



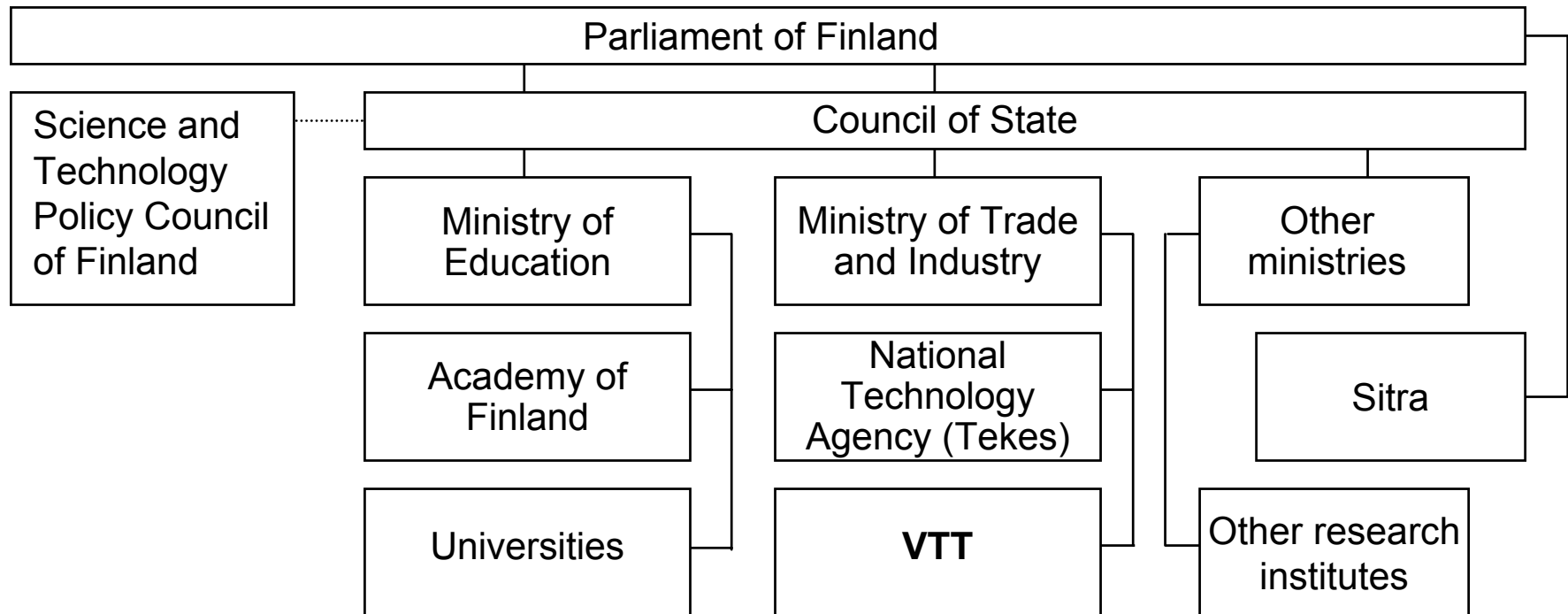
Experiences in developing software reliability management in Finnish industry

