

Integrative Approach to Medical Device Safety: Human-Centered Systems Engineering

GM Samaras, PhD, DSc, PE, CPE, CQE
Samaras & Associates, Inc.
Pueblo CO USA

Presented @ IEEE PSES 2009

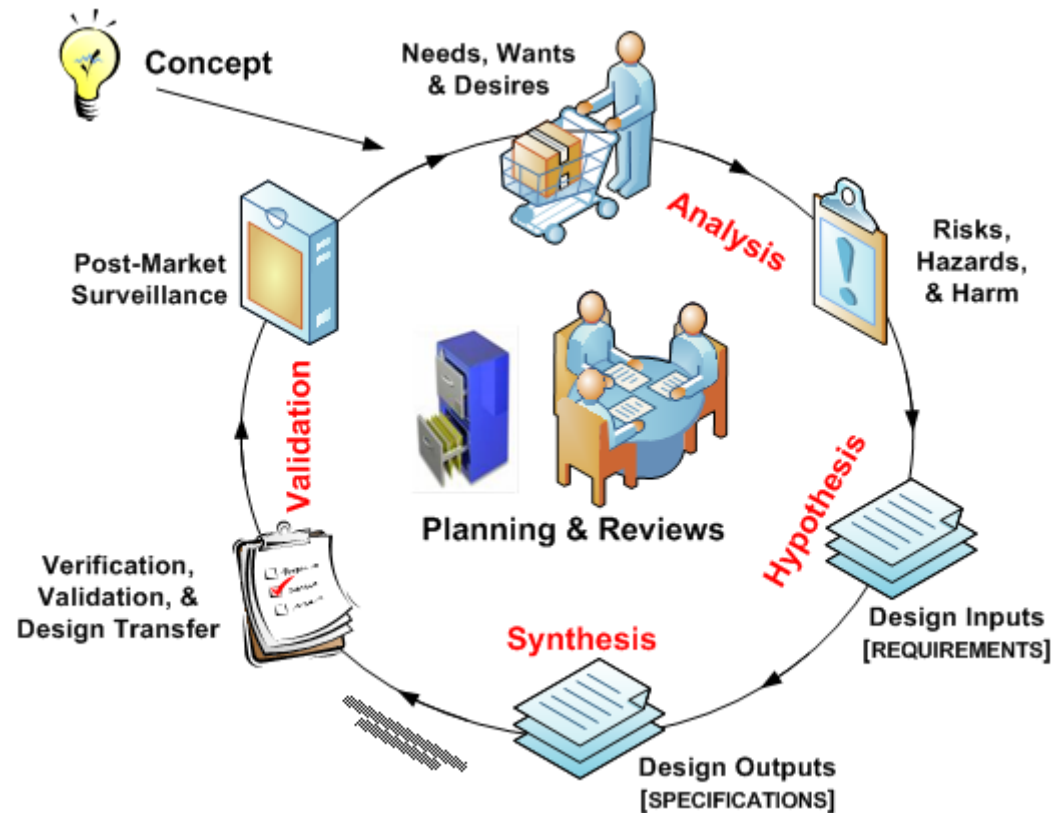
Summary of this Talk:

**It is ALL about YOUR lifecycle and
how YOU manage it!!**

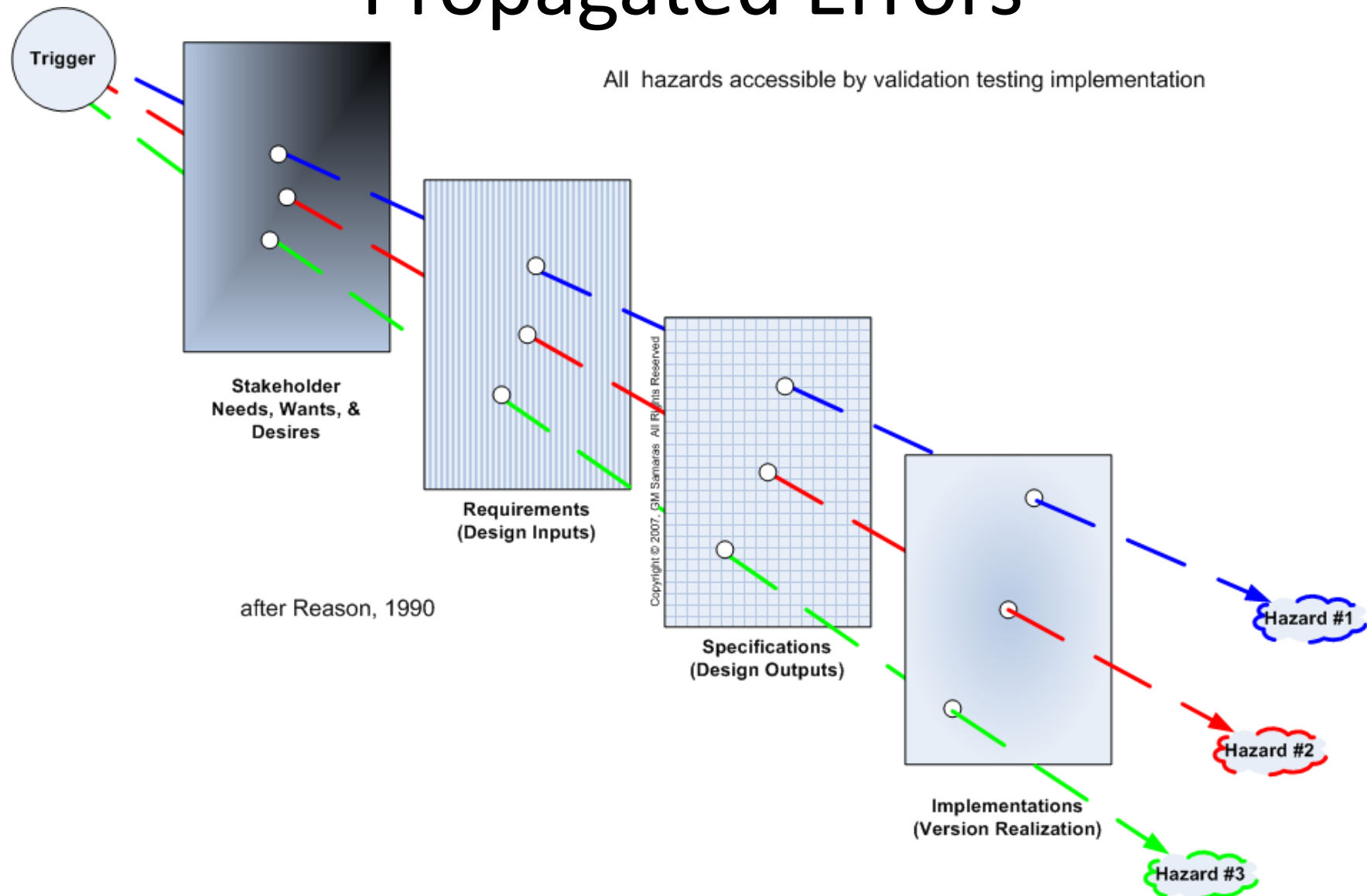
AGENDA

- **Product Development & Errors**
- Risks, Hazards, and Harm
- Humans and their Errors
- The REAL Objective
- Lifecycles, lifecycles, lifecycles
- Human-Centered Systems Engineering

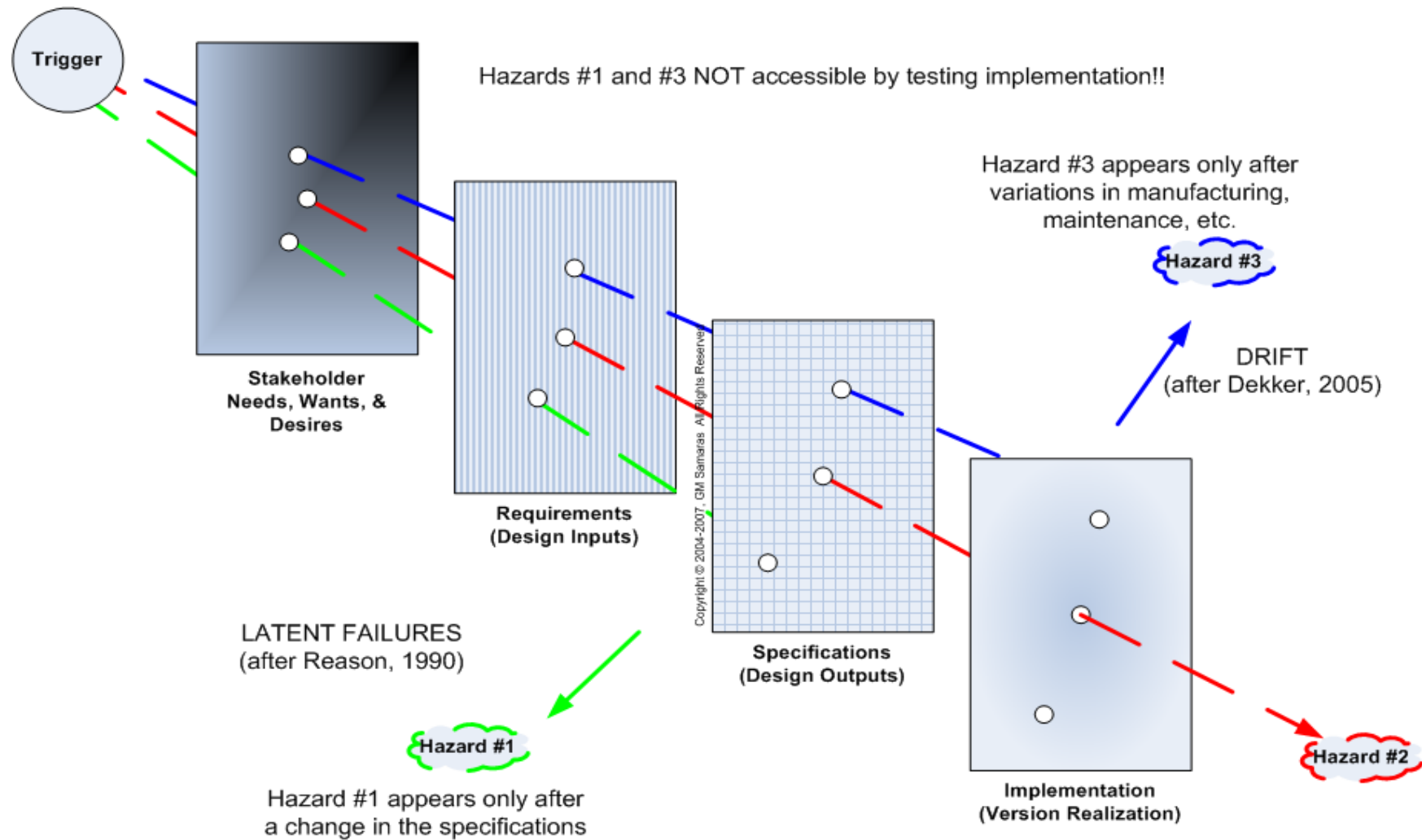
Product Development



Propagated Errors

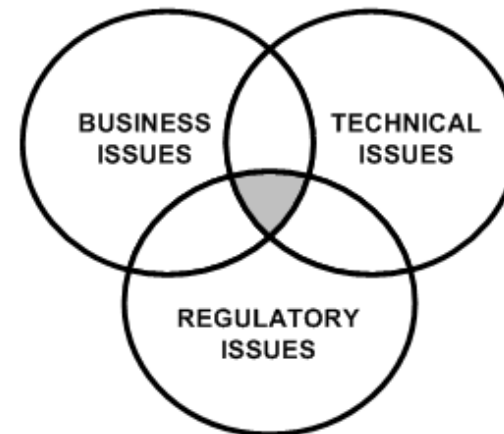
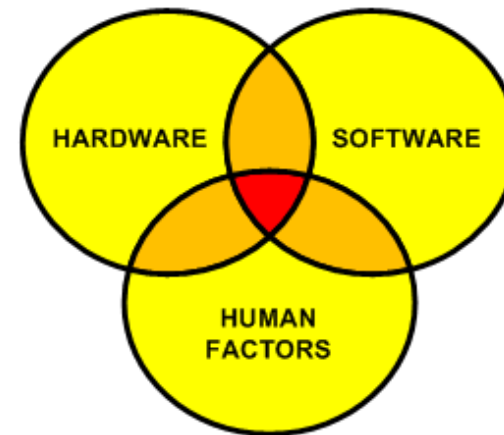


