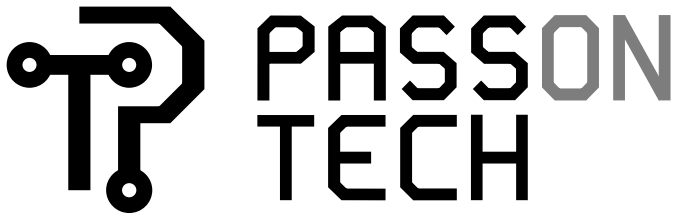
Thomas Passon

IT Security and Safety in Cyber-Physical Systems

Strategies for Risk Minimization and Standards Enhancement

v1.0.0
www.github.com/tpasson/doc-it-security-and-safety
www.passon.tech



Contents

B

BA · *Benefit of Attack*
BCRA · *Benefit-to-Cost Ratio of Attack*

C

CA · *Cost of Attack*

I

IoT · *Internet of Things*
IT · *Information Technology*

1 Introduction

„Das Internet ist für uns alle Neuland.“ - Angela Merkel
„The Internet is uncharted territory for all of us.“ - Angela Merkel

In a memorable statement[1], former German Chancellor Angela Merkel described the internet as "uncharted territory for all of us," a description that might have seemed surprising at the time of her statement and even caused amusement among some. However, over time, it has become apparent that this characterization carries a deeper truth and remarkable foresight. Indeed, the internet is a constantly evolving and rapidly advancing phenomenon whose scope and implications for society, economy, and technology continue to raise new questions. Today, in an era where digital technologies are deeply integrated into nearly every aspect of our lives, Merkel's designation of the internet as uncharted territory appears more precise and relevant than ever.

This development of the internet not only brings cultural shifts but also confronts us with increasingly complex challenges in information technology (IT), especially around cybersecurity. The constant progress and the growing interconnection of digital systems have introduced new risks and security threats. These threats range from the danger of data theft and manipulation to complex cyberattacks that can endanger critical infrastructures such as Cyber-Physical Systems (CPS).

1.1 Cyber-Physical Systems and Internet of Things

Cyber-Physical Systems (CPS) play a critical role in the changing digital landscape by combining physical processes with network and computer technology to develop systems that can interact and control in real-time. These systems are essential to applications like industrial automation, driverless cars, and smart energy grids that depend on exact synchronization between digital and physical components to guarantee effectiveness, safety, and usability.

The Internet of Things (IoT), a possible subclass of CPS [1] [2], extends this integration by focusing on connectivity. It enables a wide range of devices to be interconnected via networks, particularly the internet, permitting seamless data interchange and communication across a wide number of industries. While CPS lays the foundation for the operational and control aspects of these interconnected devices, IoT expands on this by enabling the collection, exchange, and acquisition of data, thereby enhancing the capabilities and applications of CPS.

In essence, CPS provides the framework for the real-time integration and control crucial in today's interconnected systems, while IoT contributes by adding a layer of extensive connectivity and data exchange. The interaction of CPS with IoT increases efficiency and creativity, strengthening the bond between the digital and physical realms. Despite

[1] Angela Merkel referred to the internet as "uncharted territory" during a press conference with then-US President Barack Obama on June 19, 2013, in Berlin.

this definition's attempt at clarity, technology's ever-changing and expansive character makes it difficult to pinpoint an IoT device's exact attributes. For example, servers are usually not included in the category of IoT devices. On the other hand, depending on its functionality and network access, a tiny device with internet-connected sensors may qualify as an Internet of Things device. In this explanation, Ethernet-connected devices that provide interconnectivity shall be referred to as "Node" to accommodate for these variances and uncertainties.

