The role of Software Developers:

- **Reliable –** software should function as expected without causing harm or issues for users.
- **Secure –** developers must ensure that the software is secure, protecting user data and preventing unauthorized access or exploitation.
- **Fair –** developers should strive for fairness, avoiding discrimination or bias in their code.

The impact of software on Society:

- **Business operations –** e-commerce, banking, etc.
- **Healthcare systems –** patient data management, medical devices, etc.
- **Social interaction –** social media platforms, online communities, etc.
- **Public safety –** transportation systems, security systems, etc.

Security – one of the most important aspects of software development.

- **Data breaches –** sensitive information (personal data, financial data, etc) must be protected from unauthorized access or leakage.

- **Malware –** software shouldn’t allow unauthorized code to be executed, causing harm to users’ systems.

- **Authentication & authorization –** (passwords, two-factor authentication) should be used to ensure only authorized users can access systems.

Developers are ethically obligated to test their software thoroughly and fix vulnerabilities before releasing products. Shouldn’t introduce vulnerabilities, such as backdoors.

Reliability – essential to ensure that the software functions correctly and consistently across different use cases, platforms, and environments.

- **Correctness –** software should perform the tasks it was designed to do.

- **Usability –** users should be able to use the software easily and efficiently.

- **Maintainability –** developers should write clean and understandable code to ensure that it can be maintained and improved over time.

Developers must rigorously test software, using methods like unit testing, integration testing, and user acceptance testing to ensure reliability. If issues arise, developers should act responsibly by releasing patches or updates promptly.

Bugs – unintentional errors or **flaws** in software.

- **Safety concerns –** bugs in medical devices could put patient lives at risk.
- **Privacy violations –** bugs in a financial system could expose sensitive user data.
- **Business disruption –** bugs in business-critical software could cause financial losses or operational downtime.

Developers must prioritize fixing bugs that impact security, privacy, or user safety, and should never conceal or ignore critical issues. Clear communication is crucial when bugs are discovered.

Backdoor – hidden access point deliberately created within a system, often **used for unauthorized access**. **Can be introduced by malicious actors**, or worse, **by the developers themselves**.

- **Malicious backdoors –** these can be **used by hackers to steal data or cause damage**.
- **Intentional backdoors –** developers may be pressured to introduce backdoors **for government or corporate reasons**.

*Developers have an ethical obligation to avoid creating backdoors in software. The consequences of backdoors can be far-reaching, as they can be exploited by cybercriminals, leading to data breaches, financial losses, and harm to individuals. Developers should adhere to ethical codes such as those outlined by **ACM** or **IEEE**.*

Software failures – can have significant negative consequences for users and society. Might include security breaches, system outages, or even public harm.

- **Healthcare systems –** failure of a healthcare application might lead to incorrect diagnoses or delayed treatment.
- **Automotive software –** failure in self-driving car software could result in accidents.

Developers must ensure that their software is rigorously tested for reliability and functionality before release. Developers should act transparently and responsibly when failures occur, providing timely fixes and compensating users if necessary.

The VM Emissions Scandal

Volkswagen developed software for its diesel vehicles that allowed them to pass emissions tests while emitting higher-than-allowed levels of pollution during regular driving. Later discovered to be a deliberate act of **software manipulation**.

Root causes:

- Developers and engineers designed software to cheat emissions tests, violating both legal and ethical standards.

- The software was created and deployed with the intention of deceiving regulators and customers.

Ethical failures:

- The ethical lapse was rooted in prioritizing corporate profits over public health and environmental sustainability.

- The failure to consider the long-term consequences of introducing unethical software led to significant legal, financial, and reputational damage to the company.

The Therac-25 Incident

Therac-25 was a radiation therapy machine used in the **1980s**. Due to software bugs and poor error handling in the software system, the machine delivered lethal doses of radiation to patients. This resulted in several deaths and serious injuries.

Root causes:

- The software had bugs in its error-handling mechanisms.
- Developers failed to test and verify the software thoroughly.
- The software was not updated after issues were detected.

Ethical failures:

- The failure to ensure patient safety, despite knowing about the software's flaws, was a major ethical lapse.
- The lack of transparency in communicating risks to medical professionals and patients was also an ethical concern.

The Healthcare.gov Launch (2013)

The launch of the **Healthcare.gov** website in the United States, designed to help people sign up for health insurance under the Affordable Care Act, was widely regarded as a software failure. The site faced numerous issues, including long load times, crashes, and security vulnerabilities, which prevented many users from accessing health coverage.