Compounded Errors



Error Sources

- Product Sources
 - Hardware Errors
 - Software Errors
 - Human Errors
 - System Errors
- Organizational Sources
 - Business Issues
 - Technical Issues
 - Regulatory Issues
 - Org. Systems Issues



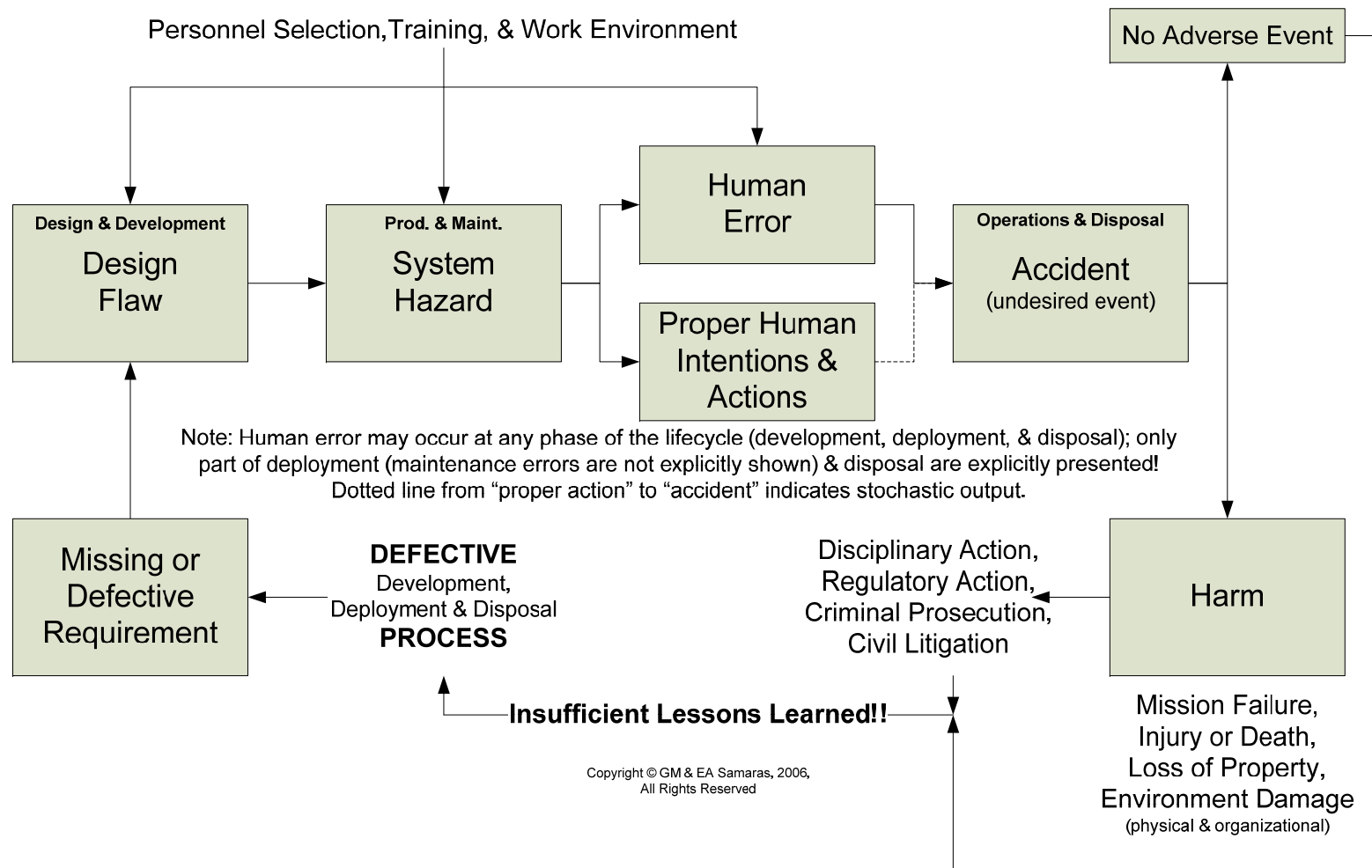
AGENDA

- Product Development & Errors
- **Risks, Hazards, and Harm**
- Humans and their Errors
- The REAL Objective
- Lifecycles, lifecycles, lifecycles
- Human-Centered Systems Engineering

Managing Risks, Hazards, & Harm



Ways to cause Harm:



Misapplication of Techniques

		Types of Data	
		Quantitative, Historical	Subjective, Experiential
Type of Risk Analysis	Inductive	Failure Modes, Effects and Criticality Analysis (FMECA)	Failure Modes Effects Analysis (FMEA)
	Deductive	Fault Tree Analysis (FTA)	Root Cause Analysis (RCA)

Copyright © 2007, GM Samaras / All Rights Reserved

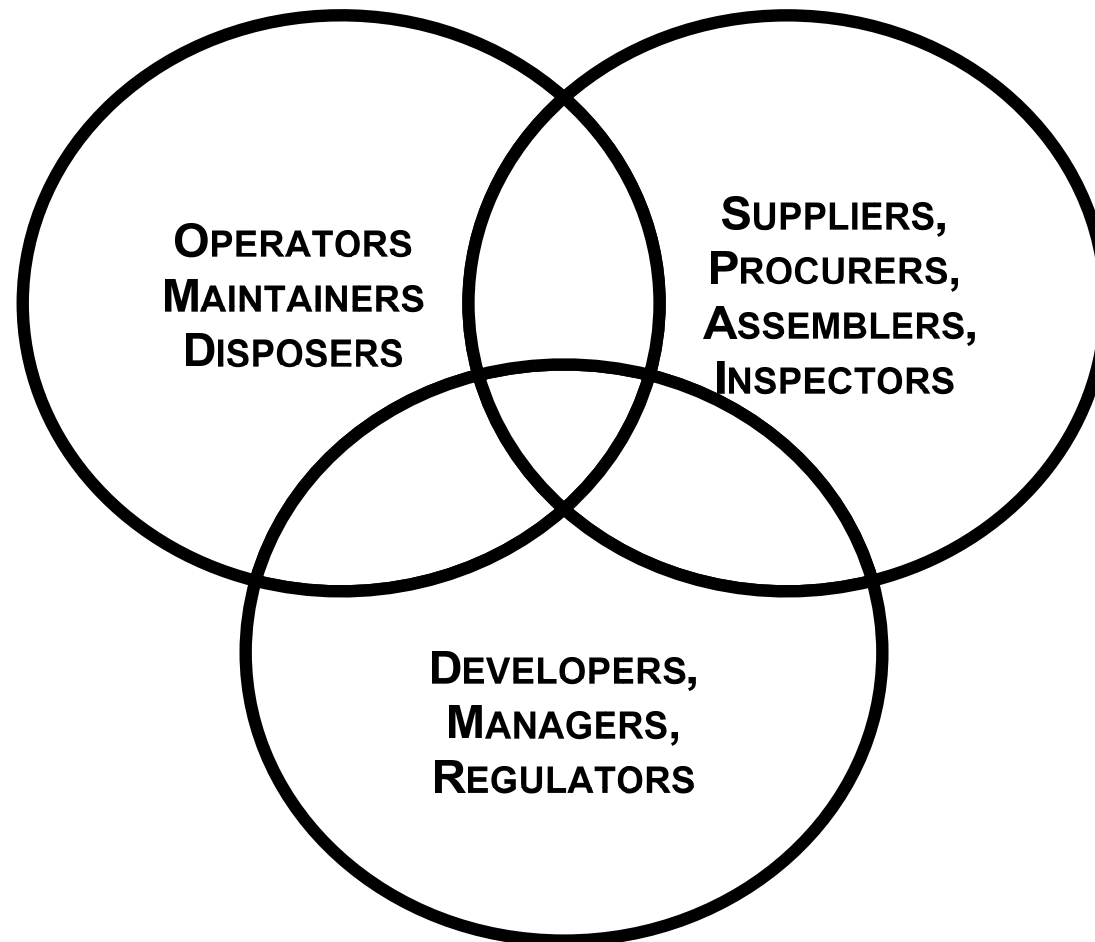
HUMAN ERROR: A **CRITICAL** Risk Factor

NB: I use “ergonomics” and “human factors engineering” interchangeably; for me they are synonymous!

