Abstract for the general public

Alan Cooper said, "Inefficient mechanical systems can cost a couple of cents on every part, but poor information processes can lose an entire company." I will add this apt quote to the fact that due to poor information processes related to the critical system (nuclear power plant, controlled traffic light, self-driving car), you can lose not only business but also life.

The modern critical system is far from a "black box". It is a conglomeration of connected, synchronously functioning elements, including people – both operators and users. And communication is the factor that makes a set of elements of the system. Communication technologies as the basis of the information society are evolving extremely fast: 1, 2, 3, 4, 5G. This is when it comes to mobile technology, without which modern man can no longer imagine. Similarly, the implementation of modern information systems for critical use (ISCU) can not ignore the impact of heterogeneous communication interface on the quality of their operation.

But how do measure the quality of ISCU? To answer this question, let's pay attention to the term "dependability" in the title of the project. Dependability is a set of indicators that allow a comprehensive assessment of the reliability and information security of a modern system with hardware and information components.

To increase the dependability, it is necessary to formulate such an algorithm for influencing the controlled parameters of the target system, so that as a result, either reliability, information security, or both of these qualities increase. Human experience shows that such an algorithm can be formed by the enumeration method. But we do not think that such an approach is successful when it comes to ISCU. That is why we in the project will resort to mathematical modelling, which will allow us to obtain an adequate problematic mathematical description of 5G communication and service processes in ISCU. It is problematic because the real processes do not take place in ideal laboratory conditions.

In our models, we take into account the impact of five current issues in the context of the project theme.

The ***first*** problem is that the speed of the 5G connection is achieved by focusing the channel of information exchange between the subscriber and the base station. If there is an obstacle between these subjects (another person, a car), the canal begins to degrade until it breaks prematurely. The problem is complicated by the fact that both the subscriber and the obstacle can be mobile. Our task is to determine how many resources the base station can spend to compensate for the phenomenon of degradation of the channel of a particular subscriber without limiting the capabilities of other subscribers.

The ***second*** problem is similar to the first, but due to a "fundamental" reason. It manifests itself when the subscriber's apartment from the base station begins to close by, for example, a new building. Our goal is to exploit the phenomenon of heterogeneity and get around the hurdle by combining 5G and WiFi technology. It is important to rationally spatially place a set of WiFi routers.

The ***third*** problem is due to the resource-competitive nature of eMBB and mMTC technologies of the 5G platform. EMBB technology is focused on meeting the information needs of humans, and mMTC technology is focused on supporting the functioning of networks of Internet of Things (IoT) devices. The amount of communication resources of the base station is finite. Our task is to manage eMBB and mMTC traffic according to the set priorities. This problem will soon be significantly exacerbated. If IoE devices now generate compact textual content, in the coming years of Industry 4.0, these devices will actively generate video content (municipal video surveillance, virtually controlled industry).

The ***fourth*** problem is the threat of cyber-physical attacks on ISCU. If such an attack is successful, the hacker can, for example, gain control of automated municipal infrastructure, medical implants, self-driving vehicles, and from the information dimension to damage the physical dimension, endangering both property and human lives. Our task is to determine a rational protection scheme by the level of aggressiveness of the area of cyberspace, where the target ISCU operates, and the potential vulnerability of its components.

The ***fifth*** problem is that there is no perfect information security. Any system will end up in a non-functional state. However, the emergency transition of the ISCU to this state is unacceptable. When detecting signs of failure of the ISCU's information security subsystem from the negative impact an appropriate information security protocol should be initiated. Our task is to assess the probability of such a circumstance, taking into account the level of aggressiveness of cyberspace and the cost of information security measures.

At final stage we will combine a set of mathematical models into a methodology, experimenting with which we will determine the optimal algorithms to increase the dependability of the ISCU with a heterogeneous wireless interface, which will be measured to prevent the above problems.

The results of the project will increase the reliability and security of Poland's critical information infrastructure, as well as make access to the information of each of its citizens more comfortable, as a more stable opportunity to communicate with family and friends is invaluable.