Ethical Issues in Systems Analysis & software engineering

CHAPTER -4

Systems Analysis & Design

Information technology has made a huge transformation in life. It isn't the technology itself that increases productivity and profits; however, it is the people who develop information systems solutions that make these benefits possible.

The key to successful development is thorough systems analysis and design to understand what the business requires from the information systems.

Who is Systems Analyst?

A business professional who uses analysis and design techniques to solve business problems by using information technology.

A systems analyst needs broad knowledge and a variety of

- Technical Knowledge and Skills
- Business Knowledge and Skills
- People Knowledge and Skills to develop information systems.

Systems analysis and design work is done by people with a variety of job titles—not only systems analyst but programmer analyst, systems consultant, systems engineer, and Web developer, among others.

Who is Software Engineer?

A **software engineer** is a person who applies the principles of **software engineering** to the design, development, maintenance, testing, and evaluation of the **software** that make computers or other devices containing **software** work.

Both professions are heavy technological positions, they are quite different and require different skill sets. If both were to work together, the software engineer would design and code an application while the system analyst would design and build the hardware to run the application.

Ethical Issues in Systems Analysis /Software Engineering

With the influence of computers on our life and the role of software in all the systems, software professionals have the power to do good or bad to the society.

The ethical problems faced by the system analyst or software engineer involve: the end product, the process of developing that product, and the human interactions in the development of the product.

Ethical Issues in Systems Analysis /Software Engineering

Fig. 1 Obligations of a Software Professional

The term ***ethical behaviour*** refers to how an individual or an organization ensures that all its **decisions, actions, and stakeholder interactions** conform to the individual's or organization's moral and professional principles.

These principles should support all applicable laws and regulations and are the foundation for the individual's or organization's culture and values. They define right from wrong.

Ethical Issues in Systems Analysis /Software Engineering

For example, if a project is running late, the project manager might be tempted to cut short the requirements definition phase, hoping to make up for some lost time. In order to get the product out the door, developers base their testing not on the requirements, but on developer descriptions of how their code will work. The team then delivers the result to the customer with possibly catastrophic consequences, such as an unusable product, contract cancellation, or lawsuits.

If a person who should know better makes wrong decisions, and if personal interests motivated those decisions, the behaviour becomes unethical.

Problems faced by a Systems Analyst/ Software Engineer

System is considered safe if it is impossible (or at least highly unlikely) that the software/hardware could ever produce an output that would cause a catastrophic event for the system that it controls.

Problems encountered by the SA/SE are:

Software Specification:

Most errors found in software can be traced to requirements shortages, above all their incompleteness. Software requirements specifications are complete if they can separate software "desirable" behaviour from unwanted program that we could get.

Problems faced by a Systems Analyst/ Software Engineer

Software Design:

When computer is used, usually a machine design is made by someone who is not expert on actual design. For example, expert on car-brakes design determines how brakes shall work, but then leaves the information to a programmer who is expert on software design but not on car-brakes design. The programmer then takes over and specifies brakes design. This extra communication step is the primary problem with software today.

Problems faced by a Systems Analyst/ Software Engineer

Extreme Pressure

- Extreme pressure that software companies feel to reduce the time to market for their products while compromising on the known bugs which are not being addressed at the right time.
- Resources and time needed to ensure quality are often cut under the pressure to ship a new product.

