

## Seminar Cyber-Physical Systems

# Security Considerations for Cyber-Physical Systems

Maximilian Ammann  
Bachelor Informatik

Datum des Vortrags \_\_\_\_\_

### **Kurzfassung**

Eine kurze Zusammenfassung der Ausarbeitung mit 10-12 Zeilen Text.

# Inhaltsverzeichnis

<b>1</b>	<b>Einführung</b>	<b>3</b>
<b>2</b>	<b>Aspekte eines Angriffes</b>	<b>4</b>
2.1	Security Definition für Cyber-Physical Systems . . . . .	4
2.2	Cyber-Physical Systems als Angriffsziel . . . . .	4
2.3	Angriffszenarien . . . . .	4
2.3.1	Klassische Szenarien . . . . .	4
2.3.2	Denial-of-Service Angriff . . . . .	4
2.3.3	Man-in-the-Middle Angriff . . . . .	4
2.3.4	Täuschungsangriff (Deception) . . . . .	4
2.3.5	Lauschangriff (Eavesdropping) . . . . .	4
2.3.6	Compromised-Key Angriff . . . . .	4
2.4	Angreifergruppen . . . . .	4
2.5	Gegenmaßnahmen . . . . .	4
2.5.1	Modellierung von Cyber-Physical Systems (als Grundlage) . . . . .	4
2.5.2	Physische Maßnahmen . . . . .	4
2.5.3	Organisatorische Maßnahmen . . . . .	4
2.5.4	Präventive Maßnahmen . . . . .	4
2.5.5	Detektion und Wiederherstellung (Detection and Recovery) . . . . .	4
2.5.6	Widerstandsfähigkeit (Resilience) . . . . .	4
2.5.7	Abschreckung (Deterrence) . . . . .	4
<b>3</b>	<b>Evaluation aktueller Maßnahmen</b>	<b>4</b>
<b>4</b>	<b>Literatur</b>	<b>5</b>

# 1 Einführung

Betriebsblindheit beschreibt einen Zustand in dem man sich Aufgrund weitreichendes Prozesswissens nicht über Fehler oder Mängel bewusst ist [GK16, S. 202]. Ist dieser Zustand einmal erreicht ist es schwer ihm wieder zu entfliehen und die Probleme in beispielsweise der Sicherheit<sup>1</sup> zu erkennen. Deshalb ist ein Ziel der Arbeit zu Motivieren sich mit Sicherheit auseinander zu setzen. Besonders in Cyber-Physical Systems ist es wichtig sich mit Sicherheit zu befassen, da diese eine erhöhte Angriffsfläche für Angriffe bereitstellen, um diese Blindheit nicht auftreten zu lassen. Gleichzeitig sind die Herausforderungen die ein solches System lösen soll und die damit verbundenen Anforderungen anderer Art als bei klassischen Systemen.

Bei Cyber-Physical Systems sind oft eingebettete echtzeit Systeme, welche eine hohe Verfügbarkeit, Robustheit, Widerstandsfähigkeit und Berechenbarkeit aufweisen müssen. Die physische Welt macht Verfügbarkeit allerdings oft schwierig und ist alles andere als berechenbar [Lee08]; [Sha+08];. Einsatzorte für diese Systeme könnten intelligente Stromnetze, symbiotische Sensornetzwerke für die Agrarwirtschaft und Katastrophenabwehr, medizinische oder assistierende Geräte, intelligente Verkehrssteuerung und intelligente Gebäude sein [Raj+10]. In all diesen Beispielen spielt zudem ein hohes Maß an Vertrauen eine Rolle [Sha+08]. Zudem unterliegt man konzeptionell bedingt auch einigen Restriktionen wie beispielsweise die Bindung an eine Batterie oder leichte Bauweise [Yan+17]. Es existiert also ein Unterschied in den Anforderungen an Cyber-Physical Systems zu klassischen Systemen, wie Anwendungsservern oder Heimcomputern.

