ETLS 509 - Validation & Verification
University of St. Thomas

John Engelman

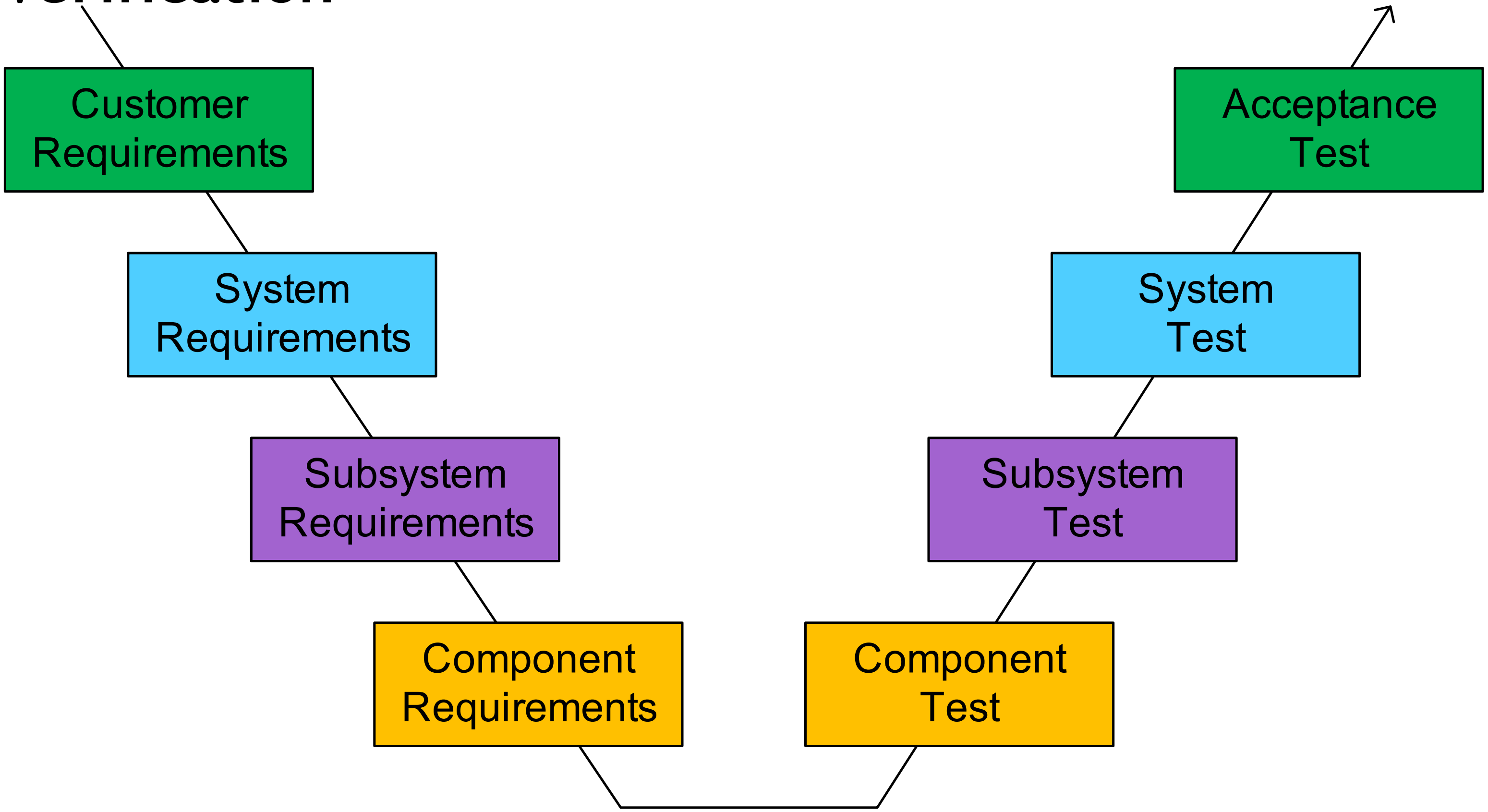
Fall 2016

ETLS 509 - Session 2

- **Questions/review**
- **The System Design Processes - the "V" model**
  - Many other system design process models
    - Spiral, waterfall, etc.
- **Define Verification**
- **Define Validation**
- **Measure of Effectiveness**
- **Technical Performance Measures**
- **System life-cycle phases & steps**
- **Case studies**
- **Verification matrix**
- **System development**
- **ETLS 509 Project**