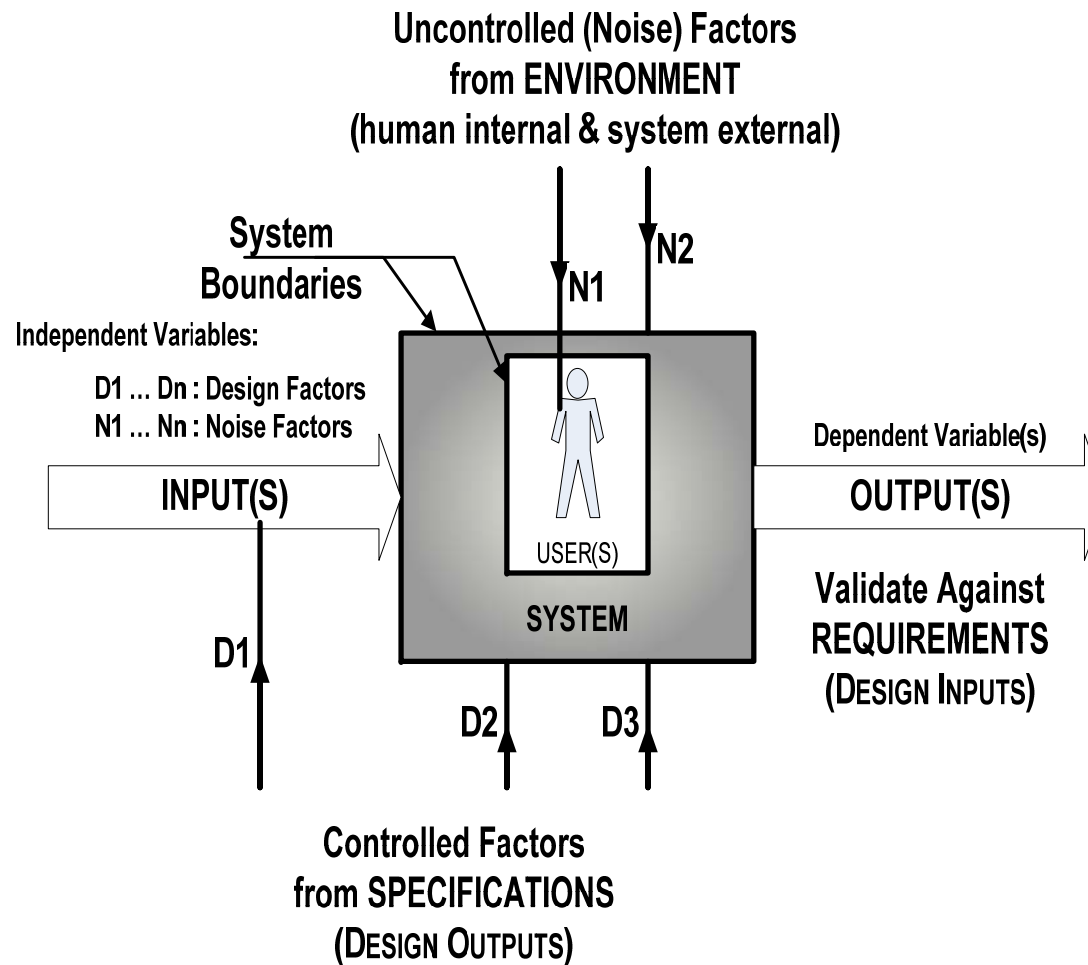
AGENDA

- Product Development & Errors
- Risks, Hazards, and Harm
- **Humans and their Errors**
- The REAL Objective
- Lifecycles, lifecycles, lifecycles
- Human-Centered Systems Engineering

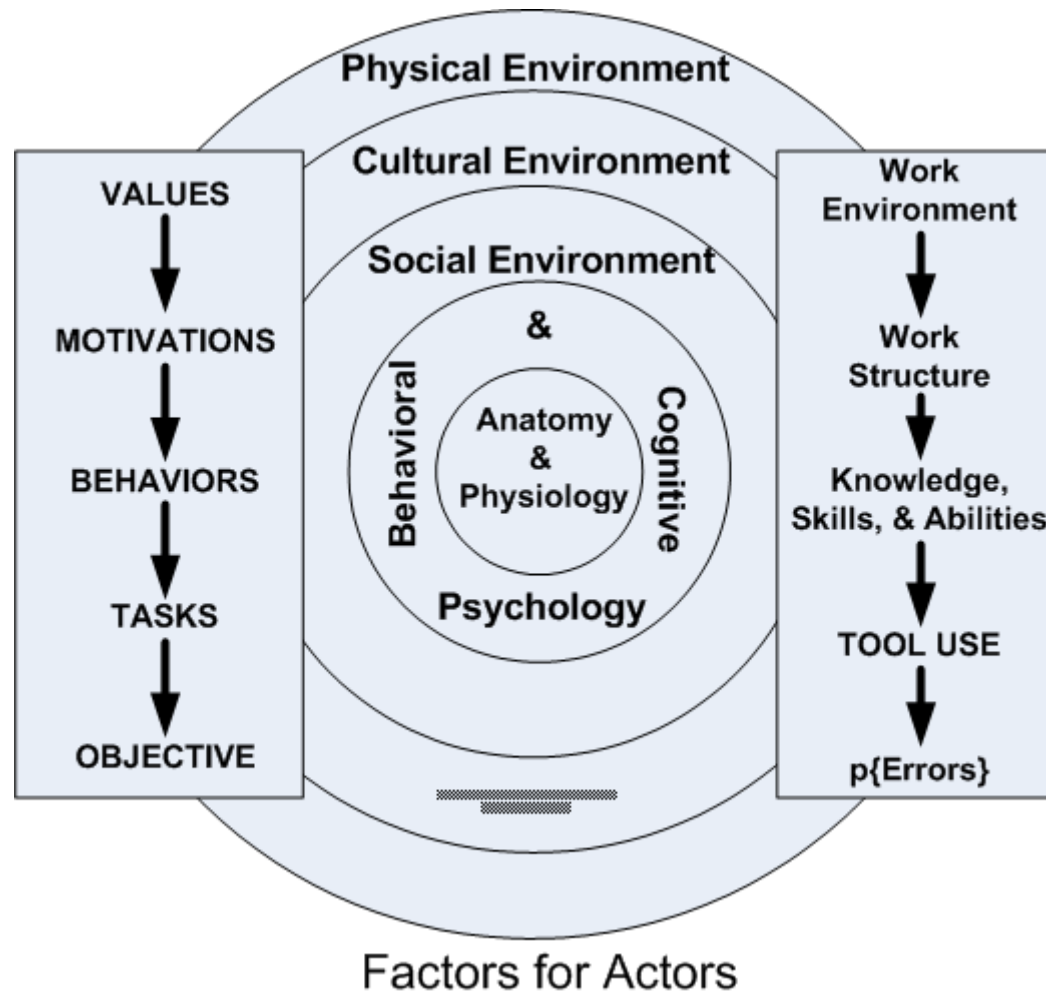
Who are those “pesky” humans?



The User Process: Systems Perspective



Factors for Actors



SYSTEM COMPLEXITY: HF PERSPECTIVE

Human(s) OPERATING
with Tool(s)

Anthropomorphometry
Biomechanics & Sensory Perception

Human(s) OPERATING with
Tool(s) with Automation

Verbal/Non-verbal Behaviors
Affective, Cognitive, & Physiological

Human(s) OPERATING
within Organization(s)

Communication & Coordination
Conventions & Expectations

Human(s) OPERATING
within Culture(s)

*Language & Artifacts**
Beliefs, Customs, Ethics, Morals

* Boulding, KE. Ecodynamics. Sage, 1978, p221.

System Complexity from Human Factors Perspective

Copyright © GM Samaras, 2006
All Rights Reserved

Micro-Ergonomics
(Physical Ergonomics)

Overt & Covert
Physical Factors

Meso-Ergonomics
(Information Ergonomics)

Overt & Covert
Behavioral Factors

Macro-Ergonomics
(Social Ergonomics)

Overt & Covert
Social Factors

Mega-Ergonomics
(Cultural Ergonomics)

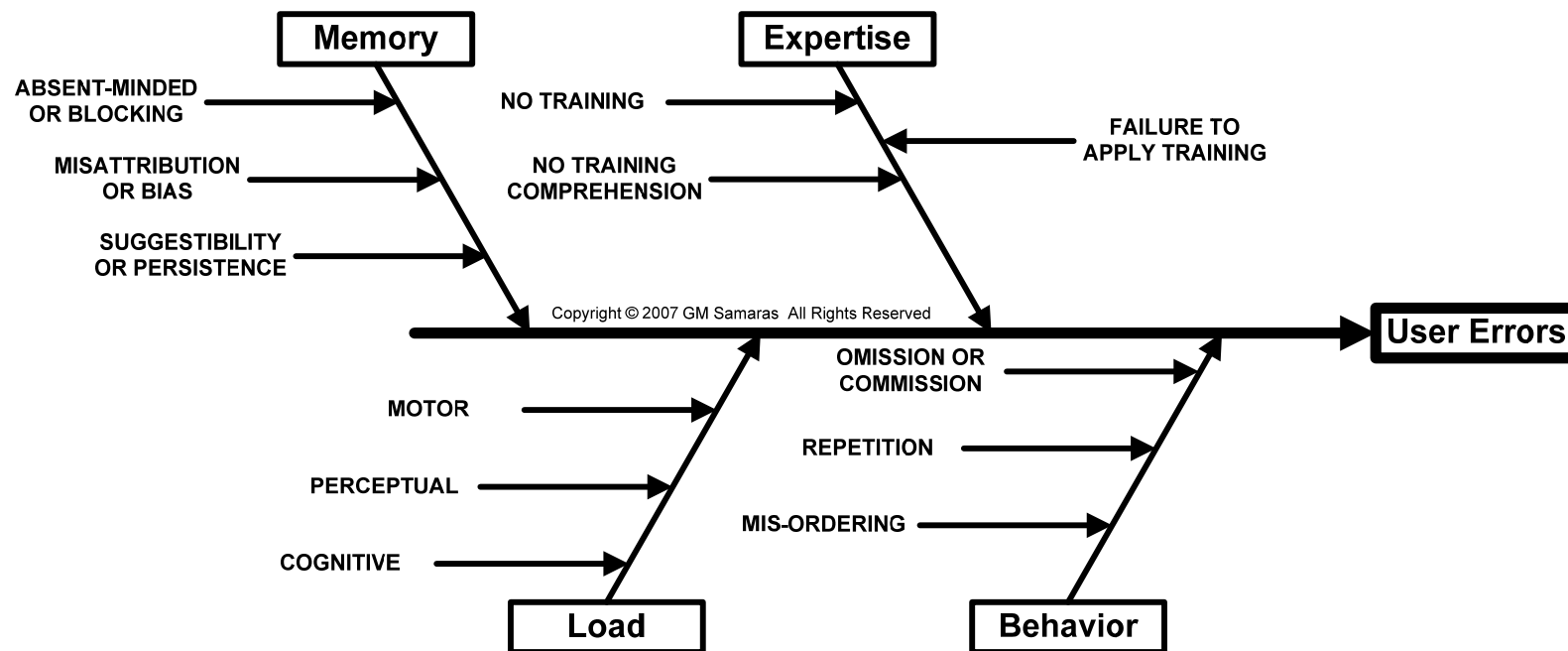
Overt & Covert
Cultural Factors

- Overt vs. Covert
- NOT Psycho-Babble!!!
- Overt: Detect with 1/5 senses
- Covert: CANNOT Detect with 1/5 senses
- Physics Example:
 - measure *acceleration*, a covert physical quantity, by the second time derivative of a *displacement*, an overt physical quantity