Problems faced by a Systems Analyst/ Software Engineer

Use of unauthorized software

- Using open-source code in their own code without properly crediting the source
- Using illegal software to perform their tasks.
- Difficult to maintain the software because of the use of illegal software

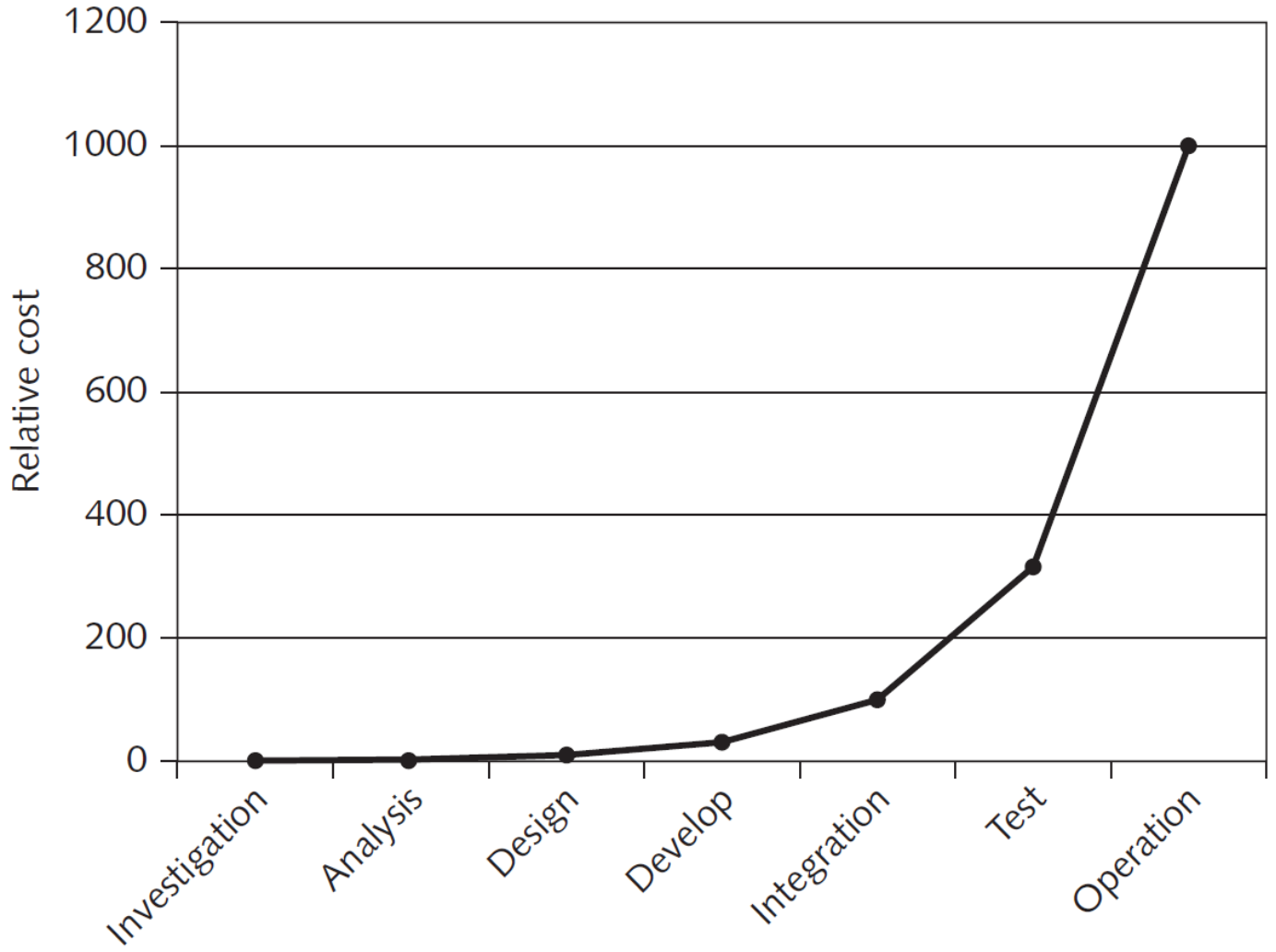
Problems faced by a Systems Analyst/ Software Engineer

Changes in software:

With changing software, it is not meant replacing a failed component by another working component.