SIPI61508
Olli Ventä 11.6.2003

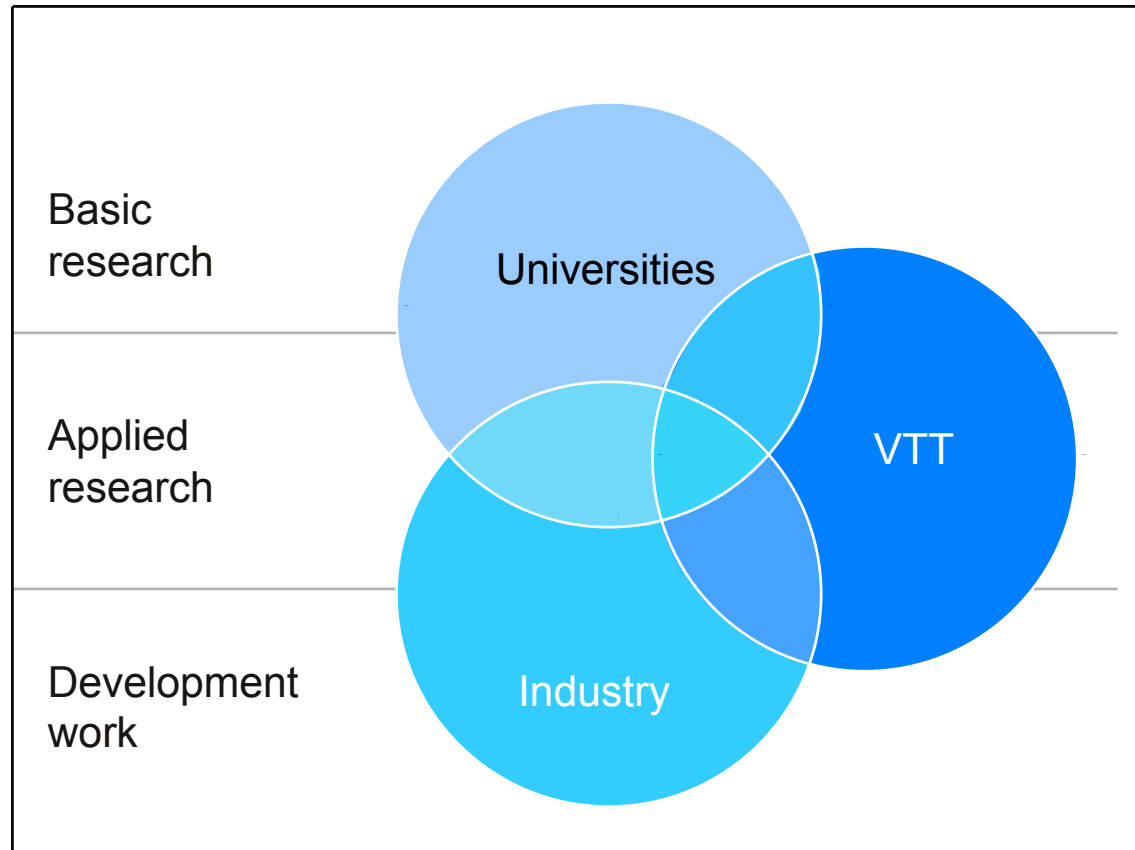


WHAT IS VTT?

THE MOST IMPORTANT DECISION MAKERS, FINANCERS AND PERFORMERS OF RESEARCH IN THE PUBLIC SECTOR



STATUS AS PERFORMER OF RESEARCH AND DEVELOPMENT WORK



WAY OF ACTION

- VTT directs and develops its activities in close interaction with industry, research institutes and universities, as well as government authorities responsible for coordinating technology policy and the financing of R&D.
- VTT operates in accordance with Finland's technology, industrial and energy policies, and plays an active role in their formulation.
- In fulfilling its mission, the primary role of VTT's research institutes is to carry out research and development work, technology transfer and testing. R&D work is performed as projects.
- VTT is a not-for-profit organization.

VTT IN BRIEF

Units:

VTT Electronics
VTT Information Technology
VTT Industrial Systems
VTT Processes
VTT Biotechnology
VTT Building and Transport