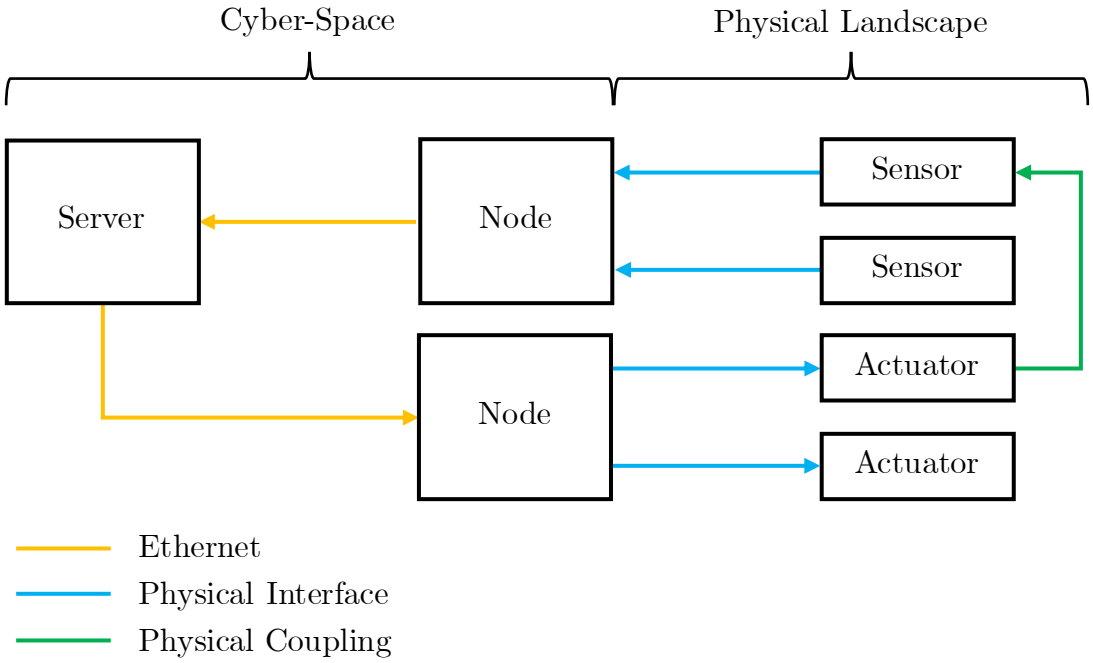


Figure 1: Example Scheme for a Cyber-Physical System

The scheme in Figure 1 presents a Cyber-Physical System (CPS) with two distinct parts:

1. In the cyber-space segment, servers and nodes are illustrated as interconnected via Ethernet, symbolizing data transfer and command pathways.
2. The physical segment is marked by sensors and actuators that interface with the physical environment.

An example within the diagram may represent a complex smart factory but also a simple room temperature regulation system, where a sensor transmits temperature readings to a node, which in turn relays the information to a cloud-based server. After processing the data, the server sends instructions to the other node to activate heaters, thus altering the temperature. This creates a feedback loop, with air serving as the medium for heat exchange to aid this process. Additionally, the system may include independent sensors and actuators that perform different functions in the CPS, all integrated within the same infrastructure.

Moreover, depending on the requirements and the derived architecture, cyber-physical systems might be higher or less integrated or even redundant while taking safety and security into consideration.

1.2 Relevance

Cyber-physical systems epitomize the rapid advancements defining the digital age, showcasing significant progress in creating more intelligent, connected, and efficient living spaces. Yet, as we delve deeper into 'uncharted territory' - a term Angela Merkel used to describe the evolving digital landscape - the critical importance of addressing privacy, cybersecurity, and ethical considerations becomes increasingly evident. This emphasizes the need for a thorough understanding of the nature and dynamics of digital threats, and for developing effective protection mechanisms based on this knowledge. Given the steadily increasing number and complexity of cyber-attacks as well as the continuous evolution of attack methods, the development of robust security strategies becomes increasingly urgent.