ETLS 509 - Session 2

- **The System Design Processes, Define Validation & Verification**



System Verification

- **System Verification** - Verification is the confirmation, through the provision of objective evidence, that **specified requirements have been fulfilled**. With a note added in ISO/IEC/IEEE 15288, verification is a set of activities that compares a system or system element against the required characteristics (ISO/IEC/IEEE 2008). This may include, but is not limited to, specified requirements, design description, and the system itself.
  - From the Systems Engineering Body of Knowledge (SEBoK)
- Discussion –
  - How does this relate to design activates
  - How does this relate to testing

System Validation

- **System Validation** - Validation is the confirmation, through the provision of objective evidence, that the **requirements for a specific intended use** or application have been fulfilled. With a note added in ISO 9000:2005: *validation is the set of activities that ensure and provide confidence that a system is able to accomplish its intended use, goals, and objectives (i.e., meet stakeholder requirements) in the intended operational environment* (ISO 2005).
  - From the Systems Engineering Body of Knowledge (SEBoK)
- Discussion
  - What is the difference between Verification an Validation

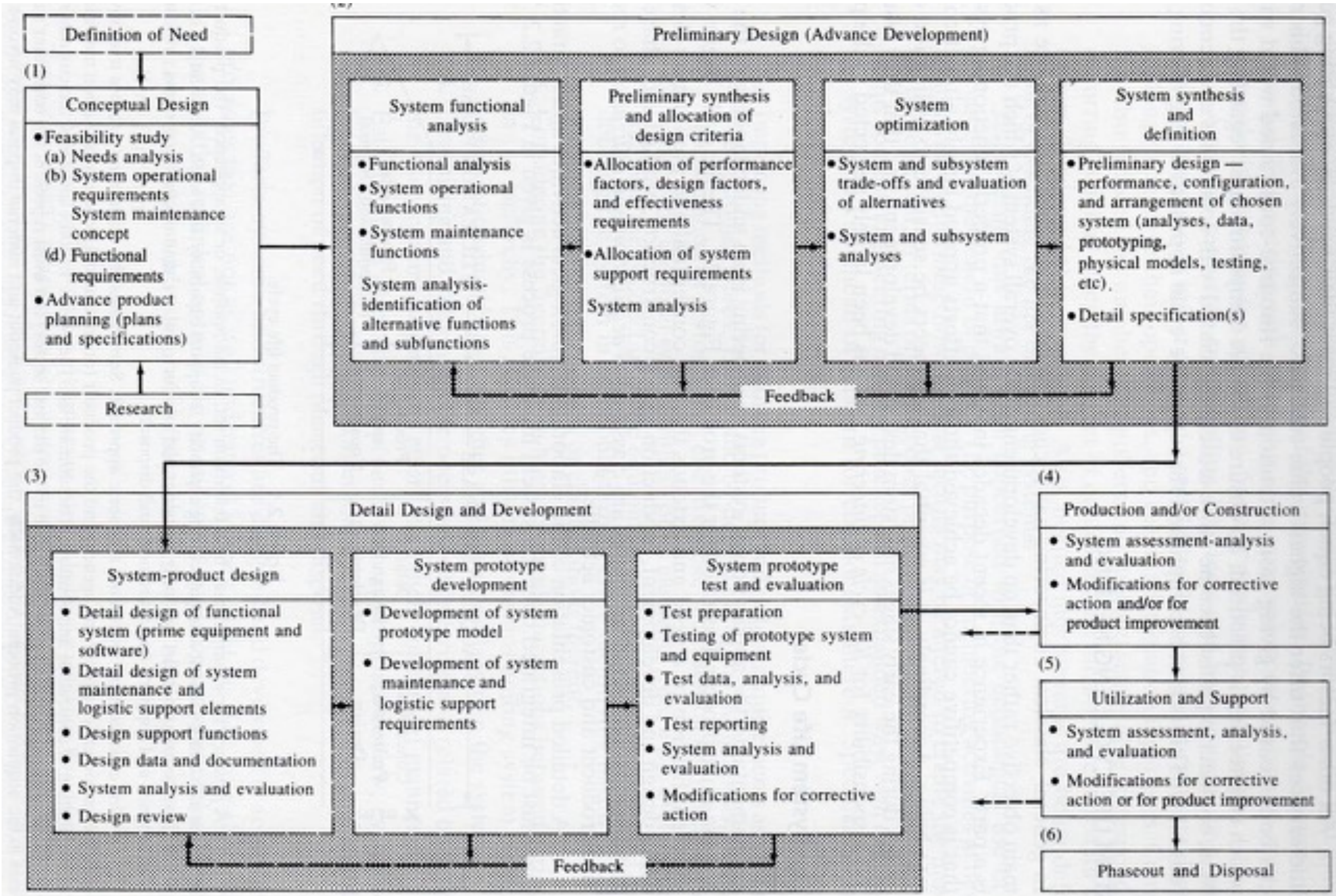
Measures of Effectiveness (MOE) / Technical Performance Measures (TPMs)

