ISRC
INFORMATION SYSTEMS RESEARCH CENTER
BİLGİ SİSTEMLERİ ARAŞTIRMA MERKEZİ

BOĞAZİÇİ ÜNİVERSİTESİ
YÖNETİM BİLİŞİM SİSTEMLERİ
SİBER GÜVENLİK MERKEZİ

BUSİBER Boğaziçi Üniversitesi Yönetim Bilişim Sistemleri Siber Güvenlik Merkezi ve Kaspersky Akademi iş birliğiyle **10-11 Kasım 2025** tarihlerinde "Eğitmenlerin Eğitimi" programının düzenlenmesi planlanmaktadır. Bu program, Türkiye'deki üniversite ve liselerin siber güvenlik bölümlerinde görev yapan akademisyenlere öğretmenlere, araştırma görevlilerine ve ileride siber güvenlik dersi verebilecek doktora öğrencilerine yönelik hazırlanmıştır.

Amacımız, siber güvenlik alanında ders veren akademisyenlerin ders içeriklerini zenginleştirmelerine, bu alandaki diğer öğretim üyeleriyle tanışarak deneyim ve bilgi paylaşımında bulunmalarına katkı sağlamaktır. Ayrıca, siber güvenlik dersi açmak isteyen akademisyenlere destek olmak ve kontenjan elverdiği ölçüde geleceğin akademisyenleri olan doktora öğrencileri ile araştırma görevlilerinin gelişimine katkıda bulunmaktır.

Eğitim kapsamında endüstriyel siber güvenlik, kritik altyapıların korunması ve ulaştırma sektörü güvenliği gibi güncel ve kritik konular ele alınacaktır. Katılımcıların, endüstriyel kontrol sistemlerinde siber tehditlere karşı koruma yöntemleri, tehdit modellemesi ve risk değerlendirmesi süreçleri hakkında derinlemesine bilgi edinmeleri hedeflenmektedir. **Eğitim, ürün tanıtımı değil, akademik içeriklidir.**

Eğitmenlerin Eğitimi programının sağladığı en önemli katkı, akademik dünyada siber güvenlik eğitimi verecek olan eğitmenlerin, teorik bilgilerini pratik uygulamalarla güçlendirmelerini sağlamasıdır. Program, tasarım aşamasından başlayarak güvenli yazılım geliştirme süreçlerine kadar uzanan geniş bir perspektif sunmakta, özellikle kritik altyapılar ve ulaştırma sistemleri gibi hayati sektörlerdeki siber güvenlik ihtiyaçlarına odaklanmaktadır. Kaspersky Akademinin alanlarında uzman uluslararası eğitmenlerinin ve araştırmacıların rehberliğinde gerçekleştirilecek bu program, Türkiye'deki gelecek nesil siber güvenlik profesyonellerinin yetiştirilmesine ve siber güvenlik eğitimlerine önemli katkılar sağlamayı amaçlamaktadır. Verilen derslerle ilgili sunulacak ek kaynaklarla katılımcılar daha derin ders içerikleri oluşturabileceklerdir.

Eğitim dili İngilizcedir.
Eğitim Ücretsizdir.
Hali hazırda kadrolu öğretim üyeleri ve görevlilerine öncelik verilecektir.

SON KAYIT: 6 Kasım 2025 (Kayıtlar daha erken de dolabilir)
Tam gün katılanlara **Katılım Sertifikası ve eğitim sonundaki sınavı geçenlere ek olarak Başarı Sertifikası** verilecektir.

