Sociotechnical Systems

WK 8

System procurement

- Acquiring a system (or systems) to meet some identified organizational need.
- Before procurement, decisions are made on:
  - Scope of the system
  - System budgets and timescales
  - High-level system requirements
- Based on this information, decisions are made on whether to procure a system, the type of system and the potential system suppliers.

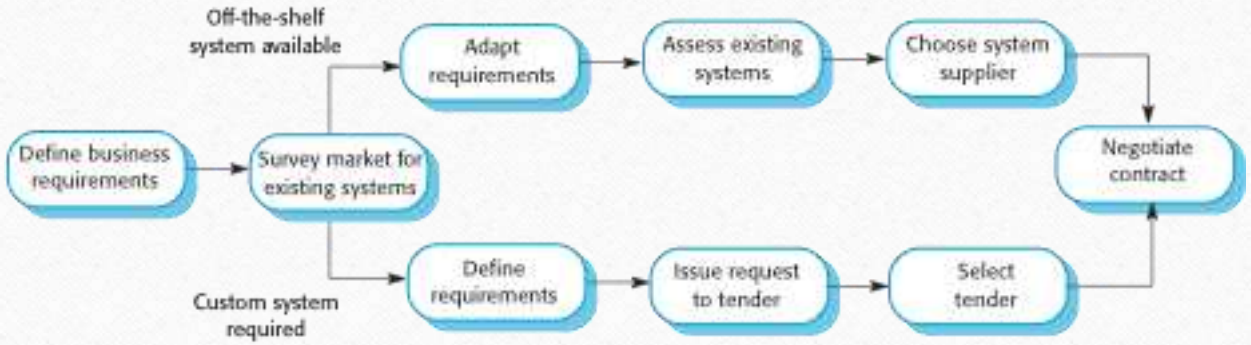
Decision drivers

- The state of other organizational systems
- The need to comply with external regulations
- External competition
- Business re-organization
- Available budget

Procurement and development

- Some system specification and architectural design is usually necessary before procurement
  - You need a specification to let a contract for system development
  - The specification may allow you to buy a commercial off-the-shelf (COTS) system. Almost always cheaper than developing a system from scratch
- Large complex systems usually consist of a mix of off the shelf and specially designed components. The procurement processes for these different types of component are usually different.

System procurement processes



Procurement issues

- Requirements may have to be modified to match the capabilities of off-the-shelf components.
- The requirements specification may be part of the contract for the development of the system.
- There is usually a contract negotiation period to agree changes after the contractor to build a system has been selected.

Contractors and sub-contractors

- The procurement of large hardware/software systems is usually based around some principal contractor.
- Sub-contracts are issued to other suppliers to supply parts of the system.
- Customer liases with the principal contractor and does not deal directly with sub-contractors.

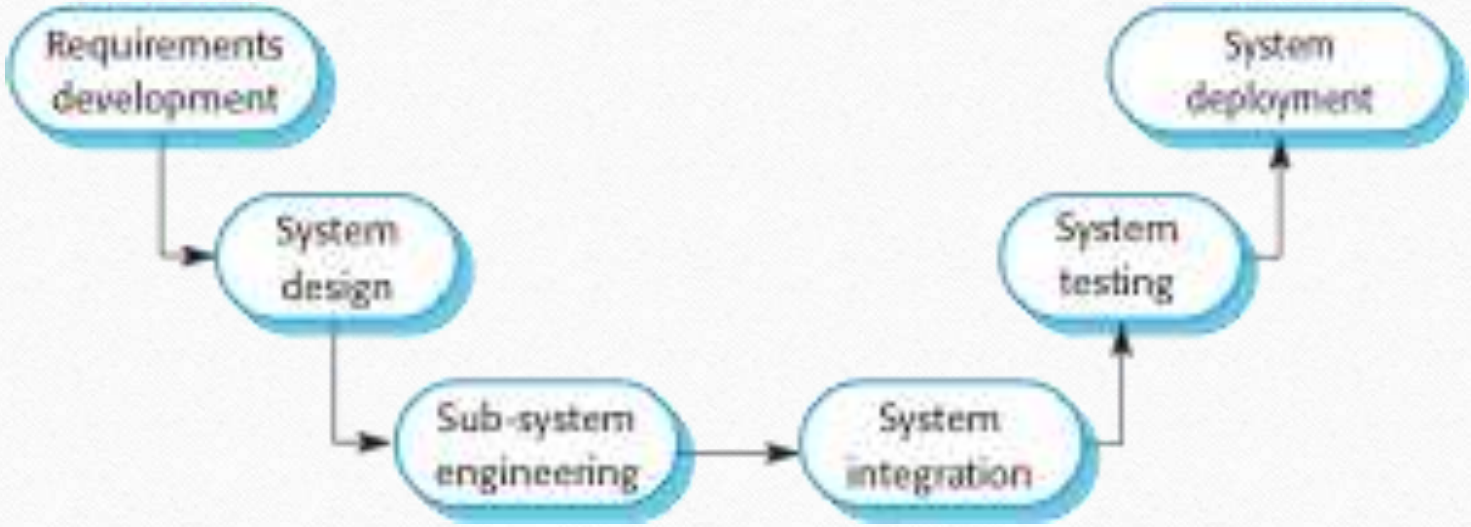
Procurement and dependability

- Procurement decisions have profound effects on system dependability as these decisions limit the scope of dependability requirements.
- For an off-the-shelf system, the procurer has very limited influence on the security and dependability requirements of the system.
- For a custom system, considerable effort has to be expended in defining security and dependability requirements.