- **MOEs are related to the intended use of the system from the user's perspective**
  - Measures how well a system in operation meets its intended goals
    - If a system is intended to operate from 0^o to 60^o, then the MOEs should reflect this
- **Technical Performance Measures (TPMs)**
  - Measures that determine how well as systems satisfies a technical requirement
    - If a system is operate with a 3.3 V +/- 5% power supply, then the TPMs would reflect this, e.g., 2 TPMs
      - Power supply minimum voltage output is 3.135 V, power supply maximum voltage is 3.465
        - » Measurement conditions need be defined – minimum current draw, maximum current draw, potentially current switching characteristics if the system is subject to significant current spikes
      - System will operate with voltage between 3.135 V and 3.465 V
- **MOEs and TPMs are two of the performance measures of interest in Verification & Validation**

System Verification and Validation & Measures

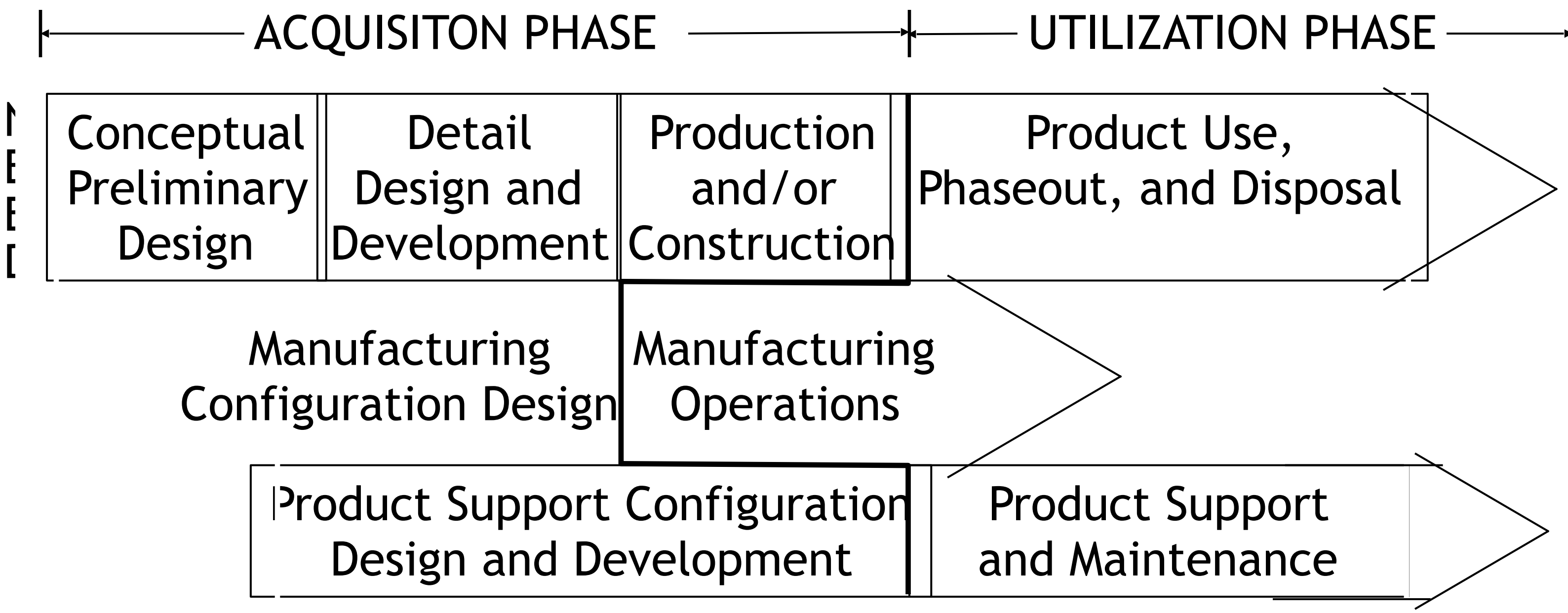
- How do MOEs relate to Verification and/or Validation
- How do TPMs relate to Verification and/or Validation