Eğitim başvuru: https://siber.bogazici.edu.tr/tr/siber-guvenlik-egitmen-egitimi

Eğitmenlerin Eğitimi Programı – 10-11 Kasım 2025, Boğaziçi Üniversitesi

1. Gün			Süre
Siber Fiziksel Sistemler ve Yönetişim	Siber Fiziksel Sistemlerin Yönetişimi ve dayanıklılığı (resilience)	**Prof. Dr. Bilgin Metin**	60 dakika
Siber Fiziksel Sistemlere Güvenliğine Giriş	Siber- fiziksel sistemlerin güvenliğini sağlamaya yönelik modern yaklaşımlar. Sistem yaşam döngüsü, siber güvenliğin yaşam döngüsündeki yeri. Tasarım aşamasında sistem mühendisliği güvenliğinin rolü. Disiplinler arası analiz. Öğretim yöntemlerine ilişkin değerlendirmeler	**Ekaterina Rudina** / Denis Babaev / Semen Kort	90 dakika
Uygulamada endüstriyel siber güvenlik	Endüstriyel siber güvenlik Endüstriyel Kontrol Sistemlerinde (ICS) siber tehditlere karşı korumanın özellikleri Endüstriyel ağ güvenliği Organizasyonel önlemler ICS'ye yönelik siber saldırıların özellikleri	**Semen Kort** /Alexander Nikolaev	90 dakika
Endüstriyel siber güvenlik ortamı	Siber güvenlik bilgi alışverişinin rolü Endüstriyel otomasyon sistemleri için tehdit ortamı 2024-2025	**Alexander Nikolaev** / Ekaterina Rudina / ICS CERT	90 dakika

	2024-2025 yıllarında sanayi kuruluşlarına yönelik en önemli APT ve finansal saldırı vakaları Tehdit profillemesi ve tehdit modellemesi ile risk değerlendirmesine ilişkin sonuç		
ICS ortamında siber güvenlik yöntemleri ve çözümleri	Anti-virüs yöntemleri ICS'de kötü amaçlı yazılımdan koruma hakkında ayrıntılar Siber saldırıların erişilebilirlik ve güvenlik üzerindeki etkisi Endüstriyel ortamda siber güvenlik çözümleri ve platformları Proaktif kötü amaçlı yazılım karşıtı yaklaşımlar Yerleşik güvenlik çözümlerine sahip altyapıların tasarlanması	**Ekaterina Rudina** / Denis Babaev	90 dakika
2. Gün			
Ulaştırma alanında siber güvenlik	Siber-fiziksel sistemler olarak ulaştırma sistemleri ve altyapıları Karayolu taşımacılığı ve platformlar. Siber güvenlik yaklaşımı Deniz araçlarının ve liman altyapılarının siber güvenliği Aviyoniklerin ve uçuş yönetiminin siber güvenliği	**Alexander Nikolaev** / Denis Babaev / Stepan Rybakov	90 dakika
ICS ve taşımacılık için tehdit modellemesi ve risk değerlendirmesi	Neden tehdit modellemesi Riskler ve risk paydaşları ICS ve taşımacılık için risk ve zarar nasıl ölçülür?	**Ekaterina Rudina** / Semen Kort /Denis Babaev	90 dakika

	Saldırı senaryoları, taktikler ve teknikler Riskler nasıl değerlendirilir ve yönetilir Risk değerlendirmesi ICS ve taşımacılıkta güvenli tasarıma nasıl katkıda bulunur?		
Tasarım yoluyla güvenlik ve ICS ve taşımacılıkta güvenli yazılım geliştirme rolü	Yaşam döngüsüne dayalı tasarımla güvenlik (Security by Design) Güvenlik yönetiminin rolü ICS ve taşımacılık için uzun ve kısa vadeli riskler Güvenli yazılım geliştirme SSDLC uygulamaları ve süreçleri Tedarik zincirinin siber güvenliği	**Ekaterina Rudina** / Alexander Nikolaev / Semen Kort	60 dakika
ICS CERT /KIPS için ayrılmıştır			60 dakika
ICS CERT /KIPS için ayrılmıştır			60 dakika

ICS CERT katılımı veya KIPS mümkün olmadığında ele alınacak ek konular:

ICS ve ulaşım ortamlarında güven, güvenilirlik ve güvence (60 dk)

Öğrenciler için seminerler, atölye çalışmaları ve tez konuları üzerine değerlendirmeler (interaktif, 60 dk)

Karayolu taşıtlarının siber güvenliği hakkında daha fazla bilgi

Deniz araçları ve aviyonikler hakkında daha fazla bilgi

Final quizi (30 dakika)

DETAYLI PROGRAM ve EĞİTMENLER:

Day 1 – November 10, 2025

60 Minute

Introduction to Cyber Physical Systems Governance

by Bilgin Metin

The governance of cyber-physical systems (CPS) requires a holistic understanding that unites information security management, risk governance, and operational resilience under a single framework. According to ISO/IEC 27001 and ISO 31000 principles, cybersecurity is not merely a technical control system but a governance process that ensures risks are identified, evaluated, and mitigated within organizational objectives. A *threat* represents a potential cause of an unwanted incident, a *vulnerability* is a weakness that can be exploited by that threat, and *risk* emerges from the intersection of both, weighted by the impact on confidentiality, integrity, and availability. In CPS environments—especially those integrating Industrial Control Systems (ICS)—the consequences of a single exploited vulnerability may cascade into physical disruption, safety hazards, and financial loss. Therefore, resilience must be engineered not only through redundancy and recovery planning but also through proactive monitoring, continuous improvement, and a culture of security awareness. Effective governance also extends beyond organizational boundaries, encompassing *third-party and supply-chain security*, where trust and verification mechanisms ensure that partners and vendors maintain comparable levels of protection. A mature CPS governance model thus aligns people, processes, and technology within a continuous improvement loop—transforming cybersecurity from a compliance requirement into a strategic enabler of safety, reliability, and sustainable innovation.

Prof. Dr. Bilgin Metin

Prof Dr. Bilgin Metin

Bogazici University,

Head of Management Information System Dept.
Head of Bogazici University MIS Cybersecurity Center

Bilgin Metin joined Bogazici University's Management

Information Systems Department in 2007, becoming a full Professor in 2021. His research covers cybersecurity, IT, AI and privacy governance, and information system design. Prof. Metin has authored over 125 publications in international journals and conferences with an h-index of 26 in Google Scholar and 23 in Scopus.
He is an Assoc. Editor in Journal of Cybersecurity Technology (Taylor & Francis), and he serves on the editorial boards of several other prestigious journals, including Information Security Journal: A Global Perspective (Taylor & Francis), EDPACS (EDP Audit, Control, and Security Newsletter) (Taylor & Francis), and Organizational Cybersecurity Journal: Practice, Process, and People (Emerald).
Professor Metin has earned distinguished certifications, including Offensive Security Certified Professional (OSCP), Certified Information Systems Auditor (CISA), Certified Data Privacy Solutions Engineer (CDPSE), and ISO 27001 Lead Auditor.

90 min

Introduction to Cyber Physical Systems lecture

by Ekaterina Rudina

Our world is now woven together by cyber-physical systems—the intelligent, interconnected technologies that power everything from our electrical grids to our transportation networks. But with this new intelligence comes a new vulnerability, launching us into a constant quest for their security.

This journey cannot be a last-minute thought; it must be woven into the very **life cycle of the system itself**. From its first sketch on a whiteboard to its final decommissioning, cybersecurity cannot be a bolt-on addition. It must be a constant, vigilant companion.

This is where the grand discipline of **system engineering** takes center stage. It provides the master blueprint, ensuring that every component—hardware, software, and human—works in secure harmony. The guiding star for this entire effort is the principle of **Security by Design**. It's the commitment to building protection into the system's architectural DNA, not just adding locks to the doors after the house is built.

But these systems are not just technical; they exist in a complex human world. This demands **interdisciplinary analysis**, where engineers sit alongside psychologists, economists, and policy experts. Together, they anticipate not just digital threats, but human error, economic incentives, and societal impacts.

In critical environments like industrial control rooms or the cockpit of a modern airplane, the ultimate goal crystallizes into three vital concepts: **trust, trustworthiness, and assurance.** We need to know that a system is *trustworthy*—proven to be reliable and secure—so that we can place our absolute *trust* in it, backed by the verifiable *assurance* that it will perform as expected, even under duress.

And so, the final, crucial consideration falls to **how we teach this**. We must move beyond siloed lessons in coding or electrical engineering. We must mentor a new generation of builders who think in terms of life cycles, who design with security as their first instinct, and who understand that building a resilient future is a profoundly human endeavor, as much about psychology and process as it is about code and circuits.