According to a Gartner report, cyber-physical system incidents can have numerous impacts, which include the following [3]:

- **Health and Personal Safety Risks:** Failures can lead to situations where individual health and safety are compromised, including risks in medical settings or hazardous environments.
- **Environmental Impact:** Incidents that compromise the control of environmental systems can result in pollution and other forms of ecological harm.
- **Loss of Customers:** Breaches in cybersecurity can undermine customer confidence, leading to a decline in business patronage.
- **Fees and Lawsuits Due to Negligence or Noncompliance:** Organizations can face legal actions and financial penalties when they fail to meet cybersecurity obligations.
- **Loss of Visibility Over Production and Safety Systems:** Cyber incidents may strip organizations of the ability to monitor and manage their operational and safety systems effectively.
- **Loss of Control:** A cyber-physical attack can result in the unauthorized takeover of control systems, creating chaos and danger.
- **Denial of Service:** Such attacks can bring operations to a halt, leading to service outages and shutdowns.
- **Degraded Equipment Performance and Quality of Delivered Products:** Persistent cybersecurity issues can lead to reduced efficacy and quality in products and services.
- **Operational Shutdowns:** Targeted cyberattacks have the potential to completely cease business operations.
- **Financial Loss Due to Outages, Downtime, Recovery, Increased/Denied Insurance:** The financial consequences of cyber-physical incidents extend to cover a range of direct and indirect costs.
- **Intellectual Property Theft:** Cyber incidents can lead to the loss of proprietary information, giving competitors an undue advantage.

- **Damage and Destruction of (Physical) Property and Equipment:** These incidents can cause physical damage to assets, infrastructure, and equipment, magnifying the impact of the cyberattack.

The subsequent discussion of each point reflects own experience and analyses, expanding on the foundational information provided by Gartner.

A concerning aspect of these cyber threats is the significant economic damage attributed to them. In Germany alone, the damage from data theft, industrial espionage, or sabotage amounted to a staggering 205.9 billion euros in 2023 [4].

Moreover, the relevance of this research is further amplified by the expanding footprint of the CPS and active nodes within the digital ecosystem. By 2023, IoT devices are projected to constitute half of all networked devices, with nearly a third being wireless, as reported by Cisco [5]. This surge in CPS and IoT/nodes integration introduces additional complexity to the security landscape, as it not only increases the volume of networked devices but also diversifies the types of devices and their applications in everyday life.

1.3 Methods

Against the backdrop of the outlined relevance, this book focuses on the core question: **How can innovative approaches for assessing and enhancing the security posture be developed to meet the ever-evolving requirements of cybersecurity across various IT systems, including especially the CPS?**

An integral part of this exploration includes devising a methodology for a dynamic evaluation process that adjusts over time to accommodate the changing landscape of cybersecurity. This aims at enabling continuous refinement and recalibration of security measures to counteract new and emerging threats effectively, ensuring that security strategies not only address the present challenges but are also adaptable to future developments.

To explore this central question, this book outlines several targeted objectives:

- **Detailed Exploration of Cybersecurity Threats:** Aim to thoroughly investigate and map out the key threats that current IT systems face, as well as those that might arise in the foreseeable future. This goal involves a deep dive into the cybersecurity landscape to uncover vulnerabilities and predict potential future threats that could disrupt these tech environments.

- **Crafting and Testing New Risk Assessment and Security Boosting Methods:** The focus here is to create, implement, and rigorously evaluate new ways to accurately assess security risks. This objective strives to build a solid framework for spotting vulnerabilities within IT and IoT systems and finding the most effective ways to reduce these risks.

- **Refining the Effectiveness of Security Protocols:** This involves investigating and evaluating new strategies to strengthen existing security measures. The goal is to enhance the robustness of IT systems against a broad range of cybersecurity threats, ensuring a more secure digital space.

- **Securing Hardware and Embedded Systems:** Adding to the above, this objective emphasizes the security of hardware and embedded systems, which are crucial in IT systems. It aims to identify specific security challenges related to these components and develop strategies to assess and improve their security. This includes safeguarding against physical tampering, firmware exploitation, and ensuring secure communication between devices.