VTT Information Service
VTT Corporate Management
and Services

Staff: 3 012

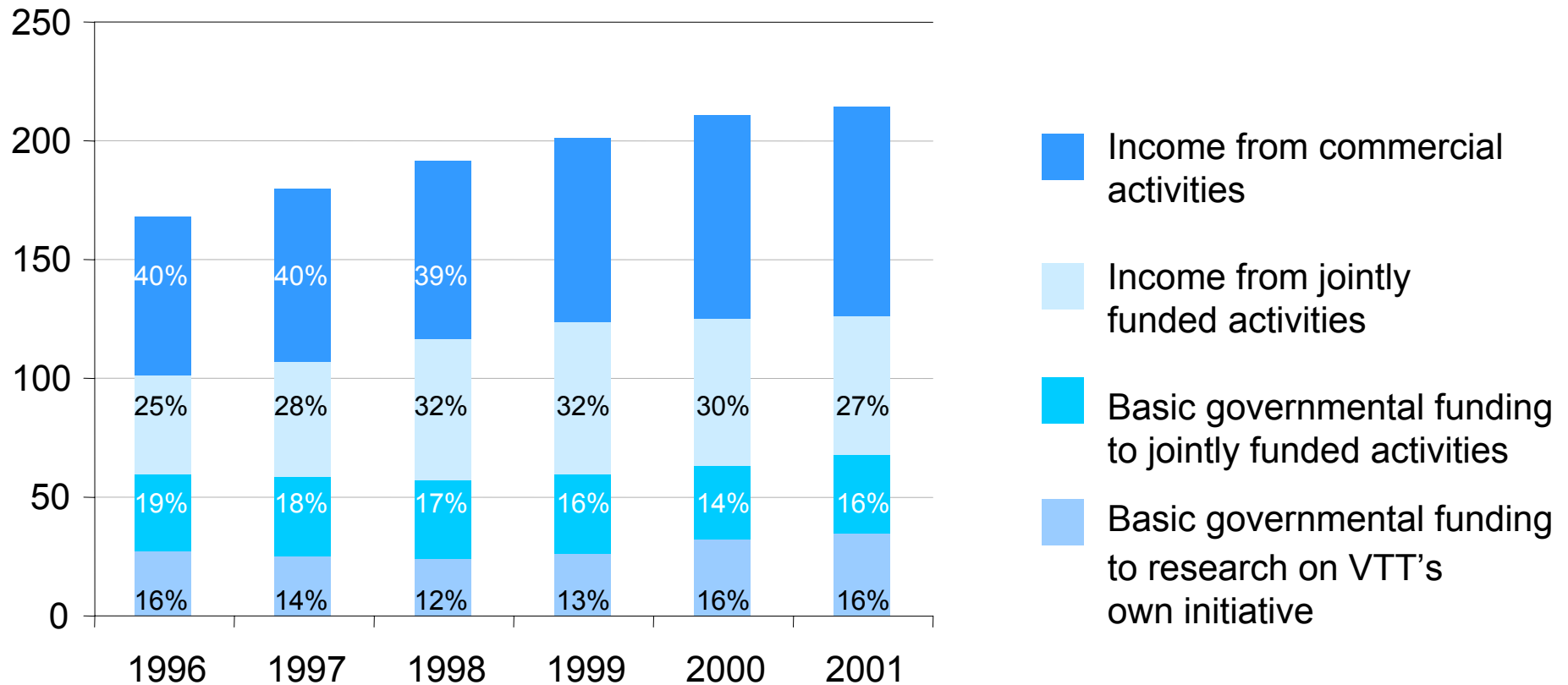
Turnover: 214 M€

- Basic govern. funding to research on VTT's own initiative 34 M€
- Jointly funded projects 92 M€
- Commercial activities 88 M€

Staff breakdown by location:

Oulu	323
Outokumpu	37
Jyväskylä	128
Tampere	332
Lappeenranta	12
Espoo	2 159
Others	21
<hr/>	
Total	3 012