Dr. Ekaterina Rudina

Information Security Group Manager

Ekaterina Rudina is an **analyst** who works for the Kaspersky Lab Future Tech Department in the scope of threat research, modeling, and risk assessment. She also provides an ongoing analytical support to the everyday work of project managers, business development managers, GR and PR managers, and other colleagues who may need the review, summary, or comments on standards, laws, guidelines, requirements and other documents related to the critical infrastructure defense.

Ekaterina is a **contributor** to ISO, IEEE, ITU, and Industrial Internet Consortium documents and national standards on security by design. After **over 20 years in computer security** and nearly 12 years in industrial cybersecurity, she believes that the systematic approach coupled with strong technical background provides the most efficient way to the secure and safe technological environment.

Ekaterina holds a **Ph.D. in Computer and Network Security** from St.Petersburg Polytechnic University of Peter the Great.

7 years' experience as an Assistant Professor in St. Petersburg Polytechnic University of Peter the Great.

90 min

Industrial cybersecurity in practice

by Semen Kort

Industrial cybersecurity is a specialized discipline focused on protecting Industrial Control Systems (ICS), which manage critical infrastructure and manufacturing processes. Its approach is distinct from IT security due to the high stakes of physical consequences and operational continuity.

The core of this field addresses the **specifics of cyberthreat protection in ICS**. These environments are sensitive to disruptions in availability and integrity, where even a minor manipulation can lead to cascading physical failures, safety risks, or prolonged downtime.

A primary line of defense is **industrial network security**. This involves architecting and securing segmented, deterministic networks using specialized protocols like OPC UA and Modbus. Protection here is designed to maintain real-time operation and prevent unauthorized access to critical controllers and sensors.

Complementing technical measures are essential **organizational measures**. These include the development of formal security policies, incident response plans tailored to operational technology (OT), and comprehensive training programs to establish a culture of security awareness among engineers and operators.

Understanding the **specifics of cyberattacks on ICS** is fundamental to building effective defenses. These attacks are typically targeted and aim to achieve physical effects. They often involve techniques like manipulating setpoints, disabling safety systems, or disrupting control loops to cause equipment damage, process shutdowns, or harm to human safety. Consequently, defense strategies are engineered to detect and mitigate these specific attack vectors.

A critical pillar of industrial defense is the systematic study of **Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) in an ICS environment**. Frameworks like the MITRE ATT&CK for ICS provide a detailed, real-world map of the adversary's playbook, cataloging the specific steps attackers take – from initial reconnaissance and lateral movement to the final manipulation of control processes. This knowledge moves defense planning from a reactive stance to a proactive one.

Understanding the "how" of an attack allows for the precise targeting of defenses. This intelligence directly informs the selection and deployment of **cybersecurity solutions engineered to mitigate these specific attacks** which we further discuss.

Dr. Semen Kort

Principal Information Security Analyst

Semen is a **Principal Security Analyst** in Kaspersky Future Tech Department.

Semen is specializing in the analysis of industrial cybersecurity solutions and cybersecurity of the Internet of Things. Semen regularly contributes to the information security standards and internationally recognized technical guides.

He is an active member of IEEE P2413 working group, ISO/IEC SC41, and Internet Industrial Consortium working groups.

Semen was giving lectures on the information security and security of network technologies and protocols at Saint-Petersburg Polytechnical University.

Semen Kort is the main author of the “Industrial cybersecurity awareness course” and regularly **gives lectures** on industrial cybersecurity for industrial employers around the world.

Semen Kort holds a **Ph.D. degree in Computer and Network Security** from St.Petersburg Polytechnic University of Peter the Great.

Over 20 years’ experience as a Professor in St.Petersburg Polytechnic University of Peter the Great and over 10 years in Kaspersky then.

90 min

Industrial cybersecurity landscape

by Alexander Nikolaev

A critical component of modern industrial defense is **the role of cybersecurity information exchange**. In an era of sophisticated threats, no single organization can defend itself in isolation. The proactive and anonymous sharing of threat intelligence—such as indicators of compromise (IoCs) and attack patterns—across a trusted community creates a collective immune system, enabling all participants to fortify their defenses against newly discovered adversaries.

