Wybrane problemy niezawodności i bezpieczeństwa transmisji informacji w systemie GSM-R

Mirosław SIERGIEJCZYK[1], Stanisław GAGO[2]

Streszczenie
W artykule przedstawiono wybrane elementy wpływające na niezawodność i bezpieczeństwo sieci cyfrowej telefonii komórkowej GSM-R. W zakresie bezpieczeństwa telekomunikacyjnego omówiono metody oraz mechanizmy pozwalające zapewnić wymagany poziom niezawodności i dostępności sieci GSM-R, zarówno w jej części radiowej, jak i przewodowej, w trybie pracy bezusterkowej i w trybie awaryjnym. Zwrócono uwagę na wpływ sposobu eksploatacji i utrzymania na bezpieczeństwo systemu GSM-R, a także powiązania bezpieczeństwa systemu z kulturą bezpieczeństwa w gremiach administracyjno-decyzyjnych.

Słowa kluczowe: system GSM-R, transport kolejowy, transmisja, niezawodność, dostępność, kultura bezpieczeństwa

1. Wstęp

Wprowadzając projekt EIRENE (*European Integrated Railway radio Enhanced Network*), Międzynarodowy Związek Kolei (UIC) miał na uwadze głównie ujednolicenie europejskich systemów łączności kolejowej. Implementacja systemu GSM-R ma wymierne korzyści finansowe dla segmentu kolejowego. Znacznie poprawia się przepustowość linii kolejowych i zwiększa się poziom świadczonych usług. GSM-R jest systemem cyfrowej telefonii komórkowej, wykorzystywanym na potrzeby transportu kolejowego, zapewniającym cyfrową łączność głosową oraz cyfrową transmisję danych. Cechuje się infrastrukturą zlokalizowaną jedynie w pobliżu linii kolejowych. System GSM-R wraz z systemem ETCS *(European Train Control System)* tworzy system ERTMS (*European Rail Traffic Management System*), tj. Europejski System Zarządzania Ruchem Kolejowym, który ma za zadanie w ciągły sposób zbierać i przesyłać dane dotyczące pojazdu szynowego takie jak prędkość czy położenie geograficzne. System GSM-R

[1] Prof. nzw. dr hab. inż., Politechnika Warszawska, e-mail: msi@it.pw.edu.pl.
[2] Dr inż., Instytut Kolejnictwa, e-mail: sgago@ikolej.pl.

jest systemem transmisyjnym dla systemu ETCS i pośredniczy przy przekazywaniu informacji maszyniście i innym służbom kolejowym. Wymienione systemy istotnie poprawiają bezpieczeństwo ruchu kolejowego, uwrażliwiają diagnostykę pojazdu w czasie rzeczywistym oraz zwiększają przepustowość linii kolejowych przez precyzyjne określenie odległości między pociągami.

Zadaniem każdej sieci telekomunikacyjnej jest przesłanie informacji w zadanym czasie i z określoną stopą błędów. Sieć GSM-R jest systemem telekomunikacyjnym, który musi charakteryzować się wysoką niezawodnością oraz zapewniać wysoki poziom bezpieczeństwa przekazywanych danych w środowisku kolejowym. Określona dostępność sieci GSM-R jest ważną kwestią dla Zarządcy infrastruktury kolejowej, gdyż bezpośrednio wpływa na bezpieczeństwo oraz płynność ruchu kolejowego.

Podstawową usługą systemu GSM-R jest zapewnienie transmisji danych dla systemu ETCS, a dodatkową usługą jest łączność głosowa do porozumiewania się załogi pociągu z „naziemnym i mobilnym personelem kolejowym". Z punktu widzenia dostępności, czy niezawodności, usługa transmisji danych ma zdecydowanie większe wymagania niż usługa przesyłania głosu. Można postawić pytanie, czy system ETCS (poziom 2/3) może działać bez systemu GSM-R? Odpowiedź jest jednoznacznie negatywna i dlatego można stwierdzić, że system GSM-R jest składnikiem systemu ETCS. Ma to o tyle znaczenie, że zarówno w wymaganiach systemowych (SRS), jak i funkcjonalnych (FRS) nie podano wymagań dotyczących dostępności systemu GSM-R, natomiast są podane wartości dostępności dla systemu ETCS. Według dokumentu UIC ERTMS Users Group z dnia 30/09/98 „ERTMS / ETCS RAMS Requirements Specification Charter 2 – RAM" dostępność systemu ETCS (hardware) wyliczono przy określonych założeniach, na poziomie A=0,99985. Przy wyliczaniu dostępności systemu ERTMS dla kolei dużych prędkości, koleje włoskie przyjęły taki sam współczynnik dostępności dla systemu GSM-R (wraz z teletransmisją).