VTT'S TURNOVER BY TYPE OF INCOME AND FUNDING

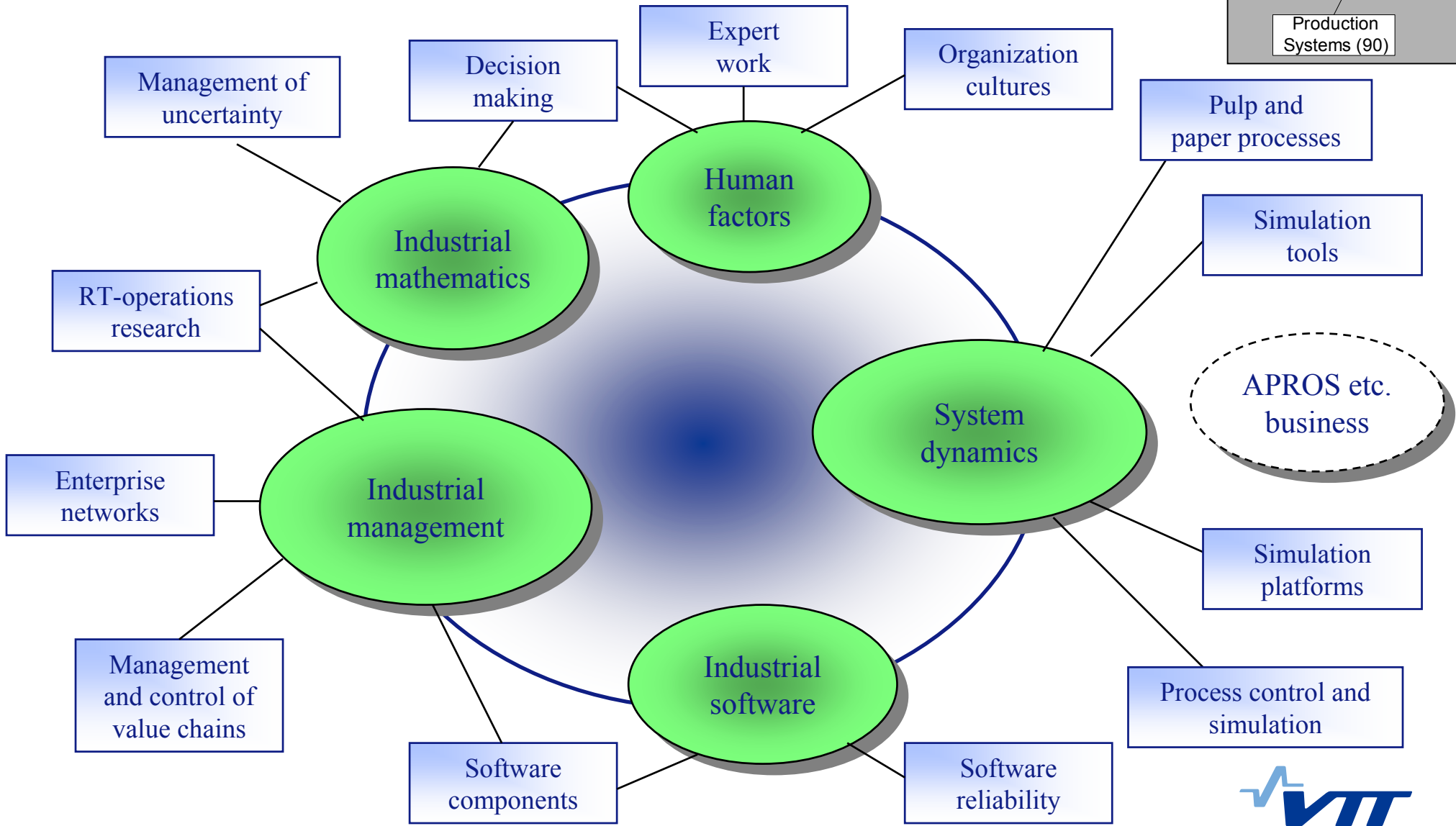


INDUSTRIAL SYSTEMS PRODUCTION SYSTEMS

Us at big VTT!

PRODUCTION SYSTEMS (about 90 people)

VTT (3000)
Industrial Systems (550)
Production Systems (90)