Software maintenance refers to changes in the software design that are either intended to correct a fault or are in response to a change in the specification because the software does not perform as the user wishes. This is entirely different from the replacement of an item of failed hardware, which merely recovers the original system functionality. The removal of a software fault represents a change to the design of the system. There are many recorded examples of so-called small changes, that supposedly just fixing faults but caused serious reductions in reliability.

The Cost of Removing Software Defects



Source Line: Used with permission from LKP Consulting Group

Problems faced by a Systems Analyst/ Software Engineer

Insufficient and Incompetent Staff

- Inadequate or no project management methodology
- Bad planning and estimating
- Insufficient senior staff on the team

The software defects in certain systems can have deadly consequences. The stakes involved in creating quality software are raised to the highest possible level. The ethical decisions involving a trade off between quality and such factors as cost, ease of use and time to market require extremely serious examination.

Red Lies

Red lies occur during meetings with clients or management, when representatives make statements about a product or project that are known to be untrue—such as stating that a project's delivery is on schedule to our customers, when the team already knows they cannot deliver on time.

Scenario No.1 : System Modification

A computer company wrote a very complex system for an anti-ballistic missile. The system is being used successfully to shoot down incoming missiles in a current military action. The military determines that the anti-ballistic missile would protect them more effectively if it shot down incoming missiles while they were further away. They ask the computer company to make immediate modifications to the system and deliver it within a week. The software engineering department decides to do the work.

Do you think the it is a realistic approach to make changes in a short period of time?

Sweep it under the rug

“Sweep it under the rug” syndrome occurs when unforeseen issues arise that could potentially damage a project or company but, to keep things running smoothly, management and/or staff ignore the issues in the hope they will vanish.

Cancelled Vacation Syndrome- Reason

Cancelled vacation syndrome arises when managers pressure staff members at the last minute to cancel planned trips or otherwise sacrifice their personal time and possibly money through, for example, non refundable trip reservations to meet a short –term deadline

How to avoid such problems?

Using Software Development Methodology

Standard work process enables controlled progress while developing high-quality software.

Use of an effective methodology protects software manufacturers from legal liability

- Reduces the number of software errors
- If an organization follows widely accepted development methods, negligence on its part is harder to prove

Quality assurance (QA):

QA Methods within the development cycle are designed to guarantee reliable operation of a product

Development of Safety-Critical Systems

Systems whose failure may cause injury or death are called **Safety Critical systems.** Safe operation relies on the flawless performance of software.

Examples: control automobiles' antilock brakes, nuclear power plant reactors, airplane navigation, elevators, and numerous medical devices (MRI, CT Scan etc).

While developing a safety critical system, Software Development Process is strongly adhered to tasks which require:

1. Rigorous and time-consuming development process
2. More thorough documentation
3. Vigilant checking and rechecking

Development of Safety-Critical Systems

Software developers must work closely with safety and systems engineer to ensure safety of the entire system.

- **System safety engineer**: Uses a logging and monitoring system to track hazards from a project's start to its finish
- **Hazard log**: Used to assess how detected hazards have been accounted for.
- **Testing**: To decide the level of sufficient testing i.e. to decide how much testing is required when a product is built whose failure could cause loss of human life.

Development of Safety-Critical Systems

Risk Analysis: When designing, building, and operating a safety-critical system a formal risk analysis is to be conducted

The quality control should conduct a formal risk analysis to consider what can go wrong, the likelihood and consequences of such occurrences and how risk can be averted, mitigated or detected so that the users are warned.

Scenario No.2 : Professional Judgement

A computer company is working on an experimental fighter. A quality control software engineer suspects that the flight control software is not sufficiently tested, although it has (finally) passed all its contracted test suites. She is being pressured by her employers to sign off on the software. Her employers say they will go out of business if they do not deliver the software on time. She signs off.

How will you judge her action?

Development of Safety-Critical Systems

Redundancy: The software should provide multiple interchangeable software components to perform a single function in order to cope with failures and errors.

