Risk-Based System Development Method – A MBSE Approach

David Feng

Principal System Engineer

Sedation System

06/24/2014

Prepared for CIMdata's System Engineering Workshop

ETHICON
PART OF THE Johnson & Johnson FAMILY OF COMPANIES

Better surgery
for a better world

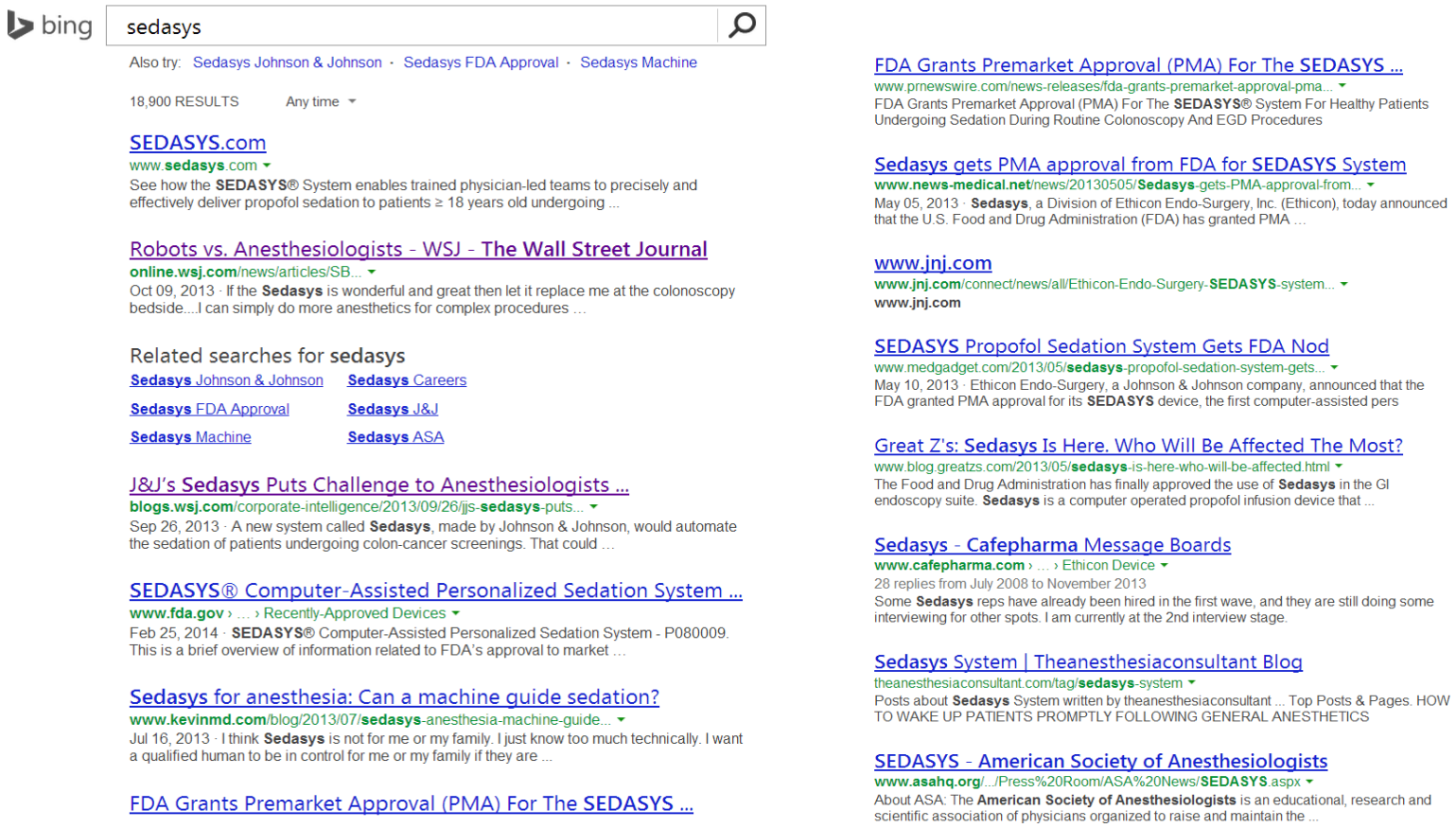
sedasys®

The Purpose of this Presentation

- To explain rational that motivates us to adopt the RBSD as life-cycle system development method.
- To demonstrate why a risk model is capable of play the principal and governing model in MBSE methodology that unifies multifarious models, and disseminates critical information whenever is needed.
- To show how the MBSE method can be developed from risk viewpoint.
- To enumerate major advantages of the RBSD method from regulatory, engineering and legal perspective.