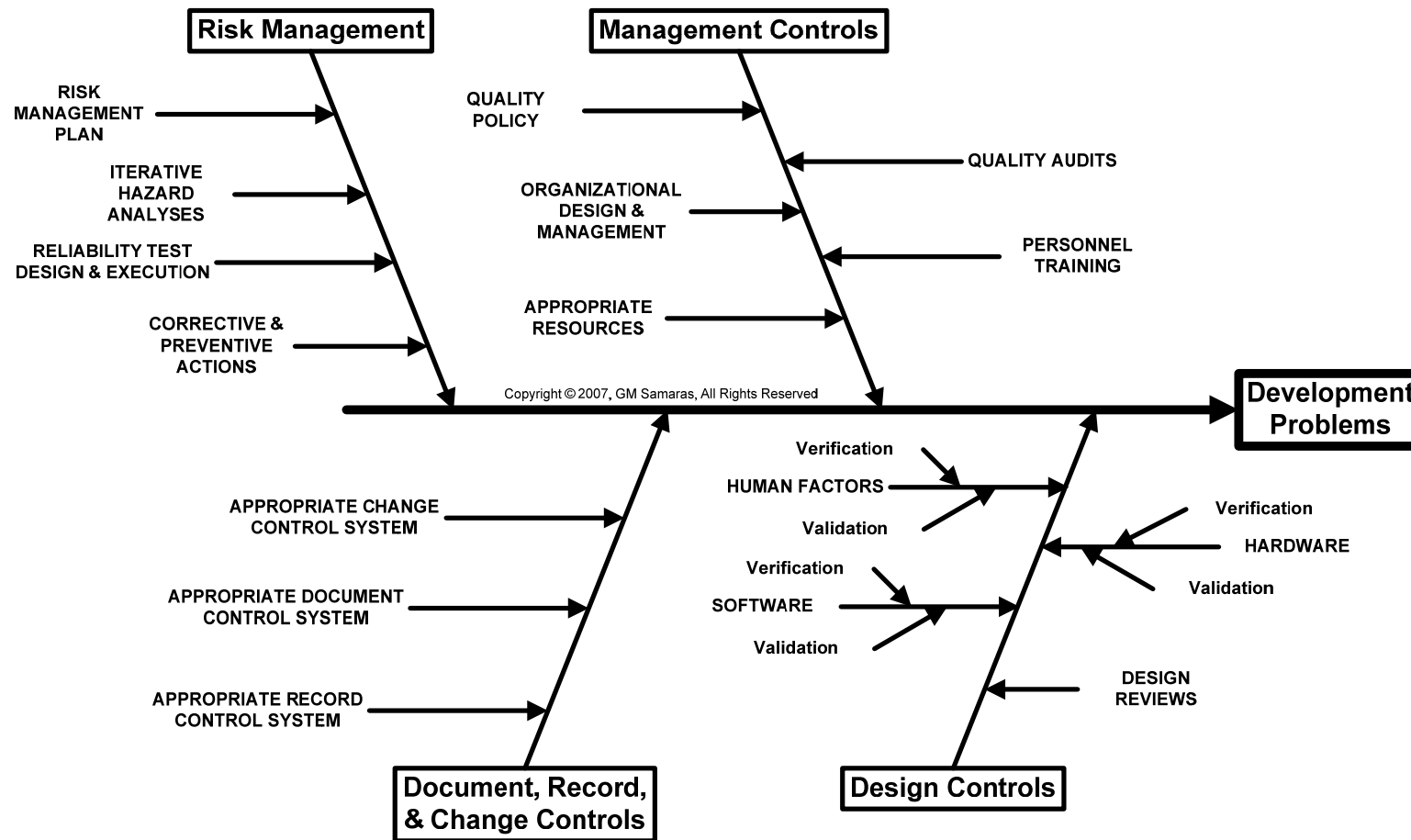
Human Error

- Two General Categories:
 - **USER** errors: errors attributable to the internal or external user environment, excluding the product itself
 - **Use** errors: errors attributable to the design and/or implementation of the product
- Four Types of Human Errors:
 - **Errors of: Use, Unexpected Use, Misuse, and Abuse**

USER Error RCA (partial)



Use Error RCA (partial)



AGENDA

- Product Development & Errors
- Risks, Hazards, and Harm
- Humans and their Errors
- **The REAL Objective**
- Lifecycles, lifecycles, lifecycles
- Human-Centered Systems Engineering

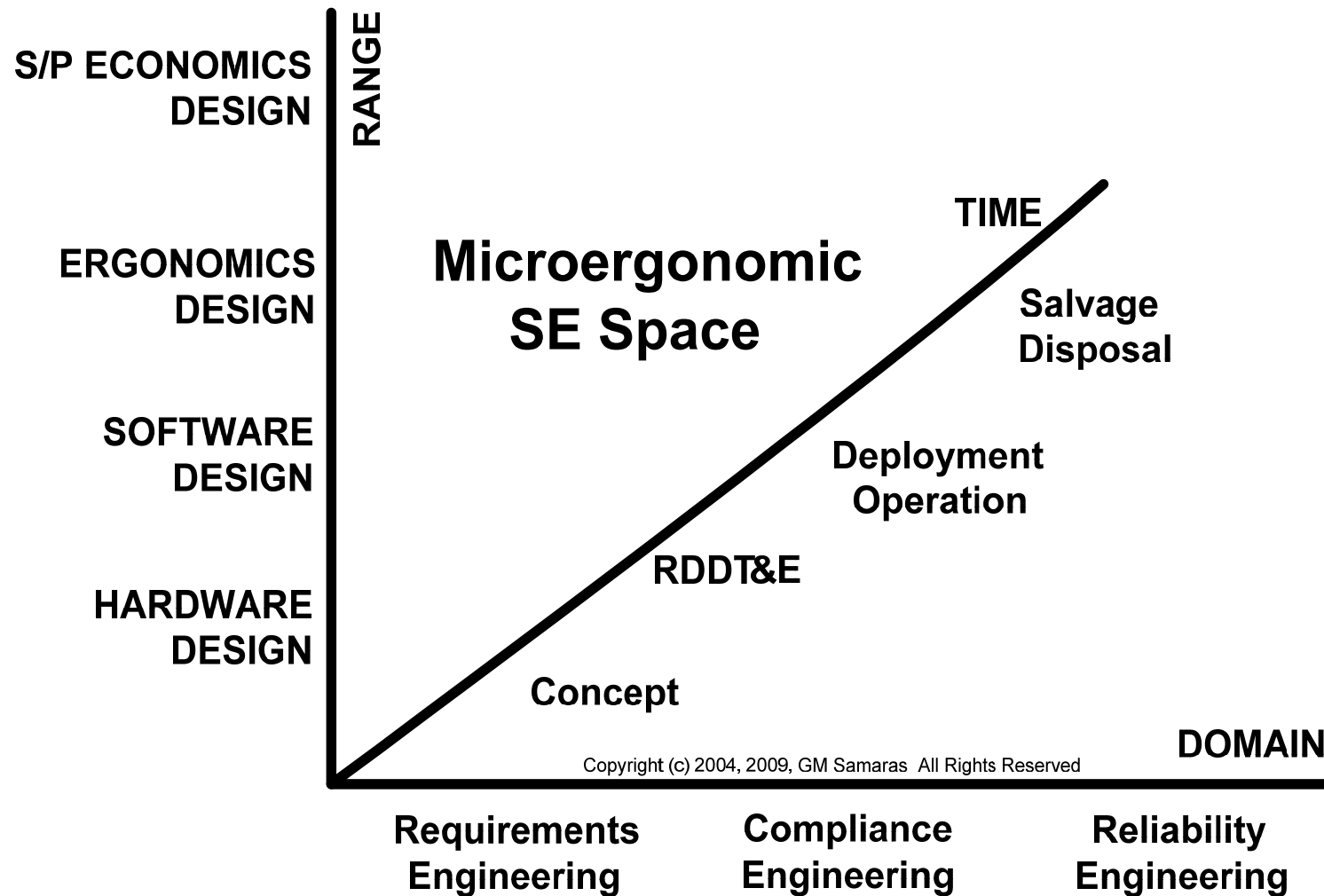
The REAL Objectives

NINE DESIGN ATTRIBUTES OF EFFECTIVENESS	
Functional SAFETY	Device helps (<i>intended use</i>)
Physical SAFETY	Device does not physically hurt (<i>basic safety</i>)
Functional SECURITY	Device prevents data loss or corruption (<i>integrity</i>)
Physical SECURITY	Device cannot be damaged or stolen (<i>denial of service</i>)
USABILITY	Device reduces probability of errors in intended use by intended users
RELIABILITY	Device operates as intended in intended environment for intended lifetime
MAINTAINABILITY	Device repaired in reasonable time at reasonable cost
AVAILABILITY	Device accessible when & where it is actually needed
AFFORDABILITY	Device manufacturer & end-user each obtain acceptable IRR (<i>real cost</i>)

AGENDA

- Product Development & Errors
- Risks, Hazards, and Harm
- Humans and their Errors
- The REAL Objective
- **Lifecycles, lifecycles, lifecycles**
- Human-Centered Systems Engineering

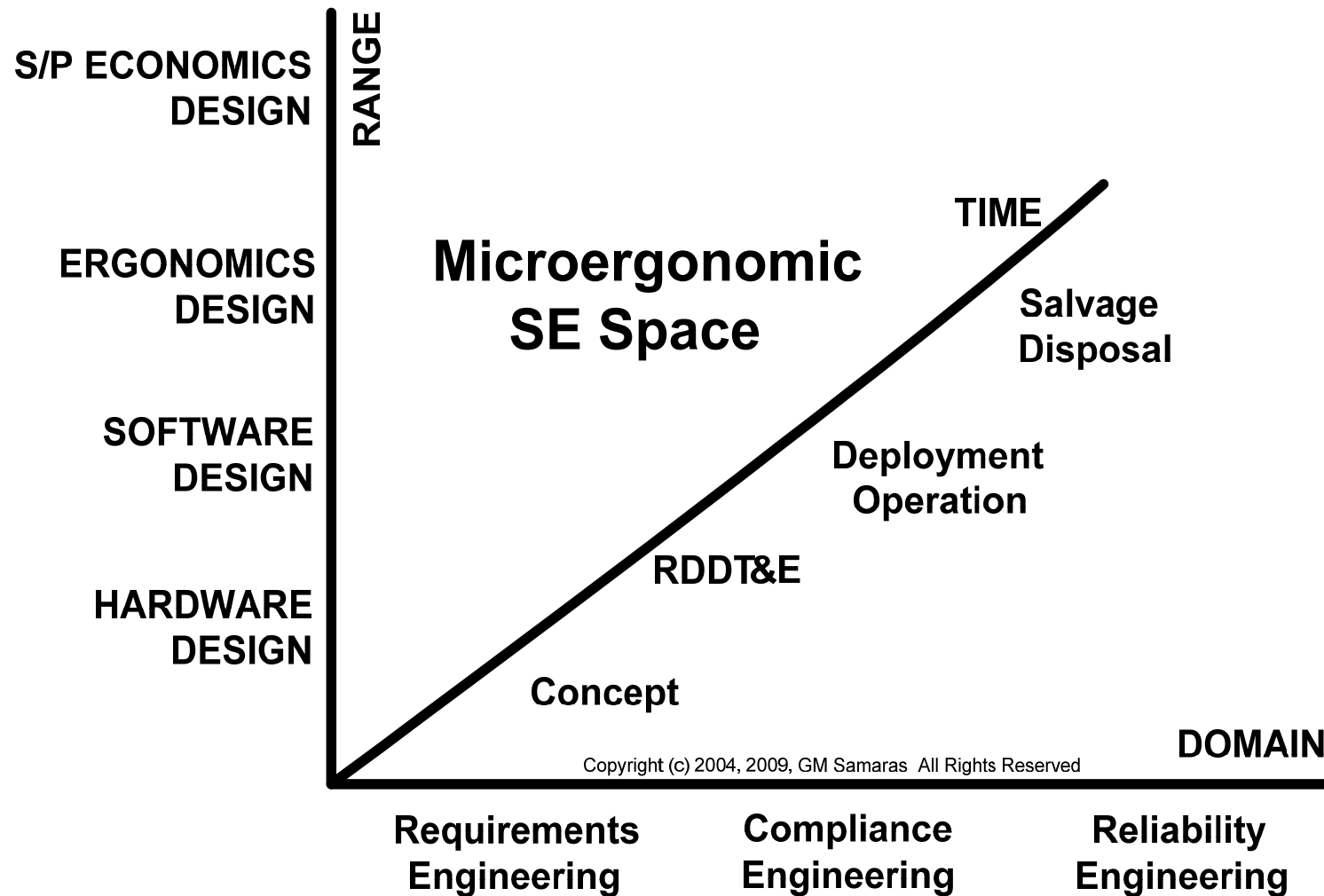
3D Systems Engineering State Space



Systems Engineering Domains

Requirements Engineering	Compliance Engineering	Reliability Engineering
Stakeholder Identification, NWD Assessment & Reconciliation	Identification of Laws, Regulations, & Standards	Defining Minimum Necessary Reliability
Hazard Analyses	Applicability Assessment	Fault Prevention
Design Input Formulation & 5 Verifications	Design Impact Assessment	Fault Removal
Version Validation	Test Design	Fault Tolerance
Version Post-Market Surveillance	Operational Considerations	Fault/Failure Forecasting
CAPA -driven Design Input Changes	Salvage and/or Disposal Considerations	Test Design

