

# **Tietoturva - Finnish information security association Ry**

**[www.tietoturva.org](http://www.tietoturva.org)**

## **Introduction to SSE-CMM**

### **Tuesday 8.5.2001**

### **Kaisaniemi, Helsinki Finland**

### **Facilitator**

### **Aaro Hallikainen, Nokia Networks**



**Security aware  
product process**

**Introducing SSE-CMM**

## **Introduction to SSE-CMM**

- **Assurance argument**
- **Product process**
- **Process areas**
- **Assessing security**

# Assurance argument

Assurance over engineering product can be stated like below.

- Degree of confidence that security needs are fulfilled.
  - Measure of confidence in the accuracy of a risk or security measurement.
  - Grounded statement of belief for system's security.
- 
- Assurance argument consists of a claim, supporting evidence and subordinate arguments, and
  - some reasoning that establishes the link between the claim and the support.

# Algebra of assurance arguments

Argument = Claim + Evidence + Supporting Arguments + Reasoning

Claim = Subject + Predicate

Example of claim:

- Entrance to laboratory is controlled.

Argument:

- Entrance to laboratory is controlled since
  - ▼ receptionists controls the only physical entrance,
  - ▼ and door is locked and it is opened with valid access card,
  - ▼ and only one person may pass the entrance per time.
- *Reasoning may be based on evidences like above.*

# Subjects in assurance arguments

Assurance argument's claims can be about:

- **People**, users, administrators, maintenance personnel, security officers, operators, librarians, receptionists, trainers, test laboratory engineers.
- **Process**, clearing users for access to the system, writing software, escorting maintenance personnel, reviewing audit logs, releasing magnetic media, scanning the system for viruses, using the system, administering the system, handling written logs, monitoring the system.
- **Environment**, geographical location (country, terrain), structural considerations (doors, windows), physical setting (locks, protected network hardware, locked computer rooms), organizational culture.
- **Technology**, access control software, point of sale terminals, encryption devices, networks, file servers, trusted workstations, office software packages.
- **Enterprise**, the whole composite of the people, process, environment and technology.

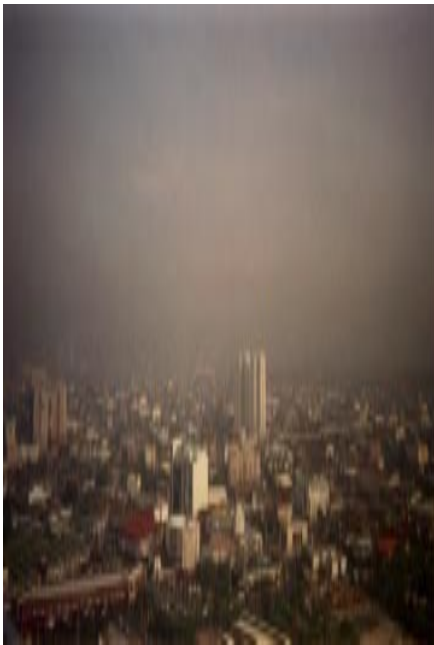
# Predicates in assurance arguments

Properties of subjects that assurance argument's may reason about:

- Analyzable - Capable of being checked
- Capable - Having required or wanted skills or faculty
- Complete - Providing a total solution
- Consistent - Uniform and steady
- Defined - Described by a fixed set of parameters
- Effective - Produces the desired result
- Efficient - Minimum of waste, expense, or effort
- Evaluated - Tested against a standard
- Recoverable - Able to be repaired or brought back from harm
- Stable - Unwavering; not subject to excessive variation
- Tested - Subjected to a regimen of testing
- Well understood - Universally comprehended across the entire enterprise

# Evidence in assurance arguments

- Evidence is **empirical data** on which a judgment or conclusion can be based.
- Anything that contributes to the believability of a claim can be considered as evidence.
- Good evidence tends to be
  - measurable,
  - repeatable and
  - testable.



Example:

- Design analysis results is an example of evidence that helps to support a correctness claim.

# Reasoning in assurance arguments

- Reasoning is a set of statements that ties together the evidence and supporting arguments to establish a claim.
- An assurance argument is more than just collection of the evidence.
- Reasoning explains how the shown evidence supports the asserted claim.
- So the evidence must be
  - relevant,
  - compelling and
  - cohesive.

Assurance derives from reduction of uncertainty.