System Life-Cycle Process



Blanchard Figure 2-2

Product, Manufacturing & Support Life Cycles



Blanchard figure 2.3

Design & Development are always brought out and highlighted, system testing verification/validation is an integral part of successful system developments

System Life-cycle Processes

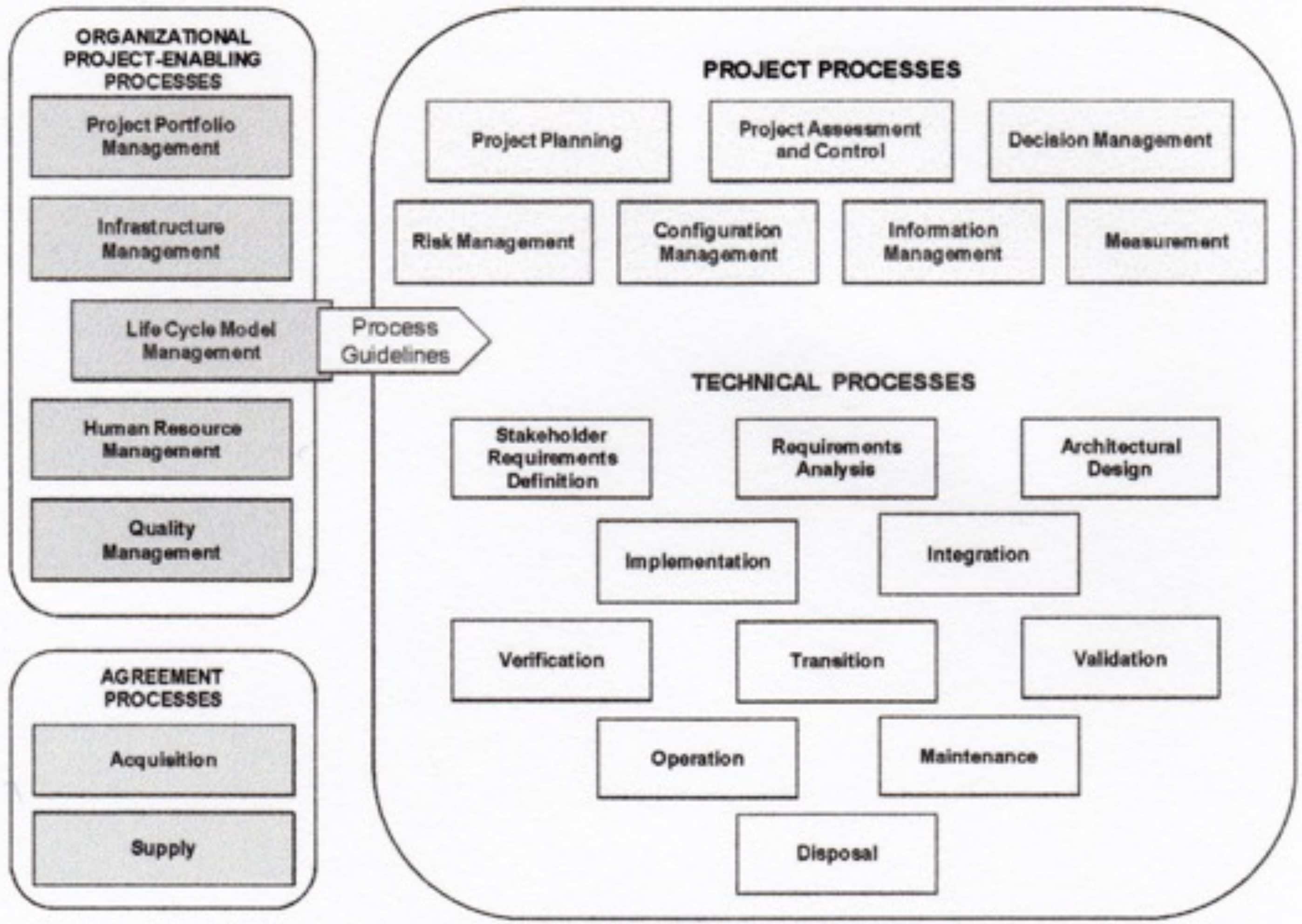


Figure 1-1 System Life-cycle Processes Overview per ISO/IEC 15288:2008

INCOSE Engineering Handbook figure 1-1

Requirements – what happens when it's wrong

- **Medical Radiation Case Study (Material from SEBoK v1.3)**
  - Radiation used in treating tumors
  - Atomic Energy of Canada (AECL) developed dual mode (X-rays or electrons) Therac-20 linear accelerator
    - Successful in clinical use
  - New development of Therac-25 integrated DEC (Digital Equipment Corporation) PDP-11 for command/control/user interface into the device
    - Software written in PDP-11 assembly code
    - Fault tree of Therac-25 did not include software