Software Reliability Research

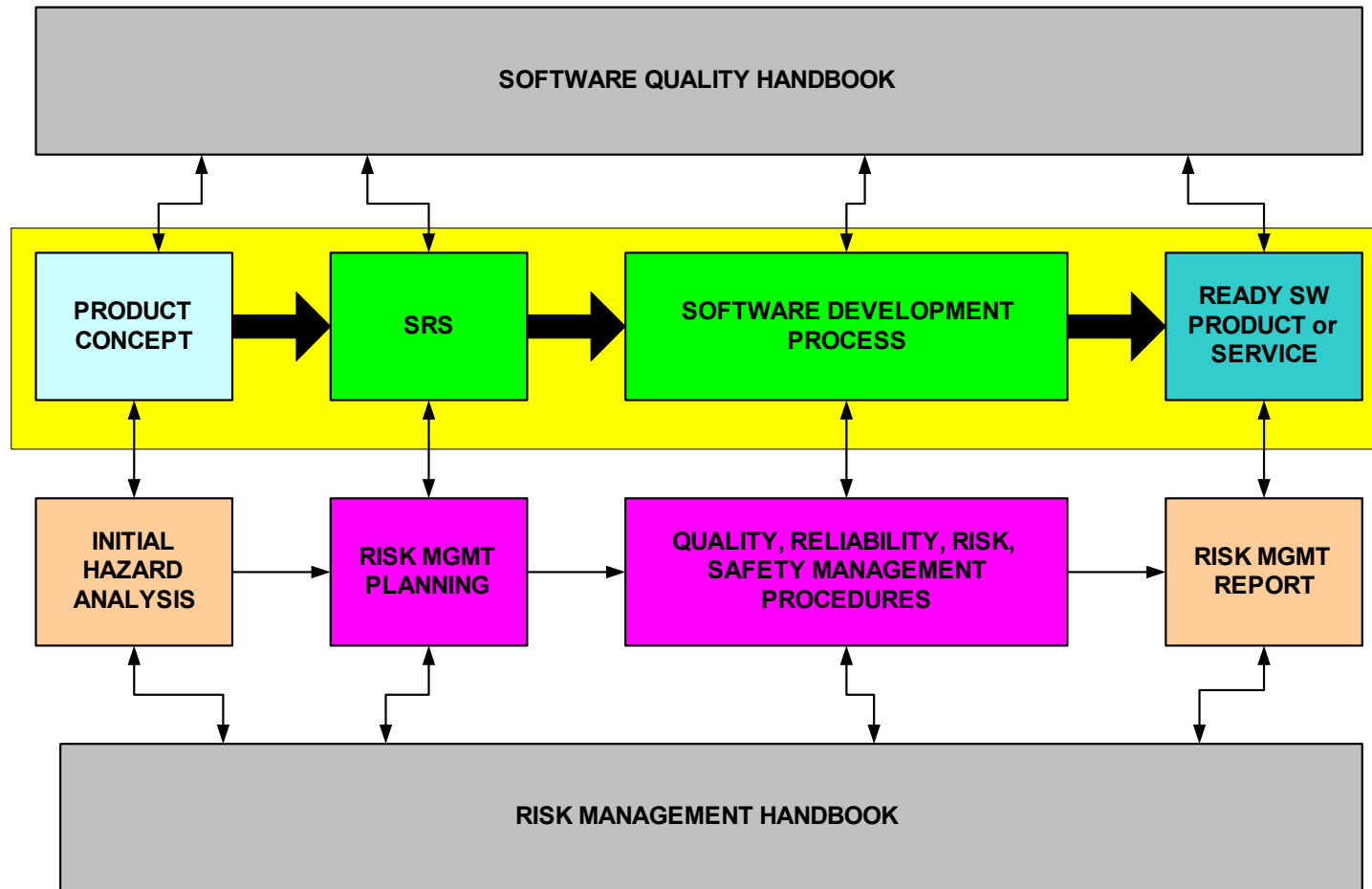
Software dependability application areas

- **Process industry**
 - authority procedures, independent assessments
 - verification, validation, and testing **integrated to development process**
 - dependability analyses, documented quality of software
 - **cost efficient** (company, product, or process specific)
- **Nuclear energy**
 - licencing/authority procedures, **independent assessments**
 - combining evidences, **Bayesian methods, statistical/probabilistic methods**, expert judgement, **safety critical software and PSA**
 - **requirements** engineering
 - validation of **human technology interaction**
 - **simulator aided automation V&V&T**
- **Medical devices**
 - verification, validation, and testing **integrated to sw-development process**
 - **authority procedures** (VTT notified body)
- **Space technology**
- **Military applications**
- **Telecommunications**
 - **statistical usage testing**
- **Software Engineering (current/future)**
 - issues on **component-based SE, COTS**
 - **integrated process development**
 - **qualitative and formal methods**
 - **cost-efficiency, just-right-reliability**
 - **dependability on business out/insourcing, business networks**
 - security

Project types

- **Basic research**
 - use of Bayesian Belief networks in combining and quantifying evidences
 - Human-System-Interaction
- **Technology/methodology state-of-art reviews from various point-of-views**
 - nuclear, medical
 - various themes of dependability
- **Best practice guidebooks**
 - Laatu automaatioissa 2001 (Quality in Automation; in Finnish)
 - Medical devices
- **Consultancy of VVT techniques**
- **Consultancy of software reliability procedures and management**
- **Consultancy as (independent) assessors**
- **Simulator assisted automation testing**
- **Notified body**
 - Medical devices
- **Other types**

IMPLICIT FRAMEWORK



There are many things to do ...

