Sociotechnical Systems

Socio-technical systems include technical systems plus people who use and manage these systems and the organizations that own the systems and set policies for their use. Business systems, command and control systems, etc.

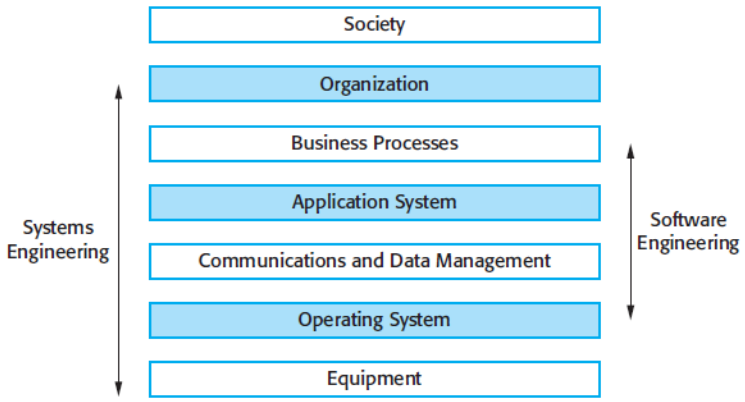


Figure 10.1 The sociotechnical systems stack

Sociotechnical systems are so complex that it is practically impossible to understand them as a whole. Rather, you have to view them as layers, as shown in Figure 10.1. These layers make up the sociotechnical systems stack:

1. *The equipment layer* This layer is composed of hardware devices, some of which may be computers.
2. *The operating system layer* This layer interacts with the hardware and provides a set of common facilities for higher software layers in the system.
3. *The communications and data management layer* This layer extends the operating system facilities and provides an interface that allows interaction with more extensive functionality, such as access to remote systems, access to a system database, etc. This is sometimes called middleware, as it is in between the application and the operating system.
4. *The application layer* This layer delivers the application-specific functionality that is required. There may be many different application programs in this layer.
5. *The business process layer* At this level, the organizational business processes, which make use of the software system, are defined and enacted.
6. *The organizational layer* This layer includes higher-level strategic processes as well as business rules, policies, and norms that should be followed when using the system.
7. *The social layer* At this layer, the laws and regulations of society that govern the operation of the system are defined.

A system is a purposeful collection of interrelated components, of different kinds, which work together to achieve some objective.

Systems that include software fall into two categories:

- **Technical computer-based systems** include hardware and software but not humans or organizational processes. Off the shelf applications, control systems, etc.
- **Socio-technical systems** include technical systems plus people who use and manage these systems and the organizations that own the systems and set policies for their use. Business systems, command and control systems, etc.

Sociotechnical systems have three characteristics that are particularly important when considering security and dependability:

- **Emergent properties:** Properties of the system of a whole that depend on the system components and their relationships.
- **Non-deterministic:** They do not always produce the same output when presented with the same input because the system's behavior is partially dependent on human operators.
- **Complex relationships with organizational objectives:** The extent to which the system supports organizational objectives does not just depend on the system itself.

Examples of emergent properties

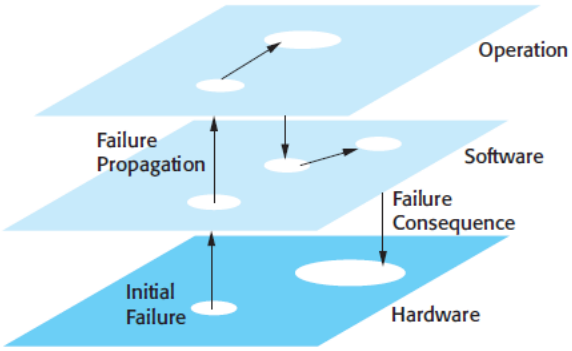
Property	Description
Volume	The volume of a system (the total space occupied) varies depending on how the component assemblies are arranged and connected.
Reliability	System reliability depends on component reliability but unexpected interactions can cause new types of failures and therefore affect the reliability of the system.
Security	The security of the system (its ability to resist attack) is a complex property that cannot be easily measured. Attacks may be devised that were not anticipated by the system designers and so may defeat built-in safeguards.
Repairability	This property reflects how easy it is to fix a problem with the system once it has been discovered. It depends on being able to diagnose the problem, access the components that are faulty, and modify or replace these components.
Usability	This property reflects how easy it is to use the system. It depends on the technical system components, its operators, and its operating environment.