This collaborative intelligence is essential for understanding the evolving **threat landscape for industrial automation systems in 2024-2025**. Current analysis provided by Kaspersky ICS CERT team indicates a landscape characterized by the deliberate targeting of operational technology (OT) by state-sponsored actors, the continued rise of ransomware groups explicitly targeting critical infrastructure, and an increasing exploitation of vulnerabilities in interconnected IT/OT perimeter devices.

This abstract landscape is given concrete form by **the most prominent cases of APT and financial attacks on industrial organizations in 2024-2025**. Recent incidents demonstrate a tactical shift. Advanced Persistent Threat (APT) groups are now conducting sustained espionage and pre-positioning within energy and manufacturing sectors, while financially motivated actors have perfected "double-extortion" ransomware campaigns that not only encrypt data but also threaten to leak it or disrupt physical operations.

The ultimate value of this shared intelligence and incident analysis lies in its application to **threat profiling and, by extension, to refining threat modeling and risk assessment**. By systematically profiling specific adversaries—their tactics, techniques, and procedures (TTPs)—organizations can move from generic defenses to targeted ones. This detailed profiling provides the empirical foundation for accurate threat modeling, ensuring that risk assessments are not based on theoretical vulnerabilities but on the concrete and documented behaviors of the most likely attackers, leading to a more resilient and intelligence-driven security posture.

Alexander Nikolaev, MSc

Senior Information Security Analyst

Alexander Nikolaev is a **Senior Security Analyst** in Kaspersky Future Tech Department. Alexander focuses on threat modeling, risk assessment and design cybersecurity architecting for industrial control systems.

Alexander has **over 14 years of experience in industrial cybersecurity** including ICS in oil and gas industry, grain processing plants, ships, airplanes and etc.
He also has experience in information security in fields of the banking sector, personal data and trade secrets.

He is a **member of the «Aviation cybersecurity» standardization** group at the Russian State Research Institute of Aviation Systems.

Alexander holds a **Master's degree in information security** (Moscow Engineering Physics Institute).

Alexander also **conducts cybersecurity trainings** for LK's customers in the oil and gas, aviation, and maritime sectors. He also takes a part at cybersecurity conferences like a speaker.
He's wide interests include the **new trends in aviation, marine, oil and gas**, and other industrial areas.

90 min

Industrial cybersecurity design approach

by Denis Babaev

The foundation for resilience in large industrial facilities is laid during the **Design phase,** including safety and security design. This is the most critical stage, where strategic decisions determine the inherent robustness of a facility. Integrating security and safety considerations at this point is not just “cost-efficient” like in other cases: this is the essential need to eventually assure them.

This principle is grounded in our direct **experience in cybersecurity architecting and design for critical infrastructures, including Nuclear Power Plants (NPPs), energy grids, and oil and gas facilities**. In these high-stakes environments, we have learned that a one-size-fits-all approach is insufficient. Each sector demands a tailored security architecture that understands its unique operational technology, regulatory pressures, and consequence profiles. AT the same time, the common approach exists and must be followed.

A fundamental challenge in this design process is **ensuring the coordination of safety and security in practice**. While safety is concerned with preventing accidental failures, security focuses on mitigating malicious, intelligent attacks. In practice, these objectives can sometimes conflict—a security measure might impede a safety function. Therefore, a disciplined, coordinated analysis is essential to align both aspects, ensuring that security controls do not compromise safety integrity and that safety systems are not vulnerable to cyber exploitation.

The primary tool to achieve this is a robust **cybersecurity architecture, built upon zoning principles and carefully selected equipment**. This involves segmenting the network into distinct security zones and conduits based on criticality and trust levels, a concept often derived from standards like IEC 62443 and IAEA requirements. This architecture dictates the placement and specification of security appliances, such as industrial firewalls and data diodes, to enforce boundaries and control the flow of traffic between zones.

The practical **aspects of cybersecurity implementation at large industrial facilities** extend beyond technology. It encompasses the development of procedures for secure remote access, patch management strategies for operational technology, and comprehensive incident response plans that account for physical processes. This implementation is a continuous lifecycle of assessment, hardening, and monitoring.