Development of Safety-Critical Systems

N-version programming: Approach to minimizing the impact of software errors by independently implementing the same set of user requirements N times

- The different versions of the software are run in parallel, and if the outputs of the different software vary, a "voting algorithm" is executed to determine which result to use.
- Multiple software versions are unlikely to fail at the same time under the same conditions

Consequences of failure can be mitigated by devising emergency procedures and evacuation plans

Following Integrity and Ethics

Integrity and ethical behavior are crucial to the success of the analyst.

Students in IT often underestimate the importance of personal integrity and ethics.

A SA or SE is required to keep

- Confidentiality of the employees' data in an organization.
- Confidentiality of corporate information.

Analysts or Engineers are expected to uphold the highest ethical standards when it comes to private proprietary information—whether the analysts are employees or outside consultants.

Following Integrity and Ethics

Ethics and integrity also include:

- follow-through on commitments,
- Dealing directly with mistakes and gaps in relevant knowledge and skills and practicing open and honest communication.
  - Because an analyst is a pivotal member of the development team, his or her lack of follow-through or task completion can cause problems that reverberate throughout the project.
  - An analyst must take honest stock of his strengths, weaknesses, and performance as well as ask for needed help and resources and be ready to provide the same to others.

Sources of Ethical Guidance

There are a few sources of ethical guidance available.

Using **deontological approach** to professional ethics.

The potential sources of **rules** to professional guidance are

- **Professional bodies:** which promotes codes of practice and conduct among its members.
- **Information systems methodologies :** Can provide a framework for systems Analyst which can be used to ensure thoroughness and completeness of IT projects. The methodologies can be extended to analyze ethical issues of IT project.

Ethical and Security Issues with IT System Administrators

Topics

- Role of a System Administrator
- Ethical Issues for a System Administrator
- Code of Ethics by LOPSA

IT System Administrator

Network and system administrators are professionals who are actively involved in preventing cybercrimes and who are also rarely recognized as denizens and protectors of the digital world.

These people are actively involved in

- Preventing information theft from their company databases and computers and
- trying to maintain their employers' digital reputation and prevent possible financial losses.

IT System Administrator

The person who is responsible for setting up and maintaining the system or server is called as the system administrator.

The system administrator is responsible for following things:

- User administration (setup and maintaining account)
- Monitor system performance
- Install software and update systems.

IT System Administrator

- Monitor network communication
- Setup and implement security policies including backup and recover policies for users. A sysadmin must have a strong grasp of computer security (e.g. firewalls and intrusion detection systems)
- Responsible for Password and identity management
- Manage cloud infrastructure.

What is so special about System Administrator's account?

SA and other privileged user access to confidential information

- databases
- usernames/passwords
- e-mail

They have an unrestricted access to the root account of the network system, so he can do anything with system.

For example, root can remove critical system files.

Ethical Issues

System/Network Administration has a great deal of responsibility, whether the company's management realizes it or not. They have access to nearly every piece of data on the company network, in the servers, Cloud, hosted, or physical. They have access to information about the usage patterns of every user on the network. They can see what information every user is gaining access to.

The power can be abused either deliberately or inadvertently which can result in serious problems.

Ethics are one of the most essential issues for system and network administrators.

Ethical Issues

Invasion of Privacy

One of the tasks a company could assign a network administrator could be looking at the browser activities and emails of employees to enforce company Internet usage policies. In this case, the network administrator could feel that it is unethical to invade employees' privacy in this way. However, if the company's employment contract states that the company could review their Internet activities, then the employees were forewarned not to do anything private on their company computers or company email accounts.

Ethical Issues

Equality in Reporting

Another ethical issue a network administrator could encounter in the process of reviewing employee browsing and email usage involves deciding what infractions to report. In other words, should the administrator report every single infraction, no matter how small, or should he only report serious infractions? In this case, the administrator may use his own values to determine what constitutes a "serious" infraction, and these values would also decide which employees will be let off and which ones could face disciplinary action.