System development

- Usually follows a plan-driven approach because of the need for parallel development of different parts of the system
  - Little scope for iteration between phases because hardware changes are very expensive. Software may have to compensate for hardware problems.
- Inevitably involves engineers from different disciplines who must work together
  - Much scope for misunderstanding here.
  - As explained, different disciplines use a different vocabulary and much negotiation is required. Engineers may have personal agendas to fulfil.

Systems development



System requirements definition

- Three types of requirement defined at this stage
  - Abstract functional requirements. System functions are defined in an abstract way;
  - System properties. Non-functional requirements for the system in general are defined;
  - Undesirable characteristics. Unacceptable system behaviour is specified.
- Should also define overall organisational objectives for the system.

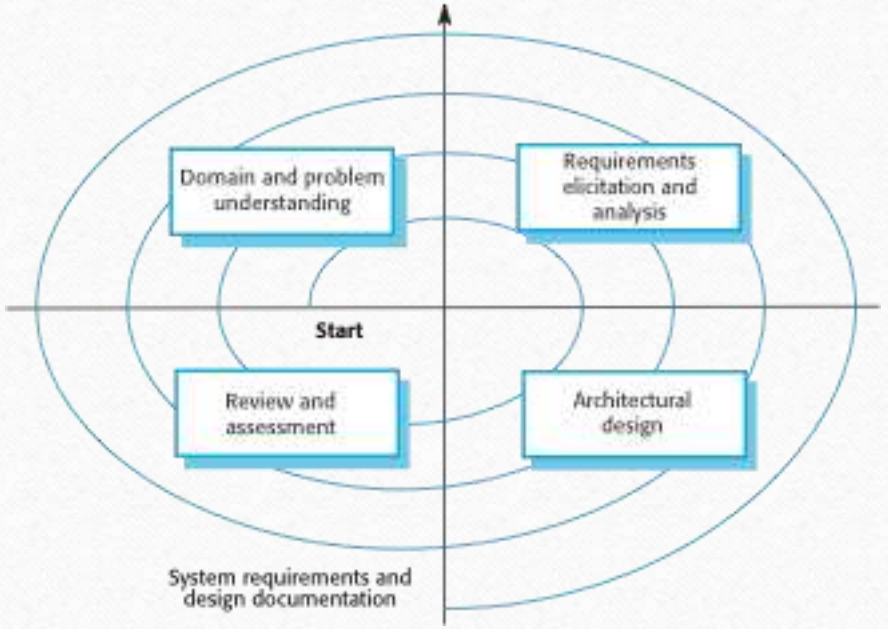
The system design process

- Partition requirements
  - Organise requirements into related groups.
- Identify sub-systems
  - Identify a set of sub-systems which collectively can meet the system requirements.
- Assign requirements to sub-systems
  - Causes particular problems when COTS are integrated.
- Specify sub-system functionality.
- Define sub-system interfaces
  - Critical activity for parallel sub-system development.

Requirements and design

- Requirements engineering and system design are inextricably linked.
- Constraints posed by the system's environment and other systems limit design choices so the actual design to be used may be a requirement.
- Initial design may be necessary to structure the requirements.
- As you do design, you learn more about the requirements.

Requirements and design spiral



Sub-system development

- Typically parallel projects developing the hardware, software and communications.
- May involve some COTS (Commercial Off-the-Shelf) systems procurement.
- Lack of communication across implementation teams can cause problems.
- There may be a bureaucratic and slow mechanism for proposing system changes, which means that the development schedule may be extended because of the need for rework.

System integration

- The process of putting hardware, software and people together to make a system.
- Should ideally be tackled incrementally so that sub-systems are integrated one at a time.
- The system is tested as it is integrated.
- Interface problems between sub-systems are usually found at this stage.
- May be problems with uncoordinated deliveries of system components.

System delivery and deployment

- After completion, the system has to be installed in the customer's environment
  - Environmental assumptions may be incorrect;
  - May be human resistance to the introduction of a new system;
  - System may have to coexist with alternative systems for some time;
  - May be physical installation problems (e.g. cabling problems);
  - Data cleanup may be required;
  - Operator training has to be identified.

Development and dependability

- Decisions are made on dependability and security requirements and trade-offs made between costs, schedule, performance and dependability.
- Human errors may lead to the introduction of faults into the system.
- Testing and validation processes may be limited because of limited budgets.
- Problems in deployment mean there may be a mismatch between the system and its operational environment.