To build this capability for the future, it is clear **which disciplines students should learn to support industrial cybersecurity**. A modern curriculum must move beyond siloed knowledge, integrating systems engineering, control systems engineering, network security for OT protocols, risk management, and an understanding of safety engineering principles. This interdisciplinary foundation is crucial for developing the next generation of architects who can design and defend our critical industrial infrastructure.

Denis Babaev, M.Sc.

Lead Information Security Analyst

Denis Babaev is a **Lead Security Analyst** in Kaspersky Lab's Future Tech Department. Denis focuses mostly on threat modeling, risk assessment and design cybersecurity architectures for industrial control systems.

His **most remarkable projects** include:

Threat analysis and risk assessment and design of cybersecurity architectures for the Russian-designed Nuclear Power Plant control system,

Cybersecurity assessment projects of I&C Systems at all operating NPP of Russian Federation,

Threat modeling for the Thermal Power Plant control system,

Information and control system cybersecurity assessment of Nuclear Icebreaker «Arktika».

Denis has **over 20 years of experience in nuclear control system engineering** and cybersecurity. He originally joined Kaspersky Lab in 2020.

Denis also works on **international standards** with the International Electronic Commission (IEC) TC 45 «Nuclear instrumentation» and SC41 «Internet of Things and Digital Twin».

Areas of interest:

Threat analysis and risk assessment for ICS,

Synthesis of cybersecurity architectures for ICS,

System approach in cybersecurity,

Digital twins for cybersecurity,

Denis holds a **Master's degree in Electronics, Automation and Control of Physical Facilities** from Moscow Engineering Physics Institute and second higher degree in computer security.

Day 2 – November 11, 2025

90 min

Cybersecurity methods and solutions in ICS environment

by Semen Kort

In Industrial Control Systems (ICS), the primary impacts of a successful cyberattack are decisively shifted from confidentiality to the **critical compromise of availability and safety**. An attack's most significant consequence is not the theft of data, but the disruption of continuous operation, which can lead to massive financial loss, or worse, the creation of unsafe conditions that pose a direct risk to human life and the environment.

To defend against these outcomes, a cornerstone of protection is the deployment of **antimalware methods in the industrial environment**. However, the application of these methods is governed by the **specifics of antimalware in ICS**. Standard, signature-based scanning is often too resource-intensive for sensitive control hardware and risks interrupting critical processes. Therefore, the required approaches must be more nuanced, prioritizing stability and integrity.

Exchange of specific indicators of compromise, the complex approach to the infrastructure health is the most efficient way to security. This is where **Cybersecurity Intelligence** becomes paramount. By leveraging global threat feeds and understanding adversary behaviors specific to OT, defenses can be tuned to detect and block known malicious activity without overburdening the system. This intelligence informs the entire defense lifecycle.

These principles are operationalized through specialized **cybersecurity solutions and platforms in the industrial environment**. These are not repurposed IT tools, but purpose-built platforms that integrate threat intelligence with monitoring and control capabilities designed for OT networks. The goal is to move beyond reactive measures and adopt **proactive antimalware approaches**, such as application whitelisting, which only allows pre-approved programs to run, and heuristic analysis to identify novel threats based on suspicious behavior.

Ultimately, the most robust defense is achieved by **architecting infrastructures with built-in security solutions**. This means designing the network from the ground up with security as a foundational element—implementing robust segmentation, secure conduits between zones, and deploying specialized, industrial-grade security appliances at key junctions. This architectural approach creates a resilient and defensible environment where security controls are an integral part of the operational fabric, rather than a disruptive afterthought

90 min

Transportation cybersecurity

By Ekaterina Rudina and Alexander Nikolaev

Modern **transport systems and infrastructures are fundamentally cyber-physical systems**, where digital command and control directly govern physical movement and safety. This deep integration makes cybersecurity a foundational requirement for operational integrity, passenger safety, and public trust across every mode of transport.

In the domain of **road transport and automotive platforms**, the attack surface has expanded dramatically with connectivity. This necessitates specific **cybersecurity approaches for telematics and Firmware-Over-The-Air (FOTA) update platforms**, which are critical gateways to vehicle systems.