2. Metody zwiększenia niezawodności sytemu

Zwiększenie pewności transmisji informacji przez system GSM-R uzyskuje się przez zapewnienie odpowiedniego pokrycia radiowego wzdłuż drogi kolejowej, uzależnionego od prędkości pociągów. Dla prędkości mniejszych od 220 km/h poziom pokrycia nie powinien być mniejszy niż –95dBm, natomiast dla prędkości większych od 280 km/h nie mniejszy niż –92dBm. Prawdopodobieństwo pokrycia tymi poziomami nie powinno być gorsze niż 95% na każde 100 m linii kolejowej, natomiast przełączanie między dwiema komórkami (*handover*) powinno być realizowane wzdłuż linii kolejowej w normalnych warunkach nie gorzej niż 99,5%.

Połączenia o najwyższym priorytecie (alarmowe) powinny być realizowane w czasie krótszym niż 2 s (dla 95% połączeń).

Istotnym parametrem świadczącym o poprawności działania systemu GSM-R jest jakość świadczonych usług QoS (*Quality of Service*), na którą składa się określone prawdopodobieństwo fałszywego połączenia, opóźnienie transmisji (przekazywania) danych, ograniczony *jiter* (zmiana opóźnienia w założonych granicach), określona stopa błędów BER *(Bit Error Rate)*.

Bezpieczeństwo telekomunikacyjne jest rozumiane jako zbiór metod oraz mechanizmów, których zastosowanie zapewnia wymagany poziom pokrycia radiowego, dostępności i ciągłości świadczenia usług przez dobranie odpowiedniej struktury systemu i topologii sieci. Przeznaczenie systemu GSM-R oraz jego wpływ na bezpieczeństwo ruchu kolejowego nakłada na projektantów obowiązek zapewnienia odporności systemu na uszkodzenia i zakłócenia.

Niezwykle ważne jest opracowanie strategii zapewniającej utrzymanie niezbędnego poziomu bezpieczeństwa oraz przygotowanie planów funkcjonowania systemu w sytuacjach szczególnych zagrożeń. Scenariusze te są określane mianem *Disaster Recovery* (odtwarzanie infrastruktury po awarii) i są to procesy i procedury związane ze wznowieniem lub utrzymywaniem infrastruktury technicznej, krytycznej dla danej organizacji, po wystąpieniu katastrofy naturalnej lub wywołanej przez człowieka.

Operatorzy kolejowi muszą wyspecyfikować dla swojej sieci strategię *Disaster Recovery*, która będzie podstawą wdrożenia jej funkcjonalności. Należy ściśle określić następujące zagadnienia oraz wymagania:

- definicja awarii,
- docelowy czas odtworzenia,
- poziom usług, które są priorytetowe po odtworzeniu (rodzaje połączeń usługi o wartości dodanej),
- metoda odtworzenia (interwencja ręczna, zdalne przeprogramowywanie, lokalizacja personelu).

Określając priorytetowy poziom usług, które muszą być zachowane po odtworzeniu, można zidentyfikować krytyczne urządzenia systemu GSM-R i zapewnić ich redundancję. Architektura systemu GSM-R powinna być tak zaprojektowana, aby uwzględniała minimalne przerwy w świadczeniu usług przy uszkodzeniu jednego lub więcej elementów. Osiąga się to przez kombinację redundancji urządzeń i odporności sieci na uszkodzenie pojedynczych elementów sieciowych. Konsekwencją poważnej awarii sieci GSM-R jest przerwa w świadczeniu usług na całej sieci kolejowej w dłuższym czasie, niż to wynika ze zdefiniowanego maksymalnego czasu naprawy. W większości przypadków tę utratę spowoduje awaria:

- aktywnego podsystemu NSS (*Network Switching Subsystem*),
- sterownika BSC *(Base Station Controller),*
- podsystemu OMC *(Operation and Maintenance Centre)* – przy czym nie jest to bezpośrednie oddziaływanie.

