis to ensure steps to find and address risks are embedded pervasively throughout the enterprise’s management environment</p>	<ul style="list-style-type: none"> • First, revise the existing policy and procedure that prescribe the steps for defining policies and procedures, adding guidance on how to put risk management steps in the appropriate places. • Second, include a requirement that all substantive policy and procedure issuances and changes be reviewed for unintended short and long term, direct and indirect side effects (i.e., risks)
<p><u>Project Processes: Project Planning Process</u>—to produce and communicate effective and workable project plans</p>	<p>This is an analogue of the Enterprise Environment Management Process, but focused on a specific project, so it is the highest-leverage point from which to permeate the project’s way of life with well-integrated risk management attitudes, practices and measures</p>	<ul style="list-style-type: none"> • Review each element of the project plans to determine two things: first, risks associated with that element (e.g., a specific project task or deliverable), and; second, where responsibilities, performance measures, project processes and resources need to include material relating to managing risk
<p><u>Technical Processes: Stakeholder Requirements Definition Process</u>—to define the requirements for a system that can provide the services needed by users and other stakeholders in a defined environment</p>	<p>It is necessary to understand which requirements have uncertainties, either ambiguities in statement or uncertainty of successful execution and then evaluate the uncertainties to see where they may pose a risk to successful realization of the requirement. It is also critical to understand where the ISO/IEC 15288 activities involved in defining (and maintaining the definition of) requirements over the system life cycle may themselves have potential weaknesses, or sources of problems, hence be risks in themselves</p>	<p>Addressing the first part of the rationale only:</p> <ul style="list-style-type: none"> • Develop a set of descriptions of the factors and levels that would describe higher or lower requirements risk (e.g., complexity, ambiguity, inconsistency, uncertainty, specific technical/quality/environmental/ etc. hurdles, and so on). • Work with systems engineering to incorporate the descriptions and steps to analyze and handle risks as an inherent part of each stage of requirements decomposition and allocation. • Work with systems engineering to ensure that these steps are written into their processes and any other relevant documents. • Provide training and support on an ongoing basis as required and agreed upon.

Table 2: Embedding Risk Management in ISO/IEC 15288 Processes

ANSI/EIA Process Title & Purpose	Embedding Rationale	Steps to Take
<u>Acquisition and Supply: Supply Process</u> —to arrive at an agreement with another party to accomplish specific work and to deliver required products	Risks must be considered by a prudent developer when establishing an agreement to be a supplier. Further, steps to identify, handle and monitor risks should be included in the tasks they propose to do, whether they are in an internal or external supplier role	<ul style="list-style-type: none"> • Lay out steps to identify and handle risks in each part of the proposed tasks and ensure that the risks found and their proposed treatment are included in the appropriate information sections of the agreement, or in internal annexes or plans supporting it
<u>Technical Management: Planning Process</u> —to support enterprise and project decision making and to prepare necessary technical plans that support and complement project plans	This is the core definition of the technical work to be accomplished, from strategy to detailed tasks, hence a clear understanding of potential threats to success for every element of the technical effort must be an innate part of planning	<ul style="list-style-type: none"> • Include consideration of risks and their handling in each of the tasks for each of the requirements of the Planning Process. • Also, assess where the abilities to plan and do each task may themselves have potential weaknesses, or sources of problems, hence be risks in themselves
<u>System Design: Requirements Definition Process</u> —to identify, collect and define acquirer and other stakeholder requirements and transform them into a set of validated system technical requirements	It is necessary to understand the uncertainties in finding all stakeholders and the risks in determining how to weigh or set precedence to their requirements. Equally, it is critical to find which requirements have uncertainties, either ambiguities in statement or uncertainty of successful execution and then evaluate the uncertainties to see where they may pose a risk to successful realization of the requirement. It is also vital to understand where the EIA 632 tasks involved in defining (and maintaining the definition of) requirements over the system life cycle may themselves have potential weaknesses, or sources of problems, hence be risks in themselves	<p>Addressing a part of the rationale only:</p> <ul style="list-style-type: none"> • Develop a set of descriptions of the factors and levels that would describe higher or lower requirements risk (e.g., complexity, ambiguity, inconsistency, uncertainty, specific technical/quality/environmental/ etc. hurdles, and so on). • Work with systems engineering to incorporate the descriptions and steps to analyze and handle risks as an inherent part of each stage of requirements decomposition and allocation. • Work with systems engineering to ensure that these steps are written into their processes and any other relevant documents. • Provide training and support on an ongoing basis as required and agreed upon
<u>Product Realization: Implementation Process</u> —to transform the characterized design solution into an integrated end product that conforms to its specified requirements	The tasks to receive, assemble, test, verify and validate all of the elements that will comprise the realized system can have many things that do not go right. It is necessary and prudent to understand these potential problems and how to best avoid them before they turn into real problems	<ul style="list-style-type: none"> • Evaluate the steps involved in each of the tasks of the Implementation Process to see where risk management actions are appropriate. • Also, assess where the abilities to plan and do each task may themselves have potential weaknesses, or sources of problems, hence be risks in themselves
<u>Technical Evaluation: Systems Analysis Process</u> —to provide a decision making basis, determine progress in satisfying requirements, and support risk management	Ensuring that inclusion of uncertainties and risks in analyses of effectiveness and tradeoff is necessary to prevent decisions that do not recognize potential problems	<ul style="list-style-type: none"> • Build risk identification and analysis steps in each of the other analysis steps, as well as including consideration of risk in each of the decisions made during systems analysis