This entire field is now rigorously shaped by international regulations and standards, primarily **UN Regulations 155 and 156 and ISO/SAE 21434**, which mandate a structured, risk-based cybersecurity management system throughout a vehicle's entire lifecycle, from design to decommissioning.

The separate but important issue of threat modeling according to ISO/SAE 21434 will be covered further.

The maritime sector faces parallel challenges in the **cybersecurity of sea vessels and port infrastructures**. The industry has been alerted by a number **of known incidents** that have demonstrated tangible impacts on navigation and port operations. In response, a regulatory framework is being enforced, including the **IMO's guidelines on maritime cyber risk management** and the **IACS Unified Requirements E26 and E27** for cybersecurity in ship construction, which integrate cybersecurity resilience directly into the design and operation of vessels.

Similarly, in aviation, the **cybersecurity of avionics and flight management systems** is inextricably linked to the core objectives of **airworthiness and flight safety**. Here, security is not an add-on but a prerequisite for certification. The approach is governed by a rigorous **certification** process and well-established technical standards, such as the **ARINC cybersecurity standards**, which provide detailed guidance for securing critical aircraft data networks and ensuring the safe and secure interchange of information between vital airborne systems.

90 min

Threat modeling and risk assessment for ICS and transportation

By Ekaterina Rudina and Denis Babaev

A foundational element of any robust cybersecurity program is understanding **why threat modeling is the essential practice for risk management**. It moves the process from a theoretical exercise to a structured methodology for proactively identifying how an adversary could attack a system, making risk management targeted and actionable.

This process is fundamentally about understanding **risks, risk management, and risk stakeholders**. A risk represents a potential event that can cause harm, risk management is the continuous cycle of identifying, assessing, and mitigating those events, and risk stakeholders are the diverse group—from engineers to executives to regulators—who have a vested interest in the system's safety and security.

The core challenge then becomes **how to measure risk and harm for industrial systems**. This is typically quantified by analyzing the likelihood of a specific event occurring and the severity of its consequences, which in an industrial context translates to operational downtime, equipment damage, safety incidents, and environmental impact.

To accurately measure this, we must define specific **attack scenarios, tactics, and techniques**. These scenarios create a narrative of how an attack would unfold, using real-world adversarial methods, which allows for a concrete evaluation of the attack paths and their potential success.

This analysis directly informs **how to evaluate and manage risks**. Evaluation involves scoring the risks based on their measured likelihood and impact, allowing for prioritization. Risk management involves deciding on a strategy—whether to accept, avoid, transfer, or mitigate each risk—and implementing the appropriate security controls.

The principles of measurement are applied with domain-specific nuances. For connected and autonomous systems, **how to measure risk and harm for vehicles** focuses on impacts on passenger safety, vehicle control, and privacy. At a larger scale, **how to measure risk and harm for platforms and infrastructures** assesses systemic risks, such as cascading failures in a transportation network or the disruption of a port's logistics operations.

Ultimately, this entire discipline of **risk assessment contributes to secure design in ICS and transportation** by providing objective data. It answers critical design questions: Where are the weakest links? What are the most credible threats? This evidence-based approach ensures that security is architected into the system where it is most needed, rather than being applied indiscriminately.

This leads to a fundamental question: **Does a general approach to risk assessment exist?** While standardized methodologies like NIST SP 800-30, ISO 27005, or TARA exist, there is no universal one-size-fits-all formula. The core principles are consistent, but the specific approach must be tailored to the unique cybersecurity objectives, architecture, operational technology, and consequence profile of the system in question, whether it is a power plant, a car, or an air traffic control network.

30 min

Video Demo

By Alexander Nikolaev

This demo offers a visual and engaging video of a realistic looking attack scenario targeting a modern industrial facility. The scenario synthesizes the core concepts, adversarial techniques, and defensive principles covered throughout our two-day training, providing a dynamic illustration of how theoretical knowledge translates into a tangible sequence of events, from initial compromise to operational impact.

30 min

Quiz

30 min

Considerations on the seminars, workshops and thesis topics