Motivations for Developing RBSD Method

- Sedasys business development environments



Motivations – continue…

- Regulatory environment has changed greatly over the years:
  - Instead of claiming safety through satisfaction of safety standards implicitly and prescriptively.
  - Manufacturers are required to demonstrate explicitly and descriptively that their devices have achieved an acceptable level of safety assurance.
- Most of system development methods including MBSE in literature today are developed either isolated or independent from risk process, which is inadequate to keep pace with the change of regulatory environment and to support safe system development.
- Recently, FDA recommends assurance case (AC) as a part of medical device submission. It is challenge to construct AC without an adequate risk management framework.

What is Model-Based System Engineering?

- The central premise of the MBSE method is that building a coherent system model for the system development life cycle
  - can better harmonize system requirements development, analysis, design and integration;
  - can better capture the interrelationships between model elements; and
  - can minimize misinterpretation and omission of system characterizations
- The natural question becomes what type of system models play this coherent role?
- We believe that risk model is a natural candidate for this role since it addresses common concerns shared by all stakeholders. More importantly, they use a common language understood by all stakeholders.

What is Risk-Based System Development?

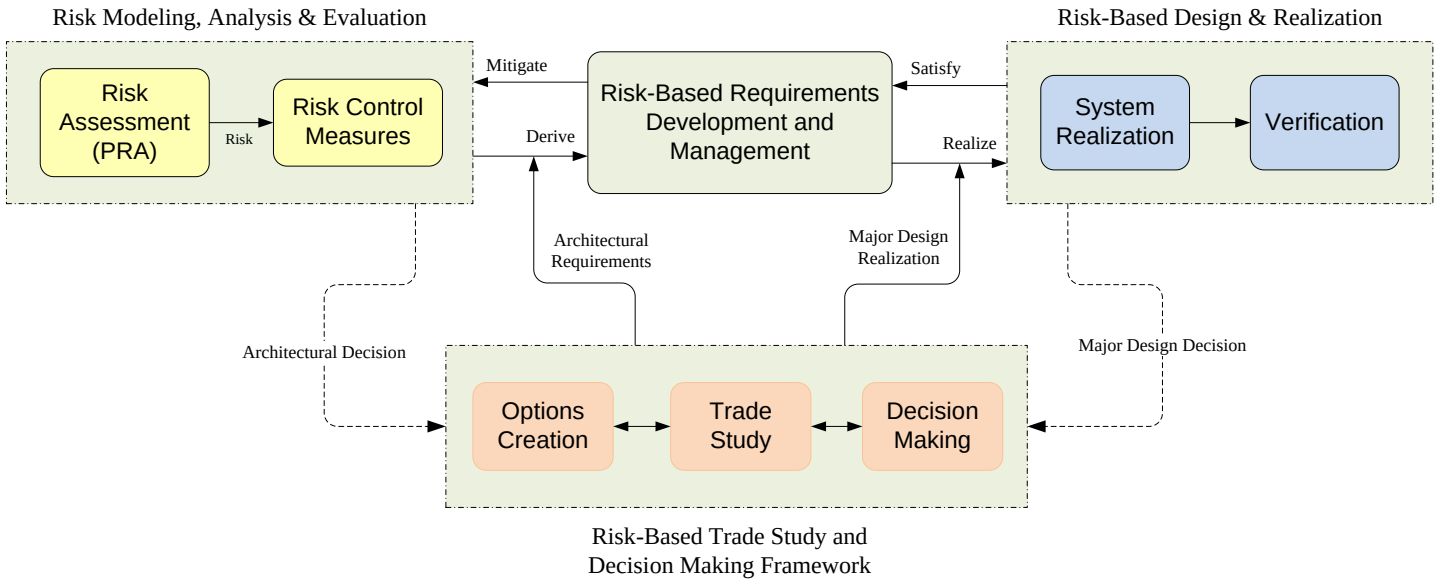
- The fundamental premise for RBSD is that risk is inherent in all systems or processes, whether the risk is a safety, security or business.
  - Conceptually, the RBSD is a MBSE methodology, which elevates the risk models to a principal and governing role in the entire life cycle system development.
  - Operationally, the RBSD utilize the risk models as a common denominator to unify multifarious modeling methods
    - By a common set of risk attributes – a triplet {scenarios, likelihood, severity}
    - By using the probabilistic risk assessment (PRA) as common language to characterize risk and its corresponding contributions to the overall system profile.
  - As a result, the effectiveness of system development can be measured quantitatively or/and qualitatively in probabilistic terms.