# Security engineering in product process

Some goals for security engineering:

- Gain understanding of the security risks associated with enterprise.
- Establish a balanced set of security needs in accordance with identified risks.
- Transform security needs into security guidance to be integrated into the activities of other product process disciplines.
- Establish confidence in the correctness and effectiveness of applied security mechanisms.
- Determine that operational impacts due to security vulnerabilities in a system's operation are tolerable – i.e. risks are acceptable.
- Integrate the efforts of all engineering disciplines and specialties into a combined understanding of the trustworthiness of a system.

# Process areas

In SSE-CMM the product process is divided to

- 11 **systems security process areas** and
- 11 **project and organizational process areas.**
- ▶ Each process area is described by listing **base practises**, which satisfy needs stated by generic practises. There is 4-10 base practises per one process area.
- **Common features** describe each process area's matureness.
- Common features are defined by listing **generic practises** for each common feature.





# Some generic practises

## Common feature

- 3.3 Coordinate practises
  - ▶ GP 3.3.1 Perform intra-group coordination
  - ▶ GP 3.3.2 Perform inter-group coordination
  - ▶ GP 3.3.3 Perform external coordination
- 2.2 Disciplined performance
  - ▶ GP 2.2.1 Use plans, standards, and procedures
  - ▶ GP 2.2.2 Do configuration management

# Some security engineering base practises

## Security engineering process area

- PA06 Build assurance argument
  - ▶ BP.06.01 Identify the security assurance objectives.
  - ▶ BP.06.02 Define a security assurance strategy to address all assurance objectives
  - ▶ BP.06.03 Identify and control security assurance evidence.
  - ▶ BP.06.04 Perform analysis of security assurance evidence.
  - ▶ BP.06.05 Provide a security assurance argument that demonstrates the customer's security needs are met.

# Some project and organizational base practises

## Project and organizational process area

- PA13 Manage configurations
  - ▶ BP.13.01 Decide among candidate methods for configuration management.
  - ▶ BP.13.02 Identify configuration units that constitute identified baselines.
  - ▶ BP.13.03 Maintain a repository of work product baselines.
  - ▶ BP.13.04 Control changes to established configuration units.
  - ▶ BP.13.05 Communicate status of configuration data, proposed changes, and access information to affected groups.

# Systems security process areas in SSE-CMM

- PA01 Administer security controls
- PA02 Assess impact
- PA03 Assess security risk
- PA04 Assess threat
- PA05 Assess vulnerability
- PA06 Build assurance argument
- PA07 Coordinate security
- PA08 Monitor security posture
- PA09 Provide security input
- PA10 Specify security needs
- PA11 Verify and validate security

# Project and organizational process areas

- PA12 Ensure quality
- PA13 Manage configurations
- PA14 Manage project risk
- PA15 Monitor and control technical effort
- PA16 Plan technical effort
- PA17 Define organization's systems engineering process
- PA18 Improve organization's systems engineering process
- PA19 Manage product line evolution
- PA20 Manage systems engineering support environment
- PA21 Provide ongoing skills and knowledge
- PA22 Coordinate with suppliers

# Common features per maturity level

## Level 2, Planned and tracked

- ▶ 2.1 Planning performance
- ▶ 2.2 Disciplined performance
- ▶ 2.3 Verifying performance
- ▶ 2.4 Tracking performance

## Level 1, Performed informally

- ▶ 1.1 Base practices are performed

## Level 0, Not performed



# Common features per maturity level

## Level 4, Quantitatively controlled

- ▶ 4.1 Establishing measurable quality goals
- ▶ 4.2 Objectively managing performance

## Level 3, Well defined

- ▶ 3.1 Defining a standard process
- ▶ 3.2 Perform the defined process
- ▶ 3.3 Coordinate the process