System operation

- Operational processes are the processes involved in using the system for its defined purpose.
- For new systems, these processes may have to be designed and tested and operators trained in the use of the system.
- Operational processes should be flexible to allow operators to cope with problems and periods of fluctuating workload.

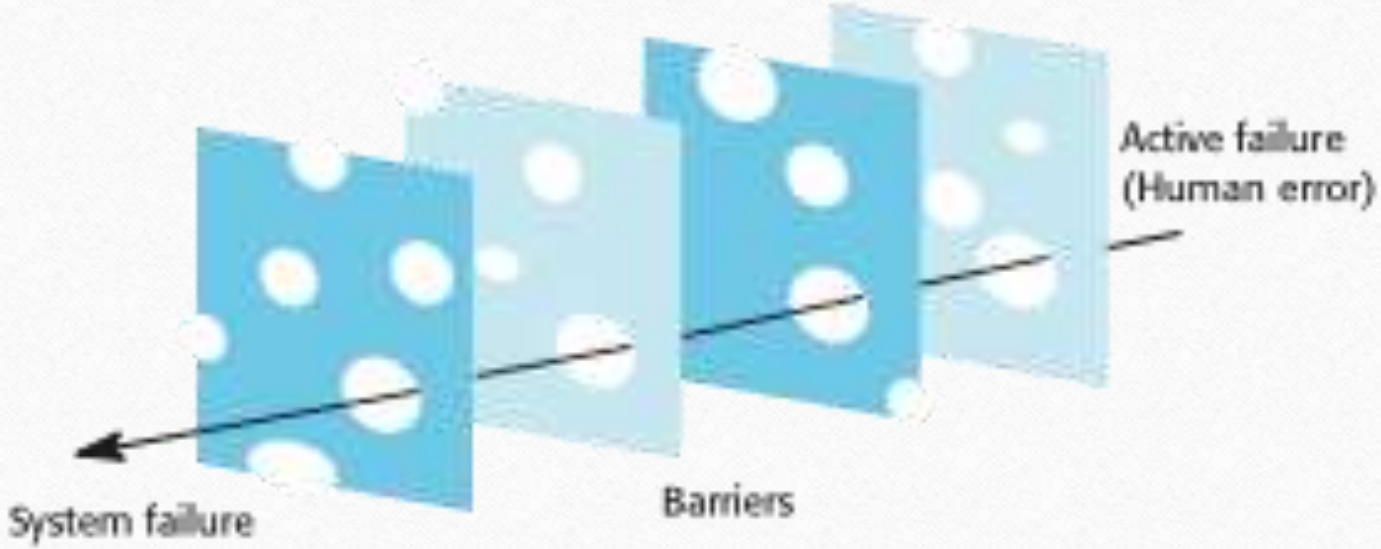
Human error

- Human errors occur in operational processes that influence the overall dependability of the system.
- Viewing human errors:
  - The person approach makes errors the responsibility of the individual and places the blame for error on the operator concerned. Actions to reduce error include threats of punishment, better training, more stringent procedures, etc.
  - The systems approach assumes that people are fallible and will make mistakes. The system is designed to detect these mistakes before they lead to system failure. When a failure occurs, the aim is not to blame an individual but to understand why the system defenses did not trap the error.

System defenses

- To improve security and dependability, designers should think about the checks for human error that should be included in a system.
- As I discuss in later lectures, there should be multiple (redundant) barriers which should be different (diverse)
- No single barrier can be perfect.
  - There will be latent conditions in the system that may lead to failure.
- However, with multiple barriers, all have to fail for a system failure to occur.

Reason's Swiss cheese model of system failure



Defenses in an ATC system

- Conflict alert system
  - Raises an audible alarm when aircraft are on conflicting paths
- Recording of instructions
  - Allows instructions issues to be reviewed and checked.
- Sharing of information
  - The team of controllers cross-check each other's work.

System evolution

- Large systems have a long lifetime. They must evolve to meet changing requirements.
- Evolution is inherently costly
  - Changes must be analysed from a technical and business perspective;
  - Sub-systems interact so unanticipated problems can arise;
  - There is rarely a rationale for original design decisions;
  - System structure is corrupted as changes are made to it.
- Existing systems which must be maintained are sometimes called legacy systems.

Evolution and dependability

- Changes to a system are often a source of problems and vulnerabilities.
- Changes may be made without knowledge of previous design decisions made for security and dependability reasons.
  - Built-in safeguards may stop working.
- New faults may be introduced or latent faults exposed by changes.
  - These may not be discovered because complete system retesting is too expensive.

Key points

- System procurement covers all of the activities involved in deciding what system to buy and who should supply that system.
- System development includes requirements specification, design, construction, integration and testing.
- When a system is put into use, the operational processes and the system itself have to change to reflect changing business requirements.
- Human errors are inevitable and systems should include barriers to detect these errors before they lead to system failure.