3D Systems Engineering State Space

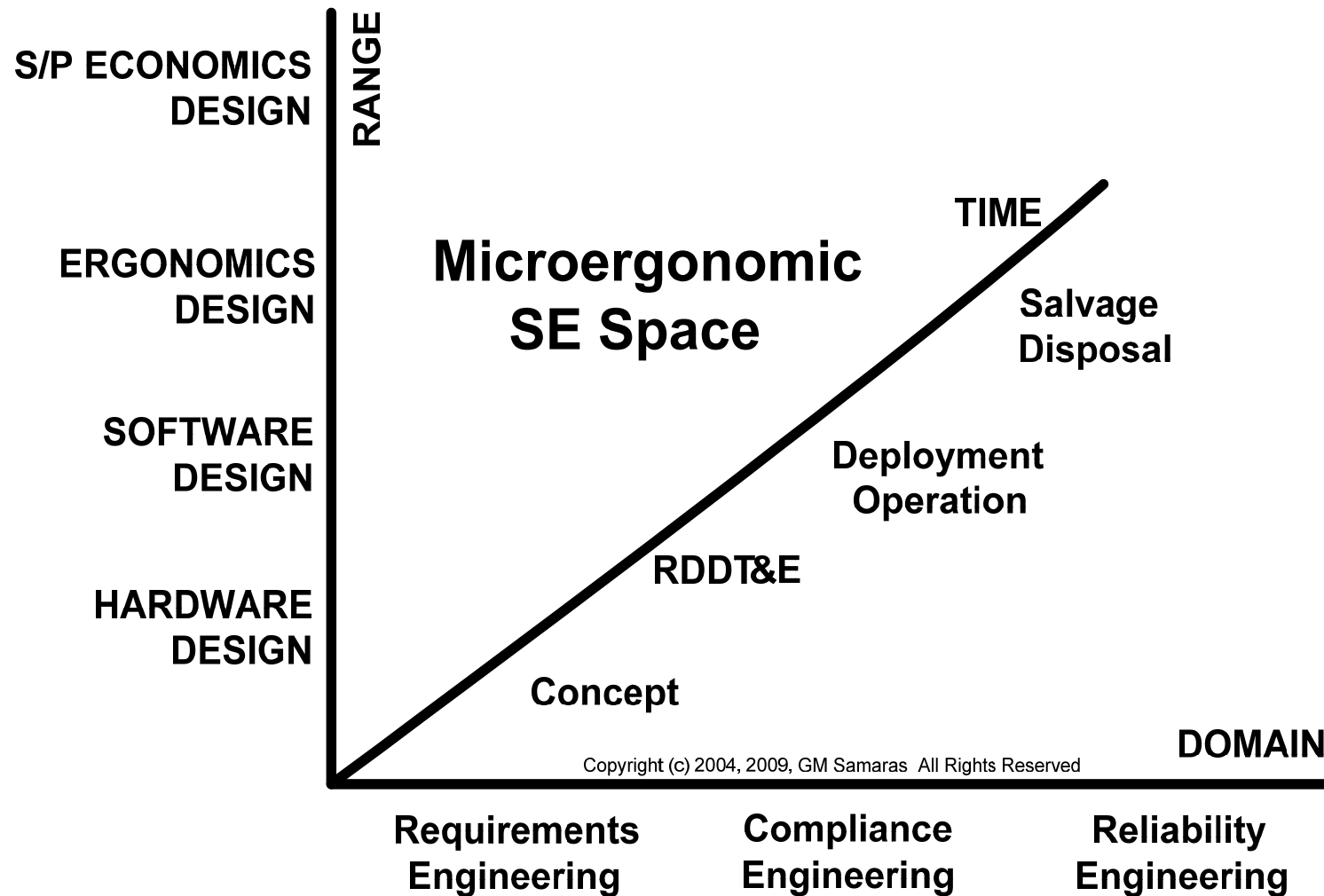


SE Range Elements

(multiple sub-disciplines in each)

HARDWARE	SOFTWARE	HUMAN FACTORS	Seller & Purchaser ECONOMICS
Electrical	Embedded SW	Physical HF	Seller <u>Costs</u>
Mechanical	Applications SW	Behavioral HF	Seller Revenue
etc.	Assemblers/ Compilers	Social & Org. HF (macroergonomics)	Purchaser <u>Costs</u>
etc.	etc.	etc.	Purchaser Revenues

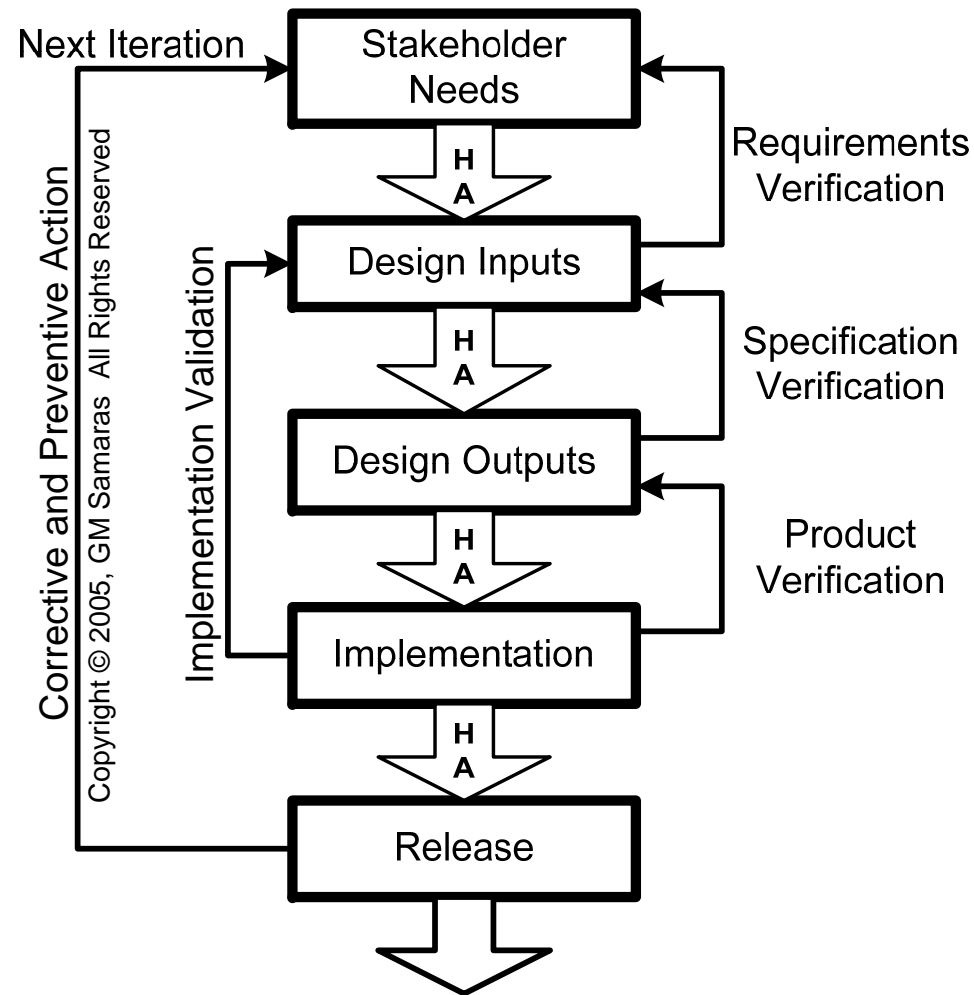
3D Systems Engineering State Space



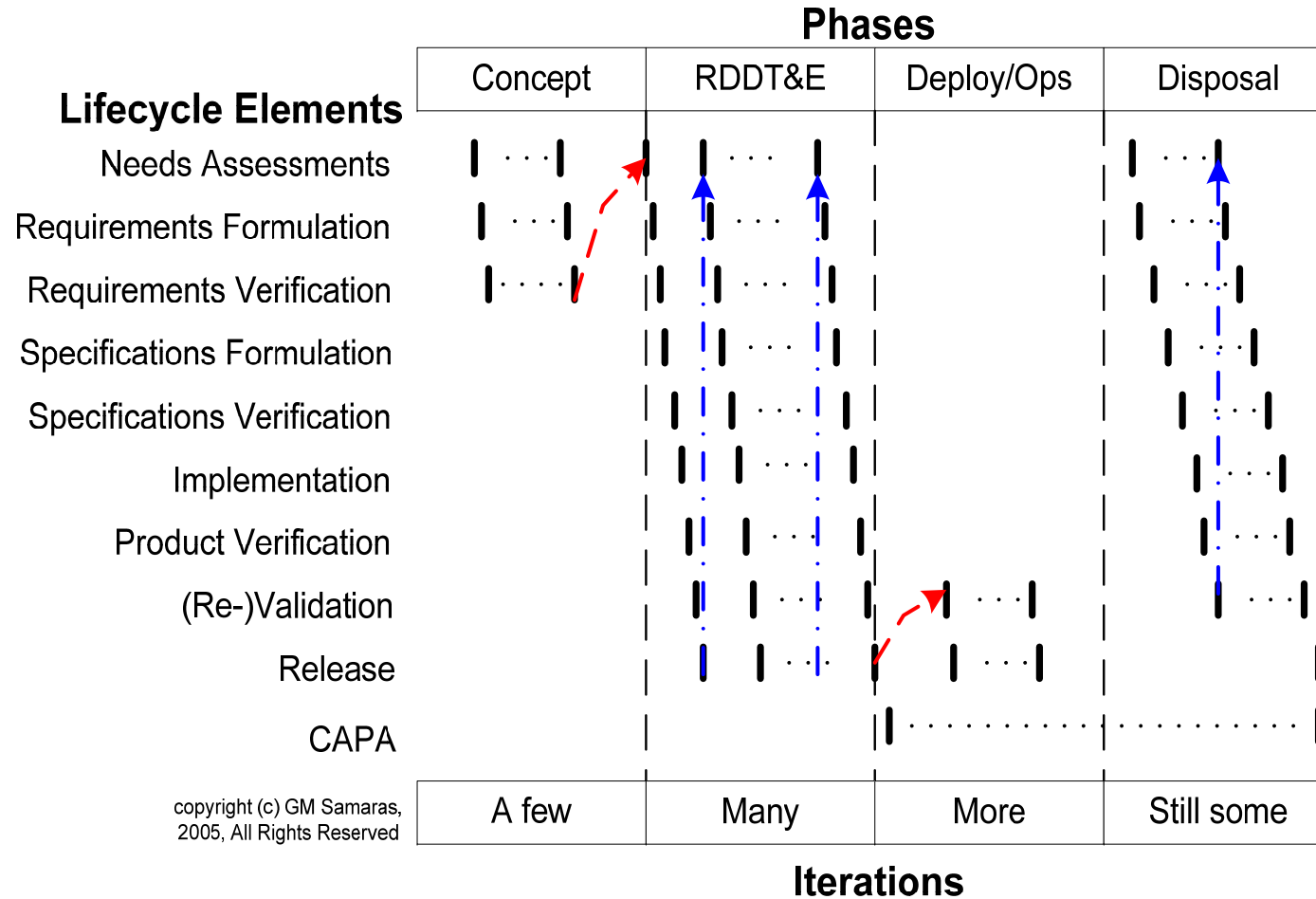
Systems Engineering Time Frame

“from LUST to DUST”