Planowanie *Disaster Recovery* jest częścią większego procesu planowania ciągłości działania i powinno obejmować określenie procedur wznowienia aplikacji, danych, sprzętu i łączności. Wyróżnia się trzy podstawowe fazy wchodzące w skład działań dotyczących zdarzeń katastroficznych:
- faza przygotowań – przed wystąpieniem awarii lub katastrofy,
- faza przystąpienia do naprawy – rozpoczynająca się w momencie zdiagnozowania awarii lub katastrofy i podjęcia pierwszych działań mających na celu przywrócenie sprawności systemu,
- faza naprawy – rozpoczynająca się kilka dni lub tygodniu po wystąpieniu awarii lub katastrofy.

W procesie projektowania sieci zakłada się pewne scenariusze, w których poszczególne elementy systemu ulegają awarii lub zniszczeniu, np. w wyniku pożaru lub kataklizmu. Przewidywanie tego typu zdarzeń pozwala określić elementy krytyczne dla funkcjonowania całego systemu i dobrać odpowiedni sposób ich zabezpieczenia. Naturalną metodą, pozwalającą na zwiększenie niezawodności, bezpieczeństwa i dostępności sieci, jest redundancja, oznaczająca nadmiarowość, zastosowanie dodatkowych elementów. Odnosi się ona zarówno do informacji przechowywanych w rejestrach, jak i do elementów sprzętowych, które mogą być dublowane w różny sposób m.in. n+1, 1+1, 1:n. Nadmiarowość może dotyczyć wykonywania kopii całości danych lub też tylko tych, których wartość jest szczególnie ważna. Redundancji może podlegać:
- cały system,
- poszczególne podsystemy np. podsystem stacji bazowych BSS (*Base Station Subsystem)*, komutacyjno-sieciowy NSS, centrum eksploatacyjno-utrzymaniowe OMC,
- poszczególne elementy wchodzące w skład systemu np. centrala MSC (*Mobile Switching Centre*), rejestr HLR (*Home Location Register*),
- poszczególne składniki wchodzące w skład elementów systemu np. karty procesorowe centrali MSC, interfejsy.

Przy układaniu planu aplikacji *Disaster Recovery* należy rozpatrzeć kilka opcji:
1. Zdublowanie wszystkich systemów szkieletowych sieci i umieszczenie ich w innej odległej lokalizacji. W tej opcji przywrócenie funkcjonalności sieci jest najszybsze, choć koszty największe. Niezbędne też będą dodatkowe łącza telekomunikacyjne.

2. Aplikację *Disaster Recovery* dostarcza trzecia strona (np. operator sąsiedniej kolei). Należy przewidzieć wystąpienie wszystkich możliwych komplikacji przy przełączeniu podsystemu NSS GSM-R, gdyż macierzyste systemy NSS i BSS muszą być ze sobą kompatybilne.
3. Budowa w odległej lokalizacji z podłączonym zasilaniem i łączami telekomunikacyjnymi, ale bez urządzeń GSM-R. W przypadku podpisanej umowy z zaufanym dostawcą, przywrócenie funkcjonalności sieci trwałoby do kilku tygodni.
4. Rozproszenie wszystkich kluczowych urządzeń w różnych lokalizacjach, co ograniczy wpływ uszkodzenia pojedynczych elementów.

Centrala MSC i rejestr HLR są podstawowymi urządzeniami podsystemu NSS i zaleca się, aby przy wdrażaniu były one zwymiarowane jako N+1. Zapewnienie redundancji centrali MSC jest szczególnie ważne ze względu na dwie funkcje: grupowe połączenia głosowe VGCS *(Voice Group Call Service)* ze szczególnym uwzględnieniem kolejowych połączeń alarmowych REC *(Railway Emergency Call)* oraz połączeń punkt-punkt niezbędnych do funkcjonowania systemu ETCS. Zdublowane urządzenie może być zainstalowane w stanie wyczekiwania, fizycznie rozłączone z siecią lub może być w stanie aktywnym i przetwarzać dane.