Ethical Issues

Sensitive Information

A network administrator must know everything about his employer's technology infrastructure. This can include proprietary technologies and business practices. If a network administrator begins a new job at a different company, he could find himself in a situation where he could use knowledge from his previous employment for gain at his new job. In this case, the network administrator has to look for ethical, as well as legal, guidance to any non-disclosure agreements he may have signed at his old company.

Ethical Issues

Whistle Blower Situations

In this course of a network administrator's job with unlimited access to any file on the company's servers, he may come across information that implicates his company in activities that are either unethical or strictly illegal. In this case, the network administrator may find himself torn between reporting his employer and his own job security. The employee needs to balance whether the activity is strictly illegal or simply unethical, with the constraints of any non-disclosure agreements he may have signed before going forward to report her employer.

Ethical Issues

Compromising the Security

If a client asks a SA to save money by cutting out some of the security measures that he has recommended, yet his analysis of the client's security needs show that sensitive information will be at risk if he do so?

Should he go ahead and configure the network in a less secure manner even if he try to explain this risk factors to the client?

Ethical Issues

Consultation fees

The proliferation of network attacks, hacks, viruses, and other threats to their IT infrastructures have caused many companies to "be afraid." As a security consultant, it may be very easy to play on that fear to convince companies to spend far more money than they really need to.

The slippery slope

This pertains to the ease with which a person can go from doing something that doesn't really seem unethical, such as scanning employees' e-mail "just for fun," to doing things that are increasingly unethical, such as making little changes in their mail messages or diverting messages to the wrong recipient.

For example, the information you gained from reading someone's e-mail could be used to embarrass that person, to gain a political advantage within the company, to get him disciplined or fired, or even for blackmail.

Ethical Policies

One basic widespread approach to making use of ethics policies is to utilize **informed consent.** When applied to system and network administration, informed consent implies:

- People should know the rules under which they are living.
- Users need to know how the system will operate in various situations.

Code of Ethics by LOPSA

In the early 2000s, an organization called "The League of Professional System Administrators" – LOPSA (www.lopsa.org) announced a Code of Ethics. It begins, "We as professional System Administrators do hereby commit ourselves to the highest standards of ethical and professional conduct and agree to be guided by this Code of Ethics and encourage every System Administrator to do the same."

The Code deals with professionalism, personal integrity, privacy, laws and policies, communication, system integrity, education, responsibility to the computing community, social responsibility, and ethical responsibility.

Code of Ethics by LOPSA

1. Professionalism
2. Personal Integrity
3. Privacy
4. Laws and Policies
5. Communication
6. System Integrity
7. Education
8. Responsibility to Computing Community
9. Social Responsibility
10. Ethical Responsibility

User Code of Conduct

Each organization needs guidelines for the acceptable uses of the organization's computing systems.

- Under what circumstances is personal use of the organization's equipment/software permitted?
- What types of personal use are forbidden?
- What websites are restricted from browsing?
- How do the rules change if you are using the equipment from home?
- What are defined as harassing communications?

Privileged Access Code of Conduct

Some users need privileged access to do their jobs. For example, some users may need to install their own software, access and update information in particular databases, and publish webpages. A code of conduct is very likely to need to address the following issues.

- Require the user to acknowledge that their privileged access comes with a responsibility to use it properly.
- Limitations about the type of work that can be done with these elevated privileges.

Privileged Access Code of Conduct

The company should acknowledge that mistakes happen and addresses approaches to ensure that minimal damage results from mistakes.

- Backups
- Retain software sources

Building a Security Culture

Essentially, information security is not comprised only of technological superiority but should be treated as a culture within organizations and its employees.

All employees should be **security conscious** at all times, and thus assist their security departments in preventing hacking attempts.

System administrators have the **knowledge and the authority** to monitor any and every activity for any user in their domain, thus it becomes extremely important for them to adhere to a code of ethics.