ETLS 509 - Validation & Verification
University of St. Thomas

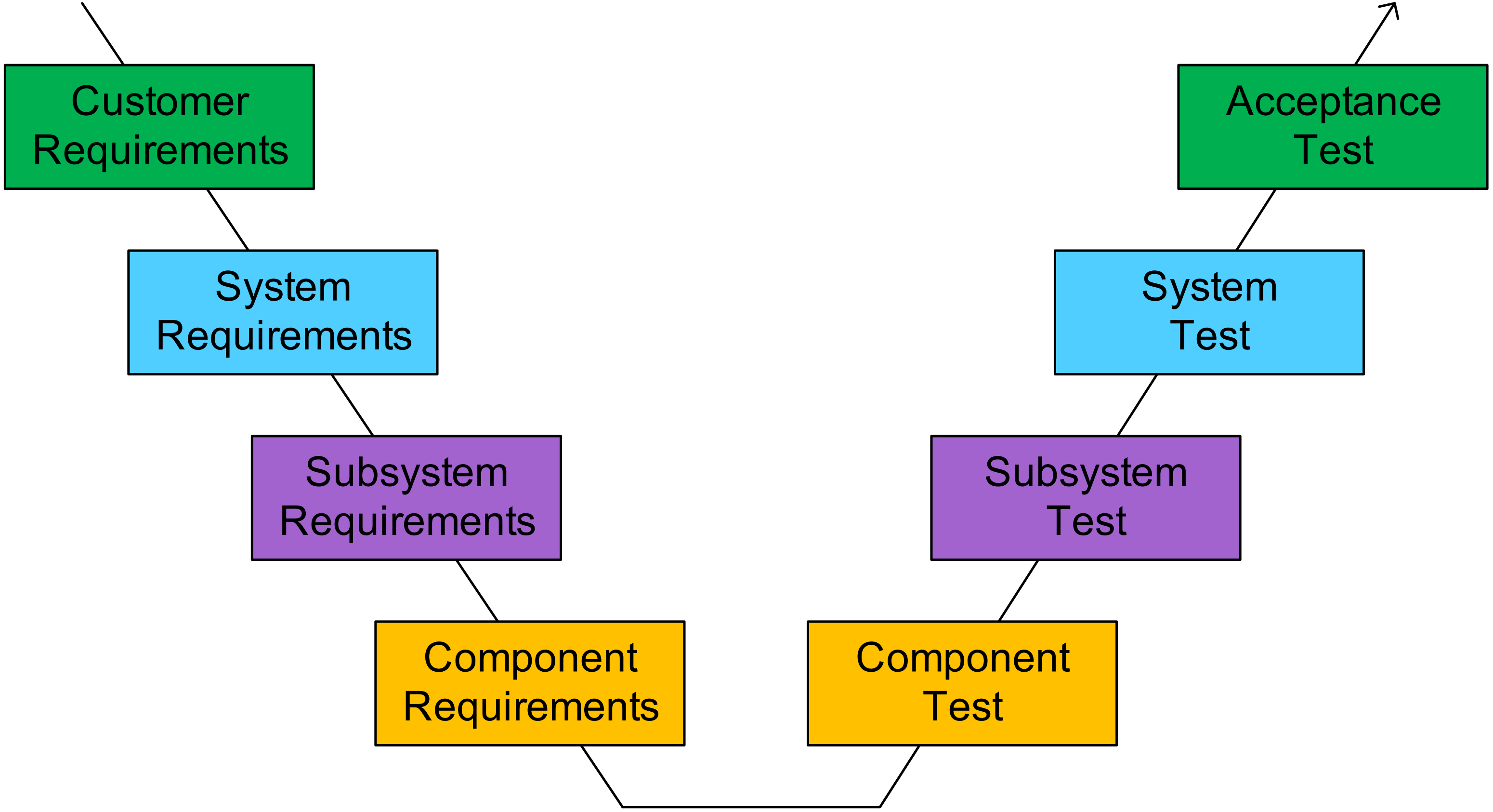
John Engelman

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 - Session 2

- The System Design Processes, Define Validation & Verification



Customer Requirements

System Requirements

Subsystem Requirements

Component Requirements

Component Test

Subsystem Test

System Test

Acceptance Test

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)

- **MOEs are related to the intended use of the system from the user's perspective**
  - Developed with the customer's requirements
  - Demonstrate the the designed system satisfies the customer's needs
  - Measure how well an <u>operational task</u> is accomplished by the system
  - Data used to measure comes from use of the system in its <u>expected environment</u>
- **Defining an MOE**
  - Can be stated as a question or statement
  - Often state in terms of gain per cost incurred

