Kaspersky Lab ICS CERT

KASPERSKY lab

Challenges of industrial cybersecurity

Evgeny Goncharov

05.12.2018 Version 1.0

In their swift development over the past decade, modern enterprises in energy, petrochemistry, metallurgy, pharmaceuticals, food processing, transport, logistics and other sectors have crossed the invisible line separating the physical world of machines and mechanisms from the virtual world of computer software. They have essentially evolved into cyber-physical systems, where instructions in machine code control physical objects. These cyber-physical systems are built using modern IT technologies. They are connected to each other and to the external cyber-world with wired and wireless communication channels. Although this makes effectively using and further developing such systems much easier, it also makes them vulnerable to computer attacks.

The danger posed by cyber-physical technologies to the industrial process and equipment is increasingly acknowledged by specialists working at industrial enterprises, information security researchers and government agencies of most countries. At the same time, most people who are responsible for or otherwise involved in ensuring the cybersecurity of industrial enterprises admit that implementing security measures is a very long process. As a rule, they cite a variety of reasons and factors that make progress towards protecting industrial facilities from cyberthreats difficult and slow or even downright impossible.

In this paper, we have summarized our knowledge and expertise accumulated over years of practical work (conducting security audits and penetration tests, investigating incidents, detecting and preventing attacks, designing and deploying protection, providing training to cybersecurity specialists and employees at industrial enterprises, participating in the development of recommendations and requirements for industry regulators) and communication with experts representing industrial enterprises, academic institutions and government agencies from different countries.

We have developed a list of factors that, in our opinion, affect, now and in the foreseeable future, the threat landscape and the development, implementation and use of organizational and technical measures designed to protect industrial facilities, as well as the major industrial cybersecurity issues which are not likely to be resolved in the near future.

Objective factors affecting the cybersecurity of industrial enterprises

1. **Evolution of industrial processes**

   The need to make new, more sophisticated products results in changes to requirements for industrial control systems (ICS).

2. **Evolution of industrial control**

   Moving monitoring and control functions to higher levels in the hierarchy (from a production line on the ground floor to the chief engineer's office higher up and further – to the transcendental heights of the industrial internet of things and Industry 4.0).

3. **Ever increasing complexity of industrial control systems**

   This leads to the adoption of new technologies when designing new industrial control systems. These new technologies:

   - are often developed by third parties;
   - are borrowed from IT;
   - are used by a large number of vendors.

4. **Shortening ICS lifespans**

   On the one hand, upgrading industrial automation systems partly addresses the issue of having to maintain compatibility with legacy products and systems when developing and implementing security measures and tools.

   On the other hand, it leads to shorter development and support cycles of products designed for industrial control systems. Given the constantly increasing complexity of such products, this places additional constraints on the costs that can be spared by vendors to identify and address cybersecurity issues affecting their products.

5. **Growing automation rates, getting rid of manual labor**

   - The number of automation systems and other information systems used in industrial facilities is constantly growing.
   - The variety of information systems is broadening; new system types that did not exist before are being developed and deployed.
   - The connectivity between systems is increasing.

6. **Consolidation of industrial production; mergers and acquisitions**

   - When industrial facilities consolidate and merge, the resulting facilities often have a much greater variety of automation systems.
   - New systems and technologies are being used to unify the monitoring and control of previously unrelated facilities and systems.
   - Enterprises look for the right solutions to centralize industrial process monitoring and control systems.
   - Growing numbers of suppliers and contractor organizations.
   - Increasingly complicated chains of command and decision-making processes.

7. **Higher security levels of cybercriminals' "traditional" victims**

   - More and higher-quality tools protecting from traditional attacks, higher awareness levels of potential victims and greater maturity of security processes.
   - The availability of managed security services offered by leading players in the information security market makes high expertise in detecting and preventing attacks more accessible to organizations and individuals, i.e., attackers' potential targets.
   - Law enforcement agencies are raising their level of expertise in investigating cybercrimes against home users, companies and organizations, such as the theft of money and the disruption of IT systems' operation. This makes traditional cyberattacks an increasingly risky type of illegitimate activity.
   - The result of this is that cybercriminals are more actively searching for new targets that have lower levels of protection.