- **Ensuring Safety in Cyber-Physical Systems (CPS):** This objective focuses on integrating safety measures within cybersecurity strategies for CPS. It aims to develop approaches that not only protect against cyber threats but also ensure the operational safety of these systems, which often control critical infrastructure and industrial processes. This includes real-time monitoring and response systems to prevent and mitigate the impact of cyber-attacks on physical operations.

2 Economic Principles

2.1 The Benefit-to-Cost Ratio of Attack

In the context of cybersecurity, the concept of the Benefit-to-Cost Ratio of Attack (BCRA), as discussed in "Softwar" by Jason P. Lowery from 2023, offers a profound analogy to nature and its survival strategies. This concept illustrates how organisms in nature must constantly balance their own BCRA to secure their survivability - a notion that seamlessly translates to the digital security landscape, [6, p. 67].

The BCRA is defined as the ratio between the benefit of an attack (BA) and the cost of that attack (CA), formally expressed by the equation [6]:

$$BCR_A = \frac{B_A}{C_A}$$

Here, BCRA stands for the Benefit-to-Cost Ratio of Attack, BA for the Benefit of Attack, and CA for the Cost of Attack [6].

This formula enables the quantitative assessment of the attractiveness and vulnerability of networks and systems to cyber-attacks. Just as organisms in nature must increase their ability to inflict physical costs on attackers to optimize their own BCRA, digital entities must strengthen their security mechanisms to raise the costs for potential attackers and thus minimize their attack surface [6]. The analogy to Lowery's description provides a perspective that clarifies how the management of security risks in IT systems follows a similar economic principle rooted in primordial survival in nature.

In an era where cyber-attacks are becoming increasingly sophisticated, understanding the BCRA underscores the need for organizations and individuals to proactively take measures that minimize the potential benefits for attackers as well as maximize the costs and difficulties of a successful attack. Insights from Lowery's "Softwar" encourage a strategic reassessment of cybersecurity that goes beyond traditional protective measures and promotes a more dynamic, economically oriented way of thinking about security.

2.2 The Extended Benefit-to-Cost Ratio of Attack

The current model of the Benefit-to-Cost Ratio of Attack (BCRA) is static, considering the benefits and costs at a specific point in time. However, cybersecurity threats and the defensive measures against them are dynamic and evolve continuously. Thus, it is hypothesized that the BCRA model can be extended to include a time-variant analysis.

We introduce a time-variant BCRA, denoted as $bcr_A(t)$, where the benefits of attack $b_A(t)$ and the costs of attack $c_A(t)$ are functions of time. The time-dependent BCRA is formally expressed as:

$$bcr_A(t) = \frac{b_A(t)}{c_A(t)}$$

This dynamic model aims to assess how the attractiveness and vulnerability of systems to cyber-attacks change over time. By analyzing $bcr_A(t)$, it is possible to identify trends and predict potential future vulnerabilities. This proposed approach provides a potentially more robust framework for understanding and managing cybersecurity risks, with the goal of ensuring that security strategies not only address present challenges but are also adaptable to future developments.

2.2.1 Time-Variant and Time-Dependent Systems in Systems Engineering

In systems engineering, understanding the difference between time-variant and time-dependent systems is crucial for designing effective strategies and solutions.

Time-Variant Systems: These systems exhibit behaviors and characteristics that change over time. The parameters and structures of these systems are not constant and can evolve due to external influences or internal dynamics. In the context of IT infrastructure, a time-variant system reflects the reality of ever-changing technology and threat landscapes. For example, cybersecurity defenses must adapt continuously to new types of attacks and changing network configurations. The Benefit-to-Cost Ratio of Attack (BCRA) in such systems is inherently dynamic, as both the benefits and costs of attacks fluctuate with time and varying circumstances.