Classical SE Lifecycle Paradigm



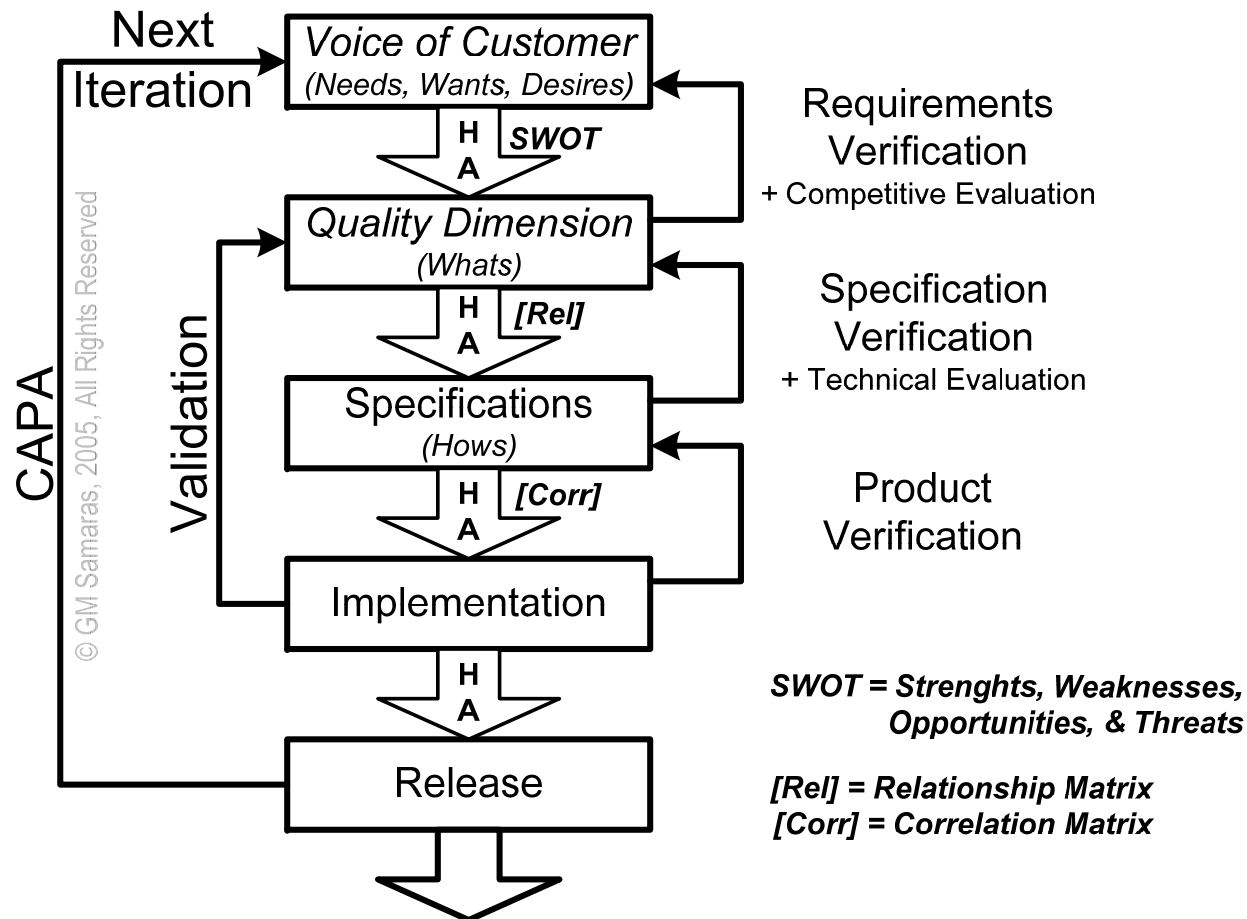
Gantt Perspective



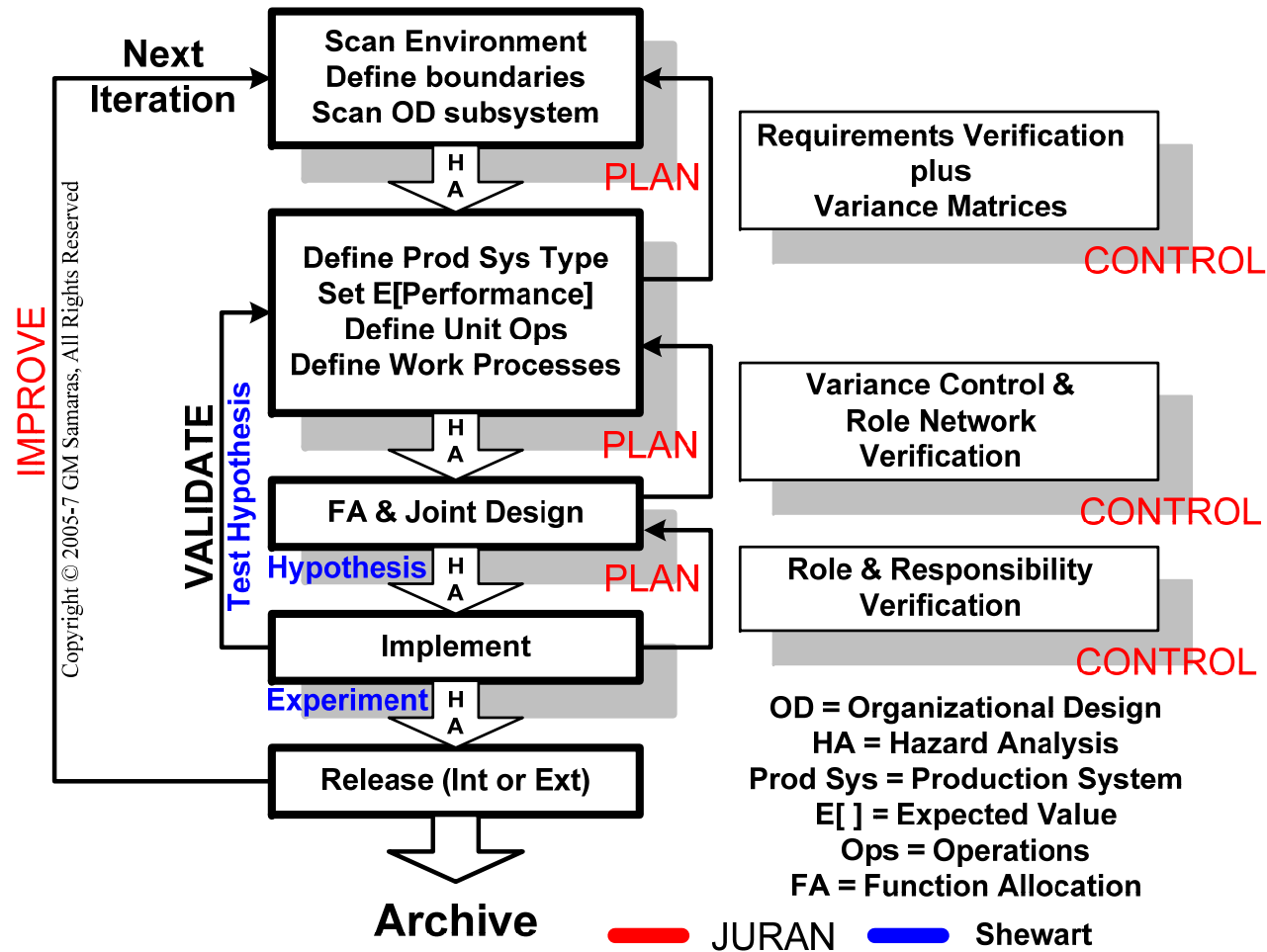
Masqueraders

- Many Development Paradigms are actually Classical SE by a different name!
 - Quality Function Deployment (next slide)
 - Macro-Ergonomic Analysis & Design (following slide)
 - Six (6) other examples in 2005 J. Biomedical Informatics article

