

Inhaltsverzeichnis

Vorwort	I
Zusammenfassung	III
Abstract	V
1. Einleitung	1
1.1 Motivation	1
1.2 Zielsetzung	3
1.3 Aufbau der Arbeit	3
2. Verwandte Arbeiten	5
2.1 Ermittlung der Signalgüte eines gesendeten Zeitzeichensignals	5
2.2 Sicherheitsdienst für schmalbandige Funkkanäle	5
2.3 Bestimmung des Sekundenbeginns aus einem gesendeten Zeitzeichensignal	7
2.4 Network Time Protocol	8
2.5 Verifikation von Zeitinformationen mit digitalen Signaturen	11
2.5.1 Verifikationsmechanismen von Daten mit digitalen Signaturen	11
2.5.2 Integration digitaler Signaturen in einen Broadcast-Funkdienst	12
2.5.3 Sicherheitsanalyse und Realisierungsaufwand	14
2.6 Verifikation von Zeitinformationen in Empfängern mit integriertem Rückkanal	16
2.6.1 Einleitung	16
2.6.2 Verfahren	16
2.6.3 Sicherheitsanalyse für Empfänger mit integriertem Rückkanal	18
3. Broadcast Zeitverteildienste	19
3.1 Einführung	19
3.2 Langwellen-Zeitverteildienste	19
3.2.1 DCF77 Zeitzeichendienst	19
3.2.2 JJY40/60 Zeitzeichendienst in Japan	23
3.2.3 WWVB Zeitzeichendienst in Amerika	25
3.2.4 MSF Zeitzeichendienst in Großbritannien	27
3.3 Amerikanische Kurzwellen-Zeitzeichensender WWV und WWVH	28
3.4 Zeitinformationen in der Funkrundsteuertechnik	29
3.5 Zeitinformationen in globalen Navigationssystemen	34
3.5.1 Einleitung	34
3.5.2 NAVSTAR-GPS	35
4. Sicherheitsanalyse bestehender Broadcast Zeitverteildienste	41
4.1 Einleitung	41
4.2 Angriffe auf drahtlose Broadcast-Zeitverteildienste	42

4.3 Systemanalyse für Broadcast Zeitverteildienste	42
4.4 Bedrohungsanalyse	44
4.4.1 Allgemein	44
4.4.2 Passive Angriffe	45
4.4.3 Aktive Angriffe	46
4.4.3.1 Denial of Service (DoS)	47
4.4.3.2 Man in the middle (MITM)	49
4.4.3.3 Replay-Angriff	50
4.4.4 Auswertung	51
4.5 Definition von Sicherheitsanforderungen	51
5. Verifikation von Zeitinformationen durch Auswertung der Trägerfrequenz	55
5.1 Einleitung	55
5.2 Grundlagen der Zeit- und Frequenzmessung	56
5.3 Definition von Zeitzeichen und Zeittelegramme	58
5.4 Verfahren	59
5.5 Physikalische Differenzzeitmessung	65
5.5.1 Einleitung	65
5.5.2 Zeitmessung mit FSK-modulierten Empfangsdaten	65
5.5.3 Zeitmessung mit ASK-modulierten Empfangsdaten	67
5.5.4 Zeitmessung mit PSK- und BPSK-modulierten Daten	69
5.5.5 Zeitmessung in Codemultiplex-Systemen	71
5.6 Kombinationen von Modulationsverfahren	72
5.7 Beispielszenarien	72
5.8 Variationsmöglichkeiten	75
5.8.1 Taktquelle Netzfrequenz	75
5.8.2 Taktquelle interne Oszillatoren	77
5.9 Sicherheitsanalyse	77
6. Restrisikoanalyse	79
7. Implementierung der Verifikationslogik	81
7.1 Einleitung	81
7.2 Implementierung der Testempfänger	84
7.2.1 FPGA-Verifikationslogik für DCF77	85
7.2.2 FPGA-Verifikationslogik für Funkrundsteuerzeittelegramme	89
7.2.3 Die Messauswertung	93
8. Testumgebung und Testergebnisse	95
8.1 Datensniffer für EFR-Funkrundsteuertelegramme	95
8.2 FSK-Sender-Frontend	96

8.3 Das Programm „Zeitanzeige“	98
8.4 Kanalmessungen EFR-Übertragungssystem	101
8.5 DCF77-Kanalmessung ohne zusätzliches Rauschen	104
8.6 DCF77-Kanalmessung mit Störrauschen	107
8.7 DCF77-Kanalmessung mit 50 Hz-Netzfrequenz	114
9. Fazit und Ausblick	117
A. Abkürzungen	119
B. Variablenverzeichnis	121
C. Patente zum Thema „Verifizierung von Zeitinformationen“	123
C.1. Patent: DE 10 2014 215 737 B3	123
C.2. Patent: EP 3 001 592 B1	125
C.3. Patentanmeldung: US 2017/0280402 A1	126
Abbildungsverzeichnis	127
Tabellenverzeichnis	131
Literaturverzeichnis	133
Patente und Patentanmeldungen	143