W przypadku zdublowania centrali MSC rozpatruje się dwa rozwiązania:

1. *Load Sharing (z podziałem zasobów)* – każda centrala MSC jest podłączona do sieci i jest aktywna. Sterowniki BSC funkcjonujące w sieci są przypisane do poszczególnych central MSC. Ponieważ sterownik BSC może być podłączony tylko do jednej centrali MSC, w przypadku awarii wszystkie podłączone do niej sterowniki BSC stracą zdolność obsługi do momentu, aż ruch będzie przekierowany do elementu rezerwowego. Rozwiązanie to wymaga rekonfiguracji rezerwowej centrali MSC i sterowników BSC, przełączenia łączy transmisyjnych oraz uaktualnienia informacji w rejestrze VLR. Sterowniki BSC podłączone do uszkodzonej centrali MSC sygnalizują utratę usługi.
2. *Standby* (tryb rezerwy) – dodatkowa centrala MSC nie jest fizycznie połączona z siecią i pracuje w trybie rezerwy. W przypadku uszkodzenia centrali MSC, brak usługi wykazują wszystkie sterowniki BSC obsługiwane przez tę centralę. Rozwiązanie to wymaga skonfigurowania rezerwowej centrali MSC, w celu zastąpienia funkcji uszkodzonej centrali MSC (w przypadku, gdy sieć ma jedną aktywną MSC, można przyjąć, że konfiguracja MSC będącej w stanie oczekiwania jest już przygotowana), przełączenia łączy transmisyjnych oraz uaktualnienia informacji w rejestrze VLR. Sterowniki BSC podłączone do uszkodzonej centrali MSC sygnalizują utratę usługi. Liczba sterowników BSC pozostających bez obsługi jest większa niż w opcji *load sharing*, a ich konfiguracja nie jest wymagana, ponieważ rezerwowa centrala MSC zastępuje w pełni tę uszkodzoną.

Często stosowanym rozwiązaniem jest ciągła synchronizacja rejestrów VLR (*Visitor Location Register*), GCR *(Group Call Register)* oraz HLR *(Home Location Register)*, która umożliwia skrócenie czasu przełączenia na elementy rezerwowe. W przypadku zastosowania architektury R4, oprócz rejestrów mogą być dublowane oba elementy składowe centrali MSC (Serwer MSC, Brama Medialna MGW) lub tylko jeden. Jeden Serwer MSC może obsługiwać kilka Bram Medialnych MGW, związku z tym ważnym aspektem jest zapewnienie różnych dróg transmisyjnych. W przypadku zastosowania jednego Serwera MSC i kilku Bram Medialnych MGW i przy zapewnieniu co najmniej jednej alternatywnej drogi transmisyjnej, awaria którejkolwiek z bram nie spowoduje przerwy w świadczeniu usług.

Niektóre funkcjonalności kluczowe do sprawnego prowadzenia ruchu wymagają zastosowania pewnych elementów (np. węzłów sieci inteligentnej IN) i powinny być realizowane nawet w przypadku poważnej awarii. Dublowanie elementów podsystemu NSS powinno być rozpatrzone przy uwzględnieniu kluczowych usług i funkcjonalności. W celu zrealizowania takich funkcji, jak LDA (*Location Dependent Addressing*), czy REC, obligatoryjnych z punktu widzenia interoperacyjności kolei europejskich, elementy odpowiadające za ich realizację powinny być dublowane. Określając priorytetowy poziom usług, które po odtworzeniu muszą być zachowane, można zidentyfikować krytyczne urządzenia systemu GSM-R i zapewnić ich redundancję.

Należą do nich indywidualne karty i łącza telekomunikacyjne. Praktycznie zaleca się, aby były redundantne wszystkie stacjonarne łącza telekomunikacyjne, układy nadawczo-odbiorcze TRX w stacjach bazowych BTS, karty w sterowniku BSC oraz karty w transkoderze TRAU *(Tanscoder Rate Adapter Unit).* W systemie GSM-R redundancja podsystemu BSS powinna być wykonana z podwójnym pokryciem radiowym, realizowanym przez stacje bazowe BTS (kolokowane lub naprzemienne) na liniach kolejowych wyposażonych w system ETCS i wiele sterowników BSC podłączonych do jednej lub drugiej centrali MSC. Liczba sterowników BSC powinna być tak zaplanowana, aby każda linia kolejowa wyposażona w system ETCS była podłączona, do co najmniej dwóch sterowników BSC przyłączonych do dwóch różnych central MSC. Na liniach kolejowych bez systemu ETCS pokrycie radiowe może być pojedyncze, a stacje bazowe BTS naprzemiennie podłączone do dwóch różnych sterowników BSC, w miarę możliwości przyłączonych do dwóch różnych central MSC.