In Kapitel 2.1 wird zunächst der Begriff Sicherheit speziell für Cyber-Physical Systems definiert. In den Kapiteln 2.2, 2.3, 2.4 werden mögliche Angriffsszenarien beleuchtet um im Kapitel 2.5 adequate Gegenmaßnahmen darzustellen. Zuletzt soll im Kapitel 3 auf vergangene Vorfälle im Bereich der Security eingegangen werden.

---

<sup>1</sup>Sicherheit wird hier (falls nicht anders hingewiesen) unter dem Begriff der Security verstanden

## **2 Aspekte eines Angriffes**

### **2.1 Security Definition für Cyber-Physical Systems**

### **2.2 Cyber-Physical Systems als Angriffsziel**

### **2.3 Angriffsszenarien**

#### **2.3.1 Klassische Szenarien**

#### **2.3.2 Denial-of-Service Angriff**

#### **2.3.3 Man-in-the-Middle Angriff**

#### **2.3.4 Täuschungsangriff (Deception)**

#### **2.3.5 Lauschangriff (Eavesdropping)**

#### **2.3.6 Compromised-Key Angriff**

### **2.4 Angreifergruppen**

### **2.5 Gegenmaßnahmen**

#### **2.5.1 Modellierung von Cyber-Physical Systems (als Grundlage)**

Noch nicht sicher.

Um hierbei dem Standard an Sicherheit zu genügen schlägt Lee sogar vor eine neue Grundlage für diese Systeme zu etablieren [Lee08].

#### **2.5.2 Physische Maßnahmen**

#### **2.5.3 Organisatorische Maßnahmen**

#### **2.5.4 Präventive Maßnahmen**

#### **2.5.5 Detektion und Wiederherstellung (Detection and Recovery)**

#### **2.5.6 Widerstandsfähigkeit (Resilience)**

#### **2.5.7 Abschreckung (Deterrence)**

## **3 Evaluation aktueller Maßnahmen**

## 4 Literatur

- [BG11] Radhakisan Baheti and Helen Gill. “Cyber-physical systems”. In: *The Impact of Control Technology*. Ed. by T. Samad and A. M. Annaswamy. IEEE Control Systems Society, 2011, pp. 161–166.
- [Bra14] Jim Brodie Brazell. “The Need for a Transdisciplinary Approach to Security of Cyber Physical Infrastructure”. In: *Applied Cyber-Physical Systems*. Ed. by Sang C. Suh et al. New York, NY: Springer New York, 2014, pp. 5–14. ISBN: 978-1-4614-7336-7.
- [Car+09] Alvaro Cardenas et al. “Challenges for securing cyber physical systems”. In: *Workshop on future directions in cyber-physical systems security*. Newark, NJ, USA, July 2009.
- [CAS08] Alvaro A. Cardenas, Saurabh Amin, and Shankar Sastry. “Secure Control: Towards Survivable Cyber-Physical Systems”. In: *The 28th International Conference on Distributed Computing Systems Workshops*. IEEE, June 2008. DOI: 10.1109/icdcs.workshops.2008.40.
- [Fru+18] M. Frustaci et al. “Evaluating Critical Security Issues of the IoT World: Present and Future Challenges”. In: *IEEE Internet of Things Journal* 5.4 (Aug. 2018), pp. 2483–2495. ISSN: 2327-4662. DOI: 10.1109/JIOT.2017.2767291.
- [GK16] Dieter Gollmann and Marina Krotofil. “Cyber-Physical Systems Security”. In: *The New Codebreakers: Essays Dedicated to David Kahn on the Occasion of His 85th Birthday*. Ed. by Peter Y. A. Ryan, David Naccache, and Jean-Jacques Quisquater. Springer Berlin Heidelberg, 2016, pp. 195–204. ISBN: 978-3-662-49301-4. DOI: 10.1007/978-3-662-49301-4\_14.
- [Hum+17] Abdulmalik Humayed et al. “Cyber-Physical Systems Security - A Survey”. In: *IEEE Internet of Things Journal* 4.6 (2017), pp. 1802–1831. DOI: 10.1109/JIOT.2017.2703172.
- [KC14] Dan Kruger and John N. Carbone. “Radically Simplifying Cyber Security”. In: *Applied Cyber-Physical Systems*. Ed. by Sang C. Suh et al. New York, NY: Springer New York, 2014, pp. 51–61. ISBN: 978-1-4614-7336-7.
- [Kou+18] Xenofon Koutsoukos et al. “SURE: A Modeling and Simulation Integration Platform for Evaluation of Secure and Resilient Cyber-Physical Systems”. In: *Proceedings of the IEEE* 106.1 (Jan. 2018), pp. 93–112. DOI: 10.1109/jproc.2017.2731741.
- [KP14] Md E. Karim and Vir V. Phoha. “Cyber-physical Systems Security”. In: *Applied Cyber-Physical Systems*. Ed. by Sang C. Suh et al. New York, NY: Springer New York, 2014, pp. 75–83. ISBN: 978-1-4614-7336-7.
- [Lan11] Ralph Langner. “Stuxnet: Dissecting a Cyberwarfare Weapon”. In: *IEEE Security & Privacy* 9.3 (2011), pp. 49–51. DOI: 10.1109/MSP.2011.67.