System reliability is a good example of an emergent property. Because of component inter-dependencies, faults can be propagated through the system. System failures often occur because of unforeseen inter-relationships between components. It is practically impossible to anticipate all possible component relationships. Software reliability measures may give a false picture of the overall system reliability.

System reliability is influenced by:

- **Hardware reliability:** What is the probability of a hardware component failing and how long does it take to repair that component?
- **Software reliability:** How likely is it that a software component will produce an incorrect output. Software failure is usually distinct from hardware failure in that software does not wear out.
- **Operator reliability:** How likely is it that the operator of a system will make an error?

Failures are not independent and they propagate from one level to another.



System reliability depends on the context where the system is used. A system that is reliable in one environment may be less reliable in a different environment because the physical conditions (e.g. the temperature) and the mode of operation is different.

Systems engineering

Systems engineering encompasses all of the activities involved in procuring, specifying, designing, implementing, validating, deploying, operating, and maintaining sociotechnical systems. Systems engineers are not just concerned with software but also with hardware and the system's interactions with users and its environment. They must think about the services that the system provides, the constraints under which the system must be built and operated, and the ways in which the system is used to fulfill its purpose or purposes.

There are three overlapping stages (Figure 10.4) in the lifetime of large and complex sociotechnical systems:

1. *Procurement or acquisition* During this stage, the purpose of a system is decided; high-level system requirements are established; decisions are made on how functionality will be distributed across hardware, software, and people; and the components that will make up the system are purchased.
2. *Development* During this stage, the system is developed. Development processes include all of the activities involved in system development such as requirements definition, system design, hardware and software engineering, system integration, and testing. Operational processes are defined and the training courses for system users are designed.
3. *Operation* At this stage, the system is deployed, users are trained, and the system is brought into use. The planned operational processes usually then have to change to reflect the real working environment where the system is used. Over time, the system evolves as new requirements are identified. Eventually, the system declines in value and it is decommissioned and replaced.

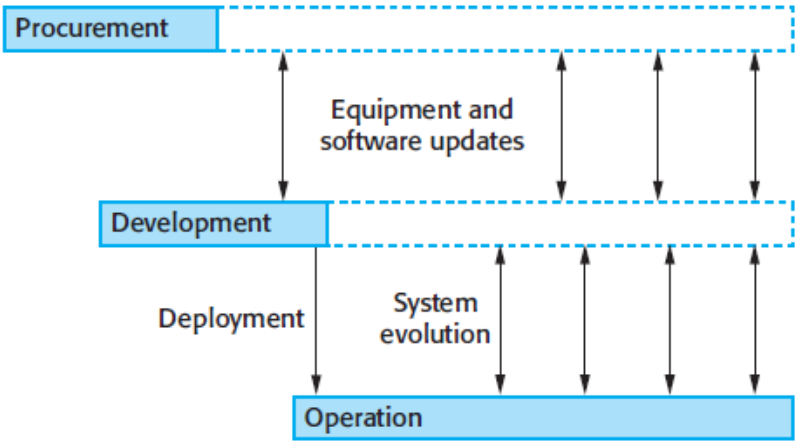


Figure 10.4 Stages of systems engineering

System procurement

The initial phase of systems engineering is system procurement (sometimes called system acquisition). At this stage, decisions are made on the scope of a system that is to be purchased, system budgets and timescales, and the high-level system requirements. Using this information, further decisions are then made on whether to procure a system, the type of system required, and the supplier or suppliers of the system. The drivers for these decisions are:

1. *The state of other organizational systems* If the organization has a mixture of systems that cannot easily communicate or that are expensive to maintain, then procuring a replacement system may lead to significant business benefits.
2. *The need to comply with external regulations* Increasingly, businesses are regulated and have to demonstrate compliance with externally defined regulations (e.g., Sarbanes-Oxley accounting regulations in the United States). This may require the replacement of noncompliant systems or the provision of new systems specifically to monitor compliance.
3. *External competition* If a business needs to compete more effectively or maintain a competitive position, investment in new systems that improve the efficiency of business processes may be advisable. For military systems, the need to improve capability in the face of new threats is an important reason for procuring new systems.
4. *Business reorganization* Businesses and other organizations frequently restructure with the intention of improving efficiency and/or customer service. Reorganizations lead to changes in business processes that require new systems support.
5. *Available budget* The budget available is an obvious factor in determining the scope of new systems that can be procured.

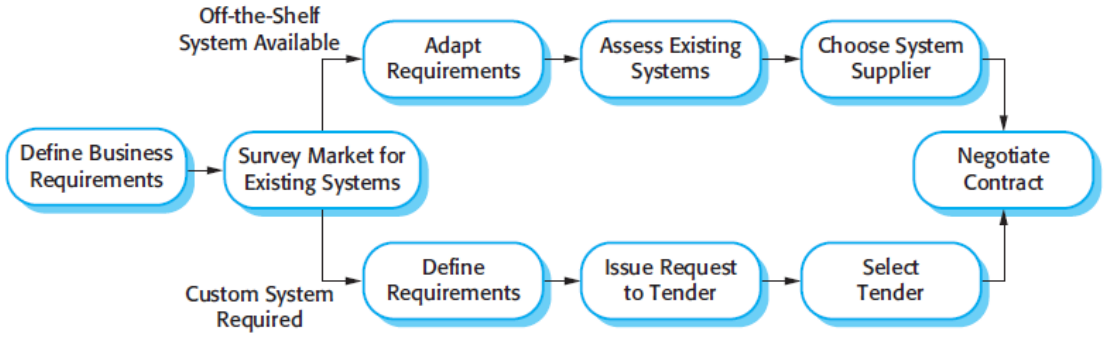


Figure 10.6 System procurement processes

System development

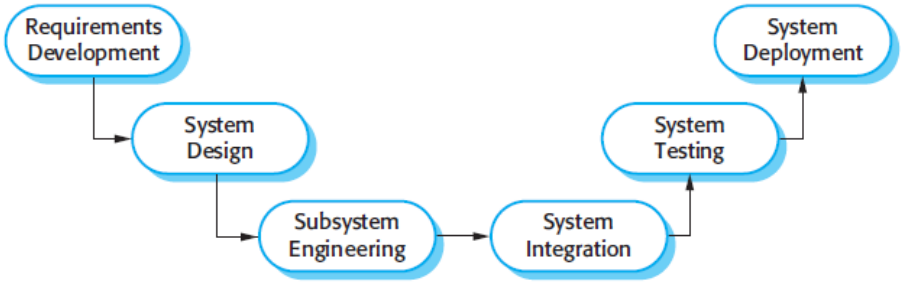


Figure 10.7 Systems development

The system development process:

- **Requirements engineering:** The process of refining, analyzing and documenting the high-level and business requirements identified in the conceptual design.
- **Architectural design:** Establishing the overall architecture of the system, identifying components and their relationships.
- **Requirements partitioning:** Deciding which subsystems (identified in the system architecture) are responsible for implementing the system requirements.
- **Subsystem engineering:** Developing the software components of the system, configuring off-the-shelf hardware and software, defining the operational processes for the system and re-designing business processes.
- **System integration:** Putting together system elements to create a new system.
- **System testing:** The whole system is tested to discover problems.
- **System deployment:** the process of making the system available to its users, transferring data from existing systems and establishing communications with other systems in the environment.