The Target Data Breach (2013)

The **Target data breach** was one of the largest retail data breaches in history, where hackers gained access to the retailer's systems and stole the credit and debit card information of over 40 million customers. The breach was facilitated by a vulnerability in Target's point-of-sale (POS) system, which was compromised after an initial infection through a third-party vendor.

Apple Maps (2012)

When Apple launched its own mapping service, **Apple Maps**, as part of **iOS 6** in **2012**, it quickly became infamous for its inaccuracies. The software displayed incorrect locations, misplaced landmarks, and missing data, leading to significant public backlash. The problem was compounded by Apple’s decision to replace Google Maps, which had been well-regarded, with the new, unpolished solution.

Freedom of Speech – a **fundamental human right that is enshrined in many constitutions around the world**. It is right to express one's thoughts and opinions without fear of reprisal. Essential for a healthy democracy, it allows for the free flow of information and ideas, which is necessary for informed decision-making.

Allowing us to:

- Share our ideas with others.
- Challenge the status quo.
- Hold our governments accountable.

Certain types of speech that are not protected, such as:

- Speech that incites violence or hatred.
- Speech that is defamatory.
- Obscenity.

FoS isn't the only important right, we also have the right to:

- Privacy.
- Freedom from discrimination.
- A good reputation.

Social networking – has become an integral part of our lives, connecting us with friends, family, and colleagues from all over the world.

Privacy and security:

- Be mindful of what information you share online.
- Choose platforms with strong privacy policies.
- Be careful about the third-party apps you connect to your social media accounts.

Cyberbullying and harassment:

- Be respectful of others online.
- Avoid engaging in cyberbullying or harassment.
- Report cyberbullying or harassment.

Misinformation and disinformation:

- Be critical of the information you see on social media.
- Verify information with reputable sources.
- Be careful about sharing information that you are not sure is accurate.

Emerging technology – a term generally **used to describe a new technology**, may **also refer to the continuing development of existing technology**. It can have slightly different meanings when used in different areas, such as media, business, Science, or education.

Artificial Intelligence – refers to machines or software that simulate human intelligence to perform tasks such as learning, problem-solving, and decision-making.

Machine Learning – a **subset of AI**, **involves training machines to improve performance** through data and experience.

Applications:

- Healthcare
- Autonomous vehicles
- Smart assistants
- Customer service chatbots

Challenges:

- Ethical concerns
- Bias in AI algorithms.
- Job displacement
- Privacy issues

Blockchain Technology – a **decentralized**, **distributed ledger technology that securely records transactions** across many computers. **Most commonly known for being the foundation of cryptocurrencies** like **Bitcoin**.

Applications:

- Cryptocurrencies
- Secure financial transactions.
- Supply chain management
- Smart contracts

Challenges:

- Scalability
- Energy consumption
- Regulatory issues

Internet of Things (IoT) – refers to the **network of physical objects**, **devices**, **and systems embedded with sensors and software** that enable them to collect and exchange data over the Internet.

Applications:

- Smart homes
- Wearable health monitors
- Smart cities
- Traffic monitoring

Challenges:

- Security and privacy concerns
- Data overload
- Interoperability of devices

Cloud computing – involves delivering computing services over the Internet. Allows businesses and individuals to use IT resources without having to own or manage physical infrastructure.

Applications:

- Data storage
- Software-as-a-service (SaaS)
- Remote working
- Enterprise solutions

Challenges:

- Data security
- Cloud service outages
- Vendor lock-in

Cybersecurity – is **critical in protecting information from cyber threats**, including hacking, data breaches, and ransomware.

Applications:

- Encryption
- Firewalls
- Anti-virus software
- Multi-factor authentication

Challenges:

- Evolving threats
- Data privacy concerns
- Balancing convenience and security.

5G Technology – is **the fifth generation of mobile network technology**, offering faster internet speeds, reduced latency, and increased connectivity.

Applications:

- Smart cities
- Autonomous vehicles
- Augmented and virtual reality
- IoT expansion

Challenges:

- Infrastructure costs
- Health concerns
- Data privacy issues

Ethical and Social Implications – the rapid growth of emerging technologies raises significant ethical and social issues, including the impact on employment, privacy, digital divide, and environment sustainability.

Applications:

- Responsible AI development
- Data protection laws (GDPR)
- Inclusivity in technology access.

Challenges:

- Ensuring fairness
- Preventing discrimination
- Balancing innovation with regulation.