Quality and Security Usability

Luis Sousa Cardoso

QSDG Chairman

A simple operational definition

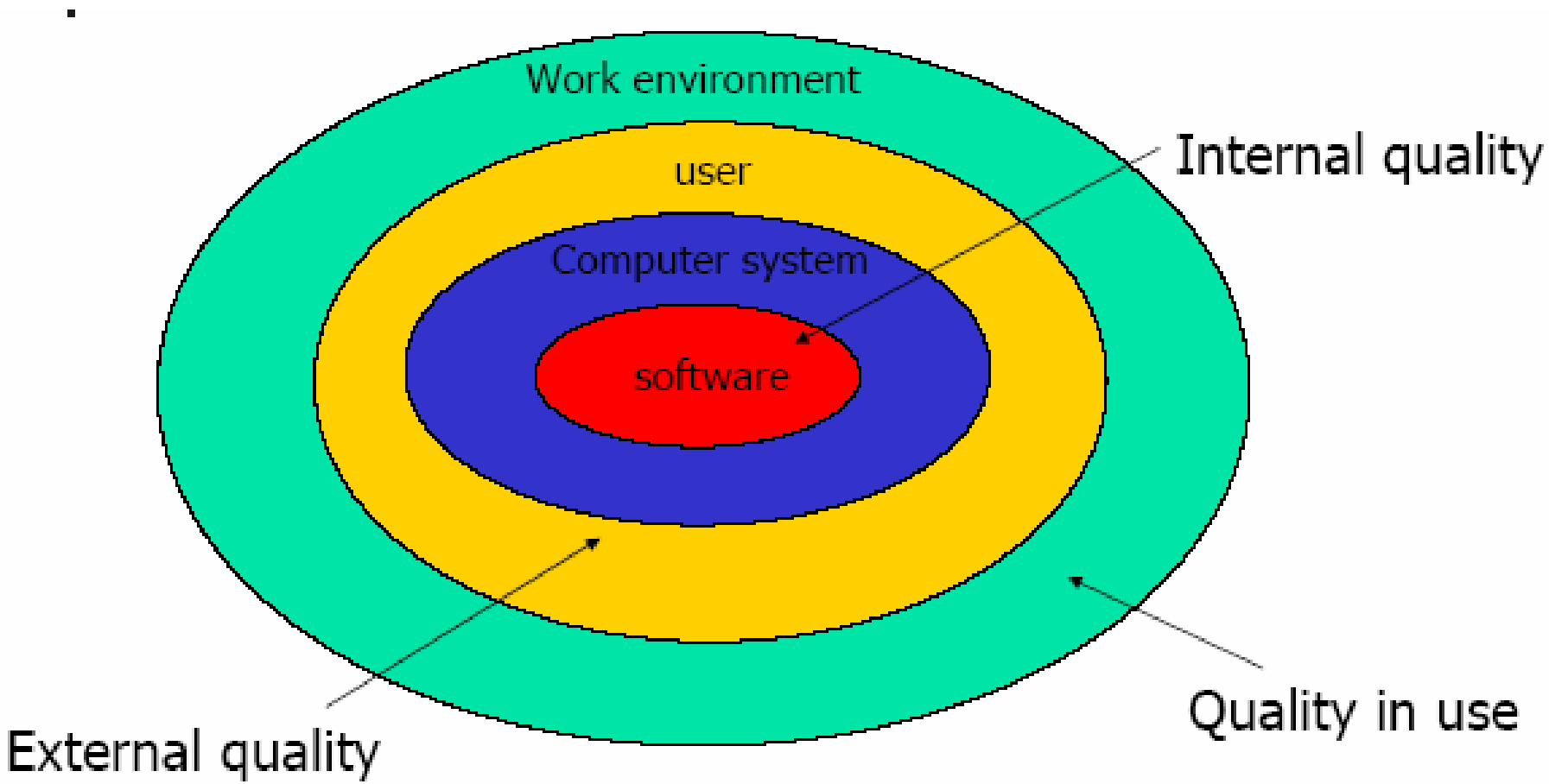
Computer Security:

“A computer is secure if you can depend on it and its software to behave as you expect it to.”

Quality is achieved when products and services are based on a contract between the customer and us. And that the customer's expectations are fulfilled – every time.

Right Quality means that each and every quality solution should be tailored so that it matches the environment's needs and demands – no more, no less