Implications Resulted from the Premise of RBSD

- The RBSD method naturally leads to an elaborate, concurrent, holistic aspect of life-cycle system development, characterized as:
  - *Every* function or process is associated with risks.
  - *Every* derived requirement is associated with at least one risk whether is safety, security, regulatory or business risk.
  - *Each* derived requirement is explicitly associated with quantitative or qualitative risks through the risk models described by PRA language.
  - The primary objective of system design aims to uncover all the risks and to mitigate them to an acceptable level.
- At the end, whether a new function is required or which an alternative should be selected is largely determined by how effectively that function or alternative mitigates identified risks to an acceptable level.

RBSD Process Framework

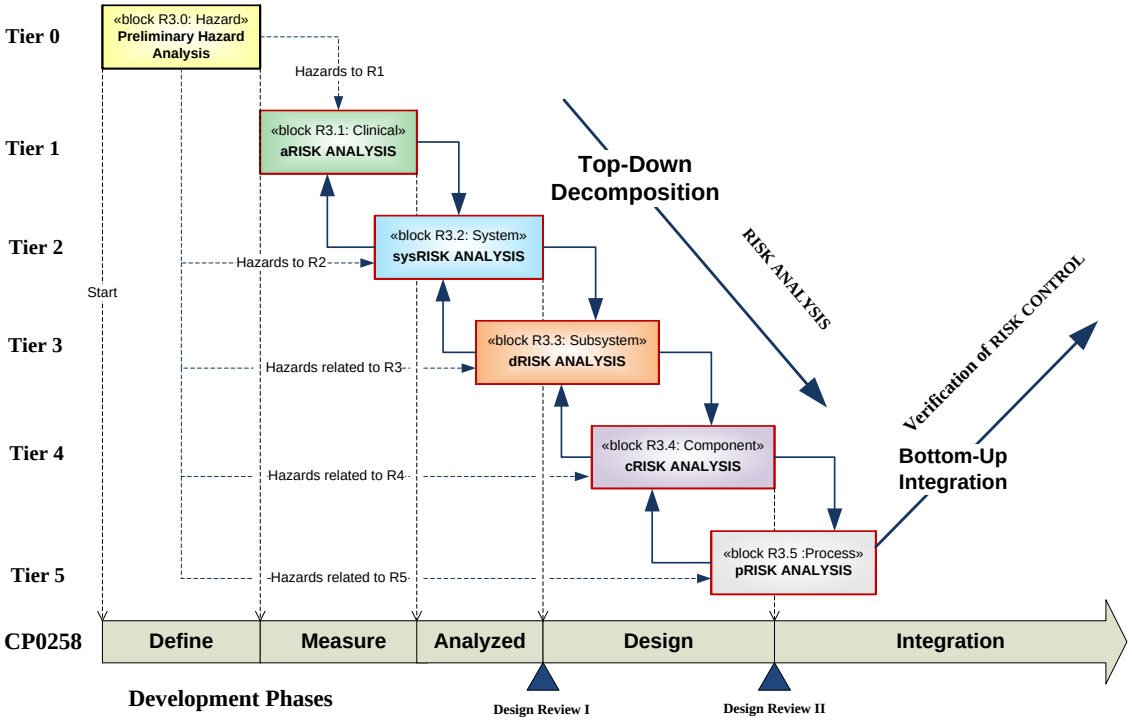
- Unlike other commonly-used development methods, the RBSD starts with risk modeling and risk assessment first, follows by risk-based trade study, then derives requirements that control the identified risks.



Risk-Based System Development Process

RBSD – An hierarchical, iterative process

- Risk modeling in the RBSD is an hierarchical and iterative process.