Time-Dependent Systems: These systems are characterized by changes or responses that are a function of time, but their underlying structure or parameters remain consistent. Time-dependent systems can be predicted and modeled with a high degree of accuracy over short periods, as their behaviors follow a known pattern or trend. In the context of BCRA, short-term predictions can be made by observing current trends and projecting them into the near future. This approach assumes a relatively stable environment where changes occur predictably.

In the context of BCRA, IT infrastructure can be considered time-variant because the infrastructure changes and threats are not entirely predictable. However, for short time spans, we can make time-dependent predictions, assuming the changes are minimal, and the system's behavior remains relatively stable. This dual approach allows for both immediate, tactical responses and long-term, strategic planning in cybersecurity management.

2.3 Resource Exhaustion Attack and API Abuse Scenario

In this section, we apply the BCRA to a real-world scenario involving a resource exhaustion attack, specifically targeting API abuse. We calculate the financial impact of such an attack on a web server, considering the costs associated with both valid and invalid requests over a 24-hour period, assuming the request rate is constant.

Scenario Details

- **Cost per 1,000 http GET requests:** $K_R = 0.0004$ USD [7]
- **Invalid requests:** $R_I = 200/s$ (requests per second)
- **Time period:** $T = 86400\,s$ (24 hours)

To calculate the harm in terms of the benefit of attack B_A, we use the following formula:

$$B_A = R_I\, K_R\, T$$

Insert the given values into the formula:

$$B_A = \frac{200}{s} \cdot \frac{0.0004\,USD}{1000}\, 86400\,s$$

Which equals:

$$B_A \approx 6.91\,USD$$

harm per day.

For a generic calculation where the invalid requests might vary over time, we can express the rate of invalid requests as a function of time, $r_I(t)$, and calculate the total harm using an integral over the 24-hour period:

Define the integral for the benefit of attack calculation considering the function rate of requests $r_I(t)$:

$$b_a(t) = K_R \int_0^T r_I(t)\, dt$$

For the constant request rate:

$$b_a(t) = \frac{0.0004\,USD}{1000} \int_0^{86400s} \frac{200}{s}\, dt$$

Simplify the term and solving the integral:

$$b_a(t) = \frac{0.0004\,USD}{1000} \cdot \frac{200}{s} \int_0^{86400s} dt$$

$$b_a(t) = \frac{0.00008\,USD}{s} \int_0^{86400s} dt$$

$$b_a(t) = \frac{0.00008\,USD}{s} \cdot t \Big|_0^{86400s}$$

$$b_a(t) = \frac{0.00008\,USD}{s} \cdot 86400s$$

$$b_a(t) \approx 6{,}91\,USD$$

Conclusion

In practical terms, considering a resource exhaustion attack on a web server reveals the tangible financial impact such an attack can have. For instance, the calculated daily harm of approximately $6.91 may seem minimal. However, when leveraging a botnet or compromised computers, the cost of executing such attacks is virtually negligible for the attacker, as they utilize resources they effectively control at no additional expense. This leads to a high BCRA in this example, as the benefit of the attack (BA) significantly outweighs the cost of the attack (CA). Furthermore, the potential harm can be exponentially higher if the scale of the attack increases. Hypothetically, if an attack targets multiple servers or an entire infrastructure, the financial damage could escalate to millions of dollars. This scenario underscores the critical need for robust and adaptive security measures.

Ultimately, the BCRA framework, particularly when extended to a time-variant model, offers a comprehensive tool for understanding and mitigating the economic impacts of cyber-attacks. This dual approach of addressing both immediate and long-term security challenges reinforces the importance of a strategic, economically oriented mindset in cybersecurity management. By continuously adapting to the shifting threat landscape, organizations can better protect their digital assets and reduce their attack surface, ensuring a more resilient cyber defense posture.