Software Requirements Verification and Validation Process

- conduct a software traceability analysis - trace software requirements to system requirements (and vice versa) and check the relationships for accuracy, completeness, consistency, and correctness; check that allocation is appropriate and complete
- conduct a software requirements evaluation - evaluate the software requirements for accuracy, completeness, consistency, correctness, testability, and understandability; assess how well the software requirements accomplishes the system and software objectives; identify critical areas of software by assessing criticality of software requirements
- for individual requirements, measure completeness by verifying existence and correctness of defining properties: initiator of action, action, object of action, conditions, constraints, source, destination, mechanism, reason
- verify correctness and appropriateness of requirements and assertions for addressing the safety algorithms and the states and integrity of the system and responses to unfavorable results of assertions and that the operation of the assertions will not adversely impact system performance
- verify correctness and appropriateness of fault tolerance requirements and that their operation of the assertions will not adversely impact system performance
- conduct a software interface analysis - evaluate software requirements with hardware, user, operator and software interface requirements for accuracy, completeness, consistency, correctness, and understandability
- coordinate with system software test planning.

Software Design Verification and Validation Process

- conduct a software design traceability analysis - trace software design to software requirements, and vice versa, and check the relationships for accuracy, completeness, consistency, and correctness
- conduct a software design evaluation - evaluate the software design for accuracy, completeness, consistency, correctness, and testability; evaluate design for compliance with software design standards (and, if appropriate, language standards) and software engineering practices; assess software design against assigned quality attributes
- conduct a software design interface analysis - evaluate software design with hardware, operator and software interface requirements for accuracy, completeness, consistency, and correctness
- verify that requirements for assertions, responses to assertions and other required system algorithm and integrity checks or fault tolerance protections have been designed into the software and are complete and accurate and will not adversely affect system performance
- apply software error, measurement, and statistical analysis techniques
- coordinate with software integration test planning.

Code Verification and Validation Process

- conduct a source code traceability analysis - trace source code to software design, and vice versa, and check the relationships for accuracy, completeness, consistency, and correctness
- conduct a source code evaluation - evaluate the source code for accuracy, completeness, consistency, correctness, and testability; evaluate source code for compliance with code standards (and, if appropriate, language standards) and software engineering practices; assess source code against assigned quality attributes
- conduct a source code interface analysis - evaluate the source code with hardware, operator, and software interfaces for accuracy, completeness, consistency, and correctness
- apply software error, measurement, and statistical analysis techniques
- apply algorithm analysis and timing and sizing analysis techniques
- evaluate draft code-related documents (e.g., user manual, commentary within the code) with source code for completeness, consistency, and correctness
- coordinate with unit test.

INTEGRATED PROCESS

- **Fault Prevention techniques**

- formalisms & languages
- standards, guides
- project organization
- planning & assessing

- **Fault Tolerance techniques**

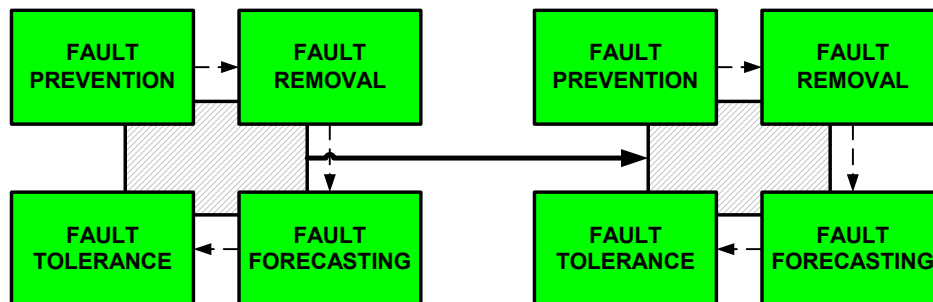
- behaviour in the presence of faults
- system partitioning (according to fault appearance)
- fault and error processing

- **Fault Removal techniques**

- verification (reviews, inspections, modeling & analysis, formal proofs, tests)
- diagnosis
- debugging & correction

- **Fault Forecasting techniques**

- objectives for dependability properties
- allocation of properties to architectural components
- evaluation (qualitative & quantitative)



... and there are many V&V&T techniques that can be applied

The challenge is to develop a **combination** of V&V&T methods that

- Serves its purpose (desired quality, SIL, ..., successful authority procedures)
- Integrates well to the existing software development process and culture
- is cost effective
- become accepted by R&D staff

Consultancy at developer/vendor

- **Identify licensing practices, rules etc. for the application area**
- **Identify company's base-line or starting point**
 - existing software development process
 - existing quality process
 - sample projects, products
- **Develop an integrated software development and quality or reliability process (combination of methods, tools, documentation)**
- **Select a representative pilot case(s)**
- **Try out**
 - proposed integrated process
 - let the customer R&D people do most of the pilot
- **Revise the process based on the experiences of the pilot**
- **Document the integrated process**
- **Iterate, extend**

What can cause trouble in such a project?

