

SPIS TREŚCI

1. Wprowadzenie.....	11
2. Zasady zapewnienia bezpieczeństwa w kolejowych systemach sterowania ruchem.....	13
2.1. Normy europejskie dotyczące bezpiecznych urządzeń stosowanych w transporcie kolejowym.....	13
2.2. Poziomy nienaruszalności bezpieczeństwa SIL.....	17
2.3. Pojęcie dowodu bezpieczeństwa.....	19
3. Analiza bezpieczeństwa systemów sterowania ruchem kolejowym.....	21
3.1. Zagadnienie bezpieczeństwa systemów.....	21
3.1.1. Stany systemu ze względu na bezpieczeństwo.....	21
3.1.2. Systemy zabezpieczające.....	22
3.1.3. Klasy systemów zabezpieczających.....	22
3.1.4. Bezpieczeństwo systemu.....	23
3.1.5. Sposoby zwiększania bezpieczeństwa systemów sterowania.....	23
3.1.6. Zwiększania bezpieczeństwa systemów srk.....	23
3.1.7. Wymagania bezpieczeństwa dla przekaźnikowych systemów srk.....	24
3.1.8. Wymagania bezpieczeństwa dla przekaźnikowych systemów srk wg karty UIC.....	24
3.1.9. Wymagania bezpieczeństwa dla elektronicznych systemów srk wg karty UIC.....	25
3.1.10. Zalecenia dotyczące oprogramowania.....	26
3.1.11. Poziomy bezpieczeństwa systemów srk wg TC - IRSE.....	27
3.2. Wymagania bezpieczeństwa dla transmisji w otwartej sieci radiowej.....	29
3.2.1. Problem elektromagnetycznego przenikania informacji w systemach sterowania ruchem kolejowym wykorzystujących transmisję bezprzewodową.....	31
3.2.2. Problem bezpieczeństwa emisji w transmisji bezprzewodowej....	33
4. Ochrona informacji w kolejowych systemach radiokomunikacyjnych.....	36
4.1. Ochrona kryptograficzna informacji.....	41
4.1.1. Szyfry bezwarunkowo bezpieczne.....	44
4.1.2. Długość krytyczna kryptogramu.....	48
4.1.3. Określenie mocy szyfrów w zależności od złożoności obliczeniowych algorytmów zdolnych do złamania szyfru.....	49

4.1.4.	Bezpieczeństwo systemów kryptograficznych.....	50
4.2.	Charakterystyka metod kryptograficznych.....	51
4.3.	Szyfry symetryczne.....	52
4.3.1.	Szyfry strumieniowe.....	52
4.3.2.	Szyfry blokowe.....	60
4.3.2.1.	Tryby pracy szyfrów blokowych.....	63
4.3.2.2.	Szyfr blokowy DES.....	66
4.3.2.3.	Modyfikacje DES.....	70
4.3.2.4.	Inne szyfry blokowe.....	71
4.4.	Jednokierunkowe funkcje skrótu.....	74
4.4.1.	Algorytm funkcji skrótu SHA.....	78
4.5.	Szyfr z kluczem jawnym - publicznym.....	81
4.5.1.	Szyfr z kluczem jawnym RSA.....	81
4.5.1.1.	Szyfr ElGamala.....	84
4.5.1.2.	Asymetryczny szyfr plecakowy Merklego-Hellmana....	85
4.5.1.3.	Koperta cyfrowa.....	85
4.6.	Specjalne funkcje systemów kryptograficznych.....	86
4.6.1.	Uwierzytelnianie.....	86
4.6.2.	Podpis cyfrowy.....	92
4.6.3.	Podpis cyfrowy bazujący na szyfrze RSA.....	93
4.6.4.	Standard DSA.....	95
4.6.5.	Protokoły kryptograficzne dystrybucji kluczy.....	96
4.6.5.1.	Protokół Diffiego-Hellmana uzgadniania klucza sesyjnego.....	98
4.6.5.2.	Trzyczęściowy protokół Shamira.....	98
5.	Systemy Łączności wykorzystywane do transmisji danych w kolejowych systemach sterowania ruchem.....	102
5.1.	Bezpieczeństwo sieci w systemie GSM-R.....	105
5.1.1.	Bezpieczeństwo karty SIM (<i>Subscriber Identity Module</i>).....	107
5.1.2.	Bezpieczeństwo teleinformatyczne.....	107
5.1.3.	Bezpieczeństwo ruchu kolejowego.....	110
5.2.	Bezpieczeństwo transmisji danych dla potrzeb kolei w systemach otwartych.....	111
5.2.1.	Zagrożenia i funkcje bezpieczeństwa na podstawie normy PN EN 50159:2010.....	112
5.2.2.	Realizacja funkcji bezpieczeństwa w systemach otwartych.....	114
5.2.2.1.	Numerowanie telegramów.....	114
5.2.2.2.	Znaczniki czasu.....	114
5.2.2.3.	Ograniczenie czasu odpowiedzi.....	115
5.2.2.4.	Identyfikacja uczestników transmisji.....	115
5.2.2.5.	Potwierdzenia zwrotne.....	115
5.2.2.6.	Procedury autoryzacyjne.....	116

5.2.2.7. Zabezpieczenia kryptograficzne i kontrola integralności danych.....	116
6. Analiza możliwości bezpiecznej transmisji danych z wykorzystaniem technologii LTE w relacji tor-pojazd.....	120
6.1. Podstawowe cechy systemów LTE.....	120
6.2. Sposób pracy i architektura LTE.....	121
6.3. Techniki MIMO w LTE.....	123
6.3.1. Wykorzystanie technologii MIMO do poprawy transmisji radiowej.....	125
6.3.1.1. Wpływ efektu Dopplera na transmisję tor - pojazd. . . .	126
6.3.1.2. Wpływ technologii MIMO na BER.....	127
6.4. Wymagania stawiane systemom LTE w systemach kolei dużych prędkości.....	128
6.5. Przepływowy model sieci radiowej LTE dla potrzeb kolejowych.....	129
Podsumowanie.....	142
Bibliografia.....	144