UNIKASSEL VERSITÄT

mrt
Mess- und Regelungstechnik
Univ.-Prof. Dr.-Ing. Andreas Kroll

Bachelor-/Masterarbeit

Entwurf und Erkennung von Cyber-Attacken auf Produktionsanlagen: Methoden und Anwendung auf die Modellfabrik µPlant

N.N.

Die Vernetzung von Maschinen mittels Internettechnologien ist die Grundlage für die digitale Transformation der Industrie sowie für die 4. Industrielle Revolution (Industrie 4.0). Der so ermöglichte Datenaustausch und Datenzugriff ermöglicht Funktionen angefangen von zustandsorientierter Wartung über Energieeinsparungen durch vorausschauende Betriebsführung bis hin zu selbstoptimierenden und resilienten Produktionsanlagen.

Andererseits vereinfacht der Einzug von Internettechnologien in den maschinennahen Bereich Angriffe auf Produktionseinrichtungen. Verschiedene Cyber-Attacken haben gezeigt, dass konventionelle Schutzmaßnahmen wie Firewalls oder Virenscanner zur Bedrohungsabwehr nicht ausreichen. Vielmehr sind maschinennahe Maßnahmen erforderlich, die Kenntnisse der Maschinendynamik wie auch der Automatisierungs- und Regelungssysteme erfordern. Ein bekanntes Beispiel ist der Stuxnet-Angriff auf eine Siemens-Steuerung einer Uran-Anreicherungsanlage, der unentdeckt blieb und so etwa 1000 Zentrifugen zerstören konnte.

Seit wenigen Jahren erfolgt eine wissenschaftliche Auseinandersetzung mit dem Problemfeld. Insbesondere werden regelungstechnische Methoden eingesetzt, die den Maschinenzustand prädizieren und mit dem beobachteten vergleichen, um einen Cyber-Angriff zu detektieren.

Im Rahmen dieser Arbeit soll eine in der Literatur vorgestellte zustandsorientierte Methodik zur Detektion von Cyberattacken auf Maschinen untersucht, umgesetzt und am Beispiel der Modellfabrik µPlant getestet und bewertet werden. Ziel von Angriffen in der Modellfabrik kann bspw. das Überlaufen von Tanks oder das Trockenlaufen von Pumpen sein. In der Modellfabrik entsprechen Signale und Automatisierungssysteme einer realen Produktionsanlage, aber es kann gefahrlos experimentiert werden, ohne Risiken für Menschen, Güter oder Umwelt zu verursachen. Folgende Teilaufgaben sollen bearbeitet werden:

- Einarbeitung in Entwurf und Erkennung maschinennaher Cyberangriffe
- Erarbeitung von Angriffsszenarien auf die Prozessinsel I oder II der Modellfabrik
- Identifikation von Prozessmodellen mittels Subspace-Identifikation
- Konzeption und Umsetzung einer Zustandsschätzung (bspw. Kalmanfilter) und Residualbewertung (bspw. Grenzwerte oder CUSUM) zwecks Angriffsdetektion
- Entwurf verdeckter (Stealth) Angriffe und Untersuchung der Grenzen der Detektierbarkeit bei verrauschten Signalen und der Unterscheidbarkeit von Effekten bei Komponentenversagen
- Dokumentation und Kolloquiumsvortrag.

Betreuer: Prof. Dr.-Ing. A. Kroll, Dr. H.J. Sommer

Beginn: sofort möglich

Geplantes Ende: TBD

Literaturhinweise:

[1] A. Athalye, C. M. Ahmed, J. Zhou. Model-based CPS attack detection techniques: strengths and limitations. In: A.I. Awad et al. (eds.) Security in cyber-physical systems, Springer, 2021.

[2] C. M. Ahmed, C. Murguia, J. Ruths. Model-based attack detection scheme for smart water distribution networks, ASIA CCS ‘17, Abu Dhabi, 101-113, 2017.

[3] J. Giraldo et al. A survey of physics-based attack detection in cyber-physical systems, ACM Computing Surveys 51, No. 4, p. 76:1 – 76:36.

[4] E. Bou-Harb. A brief survey of security approaches for cyber-physical systems. 8th IFIP International Conference on New Technologies, Mobility and Security (NTMS), Larnaca, Cyprus, 2016.