Toward an Anti-Security Security Primer for Systems Engineers

October 28-31, 2024

NDIA Systems & Mission Engineering Conference, Norfolk, Virginia

Presenter: Rick Dove, INCOSE Systems Security Working Group Chair
Collaborators: Rick Dove, Mona Humes, Greg Leach, Rich Massey, Gerry Ourada, Barry Papke, Adam Scheuer, Gary Stoneburner, Daniel Sudmeier, Luke Thomas, Adam Williams, Beth Wilson, Mark Winstead.

Abstract

In pursuing the Future of Systems Engineering (FuSE) initiative, INCOSE's working group for systems security has taken its mission from INCOSE's Vision 2035: "Security will be as foundational a perspective in systems design as system performance and safety are today." In examining the situation it appears that the current approach to systems security is itself systemic in nature – systems engineering's attitudes, processes, and actions remain consistent with tradition: security is a non-functional requirement, necessary to satisfy stakeholder compliance requirements and Authorization to Operate needs. Why and how it is time for this systemic tradition to change needs illumination.

Calling it like it is.

- Predatory hostility is an active characterization of a system's operational environment that eclipses passive characterizations that use words like threat, adversary, and cyber contested environments. Damage and destruction are the intended or ransomed outcomes.
- Complexity of attack and defense continuously increases as iterative incremental attack evolution makes yesterday's defense approach insufficient and obsolete.

Predatory hostility is not new activity, but featuring it as the bottom-line issue can change the way we think and deal with it. Increasing complexity is not a new situation, but understanding its cause and continuance can change the way we think and deal with it. The nature of predatory hostility constantly evolves ahead of systems not designed or supported for functional perseverance. With these thoughts in mind a different way of looking at things can lead to a different goal, with a different set of objectives, strategies, and requirements. That's not to say what is being done should be stopped; rather what's being done should be repositioned within something completely new and practical that more directly addresses situational reality.

This presentation makes the case for a change in mind set and goal, advances a framework of strategies, and articulates a vision of acceptance.

- Mindset: Hostile predatory environment.
- Goal: System functional perseverance in a hostile predatory environment.
- Strategies: Protect, Defend, Recover, Evolve.

Vision (of a sustainable outcome):

- SEs are comfortable and natural with security as an obvious and necessary first design priority.
  It is not perceived as a burden or distraction.
- SEs intuitively recognize, feel a sense of threat, and feel a need to correct when this isn't the prevailing situation.
  A sense of wrongness prevails.

We show that security is not simply a functional requirement, but rather a prerequisite of system's functionality and performance. We will show that SEs don't need to learn new fundamental skills, only how to apply those skills to: Security requirements development, verification, and validation while sustaining a continual sense of relevant awareness.

This foundation is guiding a *Security Primer for Systems Engineers*, in final stages of development by INCOSE's Systems Security Engineering working group.

Bio: Rick Dove is an independent researcher, systems engineer, and project manager generally focused in the system security and system agility areas. He chairs the INCOSE working groups for System Security Engineering, and for Agile Systems and Systems Engineering; and leads INCOSE's Future of Systems Engineering (FuSE) project areas for both systems engineering security and systems engineering agility. He is an INCOSE Fellow, and book author of *Response Ability – the Language, Structure, and Culture of the Agile Enterprise*.

Calling It Like It Is

**Predatory hostility is an active characterization of a system’s operational environment.
Damage and destruction are the intended or ransomed outcomes.**

**Complexity of attack and defense continuously increases
as iterative incremental attack evolution
makes yesterday’s defense approach insufficient and obsolete.**

**Predatory hostility is not new activity,
but featuring it as the bottom-line issue
can change the way we think and deal with it.**

**Increasing complexity is not a new situation,
but understanding its cause and continuance
can change the way we think and deal with it.**

Adopting a Different Point of View

Goal:

**SE enables and facilitates
security as fundamental to system design**

Problem:

SE team doesn’t have, won’t become, and can’t reasonably get embedded security expertise

Strategy:

**Remove the perceived need
for security expertise**

Adopting a Different Point of View

Goal:

~~**SE enables and facilitates**~~
~~**security as fundamental to system design**~~

Problem:

SE team doesn’t have, won’t become, and can’t reasonably get embedded security expertise

Strategy:

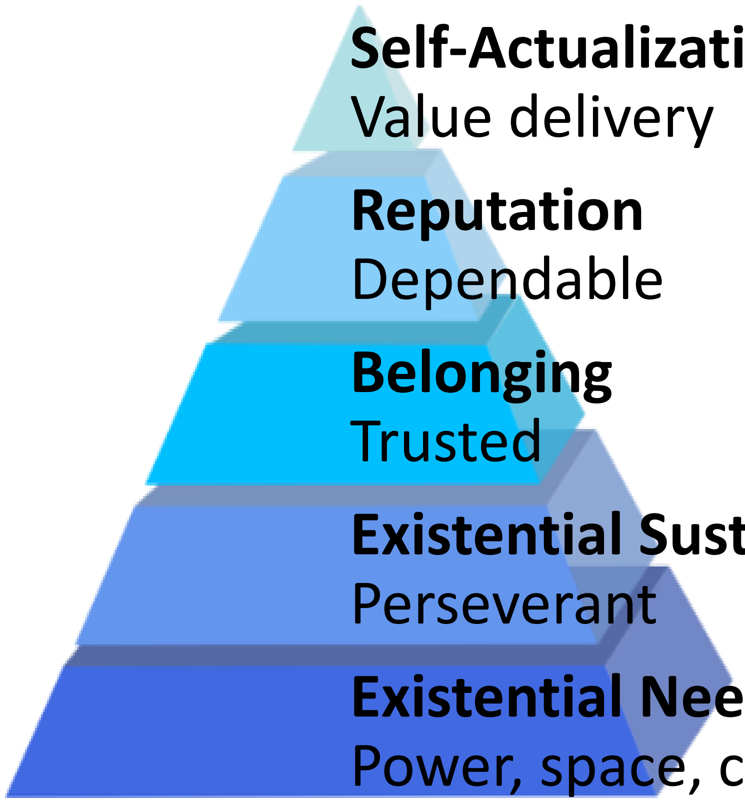
Remove the perceived need
for security expertise

================ ================

Observation:

It’s not about security (the means)
It’s about stayin’ alive (the outcome)

Stayin’ Alive is a Prerequisite of System Functionality



Self-Actualization
Value delivery

Reputation
Dependable

Belonging
Trusted

Existential Sustainment
Perseverant

Existential Needs
Power, space, cooling, shelter

Technical Hierarchy of Needs

Adaptation of Maslow’s Hierarchy of Needs

Context

Systems engineering was conceived and defined for the industrial environment.

The digital environment is demanding change:

- **Model based systems engineering.**
- **Agile systems engineering.**
- **Digital systems engineering.**
- **Systems engineering’s role in the digital security equation.**
- **Artificial intelligence impact on, and for, systems engineering.**

Front burner competition for attention and priority.

Perseverance

Continuing to make an effort to do or achieve something, even when this is difficult or takes a long time.

**What is the role of systems engineering
in creating perseverant systems …**

**ones made to endure and prevail in an environment of
constantly evolving, intelligently-directed, predatory hostility?**

"It's a list of possible side effects."