RELATIONSHIP

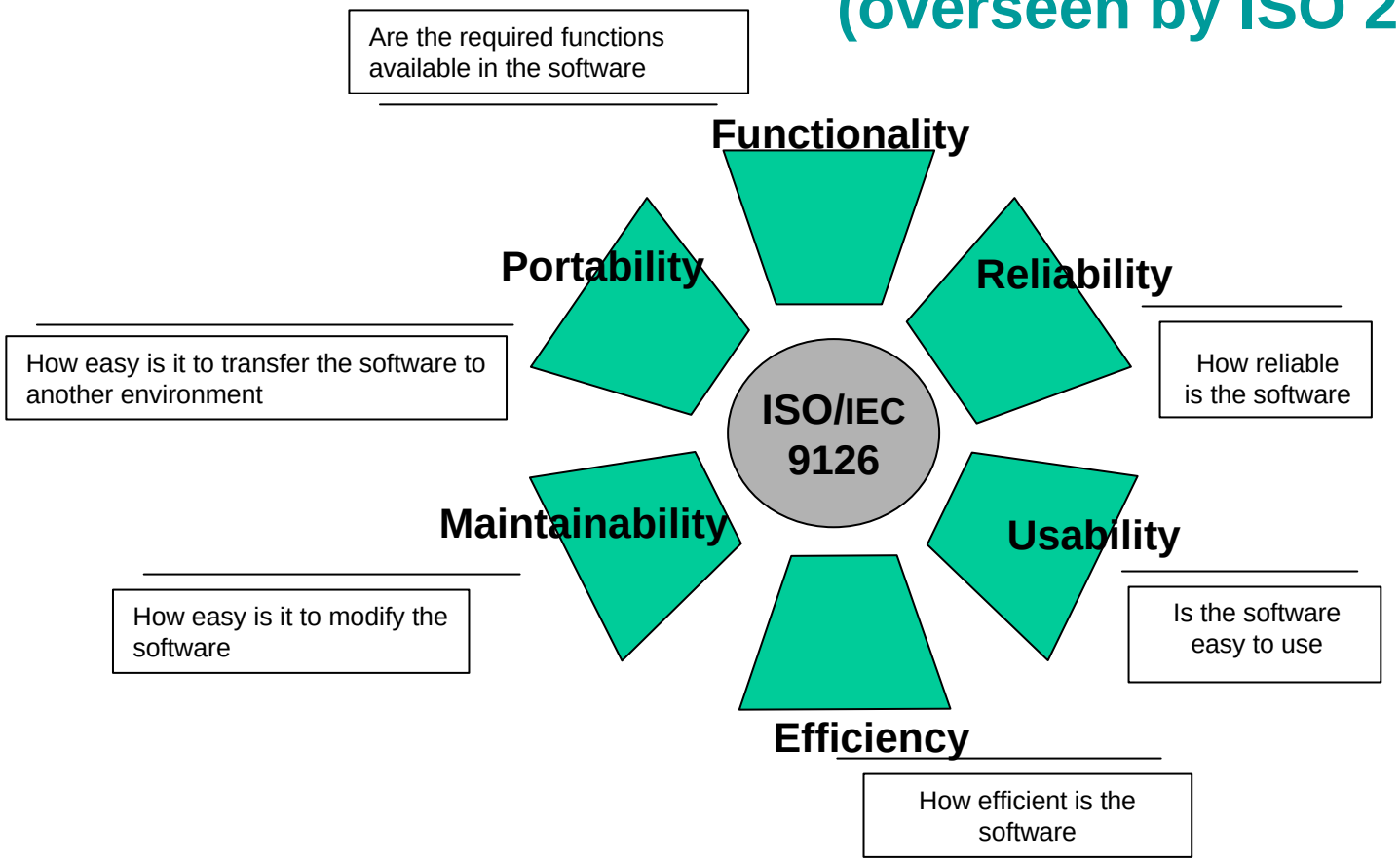


QoS can be seen as the modulation of resources to deliver requested services to users, which depends on the control and variability of resources.

Similarly, the Quality of Security Services (QoSS) involves the modulation of *security* resources, and depends on the control and variability of those security resources.