# Common features per maturity level

## Level 5, Continuously improving

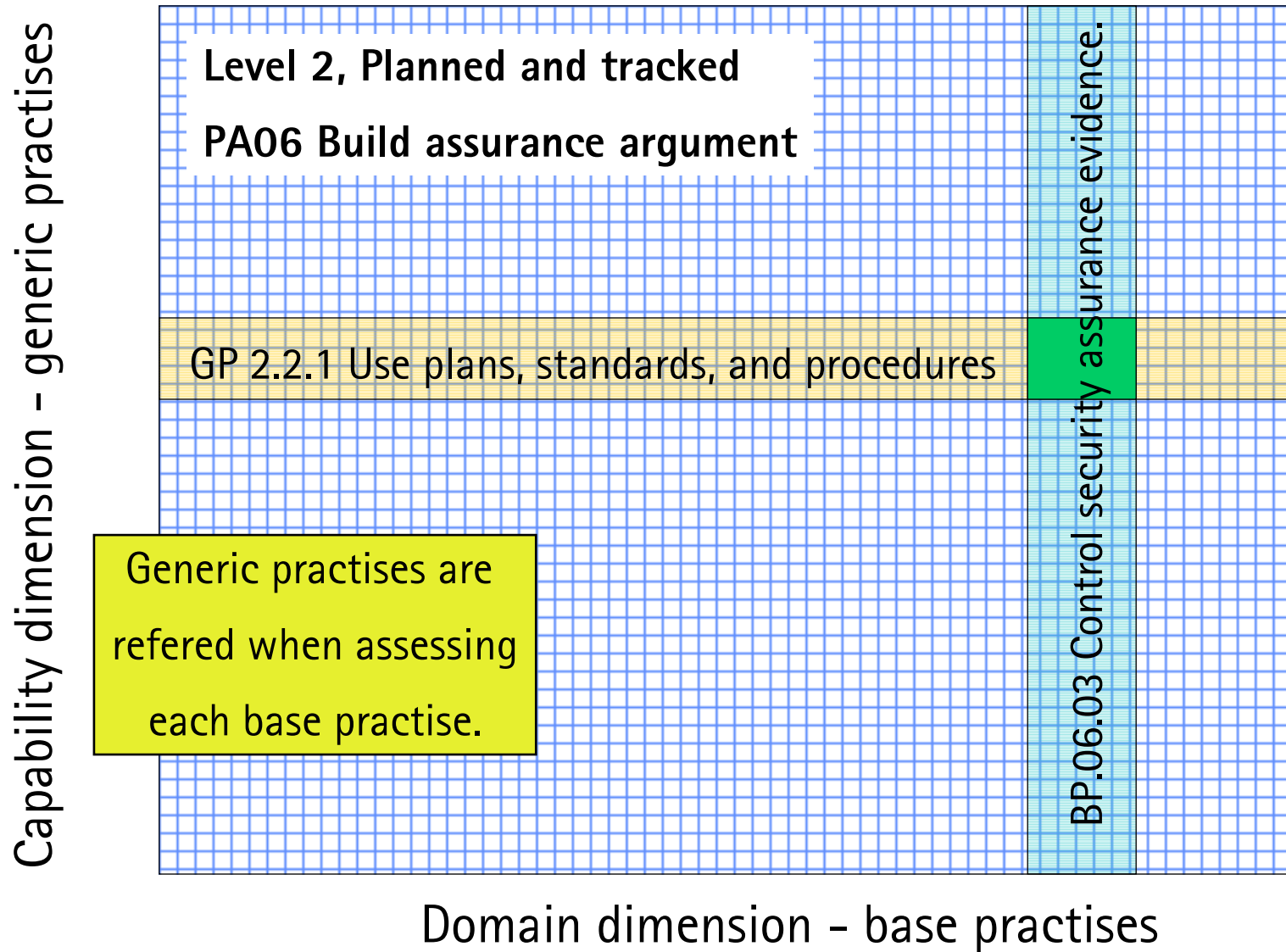
- ▶ 5.1 Improving organizational capability
- ▶ 5.2 Improving process effectiveness