**Reactive knowledge, methods, and techniques
simply broadens and extends a legacy mindset.**

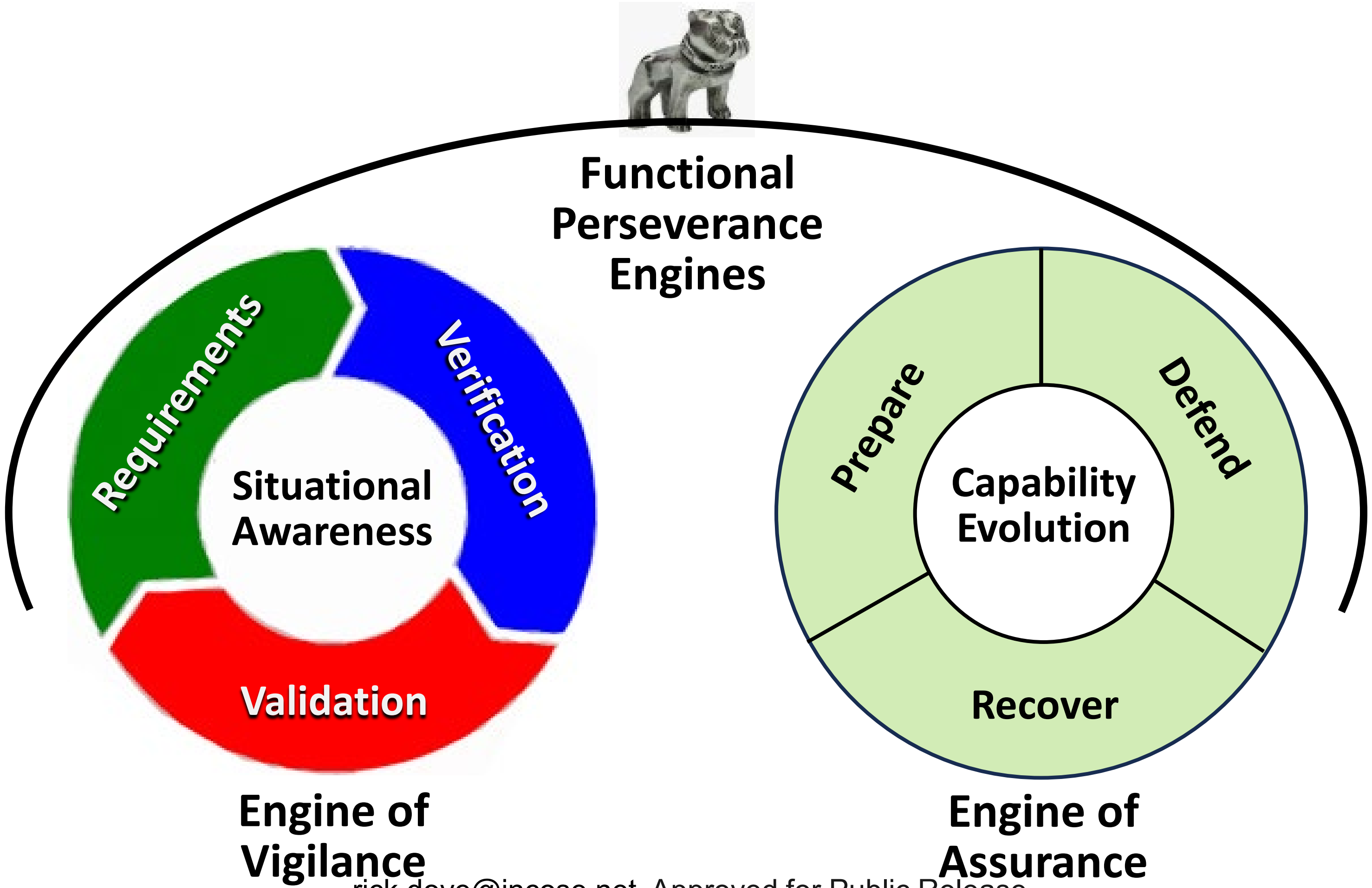
And that's not working.

**We need a systems-based mindset and doctrine,
compatible with, and enabled by, systems engineering.**

The Engines of Perseverance

Mindset: Hostile Predatory Environment
Doctrine: Functional Perseverance

Generating the horse power to survive and thrive:



People Depending on SE for Functional Perseverance of Systems

(representative sampling)