- [Lee08] Edward A. Lee. “Cyber Physical Systems: Design Challenges”. In: *11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC)*. IEEE, May 2008. DOI: 10.1109/isorc.2008.25.
- [Lin+17] J. Lin et al. “A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications”. In: *IEEE Internet of Things Journal* 4.5 (Oct. 2017), pp. 1125–1142. ISSN: 2327-4662. DOI: 10.1109/JIOT.2017.2683200.
- [Lu+14] Tianbo Lu et al. “An Analysis of Cyber Physical System Security Theories”. In: *7th International Conference on Security Technology*. IEEE, Dec. 2014. DOI: 10.1109/sectech.2014.12.
- [Raj+10] Ragunathan (Raj) Rajkumar et al. “Cyber-physical Systems: The Next Computing Revolution”. In: *Proceedings of the 47th Design Automation Conference*. DAC ’10. Anaheim, California: ACM, 2010, pp. 731–736. ISBN: 978-1-4503-0002-5. DOI: 10.1145/1837274.1837461.
- [SFJ17] Houbing Song, Glenn A. Fink, and Sabina Jeschke. “Overview of Security and Privacy in Cyber-Physical Systems”. In: *Security and Privacy in Cyber-Physical Systems: Foundations, Principles, and Applications*. IEEE, 2017. ISBN: 9781119226079. DOI: 10.1002/9781119226079.ch1.
- [Sha+08] Lui Sha et al. “Cyber-Physical Systems: A New Frontier”. In: *IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC 2008)*. Ed. by Mukesh Singhal et al. Taichung, Taiwan: IEEE Computer Society, June 2008, pp. 1–9. DOI: 10.1109/SUTC.2008.85.
- [Sin+16] J. Singh et al. “Twenty Security Considerations for Cloud-Supported Internet of Things”. In: *IEEE Internet of Things Journal* 3.3 (June 2016), pp. 269–284. ISSN: 2327-4662. DOI: 10.1109/JIOT.2015.2460333.
- [Wan+10] Eric Ke Wang et al. “Security Issues and Challenges for Cyber Physical System”. In: *IEEE/ACM Int’l Conference on Green Computing and Communications & Int’l Conference on Cyber, Physical and Social Computing*. IEEE, Dec. 2010. DOI: 10.1109/greencom-cpscom.2010.36.
- [Yan+17] Y. Yang et al. “A Survey on Security and Privacy Issues in Internet-of-Things”. In: *IEEE Internet of Things Journal* 4.5 (Oct. 2017), pp. 1250–1258. ISSN: 2327-4662. DOI: 10.1109/JIOT.2017.2694844.