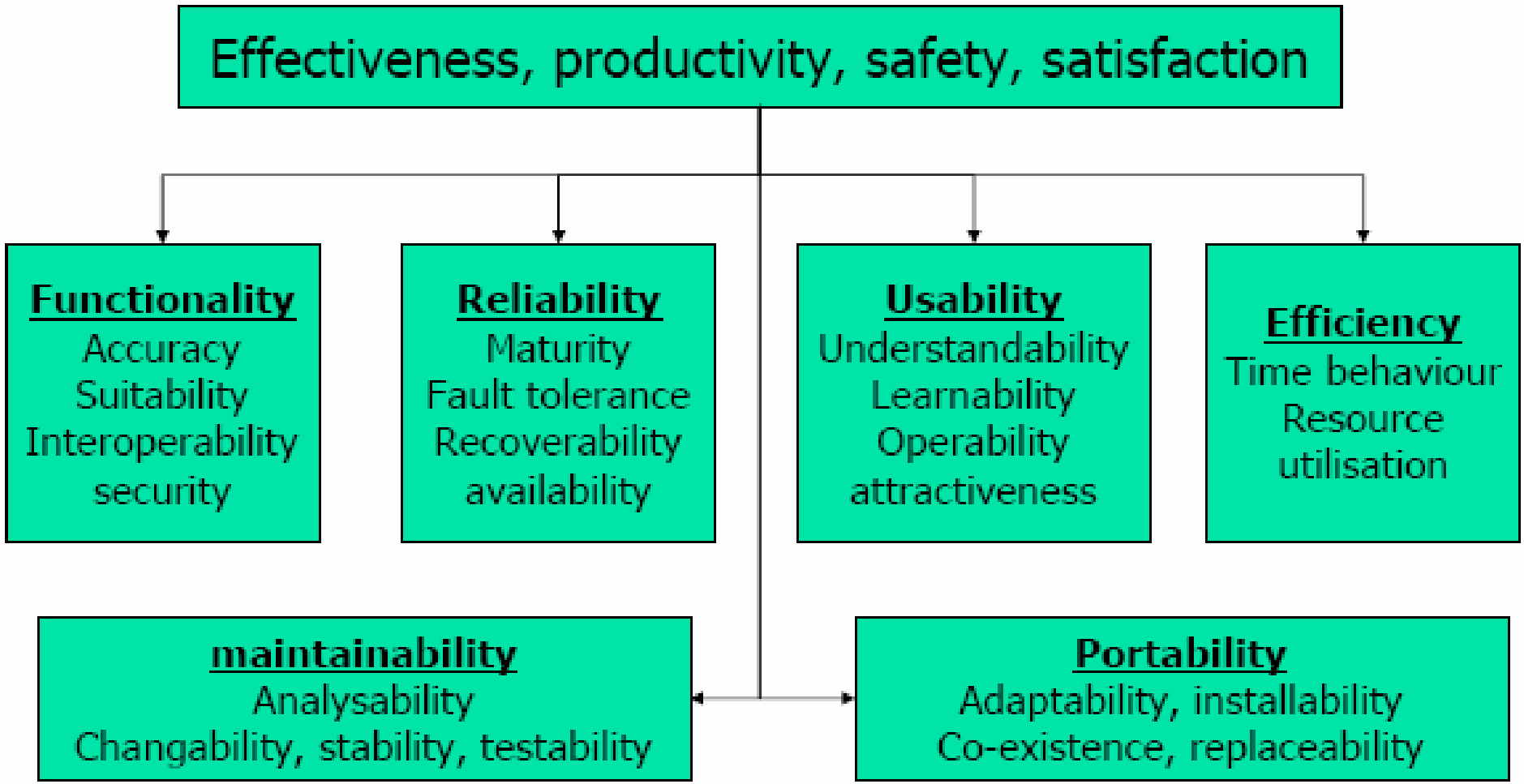
ISO 9126 Quality Factors

(overseen by ISO 25000:2000)



The Quality Factors defined by ISO/IEC 9126

QUALITY in USE



- **Functionality**
  - Suitability
  - Accuracy
  - Interoperability
  - Compliance
  - Security
- **Reliability**
  - Maturity
  - Recoverability
  - Fault Tolerance
- **Usability**
  - Learnability
  - Understandability
  - Operability
- **Efficiency**
  - Time Behaviour
  - Resource Behaviour
- **Maintainability**
  - Stability
  - Analysability
  - Changeability
  - Testability
- **Portability**
  - Installability
  - Conformance
  - Replaceability
  - Adaptability

Security is a subset of reliability.

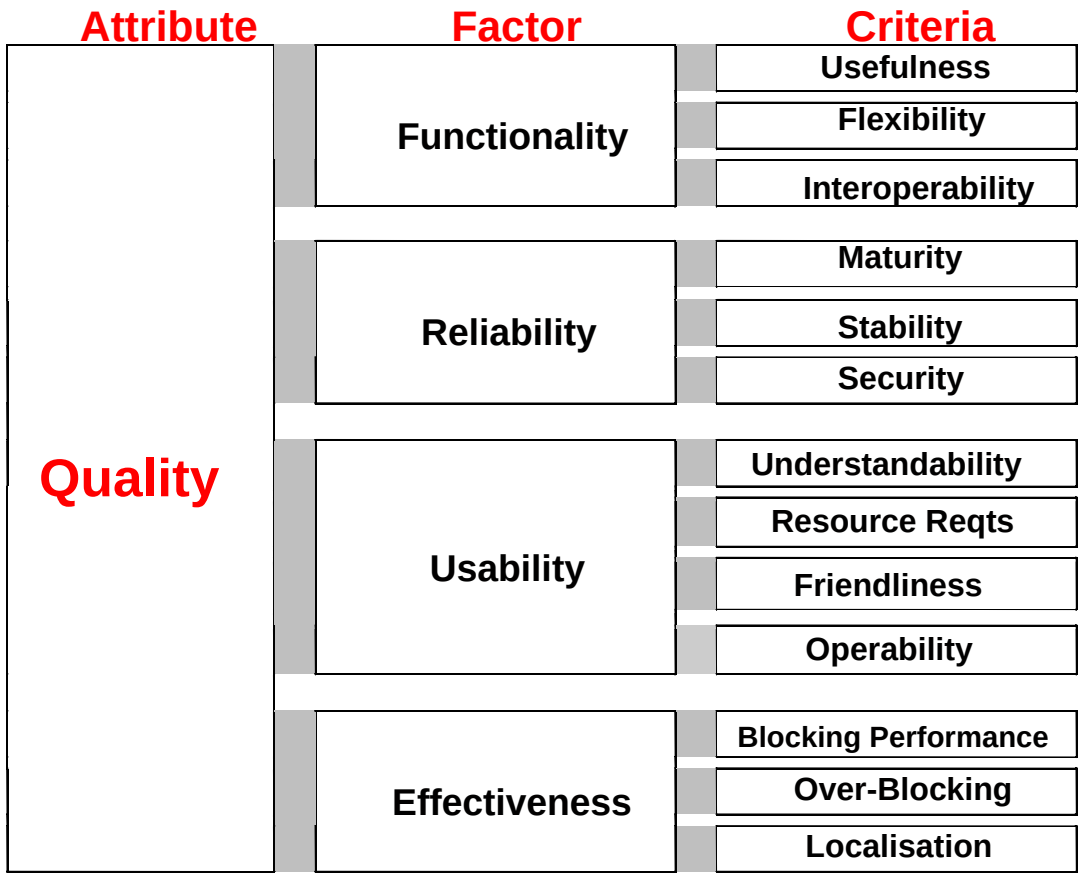
If you can completely specify your system and all of its positive and negative security possibilities, then security is a subset of reliability.

Poor *code quality* leads to unpredictable behavior, and from a user's perspective, this often manifests itself as poor usability. For an attacker, bad quality provides an opportunity to stress the system in unexpected ways.

For the end user,
quality in use is mainly a result of

- **functionality,**
- **reliability,**
- **usability and**
- **efficiency**

Quality Model



The simplified Quality Model

Quality vs. Security

Security is a mere side-effect

What do we want to PROTECT (using security measures)?