Users

have needs & loss concerns

Contract Customers

have needs& loss concerns

Program/Product Managers

have needs & loss concerns

COTS Customers

have needs & loss concerns

Incident Responders

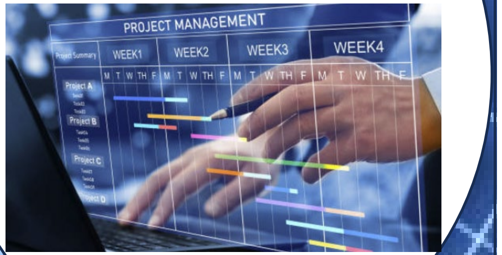
have needs & loss concerns

Developers

have needs & loss concerns

Project Managers

have needs & loss concerns



System Security Engineers

have needs & loss concerns

Grokking Your Dependents

(empathy … feeling what it's like to be that person)

Users

- Needs: Easy/seamless security; practical operations restoration; knowledge of role & response options; …
- Loss concerns: Predictable trustworthy behavior; …

Contract Customers

- Needs: Short-lived adverse behavior; cost effective verification; …
- Loss concerns: Value delivery; mission/business success, organizational reputation; …

COTS Customers

- Needs: Trustworthy operation; convenient to keep secure; …
- Loss concerns: Dependability; functionality; …

Program/Product Managers

- Needs: Satisfied owners/users; SE security champion; sufficient time and funds; …
- Loss concerns: Acquisition satisfaction; organizational reputation; personal reputation; …

Needs and loss concerns that they naturally feel, not what you want them to feel.

Grokking Your Dependents

(empathy … feeling what it's like to be that person)

Project Managers

- Needs: Comfort with system security mission; knowledge of personal role; common-mission team; …
- Loss concerns: Personal reputation; …

Developers

- Needs: Knowledge; productivity; …
- Loss concerns: Personal reputation; rework; …

System Security Engineers

- Needs: Meaningful requirements; …
- Loss concerns: Respect; ability to influence system perseverance; …

Incident Responders

- Needs: Real-time situational awareness; historical data; fallback capability; containment capability; recovery/restoration capability; …
- Loss concerns: Personal reputation; operational ownership; system functionality; behavior visibility; …

Needs and loss concerns that they naturally feel, not what you want them to feel.

What’s Newish?

Perseverance requirements engineering.
(Needs-Oriented, Loss-Driven, Capability-Based)

Active, systematic situational awareness.

Active, systematic capability evolution.

What’s Not?

Systems Engineering

Requirements Engineering

Verification and Validation

Movement: Security First

www.microsoft.com/en-us/security/blog/2024/05/03/security-above-all-else-expanding-microsofts-secure-future-initiative

Microsoft's Secure Future Initiative (May 2024)

We are making security our top priority at Microsoft, above all else—over all other features.

we will instill accountability by basing part of the compensation of the company's Senior Leadership Team on our progress in meeting our security plans and milestones.

Instilling a security-first culture

Culture can only be reinforced through our daily behaviors. Security is a team sport and is best realized when organizational boundaries are overcome. The engineering EVPs, in close coordination with SFI pillar leaders, are holding broadscale weekly and monthly operational meetings that include all levels of management and senior individual contributors. … Through this process of bottom-to-top and end-to-end problem solving, security thinking is ingrained in our daily behaviors.

Our promise is to continually improve and adapt to the evolving needs of cybersecurity. This is job number one for us.

Movement: Cyber-Informed Engineering

https://inldigitallibrary.inl.gov/sites/sti/sti/Sort_67122.pdf

CIE Implementation Guide – Quick Facts (Idaho National Labs)

PRIMARY USER

System or design engineers and technicians for critical energy infrastructure installations.

WHY TARGET ENGINEERS?

CIE extends “secure-by-design” concepts beyond the digital realm to include the engineering of cyber-physical systems. CIE introduces cybersecurity considerations at the earliest stages of system design, long before the incorporation of software and security controls. It calls on engineers to identify engineering controls and design choices that could eliminate attack vectors for cyber actors or minimize the damage they could inflict.

This approach creates new opportunities for *engineering teams*—and not just cybersecurity teams—to secure the system *using the physics and mechanics of engineering controls*—not just digital monitoring and controls

Wrap Up

Goal: Give SEs an embraceable role in the systems security equation
Strategy: Create a useful and simple mental model of what should be done for who and why

- **Security is a prerequisite for performance and safety concerns**
- **Rational appeal: can be accomplished with current SE skills applied a bit differently**
- **Emotional appeal: Personal orientation presented as a digestible quick read**
- **Objective: Get SEs started in the right direction with the right attitude and mission**

Desired reaction: “That makes sense – I can do that – I’ll listen to more in this vein.”