MOE Example

- **CardCraft system (pg. 203 - 205 of Art of Sys. Engineering)**
  - Produced secure identification cards for a user in an efficient and unobtrusive manner

Requirement	Req ID	Subsystem/Area
System shall comply with all UL USA standards	1	Agency Requirements
System shall comply with FCC I.T.E. Class A USA	2	Agency Requirements
FCC Radio ID Number USA	3	Agency Requirements
Holographic and Clear versions of both high and standard durability overlay shall exisit	4	Consumables
The printer shall support YMCK, YMCK-K, YMCKT-KT color ribbons	5	Consumables
The printer and laminate shall have the ability to print and laminate .020" to .030" plus or minus 10% (0.030" nominal) PVC, PC/PVC Composite, PET(G)/PVC Composite, and Translucent PVC/Teslin cards	6	Consumables
All Overlays shall resist delamination- High Durability Overlay applied to cards shall have: A grade ≥ 3.0 when tested using ANSI INCITS 322-2002 Tape method	7	Consumables-Durability
Overlay materials shall be tested with all printers against the ISO 24789 card life protocol tests for NID. (expected testing will be conducted externally - i.e. Eclipse lab)	8	Consumables-Durability
Final card testing shall be conducted externally - i.e. Eclipse lab)	9	Consumables-Durability
Overlay flash shall not exceed 0.5mm	10	Consumables-Quality
Unused Overlay and Laminate shall not exceed 5%	11	Consumables-Quality
Resolve the card bowing exceeding .060" ISO 7810 Card Warpage Spec	12	Consumables-Quality
Enclosure plastics Shall marked with recyclable symbol, per Resin Identification Code	13	Environmental Standards
The Printer and Laminator shall be designed for use on a desk of table top	14	Hardware
The Printer and Laminator shall weigh less than 20 pounds	15	Hardware
Height of The Printer and Laminator shall not exceed 18 inches	16	Hardware
Depth of the printer and lamnator shall not exceed 24 inches	17	Hardware
Input and output hopper capacity shall be 25 cards.	18	Hardware
Reject hopper capacity shall be 10 cards	19	Hardware
Card feeder shall feed one card at a time	20	Hardware
a mulit-LED shall display status	21	Hardware
CardCraft System shall produce audiable notifiactions when errors are encountered	22	Hardware
CardCraft shall have a display lit LCD screen with membrane buttons	23	Hardware
CardCraft System throughput shall be no less than 75 cards per hour with overaly	24	Hardware
Consumables shall be held in a removable Laminator Supply Cartridge	25	Hardware-Laminator
Laminator shall be headted with a halogen element	26	Hardware-Laminator
Laminator roller shall be constructed of hard coat anodized aluminum	27	Hardware-Laminator
Heating element shall be placed in laminator roller	28	Hardware-Laminator
Laminator heating monotired via IR sensor 1/4 the lenght of the roller	29	Hardware-Laminator
Laminator shall consistnatly hold a lamination temperature range of 160 to 200 C	30	Hardware-Laminator
Cards shall be able to pass the laminator with out contact from lamination roller	31	Hardware-Laminator

MOE	Requirement	Quantitative Measures	Measurement Method	Scoring
The CardCraft System produces personalized cards with a secure overlay quickly	24 Hardware, 42 Hardware Printer	System is able to produce 300 CPH with out and overlay and 75CPH with and overlay	Run a 300 card job without and overlay and a 75 card job with an overlay. Measure run time.	CardCraft System must meet specifications outline in requirements 24 and 42
The system provides alerts when supplies are "empty"	21, 23 Hardware	Audible and visual alerts indicate errors	Allow CardCraft system to run out of supplies in card hopper, printer ribbon, overlay, as well as manually induce a double feed card jam ensuring audible and visual alerts are seen and herd.	All errors must generate audible and visual alerts
Personalized cards are durable	8 Consumables-Durability	ISO 24789 card life protocol tests for NID	Complete ISO 24789 National ID test sequence	All test cards shall pass the ISO 24789 test sequence with minimal wear and shall be functional with the card holder clearly identifiable
CardCraft System is able to run for long periods with minimal manual interventions	85 Usability-Error Handling	Card jams preventing automatic clearing of the machine	Personalize 2400 cards (300 CPH X 8H)	≤2 manual interventions - Pass >2 manual interventions - Fail
User operates system with only basic instruction manual	86, 87, 91 Warranty and Service	User can successfully accomplish basic production level tasks on a 'Production Operation Use Checklist'	Production operation use check list encompasses basic production operation of system. Provide new user with basic instruction manual and record items that are successfully and unsuccessfully completed	≥90% - Highly Successful ≥80%, <90% - Successful <80% - Fail
CardCraft System produces high quality cards with consistent image and overlay placement without visual defects	74 Software-Usability, 102 Hardware Printer, 103 Hardware-Laminator	Secure Overlay placement ± 0.015" Long Axis, ± 0.015" Short Axis and Image placement ± 0.015" Long Axis, ± 0.005" Short Axis	Personalize 500 cards, measure image and overlay variability on 10 cards at 25%, 50%, 75% completion of the 500 card run	Secure Overlay placement >0.015" any axis = Fail : Image placement > 0.015" Long Axis = Fail, > 0.005" Short Axis = fail
System connects to Windows 7 and XP	60 Software-Controller	Connection successful / unsuccessful	Test connection from devices with the two different operating systems. Operating systems to test are Windows7 and XP.	CardCraft Systems shall work with Windows 7 and XP operating systems
The CardCraft System produces flat personalized cards with a secure overlay	12, Consumables-Quality, 32Hardware-Laminator	Measured card warpage less than 0.06"	Personalize 500 cards, measure warpage on 10 cards at 25%, 50%, 75% of total run. Warpage measured by placing cards on a flat reference surface. Highest point will be recorded.	Card Warpage ≤0.06" - Pass >0.06" - Fail