CIA² approach

- Confidentiality
- Integrity
- Availability
- Accountability

CRE² approach

- Compliance (to policy & goal)
- Reliability
- Efficiency
- Effectiveness

Today's Climate

- **Rapidly changing information technologies and compressed technology life cycles**
- **Growing complexity of IT products and systems**
- **Increasing connectivity among systems**
- **Dependence on commercial off-the-shelf IT products and systems**
- **Need for greater assurance in critical information infrastructures (both public and private sector)**

The Fundamentals

Building more secure systems depends on the use of---

- **Well defined IT security requirements and security specifications**

-describing what types of security features we want…

- **Quality security metrics and appropriate testing, evaluation, and assessment procedures**

- *providing assurance we received what we asked for…*

DEFINING REQUIREMENTS

ISO/IEC Standard 15408

A flexible, robust catalogue of standardized IT security requirements (features and assurances)

Protection Profiles

Consumer-driven security requirements in specific information technology areas

The International Standard

Common Criteria-ISO/IEC 15408

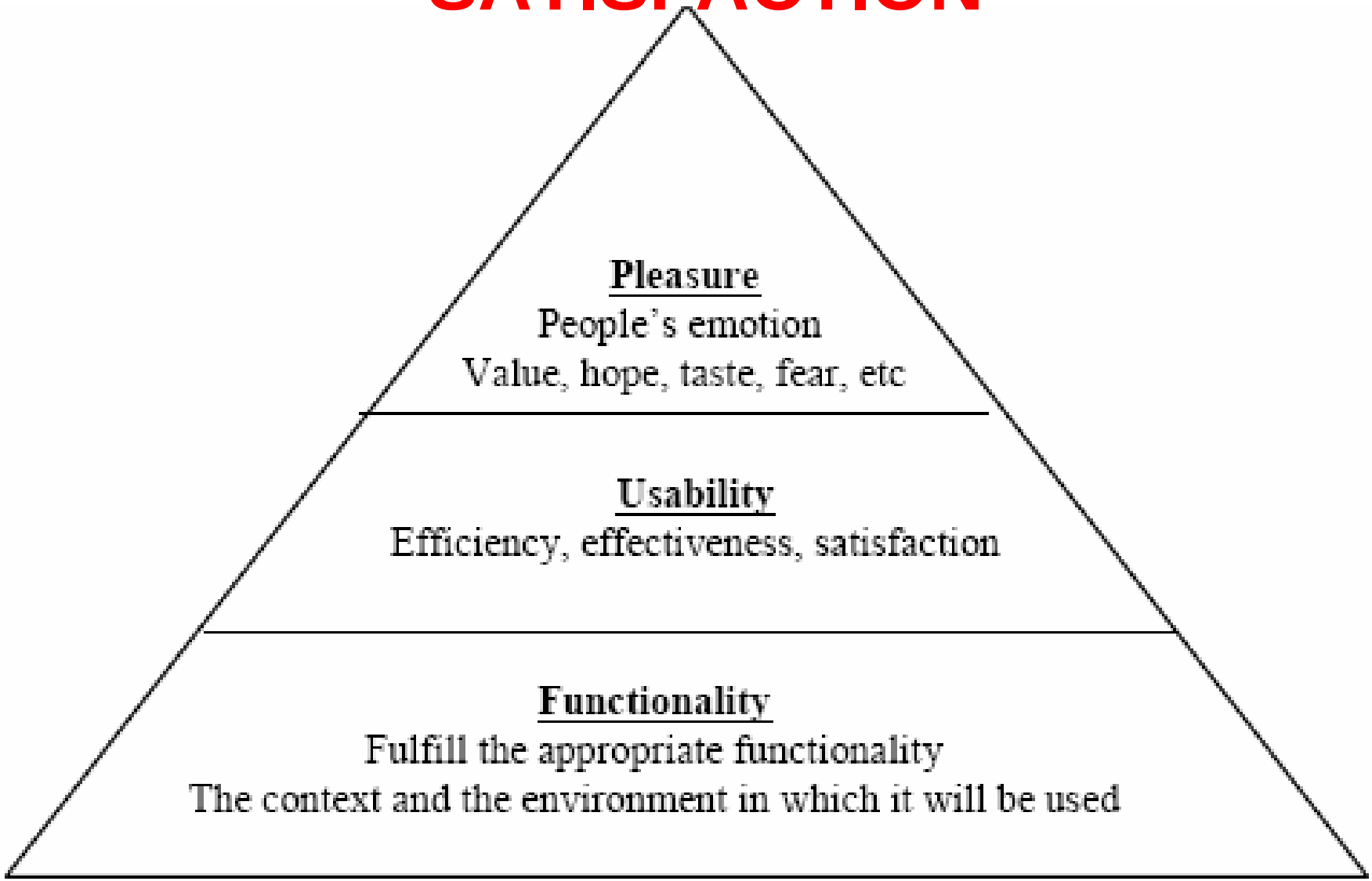
What the standard is –

- **Common structure and language for expressing product/system IT security requirements**
- **Catalog of standardized IT security requirement components and packages**