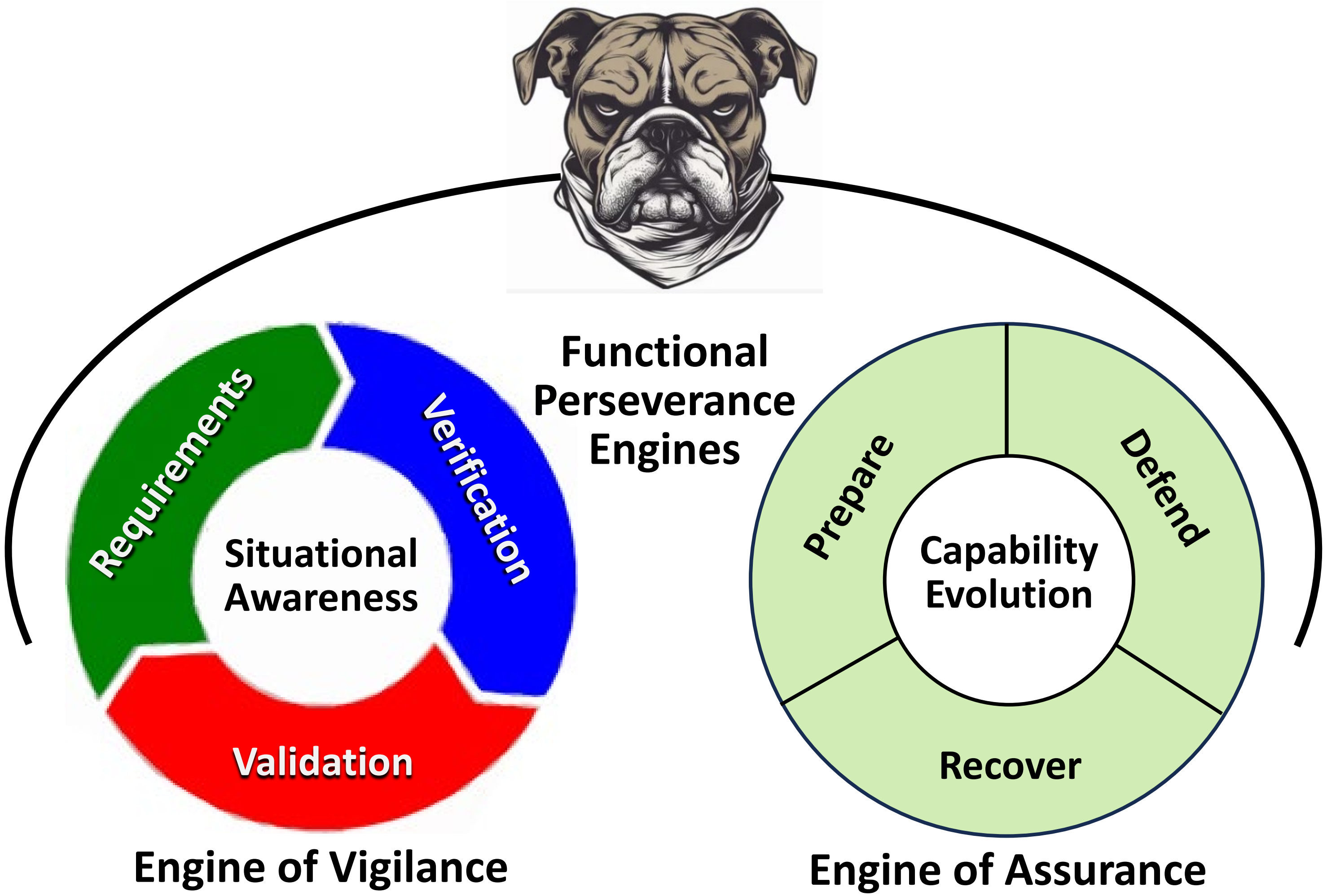
============================== ==============================

The INCOSE SE Security Guide team welcomes
practical-minded, mission-oriented, assistance
as collaborators, writers, reviewers.

contact
rick.dove@incose.net

Systems with Attitude

Discussion?