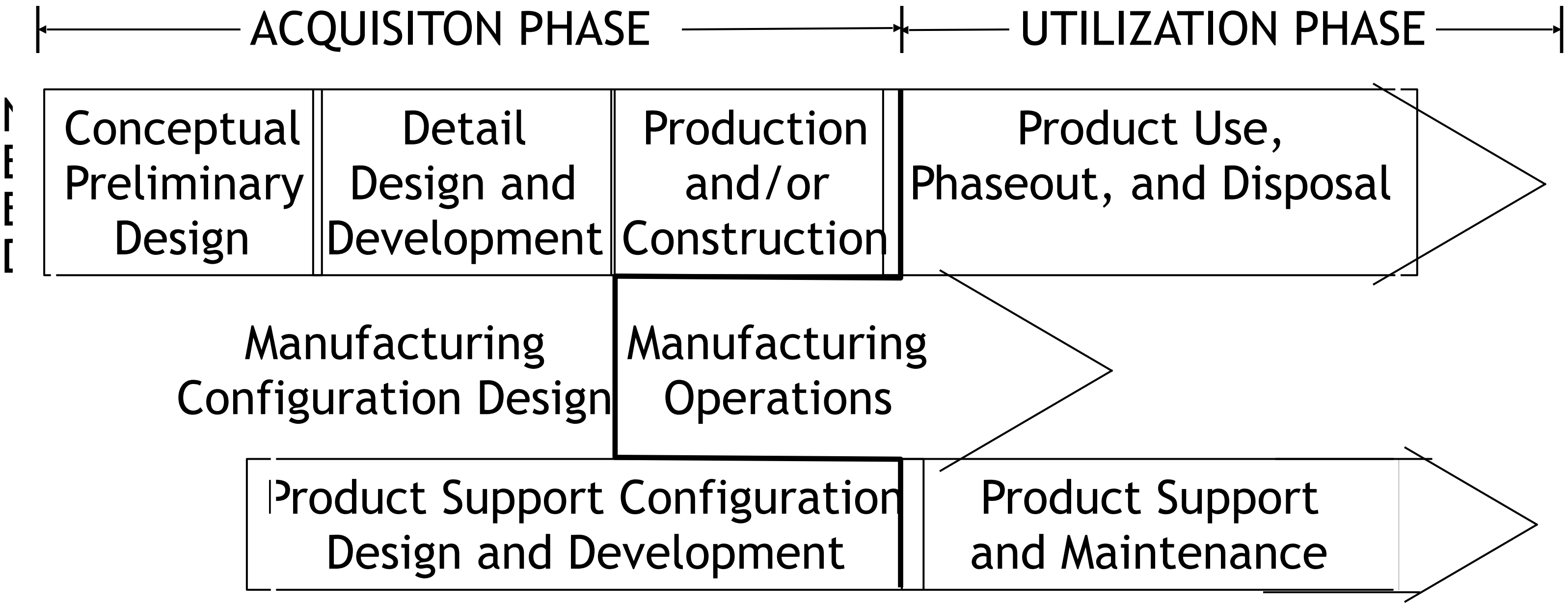
Technical Performance Measures (TPMs)