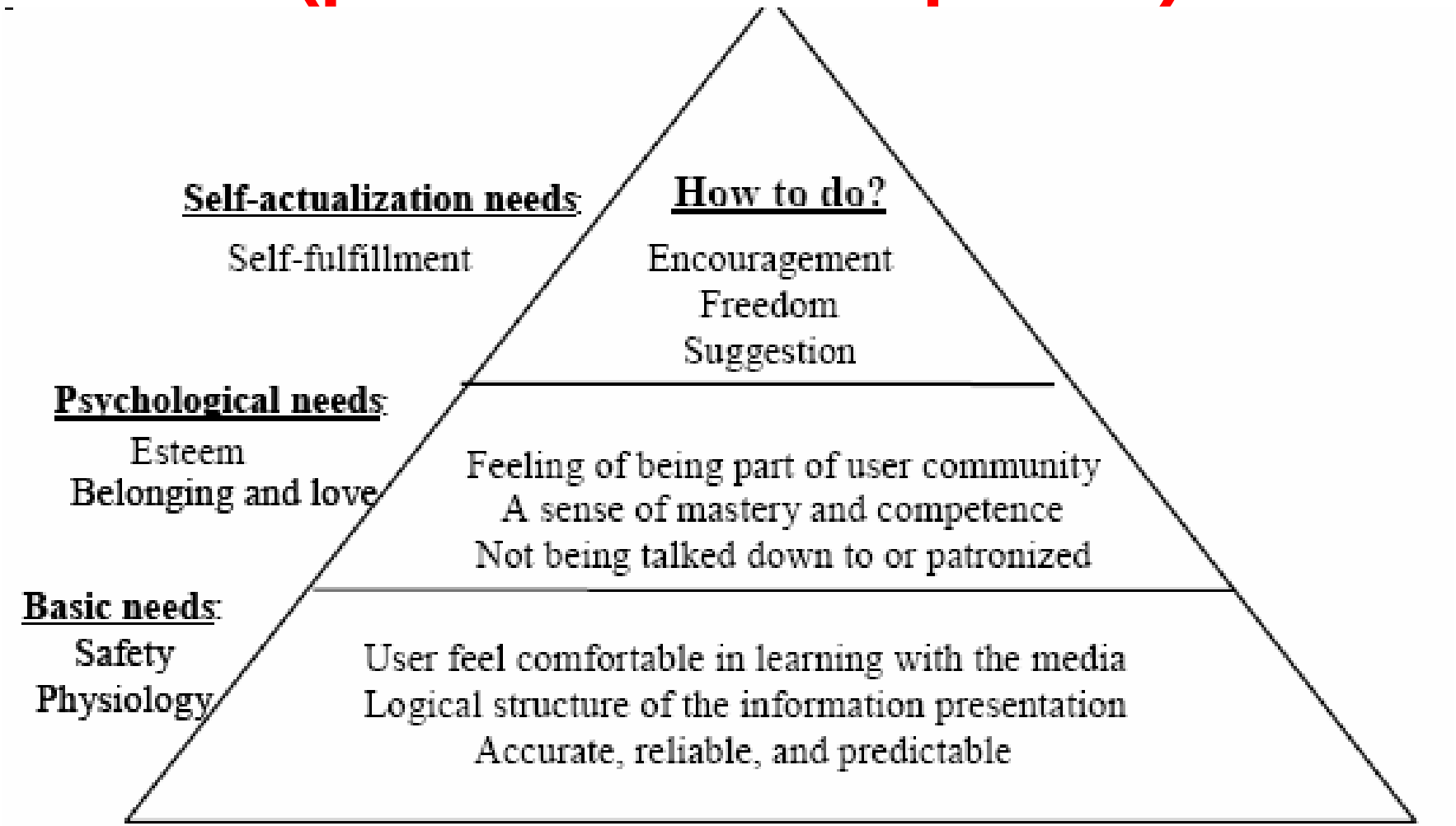
How the standard is used –

- **Develop IT security requirements and specifications for products and systems**
- **Evaluate Evaluate products and systems against known and understood IT security requirements**

SATISFACTION



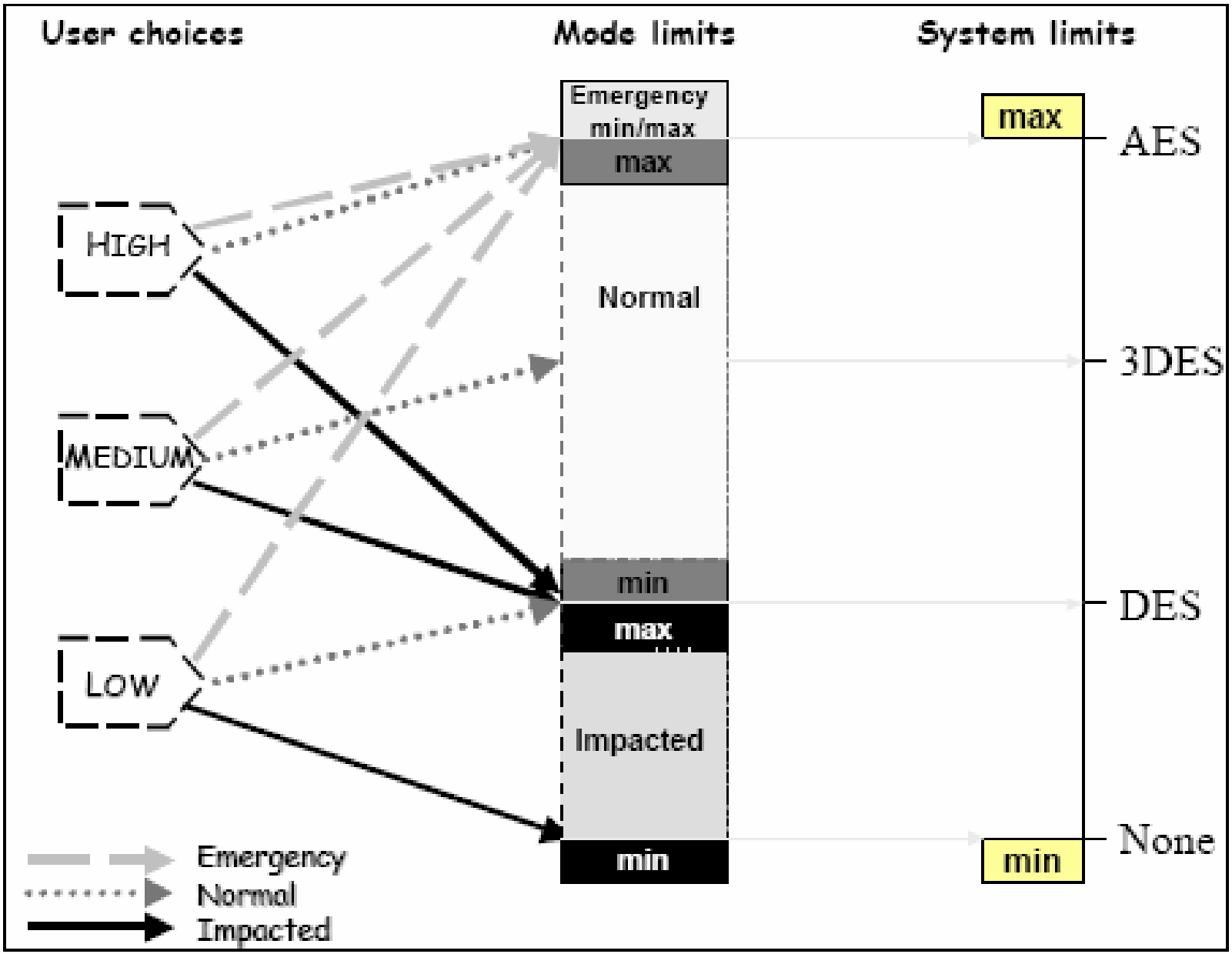
USER's NEEDS
(power of development)