System GSM-R może być zaimplementowany w rozmaitych topologiach. Należy wziąć pod uwagę, że uzyskana stopa procentowa poprawnie zrealizowanych usług typu *handover* musi wynosić przynajmniej 99,5% przy standardowych warunkach działania (warunki atmosferyczne, obciążenie sieci etc.). Redundancja jest również ważna w systemach teletransmisyjnych. Zastosowanie struktur samonaprawialnych SDH, zapewnienie dwóch dróg optycznych jako rezerwowego systemu transmi-

syjnego są przykładami nadmiarowości sieci telekomunikacyjnej, zwiększającymi niezawodność i bezpieczeństwo pracy.

Zarządca infrastruktury kolejowej dysponujący określoną kwotą pieniędzy musi określić, jaka struktura systemu jest dla niego najkorzystniejsza, nie tylko z punktu widzenia obciążeń finansowych, ale i przyszłej eksploatacji systemu. Zalecane jest, aby na liniach, na których system GSM-R ma współpracować z systemem ETCS poziom 2/3, były stosowane mechanizmy niezawodnościowe. Architektura systemu GSM-R jak i systemy teletransmisyjne SDH, pozwalają projektantom systemu dostosować przyjęte rozwiązania do wymagań stawianych przez system ETCS.

Oczywiście, im jest większa redundancja, tym system jest bardziej niezawodny, co oznacza krótszy czas niedostępności systemu w ciągu roku. Ale wraz ze wzrostem redundancji sprzętu koszty utrzymania systemu wzrastają, a także muszą być brane pod uwagę skutki opóźnień wynikające z przełączania między BSC i przełączania między MSC.

W teoretycznych obliczeniach, przy założonej niezawodności poszczególnych podsystemów systemu GSM-R (NSS, BSS, system teletransmisyjny – światłowody plus urządzenia SDH) ale różnej konfiguracji sprzętu, uzyskano następujące czasy niedostępności systemu:

- pojedyncze urządzenia (NSS, BSS) niezawodność – 99,962386%, a czas niedostępności systemu 198 min/rok,
- podwójne urządzenia (NSS, BSS) niezawodność – 99,999945%, a czas niedostępności systemu 0,29 min/rok.

Jak już wcześniej wspomniano, na potrzeby systemu ETCS poziomu 2 i poziomu 3 niezawodność systemu GSM-R nie powinna być gorsza niż 99,99985%. Warunek ten jest spełniony przy redundantnych urządzeniach NSS i BSS. Pojedyncze urządzenia GSM-R powinny być stosowane tylko dla usług głosowych i innych usług transmisji danych nie związanych ze sterowaniem ruchu pociągów – niezawodność 99,91%.

Z przedstawionych wywodów wynika, że niezawodność, a pośrednio bezpieczeństwo systemu GSM-R zależy przede wszystkim od producenta (dostawcy) systemu, tzn. ważne są niezawodności poszczególnych składników systemu, ale także niezawodność zależy od właściciela (zamawiającego) systemu, który może zamówić (zainstalować) taką, a nie inną architekturę (np. z określoną redundancją lub bez redundancji).

Bezpieczeństwo systemu zależy także od średniego czasu usuwania usterek *(MTTR – Mean Time to Repair)*. Czas ten uzależniony jest także od dostawcy, ale w większym stopniu zależy od właściciela systemu. W zasadzie, wpływ producenta ogranicza się do wypracowania odpowiednich programów diagnostyczno-testujących i urządzeń takiej konstrukcji, która będzie umożliwiała szybką wymianę

uszkodzonych elementów (np. wymiana karty, wymiana modułu, itp.). Natomiast właściciel powinien opracować odpowiednie procedury zarządzania eksploatacją i utrzymaniem sieci GSM-R (O&M), co jest szczególnie istotne przy systemach rozproszonych geograficznie, do których to systemów należy zaliczyć system GSM-R.