    - Testing was principally "integrated systems testing"
  - Operational use of Therac-25 resulted in multiple cases of radiation over exposure and multiple cases resulted in patient death
- **What went wrong?**

FBI Virtual Case File System Case Study

- **Following 9/11 there was a desire/urgent need for better sharing of information across the FBI (law enforcement in general)**
- **Money was no object, time was the only relevant factor**
  - Congress easily appropriated $380M for the FBI to create the virtual case file system. More funding would come.
    - The Trilogy Information Technology Modernization Program was created
      - Part 1 – update all 56 FBI field offices computer equipment
      - Part 2 – re-implement the FBI Intranet, LANs, etc.
      - Part 3 – Replace FBI's investigative software applications, including the obsolete Automated Case Support (ACS) system

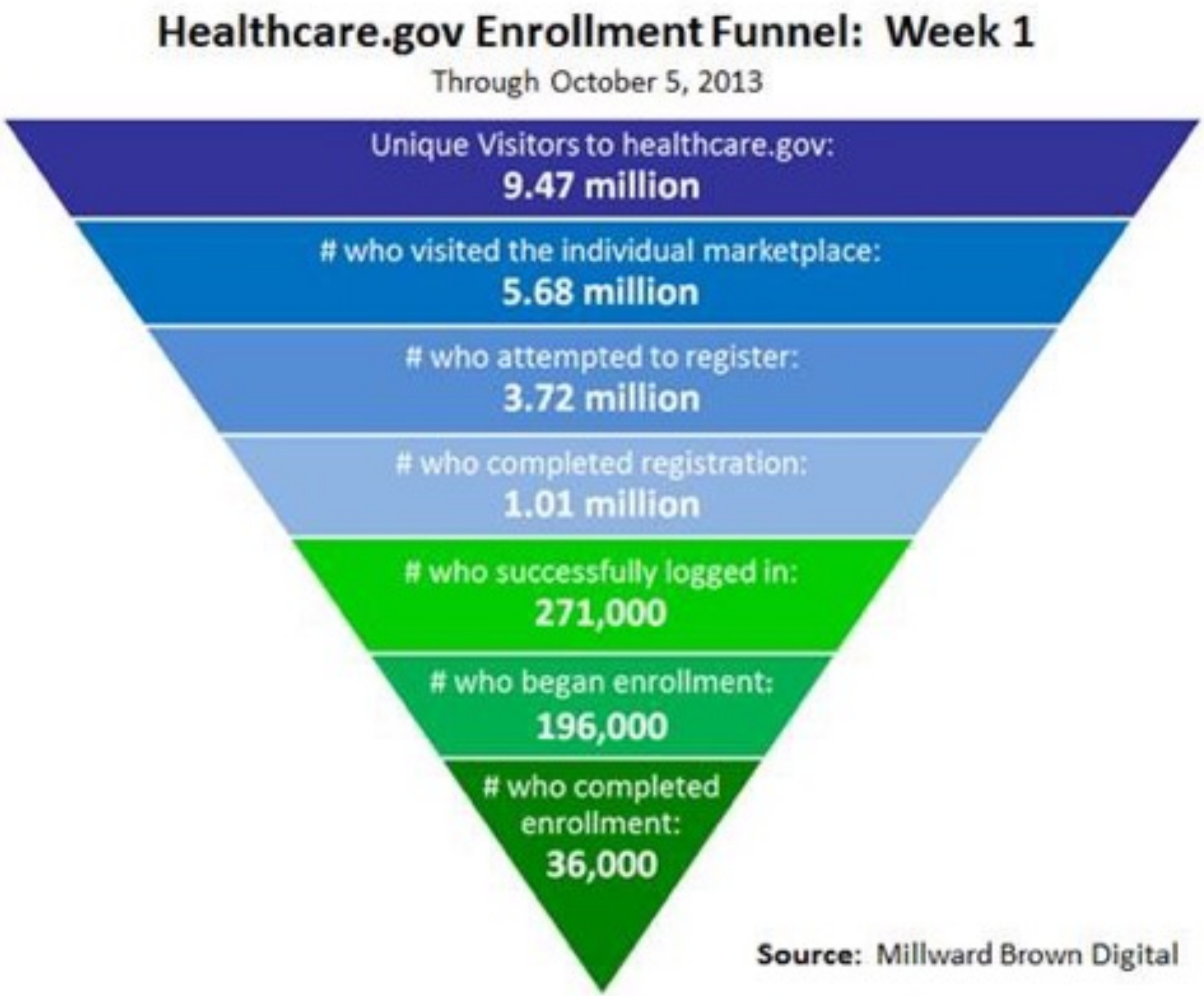
FBI Virtual Case File System Case Study – cont.