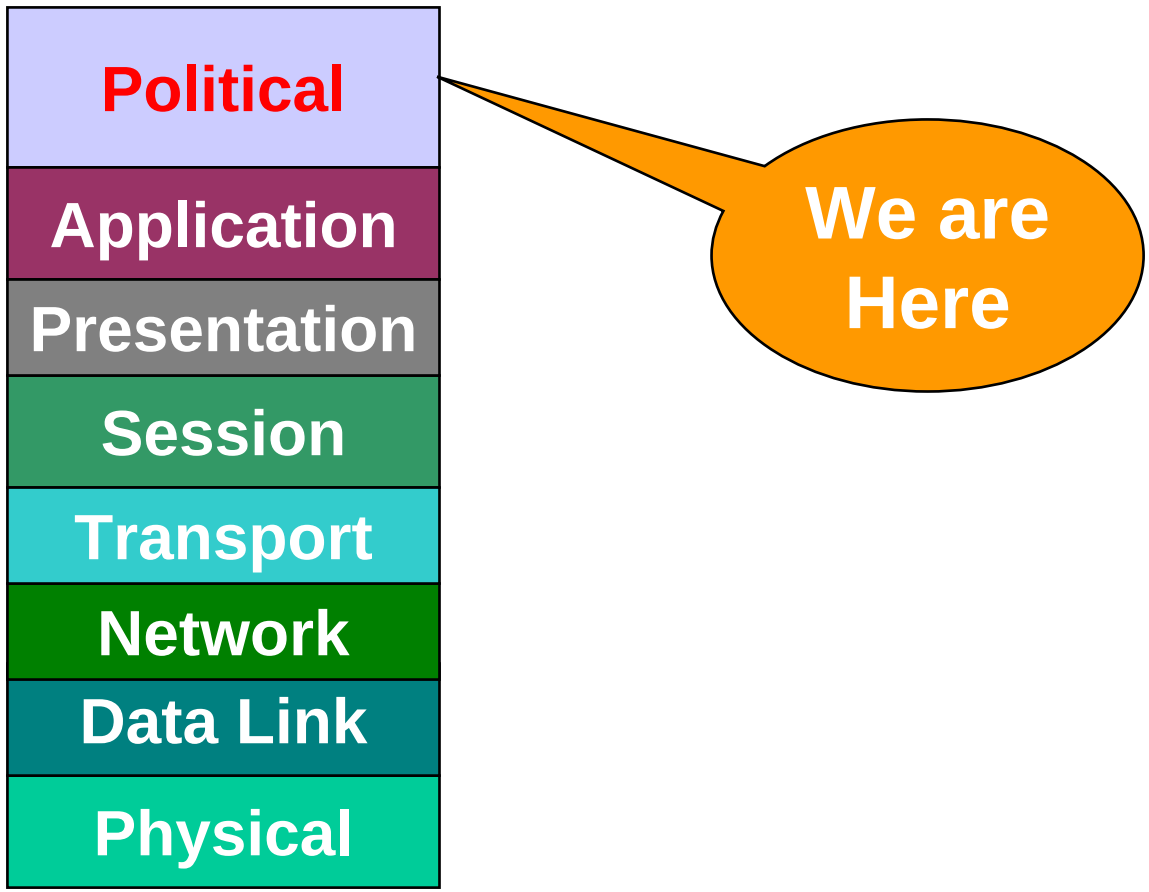
QoS involves user requests for (levels of) services which are related to performance-sensitive variables in an underlying distributed system.

For security to be a real part of QoS, then, security choices must be presented to users, and the QoS mechanism must be able to modulate related variables to provide predictable security service levels to those users.