8. **The absence of any obvious everyday threat to the functional (i.e., related to the industrial process and equipment) or physical (i.e., related to people and the environment) safety and business of industrial enterprises**

   While planning and conducting their activities, many industrial enterprises and organizations make allowances only for those consequences of cyberattacks that potentially lead to emergencies which have already been modeled and assessed for risks, while ignoring a wide variety of other possible outcomes. In most cases, the structure of these risks was shaped by the pressure of laws and regulations, as well as a traditional approach that has evolved in many industrial sectors.

   The division of responsibility between different chains of command in individual enterprises and between enterprises in a sector also plays a major role in shaping the list of risks faced by an enterprise or a specific division of an enterprise. This commonly includes risks of emergency situations arising under chance combinations of negative circumstances, which have already been assessed based on theoretical considerations and the practical experience of operating the relevant equipment.

   Objectively assessing the likelihood of a cyberattack and the relevant risks associated with the potential physical consequences of a cyberattack, is currently impossible – among other reasons, due to the fundamentally non-stochastic nature of cyberattacks. The task of modeling all possible consequences of cyberattacks on an industrial enterprise is also one that cannot currently be solved. Therefore, it is fundamentally impossible to reduce planning and implementation of organizational and technical measures of protection against cyberthreats to the traditional practices of functional and physical safety.

   Sadly, most organizations are unable or unwilling to accept this reality and try to solve problems related to assessing the threat posed by cyberattacks using the familiar apparatus of pseudo mathematical statistics. If cyberattacks on industrial enterprises were numerous and diverse and if physical incidents caused by cyberattacks were the day-to-day reality of most enterprises, then it might be possible to develop metrics and statistical models providing more or less adequate numerical evaluations of threats. In that case, it might make sense to try applying risk assessment techniques to specific threats or their components. However, at the current stage, this is an impossible task due to the lack of statistical data on the physical consequences of cyberattacks.

   Luckily, targeted attacks on industrial control systems remain few and far in between. For most people in the industrial ecosystem, such attacks are events that, although they are undoubtedly disturbing, are so rare that they cannot be used to develop reliable statistics.

Although attacks aimed at stealing money, as well as ransomware attacks, are becoming increasingly common, they have, so far, largely passed industrial enterprises by. The threat posed by such attacks is still often underestimated by representatives of industrial organizations who have never experienced them firsthand. At the same time, statistics on blocked attempts to infect industrial automation systems, which we publish on our website, clearly indicate that systems on industrial enterprises' operational technology networks are available to mass attacks and accidental infections and can therefore serve as targets for attackers who block systems and count on getting ransom for unblocking them. In 2017-2018, we published several articles on large-scale malicious campaigns aimed at stealing money from hundreds of industrial organizations in Russia and globally (those threats targeted specifically industrial companies rather than various businesses, including industrial companies). This is an indication that the threat has grown significantly.

9. Reluctant disclosure of information on vulnerabilities, attacks and incidents

Information on information security issues, vulnerabilities identified, attacks and incidents is in many cases treated as confidential at all levels of the industrial ecosystem, including ICS vendors, industrial enterprises, and government agencies.