- **Technical Performance Measures (TPMs)**
  - – Measures that determine how well as systems satisfies a technical requirement
  - – Used in decision making and trade-off analysis
  - – Often are cost drivers, lie on the critical path, or are risk items
- Example
  - System requirement to operate with a 3.3 V +/- 5% power supply
  - TPMs (2)
    - – Power Supply TPM
      - – minimum voltage output is 3.135 V
      - – 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 TPM
      - – Operate with voltage between 3.135 V and 3.465 V

System Verification and Validation & Measures

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

Product, Manufacturing & Support Life Cycles


ACQUISITON PHASE
UTILIZATION PHASE
Conceptual Preliminary Design
Detail Design and Development
Production and/or Construction
Product Use, Phaseout, and Disposal
Manufacturing Configuration Design
Manufacturing Operations
Product Support Configuration Design and Development
Product Support and Maintenance

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

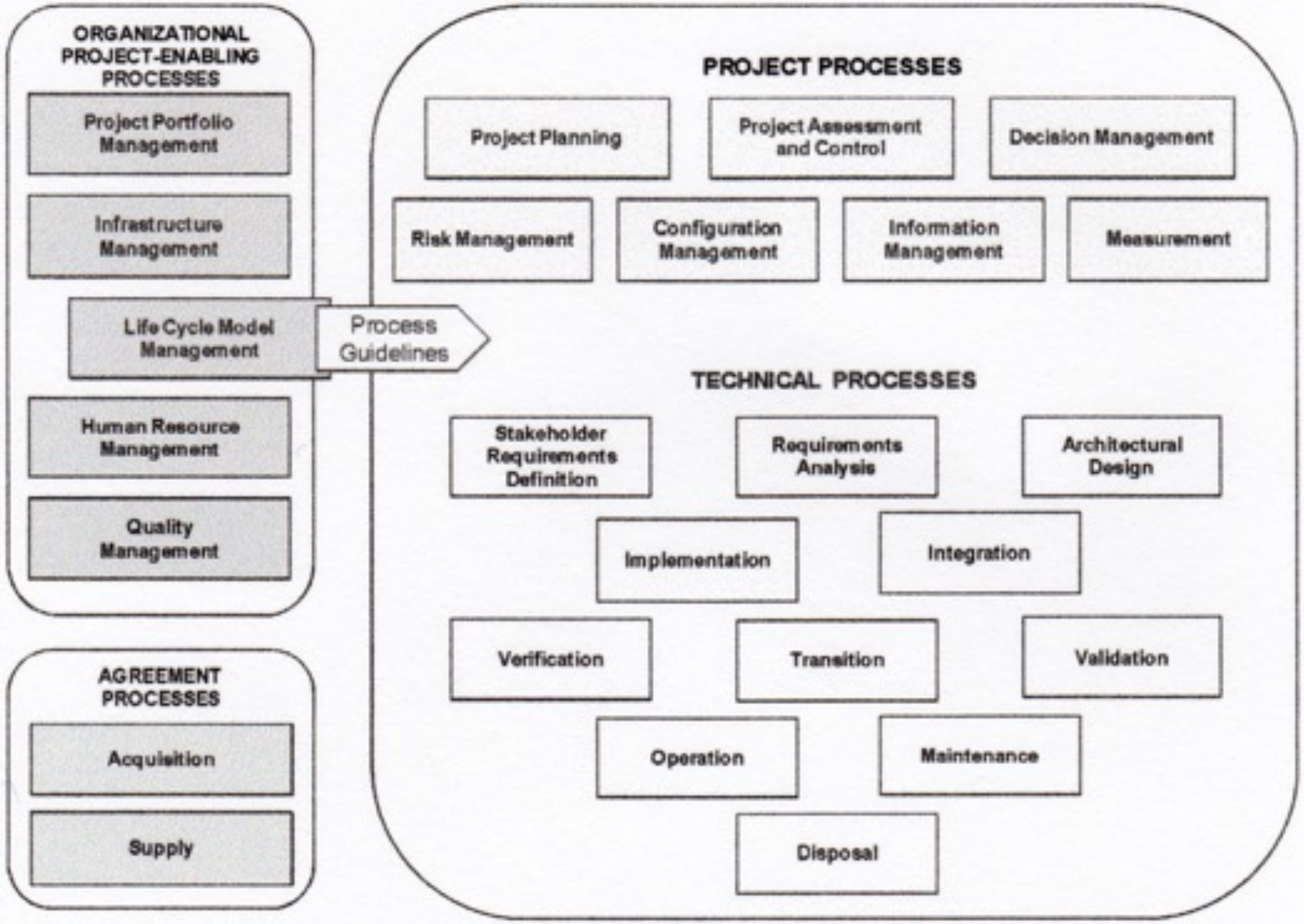


Figure 1-1 System Life-cycle Processes Overview per ISO/IEC 15288:2008

INCOSE Engineering Handbook figure 1-1

Case Studies

Medical Radiation Case Study

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

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**☺

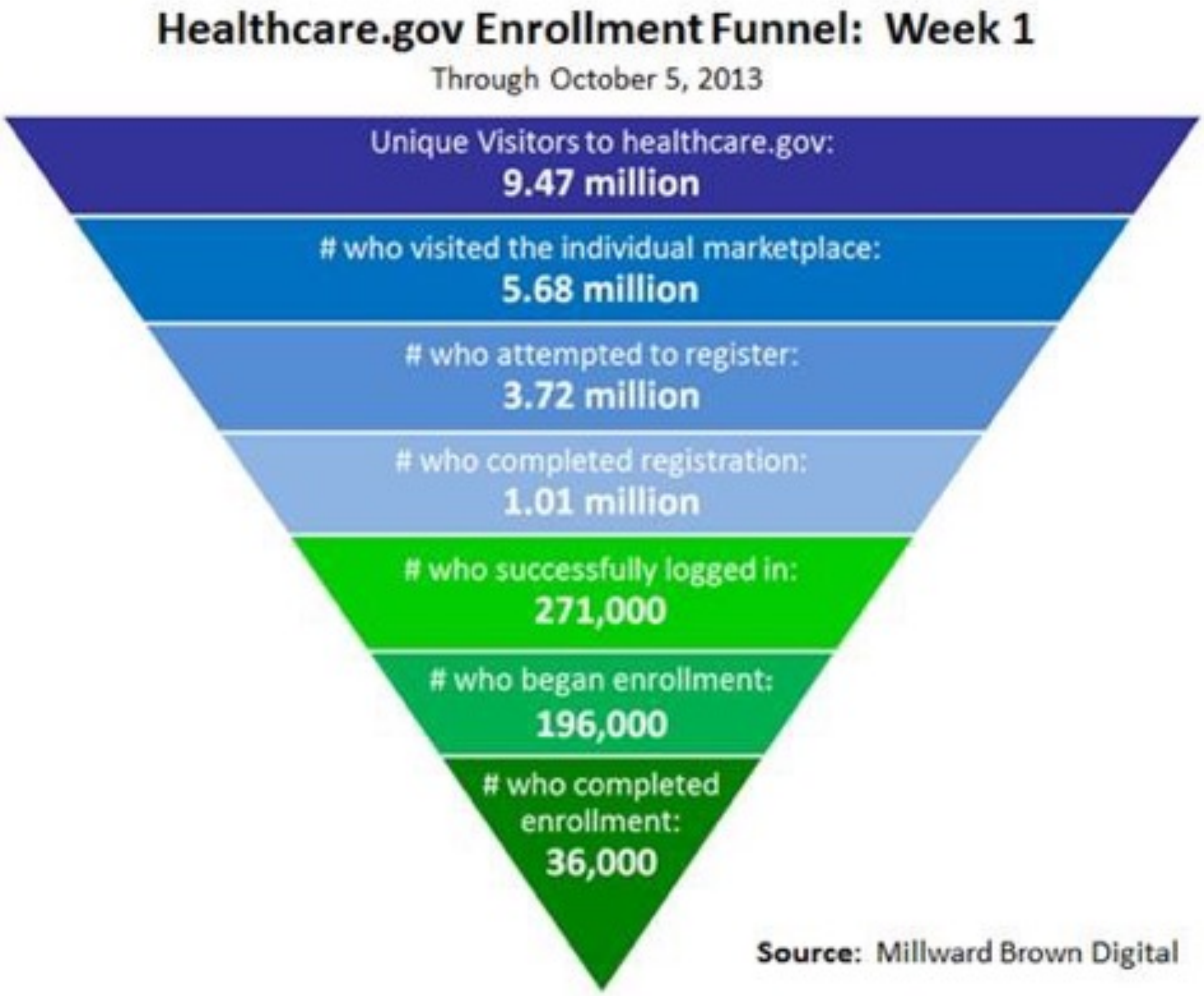
Hubble Telescope

Affordable Care Act Website

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.



Healthcare.gov Enrollment Funnel: Week 1

Through October 5, 2013

Unique Visitors to healthcare.gov:
9.47 million

who visited the individual marketplace:
5.68 million

who attempted to register:
3.72 million

who completed registration:
1.01 million

who successfully logged in:
271,000

who began enrollment:
196,000

who completed enrollment:
36,000

Source: Millward Brown Digital

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 too 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 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