Security Level and Network Mode Range Relationships



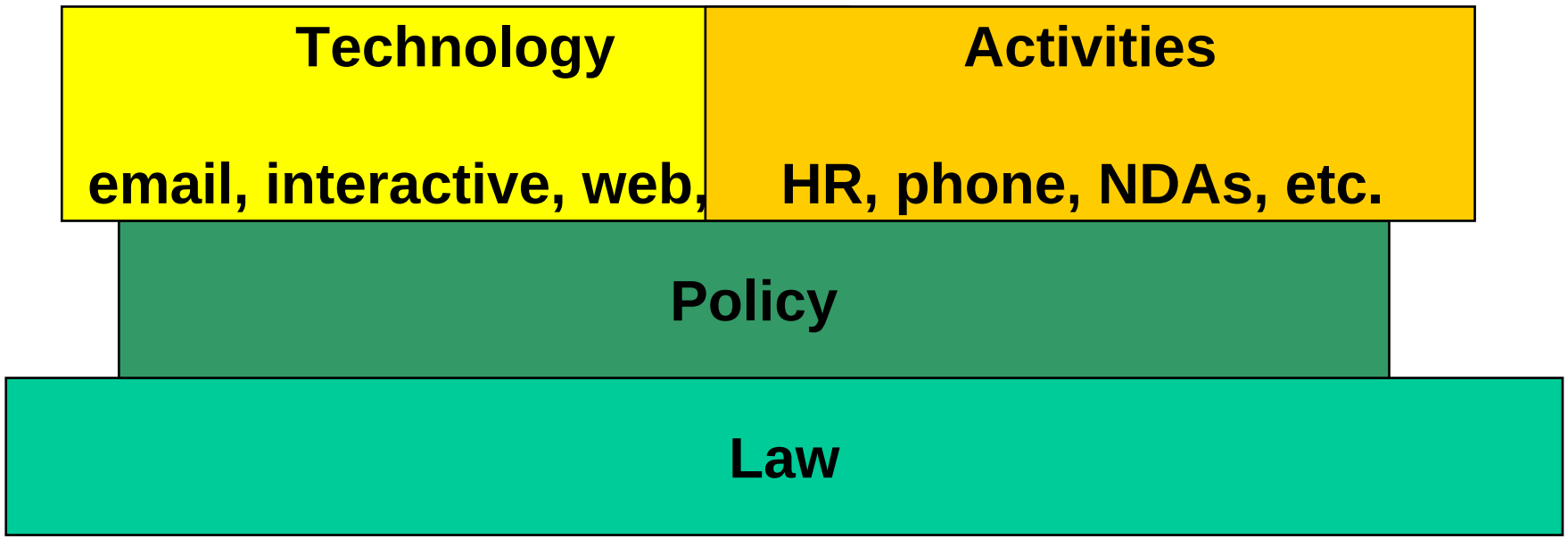
Eight layer model



So, What is “Policy”, Really?

- **Principles and goals**
- **a compass, not a map**
- **sets expectations, defines responsibilities**
- **educational**
- **enabling**

Policy is the basis for all security activities

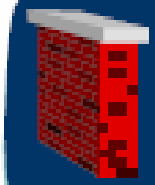


Without policy, you don't know which technology to deploy or where to "aim" it...

Secure OS
- Memory
- File Systems
- Rate Limiting
- etc.

Secure Routing
- Protocols

Security Technologies
- Crypto
- PKI
- IDS
- FW

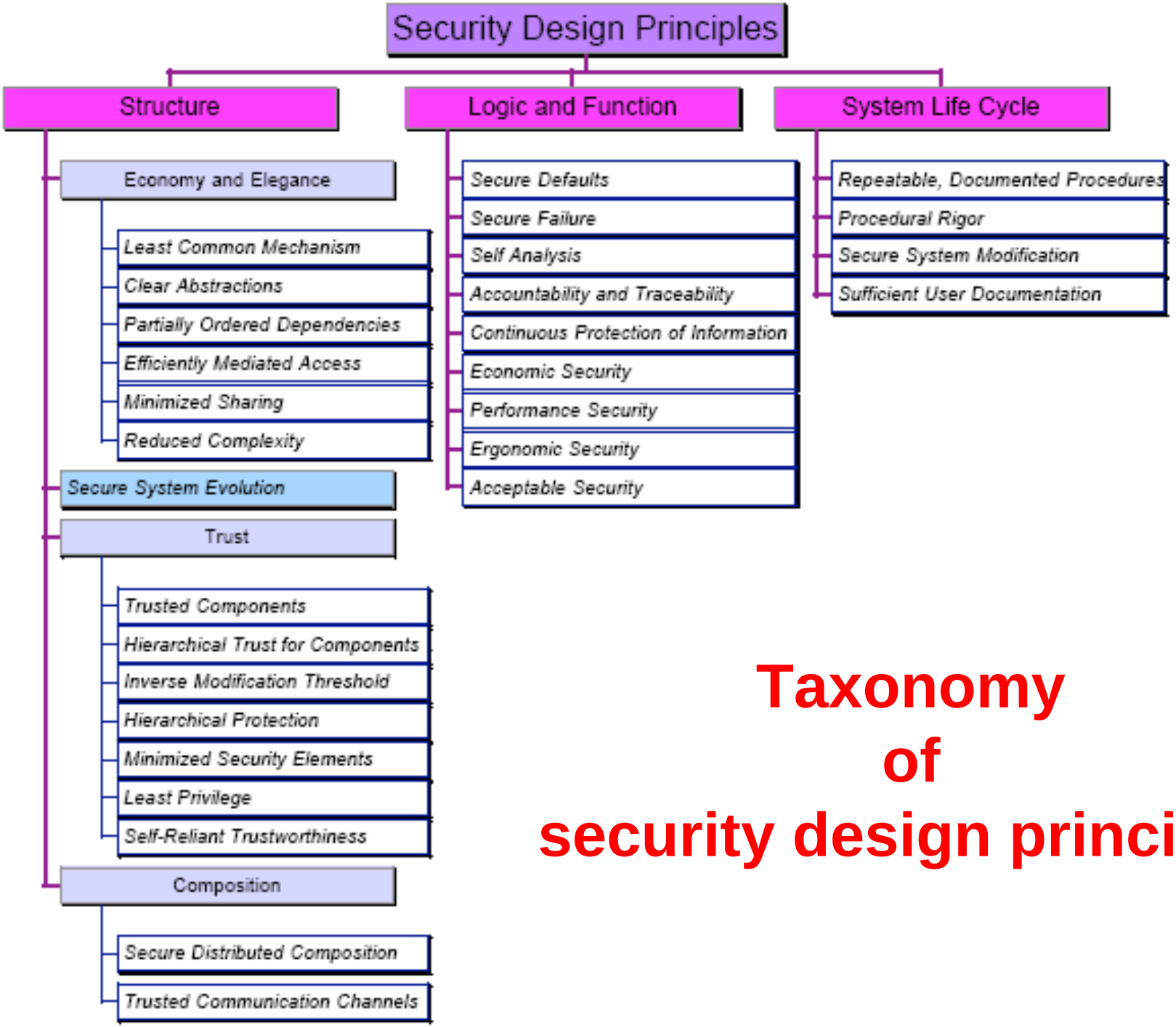


Network Infrastructure Security

Manageability Technologies
- Ease of Use
- Configuration/provisioning
- Auditing
- Image Distribution
- etc.

