

Dissertation

Entwicklung einer Referenzarchitektur zur Integritätssicherung von Cyber- Physischen Systemen in dynamischen Produktionsumgebungen

Vom Fachbereich Maschinenwesen und
Verfahrenstechnik der
Universität Kaiserslautern
zur Verleihung des akademischen Grades
Doktor-Ingenieur (Dr.-Ing.)
genehmigte Dissertation

Vorgelegt von
Diplom-Ingenieur Fabian Quint
aus Darmstadt

Tag der mündlichen Prüfung: 20.04.2018

Dekan: Prof. Jörg Seewig

Promotionskommission:

Vorsitzender: Prof. Hans-Jörg Bart

1. Berichterstatter: Prof. Detlef Zühlke

2. Berichterstatter: Prof. Martin Ruskowski

3. Berichterstatter: Prof. Martin Eigner

Inhalt

1	Einleitung.....	1
2	Stand der Technik.....	5
2.1	Grundlagen der IT-Sicherheit im Kontext der Automatisierungstechnik.....	5
2.1.1	Begriffsdefinition Sicherheit.....	5
2.1.2	Schutzziele der IT-Sicherheit.....	6
2.1.3	Bedrohungsanalyse und -bewertung.....	8
2.1.3.1	Methoden der Bedrohungsanalyse.....	9
2.1.3.2	Methoden der Bedrohungsbewertung.....	14
2.1.4	Allgemeine Maßnahmen der IT-Sicherheit.....	17
2.1.5	Gesetzliche Vorgaben und Normen der IT-Sicherheit.....	19
2.1.5.1	Gesetzliche Vorgaben.....	19
2.1.5.2	Normen und Standards.....	21
2.1.6	Zwischenfazit.....	23
2.2	Grundlagen der Steuerung von Produktionssystemen und Anforderungen an zukünftige Anlagensteuerungen.....	24
2.2.1	Steuerungsarchitekturen heutiger Produktionssysteme.....	24
2.2.2	Entwicklungstendenzen in der Produktionsautomatisierung.....	27
2.2.2.1	Verteilte Prozesssteuerung.....	27
2.2.2.2	Modularisierung.....	29
2.2.2.3	Softwarezentrierung.....	30
2.2.2.4	Cyber-Physische Systeme.....	31
2.2.2.5	Architekturmodelle.....	35
2.2.2.6	Kommunikationsprotokolle.....	41
2.2.3	Zwischenfazit.....	48

2.3	IT-Sicherheitskonzepte	50
2.3.1	IT-Sicherheitskonzepte heutiger Produktionssysteme	50
2.3.2	Anforderung an industrielle IT-Sicherheit	52
2.3.3	Kryptographie.....	55
2.3.4	Organisatorische IT-Sicherheit.....	63
2.3.5	Zwischenfazit	65
3	Problemstellung, Zielsetzung und Vorgehensweise	67
3.1	Problemstellung	67
3.2	Zielsetzung	68
3.3	Vorgehensweise	69
4	Entwicklung einer Referenzarchitektur zur Integritätssicherung von Cyber-Physischen Systemen in dynamischen Produktionsumgebungen	71
4.1	Entwicklungsmethodik und Gestaltungsparadigmen	71
4.2	Basisarchitektur	72
4.2.1	Systemkomponenten der Basisarchitektur	73
4.2.2	Rollen.....	74
4.2.3	Prozesse.....	76
4.3	Anforderungsanalyse und Systemabgrenzung.....	78
4.3.1	Anforderungen an die Basisarchitektur.....	78
4.3.2	Anforderungen hinsichtlich IT-Sicherheit.....	80
4.4	Methodische Entwicklung der Referenzarchitektur.....	84
4.4.1	Entwicklung eines abstrakten Architekturmodells durch Reengineering.....	84
4.4.2	Ableitung der Systemkomponenten.....	85
4.4.3	Entwicklung der Systemkomponenten.....	94
4.4.3.1	Cyber-Physisches System und Sicherheitsmodul.....	94
4.4.3.2	Authentifizierung	95

5	Prototypische Implementierung der Architektur zum Nachweis der Machbarkeit	105
5.1	Beschreibung des Demonstrators.....	105
5.2	Beschreibung des Anwendungsszenarios	111
5.3	Implementierung der Referenzarchitektur.....	117
5.3.1	Entwicklungsumgebung / Frameworks	117
5.3.2	Implementierung.....	119
6	Bewertung und Ausblick	121
6.1	Ergebnisse und Bewertung der Arbeit	121
6.2	Ausblick für Forschung und Industrie.....	125
7	Zusammenfassung	127
8	Literaturverzeichnis	129