- **Identify licensing practices, rules etc. for the application area**
 - too many standards
 - unpredictable authority behaviour
- **Identify company's base-line or starting point**
 - it is difficult to identify any structured SWD process, lack of documentation, late documentation, no professional software development
 - due to recently tightened legislation there exist little no quality or V&V&T culture
- **Develop an integrated software development and quality or reliability process (combination of methods, tools, documentation)**
 - need to develop all of the above first
- **Select a representative pilot case(s)**
 - past R&D projects: not always appealing
 - current R&D projects: too much interference expected
- **Try out**
 - shortage of time and/or priority
 - no real commitment
- **Revise the process based on the experiences of the pilot**
 - shortage of time and/or priority
- **Document the integrated process**
- **Iterate, extend**

Experiences of Nuclear Industry

Nuclear Related Themes at VTT

- **Automation Systems**
 - distributed architectures, alarm management, exception handling, information technology for automation, user interfaces
- **Automation Design**
 - integrated plant model, design processes, degree of automation, information management, managing global manufacturing, process simulator aided activities (automation validation, operator training, ...), requirements engineering
- **Human Factors**
 - Operator training, Diagnosis and decision making during disturbances
 - Maintenance, repair and (ndt)testing.
 - Organization and management.
 - Validation on human technology interaction
- **Risk Analysis**
 - PSA methodology: Living PSA, low power PSA, Human Reliability Analysis (HRA).
 - Risk-informed management of ageing and maintenance.
 - Using PSA in decision making. Decision analysis. Use of expert judgement.
- **Software Dependability**
 - Verification, validation and testing integrated to the development process.
 - Licensing procedures
 - Combination and quantification of evidences from various sources
 - Statistical testing.
- **Simulation**
 - simulator aided automation V&V&T

Nuclear industry: R&D affected by large projects

- FIN5 project
 - invitation to tender, vendor selection by the end of 2003
 - permit to build: 2004
 - implementation: 2005...2008...
- I&C Modernization at Loviisa NPP: present + 10 yr
- I&C Modernization at Olkiluoto NPP: present + 10 yr
- SAFIR - Safety of nuclear power plants, Finnish national research programme, 2003-2006
- other national and international activities
 - HRP, EU, NKS, Tekes, ...

Nuclear industry: R&D issues related to I&C (1)

- **Requirements management**
 - SRS reengineering at old plants
 - quality of SRS
 - theories, tools, methods, guides, standards exist; but they are not always implemented properly in practice, for various reasons
- **Qualification, licensing**
 - rules, guides, codes under development, country-specific; also international harmonization efforts underway
 - need of success stories, models of fluent qualification!
 - COTS qualification
 - programmable field devices
 - type approvals, I&C related to PSA
 - nuclear specific safety requirements vs. industry proven/qualified technologies

Nuclear industry: R&D issues related to I&C (2)

- **Evaluation of technical solutions proposed for safety critical applications**
 - comparison
 - effect of safety, reliability etc.
- **Information systems at NPPs**
 - adaptation and validation to NPP use
 - licensing
- **Human interfaces, monitoring**
 - criteria for good?
 - User needs.....SRS.....V&V.....user acceptance
 - concepts, tools, technologies and their effect to human performance
 - new plant, gradual modernization
 - licensing

Nuclear industry: R&D issues related to I&C (3)

- **HW aging**
 - new directives
 - new materials, technologies
- **Old & young generations**
 - knowledge transfer and representation
 - recruiting and education into profession

Other remarks

- Software reliability obtains attention when it is a must (there is legislation or authority)
 - direct effect
 - indirect effect
- Mainstream software industry adopts software dependability
 - slowly
 - not part of ICT education
 - lack of established software engineering profession

61508 is a huge document - still simple things in a (small) company help a lot

Write down

- how are projects managed
- who is responsible for various tasks/activities
- what documentation is needed
- what standards are to be followed
- inspections: what, how
- how are problems traced and solved
- what tools are used
- what methods are used
- code and media management
- document management
- risk management
- use templates
- use check lists