- **FBI selected Science Applications International Corporation (SAIC) to develop the software applications**
  - Search all FBI databases without having prior knowledge of its location, with a single query through the use of search engines
  - Web-enable the existing investigative applications;
  - share information inside and outside the FBI;
  - provide access - both internal and external databases
  - Etc.
- **SAIC and the FBI committed to creating an entirely new case management system in 22 months**
  - No time to follow those pesky systems engineering practices, must code, code, code…
  - By the time VCF was canceled, there were over 700,000 lines of code along with and incomplete set of requirements documented in an 800-page volume
- **Your tax dollars at work** ☺

Affordable Care Act Federal Web Site

- **This discussion IS NOT about merits of the ACA it's a discussion about the system implementation**
- **Schedule facts:**
  - **ACA signed into law on March 23, 2010**
  - **The ACA was to provide for web based health insurance sign-ups beginning on November 1, 2013**
  - **Total government schedule for developing web site and supporting infrastructure 3 years 7 months 1 week**
- **It has been well documented that on Nov. 1, the federal ACA web site as well as many of the state ACA web sites were effectively non-functional**

Affordable Care Act Federal Web Site – cont.



Affordable Care Act Federal Web Site - cont.

- **Initial Problems with**
  - Amount of testing
  - Scalability
  - Interfaces with other systems
  - Robustness of data (data being lost)
  - Allowing (obviously) incorrect data to propagate through system
  - Initial problem “punch list” contained more than 250 problems
- **What went wrong?**

A story about requirements

A long, long time ago in a far, far-away place the military leaders of the blue country military at the five sided puzzle palace looked at the capability of the red country military. Specifically, they were worried because if they got into a shooting war the red country had twice as many tanks as the blue country.

So they sat down and put together a set of requirements for a new super-tank. By and by a company built the new super tank to meet these requirements. To test their new toy the military leaders teamed the new super tank with their existing armored forces in a series of war games to see how the super tank would do.

A story about requirements…

On the first day of the war games the new super tank charged forth at 60mph while the existing troop carriers charged forth at 30mph. So the leaders at the five sided puzzle palace redesigned the troop carrier to keep up with the super tank.

A story about requirements…

On the second day of the war games the new super tank and troop carrier charged forth at 60 mph and the new tank spewed shells in all directions. But when it came time to reload they discovered that the shells for the new super tank were bigger than the shells for the old tank so the ammo carriers could not carry as many rounds. So the leaders at the five sided puzzle palace redesigned the ammo carrier to hold enough rounds for the super tank to kill all the red country tanks.