Table 3: Embedding Risk Management in EIA 632 Processes

ISO/IEC Process Title & Purpose	Embedding Rationale	Steps to Take
<p>Primary life cycle processes: <u>Acquisition process: Acquisition preparation</u>—to establish the needs and goals of the acquisition and to communicate these with the potential suppliers</p>	<p>It is necessary to understand the uncertainties in finding all stakeholders and the risks in determining how to weigh, set precedence to and resolve conflicts among their needs and goals. Whatever solution is obtained will be a compromise, which will entail risks. The process must, therefore, try to make clear and explicit the risks of one decision versus another. There are also risks in communicating effectively with the potential suppliers and these should be found and addressed as an inherent part of preparing for the acquisition</p>	<ul style="list-style-type: none"> • Evaluate the steps involved in each of the tasks of the Acquisition preparation process to see where risk management actions are appropriate. • Also, assess where the abilities to plan and do each task may themselves have potential weaknesses, or sources of problems, hence be risks in themselves
<p>Supporting life cycle processes: <u>Documentation process: Configuration management process</u>—to establish and maintain the integrity of all the work products of a process or project and make them available to concerned parties</p>	<p>Each time a change to an item is proposed, the change should be evaluated to see what new uncertainties and undesired consequences might be introduced by the change. This needs to be done as an inherent part of the decision making to accept the change.</p>	<ul style="list-style-type: none"> • Work with systems engineering and the change management function to ensure that assessments are made of the risks associated with each proposed item change at a level appropriate to the scope of the change. • Ensure that doing the assessments and making use of the results in change decisions are written into the change management process and any other relevant documents. • Work with the systems engineering and change management functions to ensure that these steps are written into their processes and any other relevant documents. • Provide training and support on an ongoing basis as required and agreed upon.
<p>Organizational life cycle processes: <u>Management process: Organizational alignment</u>—to ensure that the software processes, needed by the organization to provide software products and processes, are consistent with its business goals</p>	<p>Each of the tasks required for organizational alignment can have risks in either planning or execution, so it is necessary to ensure that these risks are identified as the alignment tasks are being planned and throughout their execution.</p>	<ul style="list-style-type: none"> • Evaluate the steps involved in each of the tasks of the Organizational alignment process to see where risk management actions are appropriate. • Also, assess where the abilities to plan and do each task may themselves have potential weaknesses, or sources of problems, hence be risks in themselves

Table 4: Embedding Risk Management in ISO/IEC 12207 Processes

IEEE Process Title & Purpose	Embedding Rationale	Steps to Take
<p><u>Requirements analysis</u>—to establish what the system shall be capable of accomplishing</p>	<p>It is necessary to understand which expectations, constraints, scenarios, utilization environments, and so on, have uncertainties, either ambiguities in statement or uncertainty of successful execution and then evaluate the uncertainties to see where they may pose a risk to successful realization of the requirement. It is also critical to understand where the IEEE 1220 activities involved in analyzing the requirements over the system life cycle may themselves have potential weaknesses, or sources of problems, hence be risks in themselves</p>	<p>Addressing the first part of the rationale only:</p> <ul style="list-style-type: none"> • Develop a set of descriptions of the factors and levels that would describe higher or lower requirements risk (e.g., complexity, ambiguity, inconsistency, uncertainty, specific technical/quality/environmental/ etc. hurdles, and so on). • Work with systems engineering to incorporate the descriptions and steps to analyze and handle risks as an inherent part of each stage of requirements analysis. • Work with systems engineering to ensure that these steps are written into their processes and any other relevant documents. • Provide training and support on an ongoing basis as required and agreed upon.
<p><u>Functional verification</u>—to assess the completeness of the functional architecture in satisfying the validated requirements baseline and to produce a verified functional architecture for input to synthesis</p>	<p>It is critical to define where there are risks in being able to fully verify the functional architecture, either because of the nature of the architecture, or because of limitations in ability to execute the planned verification testing</p>	<ul style="list-style-type: none"> • In each task of functional verification, include assessment of the risks and measures for handling them, whether due to the architecture's properties or due to weaknesses in equipment, staff, facilities, procedures or other abilities to plan and perform verification
<p><u>Control</u>—to manage and document the activities of the systems engineering process</p>	<p>The tasks under the control process involve other processes and measurements that can be used to determine risks and how to handle them (e.g., configuration management)</p>	<ul style="list-style-type: none"> • Evaluate the steps involved in each of the tasks of the Control process to see where risk management actions are appropriate. • Also, assess where the abilities to plan and do each task may themselves have potential weaknesses, or sources of problems, hence be risks in themselves

Table 5: Embedding Risk Management in IEEE 1220 Processes