BACKGROUND

On Things That Help

On Words

Survive and thrive – more than stayin' alive

- **Survival is the state or fact of continuing to live or exist, typically in spite of an accident, ordeal, or difficult circumstances; while perseverance is the persistence in doing something despite difficulty or delay in achieving success.**
- **Persistence means continuing in a course of action without regard to discouragement or opposition; while perseverance is steadfastness in doing something despite difficulty or delay in achieving success. While persistence and perseverance share some similar qualities, the key difference lies in flexibility.**
- **Endurance is having the ability and stamina to handle difficult things – in essence, short-term pain for long-term gains; while perseverance is continuing on a journey despite the obstacles, to reach a destination or goal.**
- **Resilience refers to an ability to recover and adapt after experiencing adverse events; while perseverance means to keep going even when encountering setbacks.**

Perseverance will find a way to a desired end, persistence will continue a way to a desired end, endurance will attempt to outlast whatever is opposing a way to a desired end.

Survival says you didn't die but nothing about why, and you may be crippled.

Perseverance is dynamic, persistence is static.

On Evolution

Evolution of systems is a natural process that evaluates possible system configurations and selects for persistence, e.g., survival of the fittest. (Wong et al. 2023)*

Three kinds of selection pressures are differentiated:

- **Static selection favors systems that emerge stable from a formative process.**
- **Dynamic selection favors systems that have processes which sustain persistence in an evolving environment.**
- **Novelty selection favors systems that can open-endedly invent new functions in support of persistence.**

<u>Status Quo</u>

System security as we know it does evolve.

However, among the three selection pressures the static version is what prevails, i.e., we want to develop and commission what we wish can be a secure system.

Selection favors security capabilities that support persistence upon delivery.

* Wong et al. 2023. On the roles of function and selection in evolving systems. PNAS Vol. 120 No. 43. 16 October. https://doi.org/10.1073/pnas.2310223120

On Needs-Oriented, Loss-Driven, Capability-Based Requirements

IS23-Democratizing Systems Security

From the Introduction …

Outcome-relevant stakeholders are those who can directly affect or be affected by system security. Virtually none of them are subject matter experts in system security – they are customers, users, and developers; they are systems engineers responsible for system coherence; and they are managers of all sorts that control decision-making and work priorities.

Though they can't speak with technical expertise, all stakeholders can elucidate, or validate when prompted, what they cannot afford to lose, and what they can tolerate as partial or temporary loss. Loss may be in system functionality, in system assets, or in assets the system can affect.

> **Identifying intolerable loss requires neither knowledge of vulnerabilities that can cause the loss, nor knowledge of how to protect against the loss – common sense is required, not security expertise.**

To achieve security as a broadly embraced systems foundational perspective we need understandable and meaningful security capabilities that stakeholders can articulate, support, and relate to with personal perspective as both necessary and useful. This approach is democratization: "the action of making something accessible to everyone."

Systems security is more than a collection of technologies and specialists; it is a mission that needs an aligned team of stakeholders. Stakeholders who are misaligned compromise and degrade the objectives of those who are aligned. Stakeholders who are aligned appreciate the needs of others, share their needs and priorities with others, seek non-conflicting understandings of collective needs, and will revamp personal requirements that would impair the security needs of others even if they don't feel those exact needs.

Different types of stakeholders have different security perspectives. As a sampling:

- **Contract acquisition wants unimpeded delivery.**
- **Purchase acquisition wants functional sustainment.**
- **Suppliers want a reputation for operational excellence.**
- **Program and project managers want no-surprise, incident-free smooth sailing.**
- **Developers want freedom from rework.**
- **Users want understandable needs satisfied with usable approaches.**