A story about requirements…

On the third day of the war games the new super tank, troop carriers, and ammo carriers charged forth at 60 mph, spewing shells in all direction to kill the red country tanks. But when it came time to refuel they discovered that the old tank got 2 miles per gallon and the new super tank got 2 gallons per mile and thus they did not have enough fuel. So the leaders at the five sided puzzle palace redesigned the fuel trucks to hold enough fuel for the super tanks.

A story about requirements…

On the fourth day the new super tank required maintenance so they drove it to the maintenance facility. The super tank was to big to fit thru the door of the maintenance facility so the sharp young trooper drove it thru the door. Once inside they discovered it was to heavy for the floor and sank into it. This was not the only problem because the overhead crane designed to lift off the turret was also undersized and in trying to lift the turret the beams on the maintenance facility buckled.

Thus ends the lesson on system level requirements. Where did they go wrong?

Second true story about requirements INCOSE, Spring 2008

- **Analysis of post-launch failures of space and launch vehicles**
  - 133 cases of lost SV/LV between 1964 and 2003
  - 2 cases would have been very difficult to prevent
  - 54% of SV failures were caused by deficiencies in design and analysis phases, 12% faulty tests, 9% ill-defined or lack of solid requirements
  - 64% of LV failures were caused by deficiencies in design and analysis phases, 7% faulty tests

Problems with Requirements

- **Stakeholders don't know what they really want**
- **Stakeholders express requirements in their own terms**
- **Different stakeholders may have conflicting requirements**
- **Organizational and political factors may influence the system requirements**
- **The requirements change during the analysis process.**
  - New stakeholders may emerge
  - The business environment may change
    - Certain aspects of the original requirements may prove to be unaffordable
  - Discoveries are made that yield additional requirements
  - Requirements are found to be inconsistent

Verification – INCOSE 4.6

- *The purpose of the Verification Process is to confirm that the specified design requirements are fulfilled by the system. This process provides the information required to effect the remedial actions that correct non-conformances in the realized system or the processes that act on it.*
- *Construct a Requirements Verification and Traceability Matrix (that links requirements to how verified!!!*

System Verification

- **System Verification** - Verification is the confirmation, through the provision of objective evidence, that **specified requirements have been fulfilled**. With a note added in ISO/IEC/IEEE 15288, verification is a set of activities that compares a system or system element against the required characteristics (ISO/IEC/IEEE 2008). This may include, but is not limited to, specified requirements, design description, and the system itself.
  - From the Systems Engineering Body of Knowledge (SEBoK)
- *Construct a Requirements Verification and Traceability Matrix*
  - Shows top level method used for verification of requirements
  - Lower levels of detail are required to actually perform verification.
    - This will be discussed at length later in the course

Verification Matrix

			Comply		Verification Phase			Verifiaction Method			
Requirement	Req ID	Subsystem	Y	N	D	Q	A	I	T	A	Comments
The contractor shall provide an automated toll collection solution for the bridges in the state of Euphoria.	1	Vehicle ID & Attribute	x		x	x	x	x	x	x	Model, simulate, and FAT the tolling system.
The system of systems shall operate 24 hours per day.	2	All Systems		x	x	x	x	x	x	x	Model, simulate, and FAT the system. Realistically, situations will arise that will not allow for 100% operational time.
The system of systems shall provide data on each vehicle that crosses a bridge in the state.	3	Vehicle ID & Attribute		x	x	x	x		x	x	Model, simulate, and FAT the system. Realistically, situations will arise that will not allow for 100% data collection.
The system of systems shall provide a health monitoring function, including structural sensors, equipments, and software that will be used to estimate the health of the bridges.	4	Bridge Health	x		x	x			x	x	Model and simulate the system. Simulation should include known varying degrees of bridge wear.

D - Design Test
Q - Qualification
A - Analysis

I - Inspection
T- Test
A- Analysis

System Validation

- **System Validation** - Validation is the confirmation, through the provision of objective evidence, that the **requirements for a specific intended use** or application have been fulfilled. With a note added in ISO 9000:2005: *validation is the set of activities that ensure and provide confidence that a system is able to accomplish its intended use, goals, and objectives (i.e., meet stakeholder requirements) in the intended operational environment* (ISO 2005).