# Maturity levels

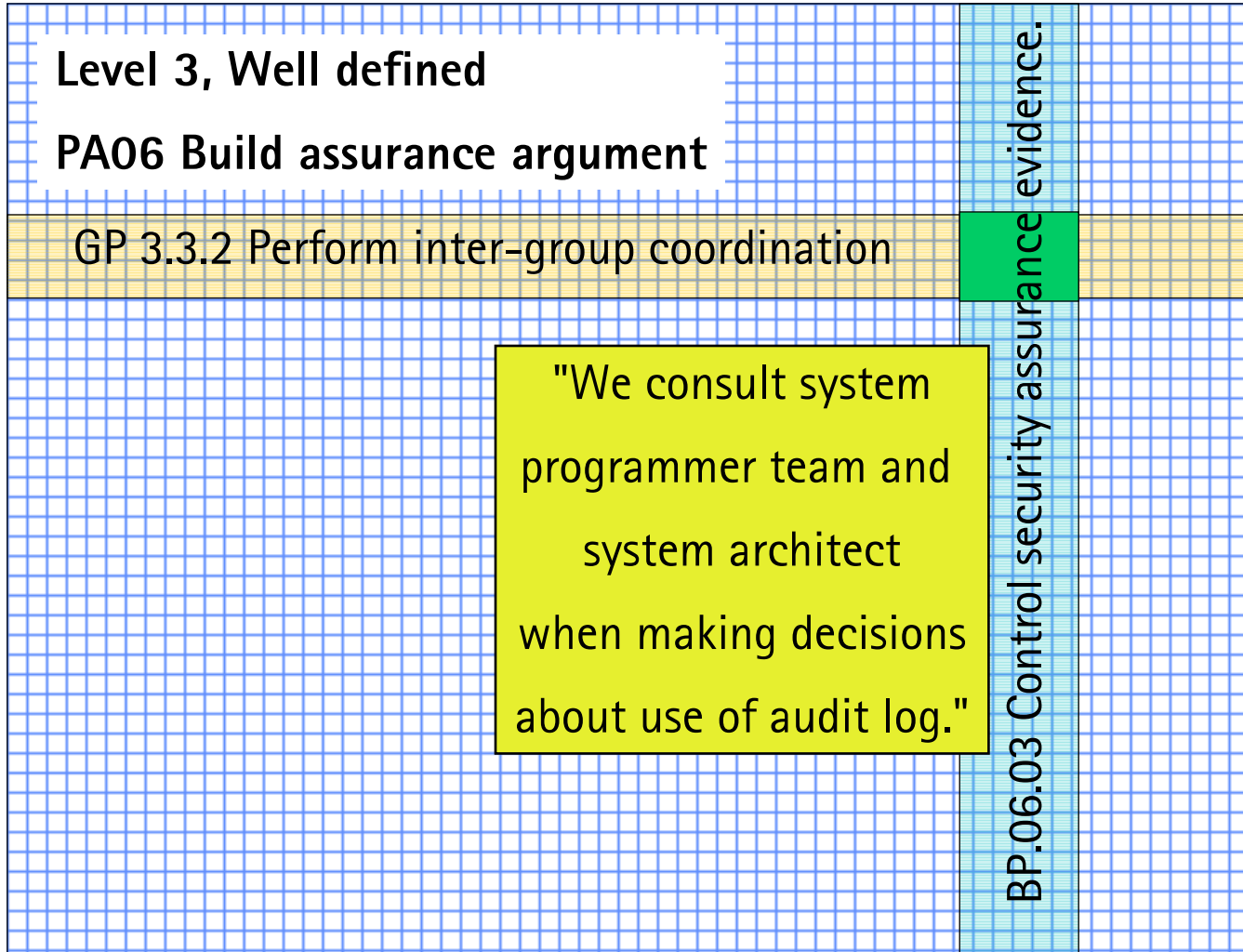
- 👉 Level 5, Continuously improving
- 😊 Level 4, Quantitatively controlled
- 😊 Level 3, Well defined
- 😊 Level 2, Planned and tracked
- 😊 Level 1, Performed informally
- 😐 Level 0, Not performed

# Generic and base practises



# Generic and base practises

Capability dimension - generic practises



Domain dimension - base practises

# BP.06.03 Control assurance evidence

## Example work products

- Security assurance evidence repository as database, engineering notebook, test report, evidence log.
  - Store of all evidence generated during development, testing, and use.
  - Assurance evidence work products can be developed from the system, architecture, design, implementation, engineering process, physical development environment, and physical operational environment.
- ▶ Plans, standards (CP 2.2.1) and cooperation (CP 3.3.2) are needed when performing this base practise in planned and defined way.