Quality Function Deployment



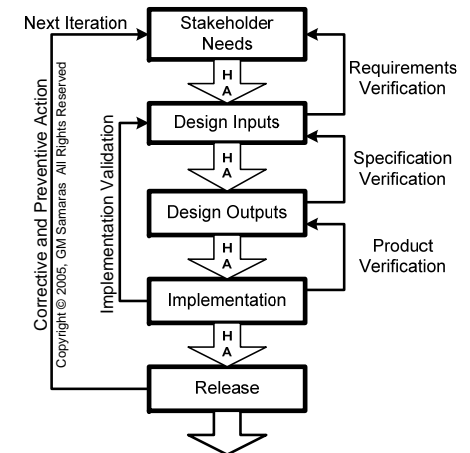
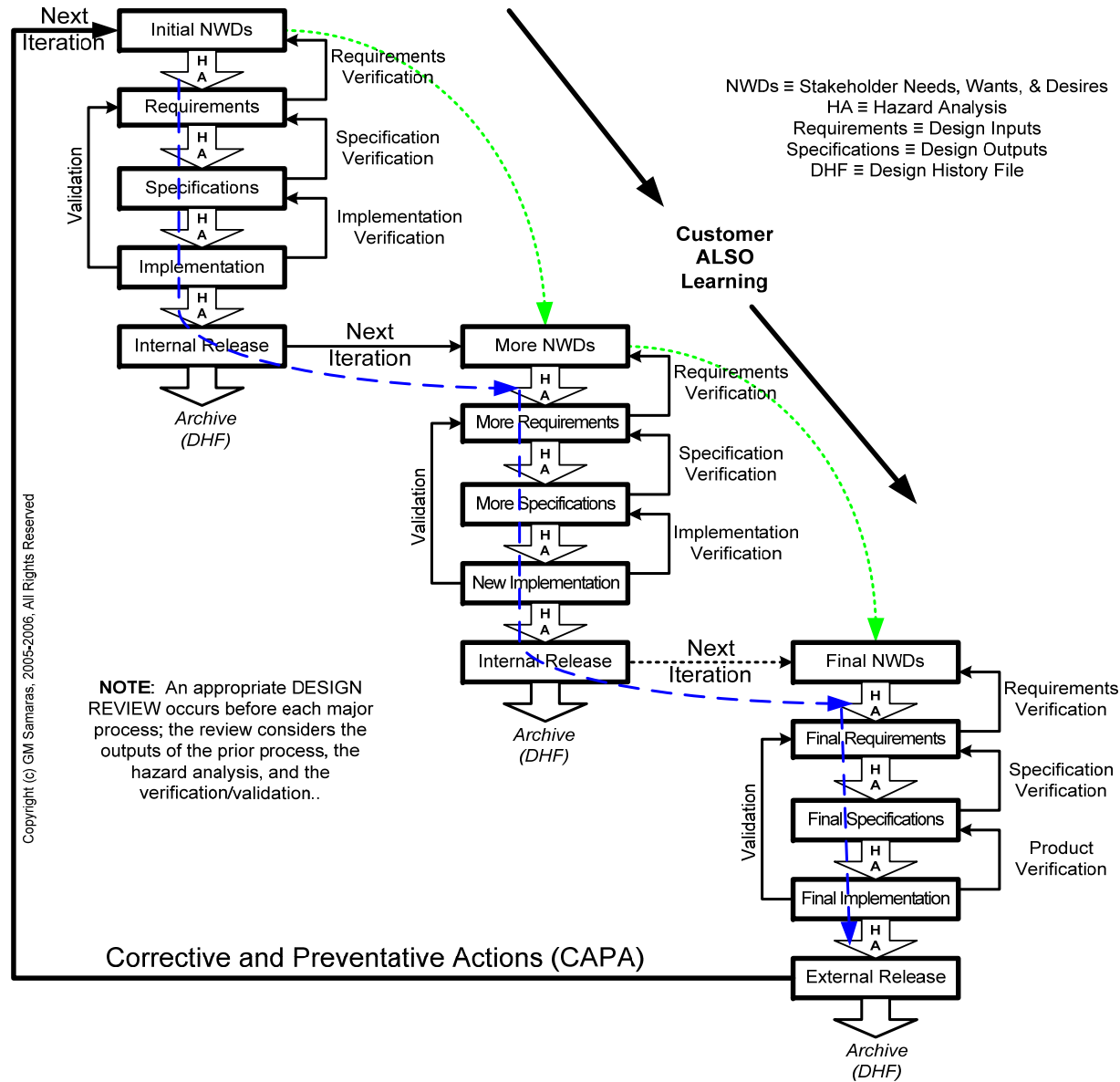
MEAD



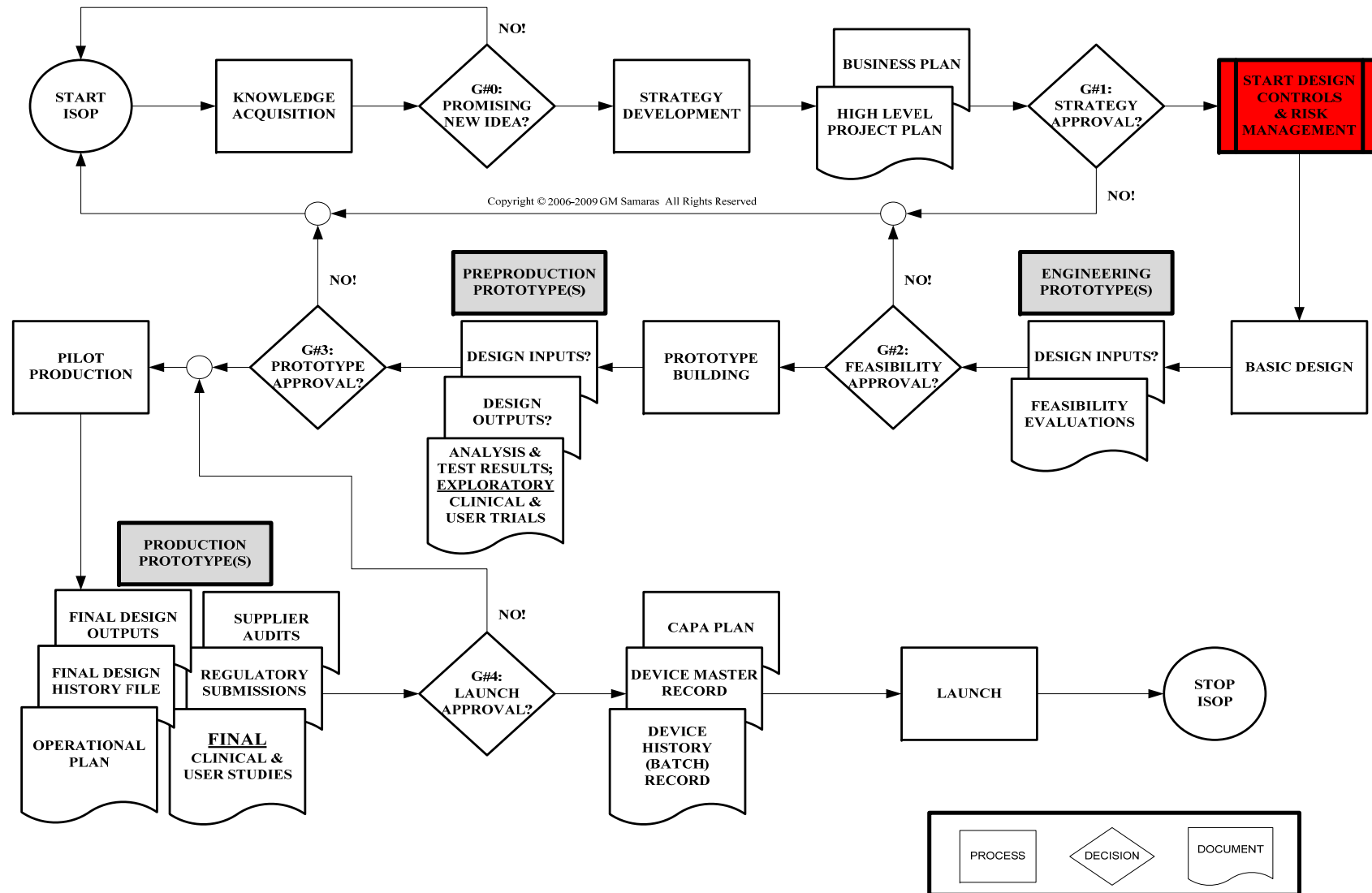
Lifecycle Notations

- Two notations
 - Condensed: Time NOT explicit
 - Expanded: Time Explicit
- So far only seen Condensed Notations
- Expanded Notation is “messy” and rarely used, because we ASSUME it is understood!

Expanded Notation



Another View



Crucial Point

- Uncontrolled designs too often are the basis for future liabilities (*recalls, litigation*) in commercial products
- Design Controls & Risk Management
START BEFORE:
 - **feasibility experiments**
 - **proofs of concept**
- If it is important enough to spend time & money on, it is important enough to do it right from the beginning

AGENDA

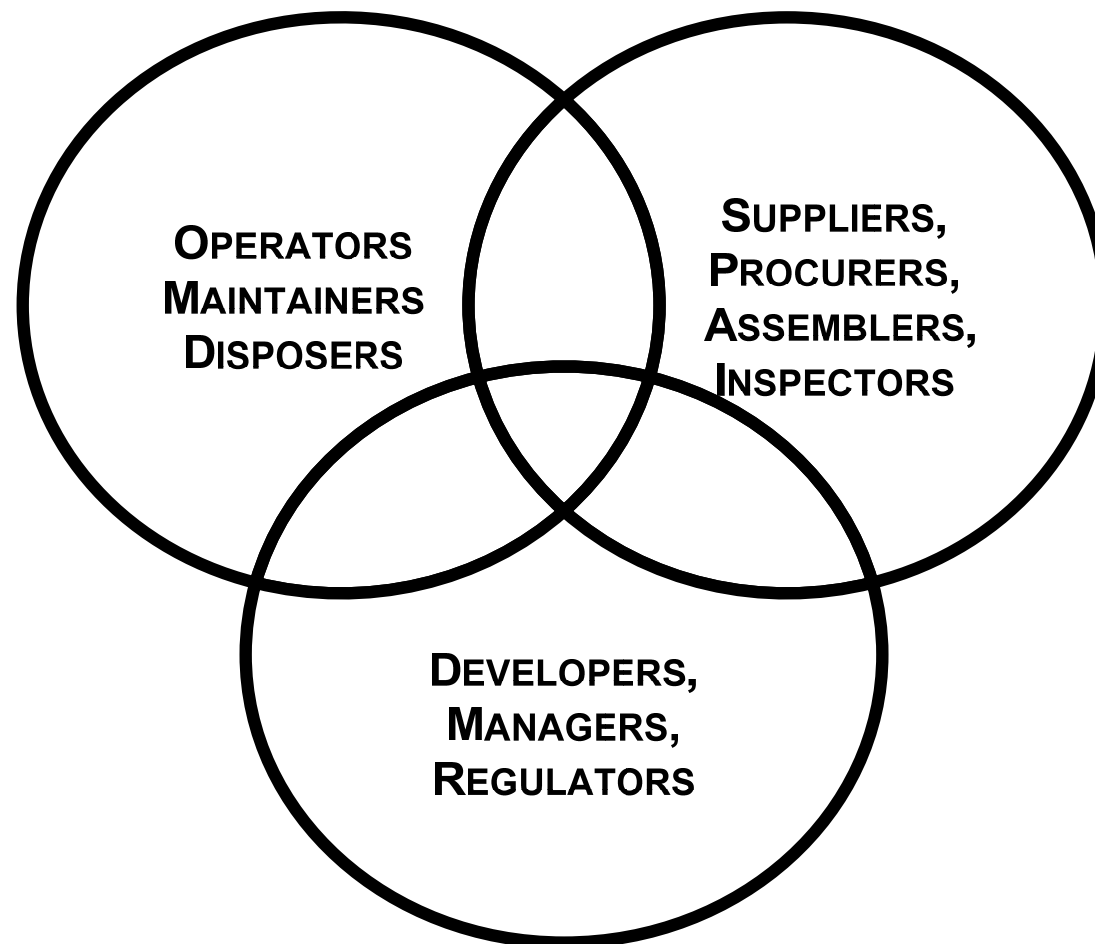
- Product Development & Errors
- Risks, Hazards, and Harm
- Humans and their Errors
- The REAL Objective
- Lifecycles, lifecycles, lifecycles
- **Human-Centered Systems Engineering**

Human-Centered Systems Engineering

- We now understand WHY we need it!
- How do we achieve it?
- Focus on the HUMAN:
 - ITERATIVE stakeholder **identification**
 - ITERATIVE stakeholder NWDs **assessment**
 - ITERATIVE **reconciliation** of conflicts
 - ITERATIVE **forecast** of evolving NWDs
 - AND, most importantly
 - ITERATIVE **validation**