10. Geopolitical considerations

The influence of governments on the security of industrial enterprises is constantly growing. This influence can be, to varying degrees, both positive (raising the awareness of threats, developing and implementing critical infrastructure facility protection requirements, coordinating efforts to fix vulnerabilities, helping to investigate incidents) and negative (restricting access to information on incidents, restricting access to security technologies, engaging in direct disinformation, organizing and conducting attacks on enterprises and individuals both within and outside the government's authority). The actions of government agencies can be defined both by domestic and foreign policy considerations, including geopolitical factors. One significant consequence is that government actions defined by geopolitical interests result in significant changes to the system of trust between industrial automation vendors, providers of automation system deployment services, vendors of security tools and security service providers, and customers, i.e., industrial organizations. Sadly, this comprehensive review of trust levels, in our opinion, plays into the hands of attackers rather than industrial organizations seeking to protect their systems from attacks.

Industrial enterprise cybersecurity issues

1. **Constantly growing threat landscape**
    - A growing number of automation systems and, as a consequence, more channels used for control and data transmission, both in industrial facilities and to connect these facilities to the outside world, including over the internet.
    - New communication channels are created to connect formerly independent facilities and provide monitoring and remote control.
    - Increasingly diverse automation tools used by enterprises make both maintaining automation systems and ensuring their security more difficult.
    - A growing number of organizations and people who have direct or remote access to automation systems, expanding attackers' capabilities related to organizing and carrying out attacks.
2. **Constantly growing interest in industrial organizations on the part of cybercriminals and secret services**
    - Falling profitability and growing risks associated with conducting cyberattacks on traditional victims make cybercriminals look for new victims, specifically among industrial organizations.
    - The complicated security management structure and the immaturity of the relevant communication processes, both of which are largely defined by the control and decision-making structure of industrial enterprises, make industrial organizations more vulnerable to the threat of cyberattacks compared with cybercriminals' traditional victims.
    - Cybercriminals also benefit from the specific ways in which industrial enterprises conduct their business and financial activities, including the system of deferred payments and settlements, complicated accounting and other factors that make timely discovery of the theft of funds more problematic.
    - When organizing attacks on industrial enterprises, cybercriminals can take advantage of their victims' unwillingness to admit that an incident has taken place or to request help from information security companies or law enforcement agencies.
    - It is widely known that many countries' secret services, as well as other organized threat groups whose activity is defined by domestic and foreign policy related interests of governments, financial and political groups, are actively involved in research and development to create toolsets for conducting espionage and terrorist attacks against industrial enterprises. In their investigations of sophisticated attacks and large-scale malicious campaigns, information security researchers keep encountering traces of such activity and artifacts pointing to such threat groups. It must be admitted that, given the current geopolitical realities, the evolution of industrial automation systems, and the transition to new processes and models of production and economic activities, this situation is going to evolve in the coming years in a direction that is unfavorable for many industrial organizations.

3. **Underestimating the overall threat level**

   The lack of publicly available information on information security issues specific to industrial enterprises, the relative rarity of targeted attacks against automation systems, the excessive reliance on safety measures and the failure to accept objective reality (such as the internet access or accidental infections of ICS components) impair the assessment of the threat level by owners and operators of industrial enterprises and their staff.

4. **Misunderstanding of the nature of threats and sub-optimal choice of security tools**

   For decades, information security techniques and technologies have developed in response to the evolution of techniques and technologies used to attack the information systems of home users, office and telecommunication networks, and suppliers of various information services. In other words, security technologies have in a way developed to catch up with offensive technologies. Although many security solution developers do try to be a step ahead of attackers, their products and technologies are based on knowledge obtained by analyzing a large number of real-world attacks. For example, Kaspersky Lab's systems automatically analyze and process over 300,000 new samples of suspicious and malicious software daily.

   A unique situation has evolved in the world of industrial enterprises and industrial automation systems: a few widely-publicized incidents resulting from targeted attacks on a very limited set of victims have created an information environment that has completely shaped the perception of the potential threat – both among security researchers and security developers and among potential users of their solutions.

   Unfortunately, publicly available information on many of these incidents has only been provided by researchers and developers of solutions designed to protect against traditional IT threats, who have concentrated mainly on the IT component of the attacks, providing very little analysis of the OT and cyber-physical aspects of these incidents.