Access Control
- Quality of Service
- Classification
- Access Control Lists
- AAA
- Passwords
- etc.

Security Technologies



Taxonomy of security design principles

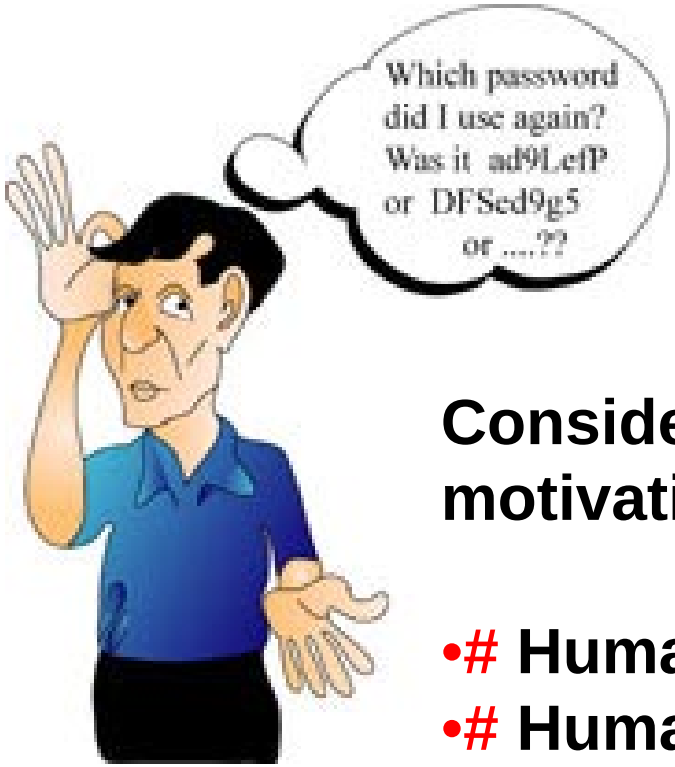
The security research community has recognised that user behaviour plays a part in many security failures, and itnhas become common to refer to users as the 'weakest link in the security chain'.

Blaming users will not lead to more effective security systems.

Security designers must identify the causes of undesirable user behaviour, and address these to design effective security systems.

Usability and Security are widely seen as two antagonistic design goals for complex computer systems.

A classic example of this argument is passwords: systems without passwords are thought to be usable, but not very secure, while systems with long passwords that must be frequently changed are thought to be secure, but not very usable.



Consider these basics of human memory and motivation applied to security technology.

- **# Human memory is limited.**
- **# Human memory fades.**
- **# Human memory**
- **# Humans are not good at dealing with**
- **randomness.**
- **# Performance matches motivation.**
- **# People like to cooperate with other people,**
- **not policies.**

This presentation argues that conventional wisdom is wrong: for the majority of users and applications, increased security cannot be achieved with technology that decreases usability.

In 1975, Saltzer and Schroeder identified eight design principles for building secure computer systems. These eight principles have become standards of the computer security lexicon:

- **Economy of mechanism;**
- **Fail-safe defaults;**
- **Complete mediation;**
- **Open design;**
- **Separation of privilege;**
- **Least privilege;**
- **Least common mechanism;and**
- **Psychological acceptability.**

On the subject of psychological acceptability, Saltzer and Schroeder wrote:

"It is essential that the human interface be designed for ease of use, so that users routinely and automatically apply the protection mechanisms correctly. Also, to the extent that the user's mental image of his protection goals matches the mechanisms he must use, mistakes will be minimized. If he must translate his image of his protection needs into a radically different specification language, he will make errors."

In other words, it must to be easier to use security mechanisms than to bypass them.

Security and usability **can be simultaneously improved by the adherence to a set of design principles.**

These principles can be inferred from a critical examination of existing systems and tested by relying upon them in the design of new systems.

Key among these principles are minimizing user input;

- **Making decisions on behalf of the user;**
- **Informing the user of actions taken upon his or her behalf; and**
- **Providing the user the ability to undo those actions when possible, and otherwise to minimize their impact.**

Case Study: The Success of SSH and SSL

The most successful cryptographic systems in use today, SSH and SSL/TLS, owe a large part of their success to their adherence to the Zero-Click principle. In fact, implementations of these protocols actually go further: they improve security and usability by removing user choice.

HCI-S Guidelines

1. Visible system state and security functions
2. Security should be easily used
3. Suitable for advanced as well as first time users
4. Avoid heavy use of technical vocabulary or advanced terms
5. Handle errors appropriately

6. Allow customization without risk to be trapped
7. Easy to setup security settings
8. Suitable Help and documentation for the available security
9. Make the user feel protected
10. Security should not reduce performance

It is concluded that existing human/computer interaction knowledge and techniques can be used to prevent or address these problems, and outline a vision of a holistic design approach for usable and effective security.

Quality and Security Usability

Luis Sousa Cardoso
QSDG Chairman

LuisSCardoso@ieee.org
Luis-s-Cardoso@telecom.pt