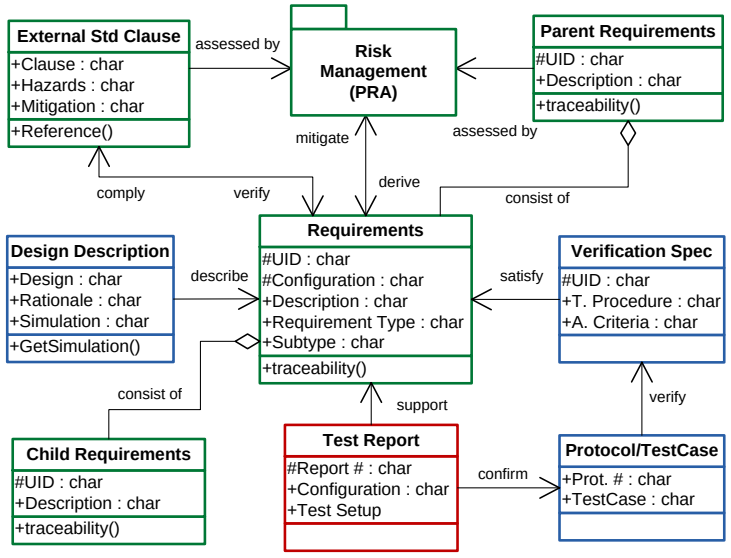


Risk Analysis Process – Left side of V-model

The block in each tier is represented by hierarchical risk modeling.

Risk Model as a Cardinal Model in MBSE

- Since risk models derive all the requirements from a system hierarchy, thus, they explicitly link risks to every aspect of system life-cycle from requirements, designs, verifications to post-production monitoring.
- The efficacy of system design is measured by how well the system controls the risks to an acceptable level. Naturally all information about risks can be disseminated from risk models to other models.
- All risk models share same language, same criteria for acceptance. This trait can abstract other models to a representation that is concerned by all stakeholders.



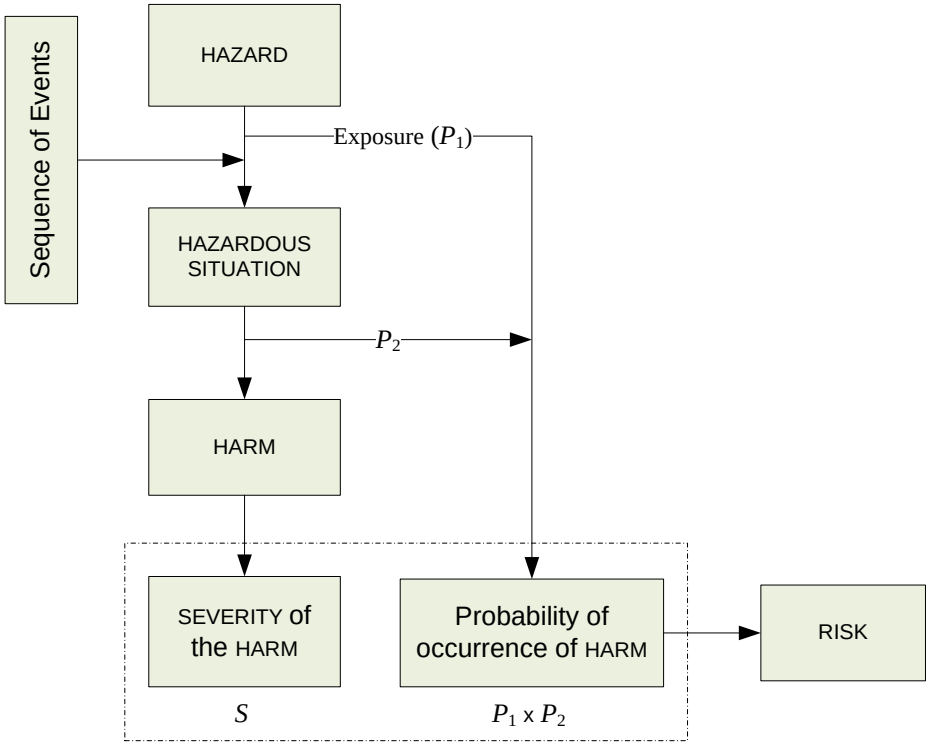
The Class Model for a Typical Requirement Object

Viewpoint Approach to Structure Risk Models

- The RBSD method adopts the viewpoint approach recommended by “IEEE 1471 – architectural description of software-intensive systems”
- Viewpoint is defined as “A specification of the conventions for constructing and using a view. A pattern or template from which to develop individual views by establishing the purposes and audience for a view and the techniques for its creation and analysis”
- Viewpoint consists of a) name, b) stakeholder addressed by viewpoint, c) concerns, d) language, modeling technique, analytical methods, etc. and e) sources.