# BP.13.04 Control changes

## Example work products

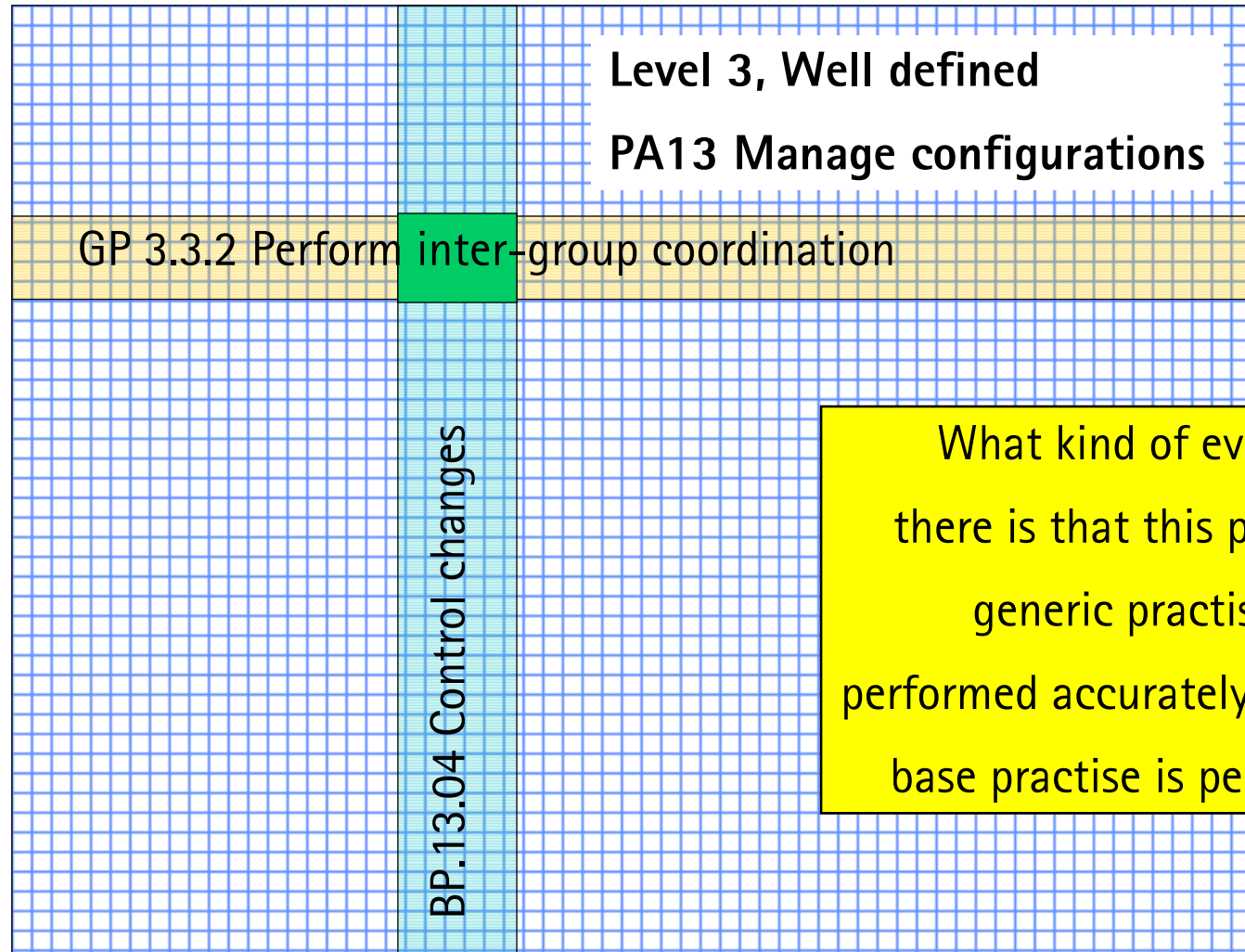
- New work-product baselines.
- Change control mechanisms can be tailored to categories of changes. For example, the approval process should be shorter for component changes that do not affect other components.



- ▶ Plans, standards (CP 2.2.1) and cooperation (CP 3.3.2) are needed when performing also this base practise in planned and defined way.

# BP.13.04 Control changes

Capability dimension - generic practises



What kind of evidence there is that this particular generic practise is performed accurately when this base practise is performed?