Stakeholder Identification

Some “annoying” stakeholders



NWD Identification

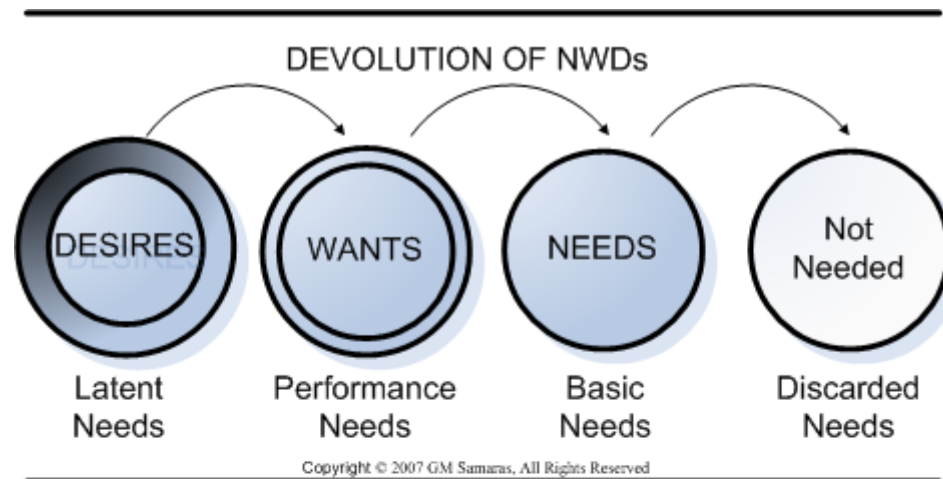
Presented @ IEEE PSES 2009

Need, Wants, & Desires

	POORLY MET	MET	VERY WELL MET
NEEDS (Basic Needs)	DISGUSTED	UNHAPPY	NEUTRAL
WANTS (Performance Needs)	UNHAPPY	NEUTRAL	HAPPY
DESIRES (Latent Needs)	NEUTRAL	HAPPY	DELIGHTED

Copyright © 2005, GM Sanatkar. All Rights Reserved

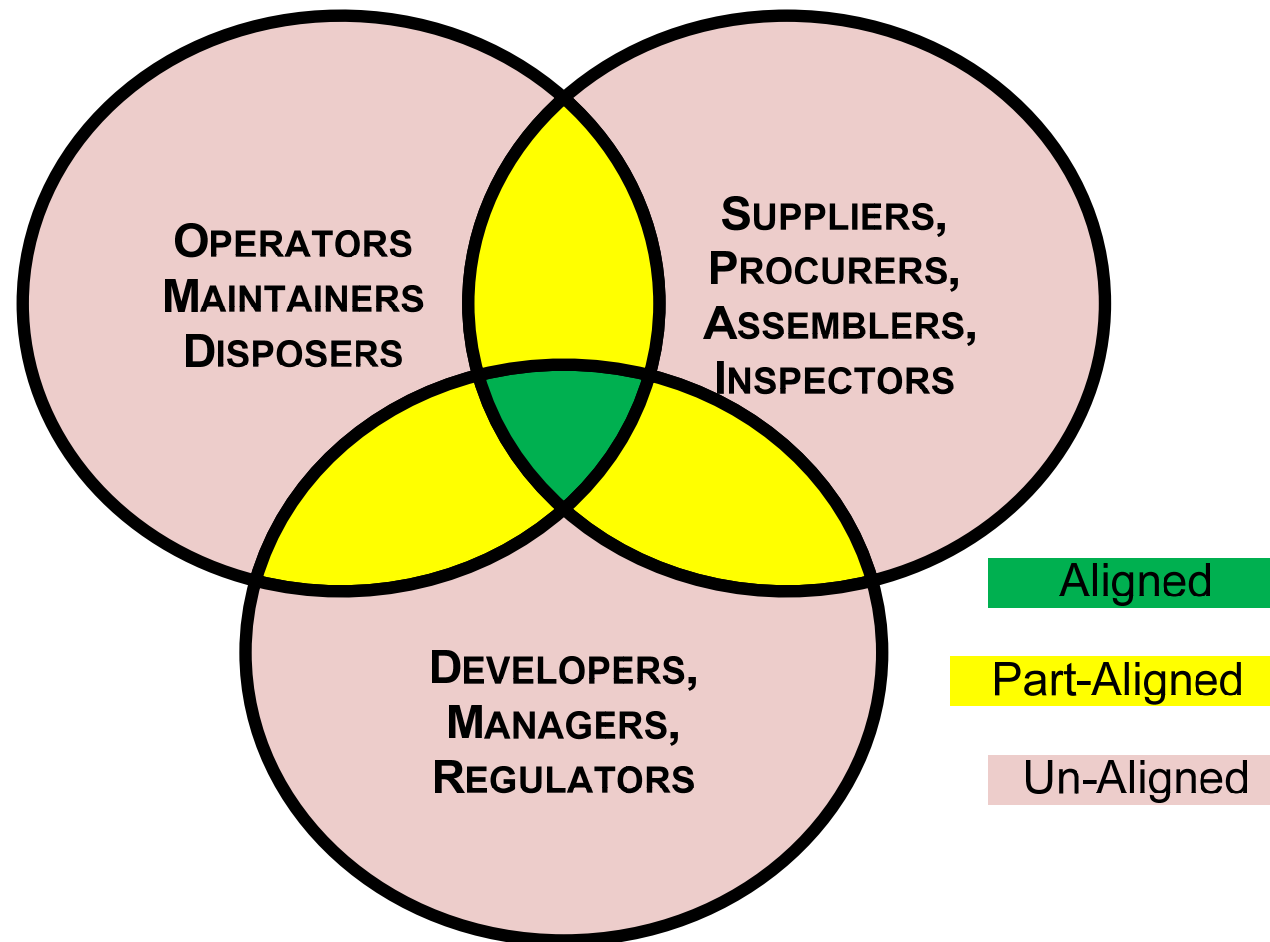
NWDs are NOT static!



NWD CATEGORIZATION			
SAFE	EFFECTIVE	EFFICIENT	SATISFYING
Stakeholder #1	Stakeholder #1	Stakeholder #1	Stakeholder #1
Stakeholder #2	Stakeholder #2	Stakeholder #2	Stakeholder #2
Stakeholder #N	Stakeholder #N	Stakeholder #N	Stakeholder #N

Stakeholder NWDs Conflict!

Non-Alignment of NWDs



NWD Reconciliation

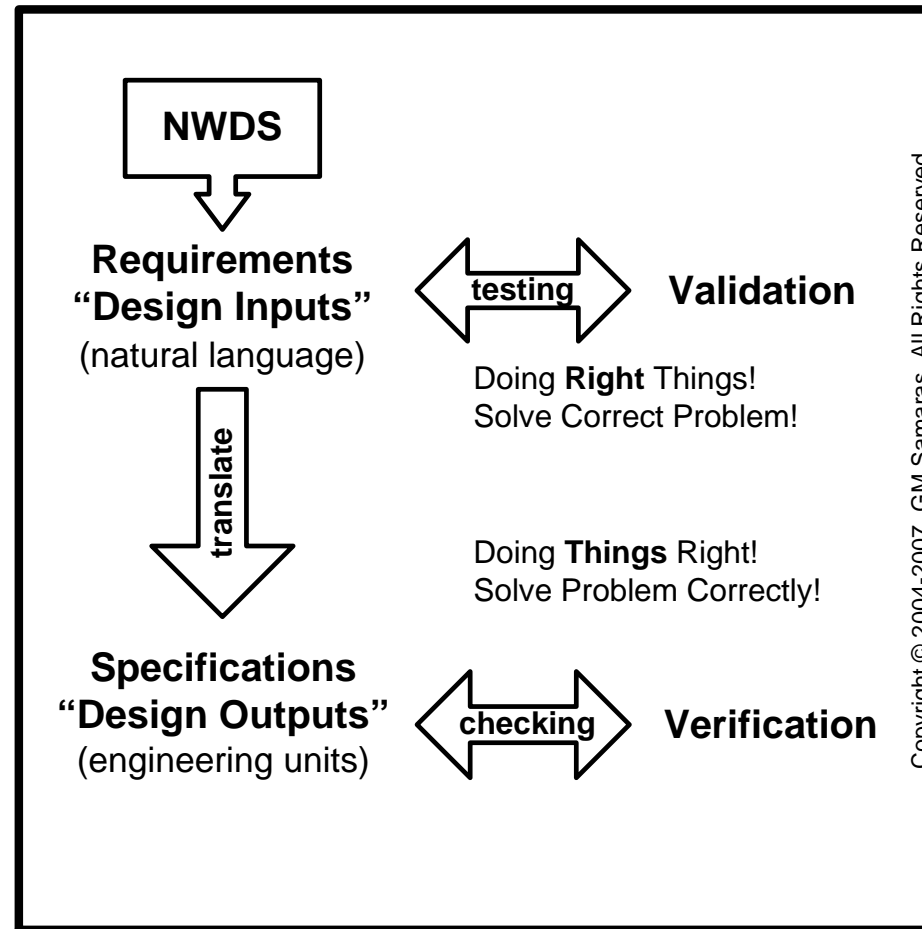
- Different stakeholder groups will have different & often competing NWDs that will change over time
- The most DIFFICULT & ARDUOUS task in HCSE is “**satisficing**” ALL stakeholder groups
- “SATISFICING” means *to obtain a good result that is good enough, though not necessarily the best, for each stakeholder*

VALIDATION

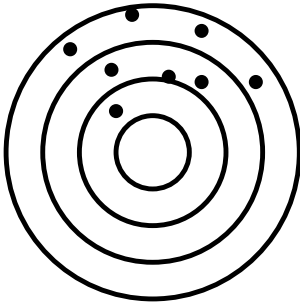
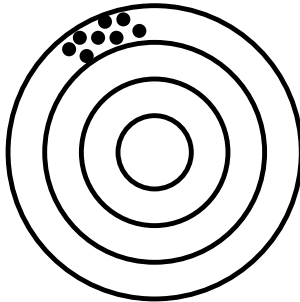
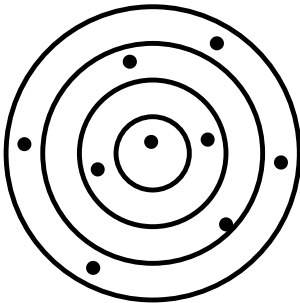
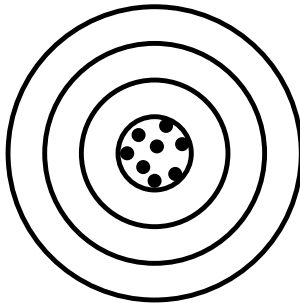
Presented @ IEEE PSES 2009

Verification versus Validation

“checking” versus “testing”



Validity presumes Reliability

	Not Reliable	Reliable
Not Valid		
Valid		

Validations

- ALL validations are “clinical” trials
- The term “*clinical*” refers to dealing with **humans**,
 - *patients* in the case of medicine and psychology,
 - *users* in the case of human factors engineering
- All clinical trials are scientific experiments conducted in real or simulated use environments
- Nobody cares if you think your product is “wonderful”, if it does not meet **THEIR** needs!

Human-centered Systems Engineering

- Identifying new stakeholders, or new stakeholder NWDs, within each iteration results in human-centered systems engineering (stakeholders are either human individuals or human organizations).
- This **human focus** continuously refines:
 - what should be built,
 - tends to eliminate extraneous “features” and costs,
 - increases the probability of acceptance;
 - the five verifications identify technical errors; and
 - validation activities identify the mismatches between what was agreed would be built and what actually was built.
- It is this **process** that has the **highest probability** of reducing economic, technical and MD&S risks.

It really is just common sense!