Risk Viewpoint – stakeholders, concerns and modeling

- Stakeholders:
  - Varied depending on hierarchy
- Concerns:
  - What can happen?
  - How likely is it to happen?
  - Given that it occurs, what are the consequences?
- Reference Modeling:
  - The RBSD adopts the model defined in Annex E of ISO 14971-2007 – Application of risk management process.

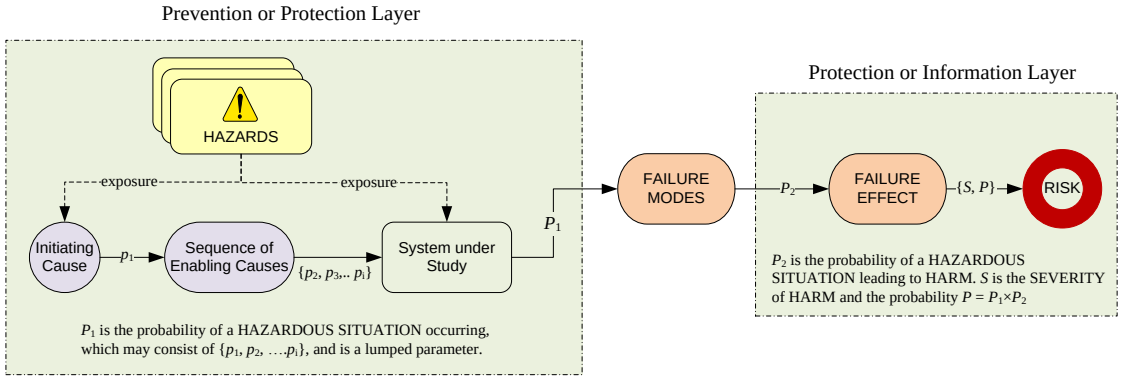


P_1 is the probability of a HAZARDOUS SITUATION occurring.
P_2 is the probability of a HAZARDOUS SITUATION leading to HARM.

Risk Model – a Triplet Concept from ISO 14971

Risk Viewpoint – modeling techniques, analytical methods and language

- Modeling techniques/methods:
  - Adopted scenario-based risk modeling, event tree modeling, etc.



Scenario-Based Risk Modeling

- Analytical methods:
  - Probabilistic risk assessment by using FT, Monte Carlos simulation, etc.

- Languages:
  - Probability, statistical inference (classical and/or Bayesian)

A Brief Summary of RBSD method

- Let's recap the risk modeling that underlies the RBSD method:
  - First, the HRM is essentially a coarse grain of modeling to unify other modeling methods, e.g., functional, behavior, use case modeling, etc. and qualify overall system success/failure behavior in probabilistic terms.
  - Second, the PRA , e.g. fault tree, could be thought as a fine grain modeling to quantify each level's success/failure contribution to the total system by assigning probabilities to each event or scenario node.
- As a result, the outcome of RBSD process is the creation of a very large set of requirements that are explicitly linked to myriad risks (only implicit or completely missing in other methods), and hierarchically organized into sets or subsets with prioritized risk rankings.
- If done well, the set of risks at any given level of hierarchy would approach a "complete set", as do the requirements.

Major Advantages of RBSD

- From regulatory perspective:
  - Precisely address regulatory concerns, i.e. safety and efficacy of a system.
  - Match regulatory trend that emphasize “explicit and descriptive” regulatory compliance
- From product development perspective:
  - an elaborate and concurrent system development method more likely result in a shorter development cycle and a safer product, particularly, in post-production monitoring.
  - Less likely miss important system requirements, and more likely generate novel system solutions.
- From legal perspective:
  - A comprehensive risk analyses are almost a “must” in any liability lawsuit.
  - Risk-based trade study is the effective way to demonstrate risk/benefit analysis in the strict liability litigation.

Risk-Based System Development – A MBSE Approach