Domain dimension - base practises

# Assessing security

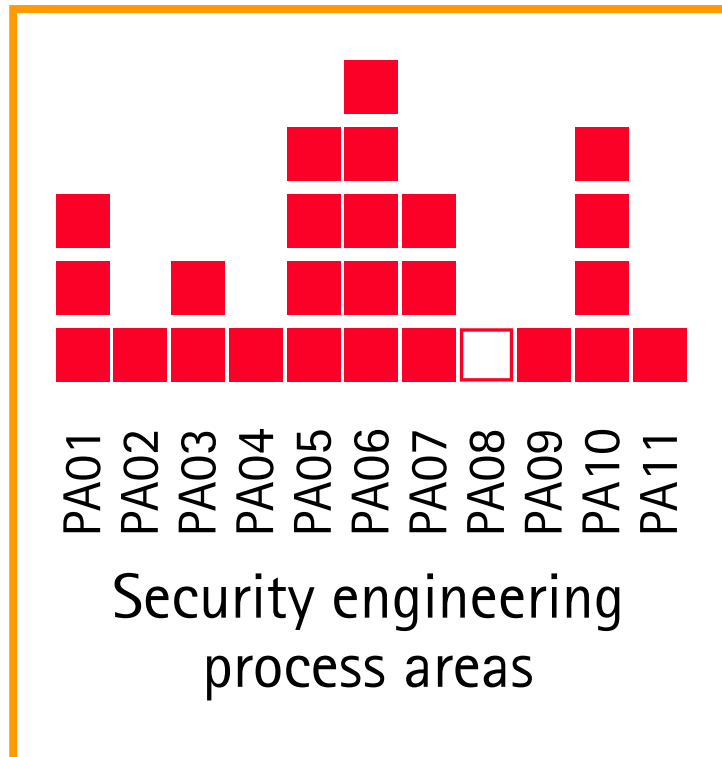
- Matureness of product process can be studied by using existing standard product process models like SSE-CMM.
- Security awareness of product process is reflected in its maturity.
- It is taken as granted that more mature product process is more capable to implement secure enough products.
- Product deliverables themselves and the way they are operated can be assessed by using standard product security guidelines like Common Criteria's protection profiles for given product family or BS7799 for operational security.

# Process capability matrix

Capability matrix is gathered by studying current working environment. It shows on what level organization is at which process area.

Capability level

Level 5  
Level 4  
Level 3  
Level 2  
Level 1



# Process capability matrix

- Process capability matrix is produced by going through all base practises and refering them to generic practises.
- To help assesment there is example work products listed for each base practise.
- Fulfillment of maturity level demands is decided for each base practise. Process area's maturity can be reasoned from that study.

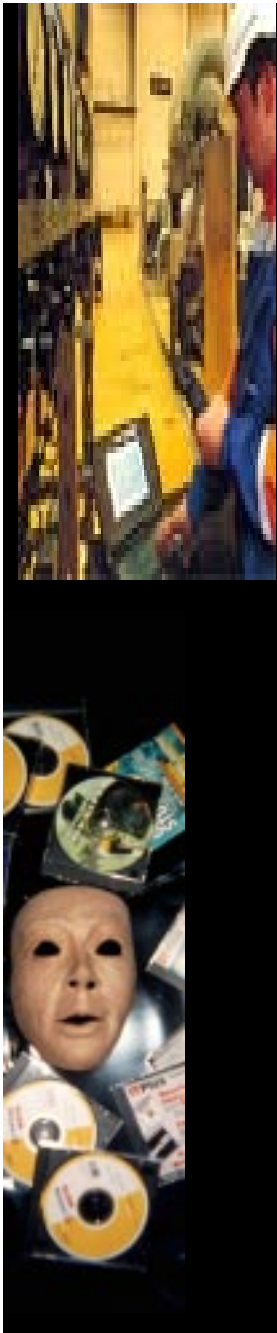
▶ Matrix can be used also for defining renovations in product process by stating the desired maturity level for target process area. Base practise and generic practise lists are studied to figure out wanted changes in current working mode.

# Assurance argumentation with SSE-CMM

- Confidence is based on the maturity of processes: capability-based assurance.
- Claim that could be based on SSE-CMM evidence: security engineering organization's process is mature.
- Claim's subject, the process, is broken down by the SSE-CMM into security-relevant process areas.
- Maturity is broken down into various properties related to maturity: planned, tracked, defined, coordinated, measured, controlled, and improving.
- Model suggests evidence for supporting these attributes as example work products of base practises and
- SSE-CMM appraisal method is defined.

# Applicability of SSE-CMM

- SSE-CMM can be adopted as guideline when implementing product process for tele- and datacommunication network elements and equipments.
- SSE-CMM appraisal method (SSAM) can be used to evaluate the capability of organization to perform engineering activities - especially systems security engineering activities.
- SSAM can be used to evaluate the processes of product developers, service providers, system integrators, system administrators, and security specialists.
- SSAM can be used to obtain a baseline or benchmark of actual practices against standards detailed in SSE-CMM.