2.4 Mitigating Resource Exhaustion Attacks with Increased Cost of Attack

One effective method to mitigate resource exhaustion attacks is by imposing infinitely scalable physical costs on control signals, inspired by the proof-of-power concept discussed in "Softwar" by Jason P. Lowery from 2023. By requiring proof-of-power receipts, the system can ensure that each control action incurs a significant physical or financial cost [6, p. 297].

2.4.1 Proof-of-Power Wall Concept

To mitigate cyber-attacks like Distributed Denial-of-Service (DDoS), E-Mail spam, API resource exhaustion, proof-of-power concept [6, p. 297] can make it superfluously costly to send control signals. By requiring proof-of-power stamps, the cost of executing malicious actions rises significantly, deterring attackers.

The proof-of-power wall concept works by rejecting all control actions that do not present proof-of-power receipts. This guarantees that only low BCRA (Benefit-to-Cost Ratio of Attack) signals are processed, thus enhancing systemic security against exploitation and abuse.

- Scalable Difficulty:
  - The difficulty of generating proof-of-power receipts can be dynamically adjusted to increase the physical costs for attackers.
  - During an attack, increasing the complexity of the proof-of-power algorithm escalates the cost for attackers, making sustained attacks economically unviable.
- Monetary Fees for Requests:
  - Introducing a small fee for each request can add an additional layer of economic dissuasion. Even a tiny cost per request can accumulate quickly, creating a significant financial barrier for attackers.
- Enhanced Security Posture:
  - By ensuring that only high-cost, low BCRA control signals are processed, the system maintains a robust defense against resource exhaustion attacks.
  - This adaptive security measure provides a sustainable approach to protecting digital assets.

Increasing the cost of cyber-attacks through proof-of-power protocols provides a strategic advantage in cyber security. By making control signals costly to execute, attackers face significant physical and economic barriers, reducing the feasibility of attacks. This approach aligns with the strategic goal of decreasing BCRA and enhancing the resilience of digital assets against persistent threats.

2.5 Symbols

K_R	Cost per request (USD)
T	Time period (s)
r_I	Time dependent invalid requests (s^{-1})
R_I	Invalid requests (s^{-1})
b_A	Time dependent benefit of attack (USD)
c_A	Time dependent cost of attack (USD)
B_A	Benefit of attack (USD)
C_A	Cost of attack (USD)
bcr_A	Time dependent Benefit-to-Cost Ratio of Attack
BCR_A	Benefit-to-Cost Ratio of Attack

3 Hardware Security

To be continued.

4 Figures

5 Bibliography

[1] L. Camarinha-Matos, J. Goes, L. Gomes and J. Martins, IFIP Advances in Information and Communication Technology, 2013.

[2] C. Barry, "Defining cyber-physical systems and other connected 'things'," 6 October 2023. [Online]. Available: https://blog.barracuda.com/2023/10/06/defining-cyber-physical-systems-and-other-connected-things. [Accessed 16 March 2024].

[3] Gartner, "Microsoft," Gartner, 2021. [Online]. Available: https://techcommunity.microsoft.com/t5/microsoft-defender-for-iot-blog/understanding-cyber-physical-system-and-iot-ot-risk-featuring/ba-p/3030164. [Accessed 17 March 2024].

[4] Statista, "Schäden durch Computerkriminalität in deutschen Unternehmen," [Online]. Available: https://de.statista.com/statistik/daten/studie/444719/umfrage/schaeden-durch-computerkriminalitaet-in-deutschen-unternehmen/. [Accessed 23 February 2024].

[5] Cisco, "Cisco Annual Internet Report (2018–2023) White Paper," [Online]. Available: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html. [Accessed 15 March 2024].

[6] J. P. Lowery, Softwar: A Novel Theory on Power Projection and the National Strategic Significance of Bitcoin, Massachusetts Institute of Technology, 2023.

[7] "Amazon S3 Preise," [Online]. Available: https://aws.amazon.com/de/s3/pricing/. [Accessed 07 July 2024].