   On the one hand, the resulting reports were too complicated for most potential users of security solutions to understand, but on the other hand, essential OT-related details were missing from these reports. This point is corroborated by the many incorrect interpretations of virtually all known incidents, which we keep encountering among engineers.

   Since there is no need to combat attacks on industrial control systems and field equipment day in and day out, numerous new vendors of dedicated security solutions for industrial automation systems (many of whom have little practical experience of developing and applying tools designed to protect against traditional IT threats) have developed products that are probably better at protecting from synthetic attack scenarios developed by information security researchers, sometimes without any reference to practical experience, than from real-world attacks. Demand for these products has been generated through the vendors' vigorous marketing activity.

   At the same time, factors mentioned in the previous sections have resulted in industrial automation systems not only being vulnerable to accidental attacks involving malware that is not specifically designed to target such systems, but also becoming increasingly attractive targets for traditional cybercriminals. This is supported by the results of our research published on ics-cert.kaspersky.com.

   Thus, a situation that we believe to be dangerous has evolved in the industry: instead of spending their efforts and budgets on addressing the top-priority task of providing protection from real-world (and increasingly frequent) attacks, cybersecurity solution vendors and customers are focusing on protection against synthetic scenarios and attacks of an imaginary future invented by security vendors without thoroughly analyzing the day-to-day threat landscape.

5. Technical and organizational difficulties associated with protecting industrial control systems

A lot has been said about the technical and organizational difficulties of protecting industrial enterprises. If all of these difficulties were enumerated and analyzed, the result would be a major work, which is far beyond the scope of this paper.

We will list only those issues which, in our opinion, constitute the greatest obstacles to ensuring the cybersecurity of industrial enterprises. Some of these issues are objective, i.e., they are due to factors that are difficult to overcome, while other problems are caused by an incorrect assessment of the situation.

Among important tasks that are difficult to resolve due to objective factors, we would like to highlight the following:

- Ensuring that security solutions are compatible with a huge variety of industrial information and automation systems, including obsolete products and technologies that remain widespread.
- Ensuring that industrial automation system vendors implement modern procedures and SDL.
- Ensuring that all newly developed ICS solutions are tested by teams of external security researchers and that ICS products are assessed for industrial use based on security requirements of the enterprise and the results of external testing.
- Mandatory training and certification of engineers and operators working at industrial enterprises in cyber-hygiene and modern practices of protection from cyberattacks.

We believe that the following issues are largely due to misjudgments of the current situation:

- The requirement for security solutions to operate passively (i.e., in monitoring mode). Data on the use of Kaspersky Lab products in active mode on hundreds of thousands of industrial automation systems across the globe demonstrate that, in the vast majority of cases, this requirement is excessive.
- The requirement for ICS vendors to ensure the certification / appraisal of all security solutions. This requirement significantly increases the cost of developing both security solutions and ICS products, but at the same time, it does not provide any additional guarantees that security and automation systems will work together seamlessly. In our experience, systems whose owners or operators require such certification or appraisal often have vast amounts of software that is much more problem-prone, and even dangerous, installed on these systems by the owners and operators themselves without requiring any certificates of compatibility with their ICS systems.

Eventually, problems of this type are likely to disappear by themselves – under the increasing pressure from attacks mounted by threat actors. However, today such issues often become barriers to using proper protection, leaving industrial automation systems vulnerable to cyberattacks.

Kaspersky Lab Industrial Control Systems Cyber Emergency Response Team (Kaspersky Lab ICS CERT) is a global project of Kaspersky Lab aimed to coordinate the efforts of automation system vendors, industrial facility owners and operators, and IT security researchers to protect industrial enterprises from cyberattacks. Kaspersky Lab ICS CERT devotes its efforts primarily to identifying potential and existing threats that target industrial automation systems and the Industrial Internet of Things.

Kaspersky Lab ICS CERT **Ics-cert@kaspersky.com**