# Conclusions

- Well managed product process produces deliverables which satisfy customer's needs.
- Features for fulfilling the customer's security needs are built in the deliverable.
- Design for security covers all product process phases from pre-study to maintenance and product withdrawal.
- SSE-CMM model gives guidelines for implementing a security aware product process.
- There exists facilitators for SSE-CMM's successful application.



# Business impact

- Impacts of changes must show in revenues
- Impact may be straight
  - Losses diminish
  - Secure product sells better
  - Working process is more effective in figures
- Impact may be implicit
  - Customer satisfaction rises
  - Quality complies better with business target
  - Working environment is more secure and safe

*"Cash rules."*

# Management's points of view

Posner, B.Z., Schimdt, W.H., Values and the American Manager: An Update, Californian Management Review, Spring, 1984

- Executives ranked their goals in order of importance as follows
  1. Organizational effectiveness
  2. High productivity
  3. Good organizational leadership
  4. High morale
  5. Good organizational reputation
  6. High organizational efficiency
  7. Profit maximation
  8. Organizational growth
  9. Organizational stability
  10. Value to local community
  11. Service to the public

*Exercise:*

How does investments  
in security and quality  
relate to this preference list?

# Process itself does not assure quality work

- CMM level improvement accounts 11% increase of productivity.
- Mature processes benefit larger projects more than small ones.
- In average project of 100'000 lines of code human factors influence productivity more than process.
- Critical to quality human characteristics are requirement analysts' capability, programmer's capability, personnel continuity, communication factors, analysts' experience, and programming language and tool experience.

See details at

B.Clark, "Quantifying the Effect of Process Improvement", IEEE Software, Vol. 17, No. 6, Nov./Dec. 2000, pp. 65-70.

- Investments in competence development and personnel management are keys to success.

# References



■ Systems security engineering capability maturity model

[www.sse-cmm.org](http://www.sse-cmm.org)

■ Software process improvement with CMM

Joseph Raynus, 198 pages, Artech House, 1999

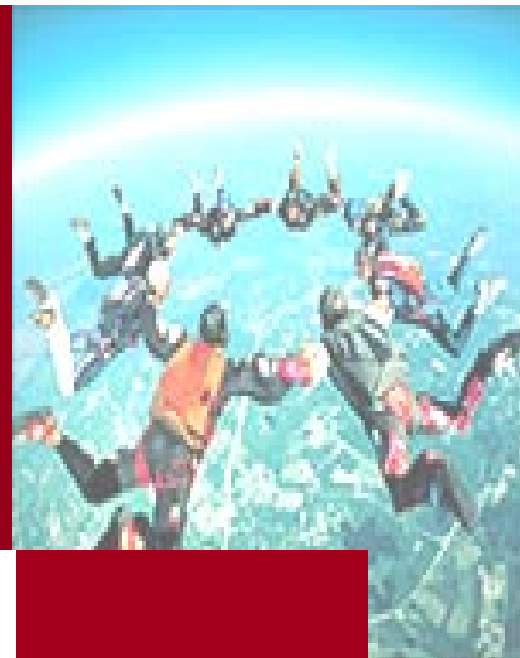
■ SSE-CMM appraisal method

[www.sse-cmm.org](http://www.sse-cmm.org)

■ A practical approach to improving and communicating assurance, Jeffrey Williams

[www.sse-cmm.org/librarie.htm](http://www.sse-cmm.org/librarie.htm)

# About authors



- ▶ Aaro Hallikainen, Nokia Networks, R&D, external protocols group, M.Sc., CISSP.
  - ▶ System programming since 1981.
  - ▶ Former assistant professor in Research and Training Center of Helsinki University.
  - ▶ 1996 to Nokia Networks at Information Systems and Software Engineering Department.
- ▶ Sami Masalin, Nokia Networks, product security coordinator, M.Sc., aspirant CISSP.
  - ▶ Information system security test planning and execution at Nokia since 1999.
  - ▶ Security process and security management development since 2000.
  - ▶ Master's thesis at Lappeenranta University of Technology on information system security management.
- ▶ Slide set can be freely used for security awareness training - authors appreciate your informing them about your use of this piece of work.

*Have a secure day!*