Budując sieć komórkową należy przyjąć za pewnik, że każda, nawet najlepiej zaprojektowana i wykonana sieć, będzie ulegała awariom i uszkodzeniom. W zależności od jakości wykonania, użytych materiałów i urządzeń, uszkodzenia mogą występować z różną częstotliwością. Organizacja serwisu i utrzymania sieci jest zatem konieczna niezależnie od wielkości sieci. Od wielkości sieci i liczby użytkowników zależy natomiast struktura służb eksploatacyjnych. Można przyjąć, że:

1. Utrzymanie w sprawności technicznej elementów sieci GSM-R wymaga systematycznych prac prewencyjnych (przeglądy, pomiary) i dobrze zorganizowanych działań, będących reakcją na zdarzenia w sieci.
2. Utrzymanie sieci GSM-R jest to zespół wszystkich działań technicznych i organizacyjnych mających na celu zachowanie struktury urządzeń GSM-R w stanie umożliwiającym wypełnianie wymaganych funkcji tych urządzeń.
3. Utrzymanie obejmuje obsługę techniczną i diagnostyczną, kontrole okresowe oraz remonty urządzeń GSM-R.
4. Informacje o zdarzeniach w sieci GSM-R pochodzą z dwóch źródeł:
   - z systemu monitoringu elementów sieci oraz
   - od użytkowników sieci zgłaszających problemy techniczne.
5. Dobrze zorganizowany serwis sieci zakłada zarządzanie siecią, awariami i użytkownikami sieci.

Utrzymanie sieci GSM-R jest to działanie na granicy między techniką i użytkownikami i powinno umożliwiać:

- ujednolicenie i scentralizowanie sposobu przechowywania informacji o klientach (abonentach) oraz szybki i łatwy dostęp do tych informacji przez uprawnione komórki organizacyjne,
- wzajemne wykorzystanie przechowywanych informacji przez odpowiednie komórki organizacyjne i służby,
- monitorowanie stanu technicznego zasobów sieci GSM-R,
- określenie efektywności pracy zespołów utrzymaniowych,
- planowanie rozbudowy sieci GSM-R pod potrzeby klientów

oraz udostępniać:

- pełny zestaw danych o abonentach, strukturze sieci i jej sprawności,
- precyzyjne i szybkie testowanie łączy,
- definiowanie i generowanie raportów,

a także zapewniać bezpieczeństwo i poufność przechowywanych informacji.

Działania związane z zarządzaniem eksploatacją i utrzymaniem sieci GSM-R powinny trwać 24 godziny na dobę przez siedem dni w tygodniu. Bezpieczeństwo sieci GSM-R zależy także od czynności eksploatacyjnych, do których można zaliczyć:

- administrowanie siecią,
- monitorowanie działania elementów sieci, automatyczną detekcję zagrożeń i przeciążeń w sieci,
- zarządzanie ruchem teletransmisyjnym,
- zarządzanie zasobami,
- zarządzanie usługami,
- archiwizację stanów urządzeń i raportów,
- lokalizację i usuwanie uszkodzeń i awarii elementów sieci (kable światłowodowe, urządzenia aktywne sieci, urządzenia radiowe),
- paszportyzację sieci (ewidencja zasobów sieci, utrzymanie dokumentacji technicznej i eksploatacyjnej sieci),
- systematyczne przeglądy i prewencyjne prace konserwacyjne,
- aktywację i dezaktywację zakończeń sieci (przyłączanie i odłączanie użytkowników sieci),
- sporządzanie raportów o stanie sieci i usług,
- rekonfiguracje sieci, w tym zmiany konfiguracji struktury sieci, likwidacja elementów sieci, rozbudowa sieci o nowe elementy.

Podmiotami, które mają wpływ na bezpieczeństwo systemu GSM-R są także jego użytkownicy (interesariusze), tj. administracja, przewoźnicy, operatorzy infrastruktury. Są to podmioty, które tworzą „byt organizacyjno-decyzyjny" związany z bezpieczeństwem ruchu kolejowego. Kultura bezpieczeństwa w tej Organizacji jest wytworem indywidualnych i grupowych wartości, postaw, postrzegania, kompetencji i wzorów zachowań, które określają zaangażowanie, styl i znajomość uwarunkowań „zdrowej organizacji" oraz zarządzanie bezpieczeństwem. Kultura bezpieczeństwa jest stosowana jako program ramowy do omówienia zagrożeń i działań łagodzących negatywne skutki tych zagrożeń z perspektywy człowieka, technologii i organizacji (zainteresowanych instytucji). Kultura bezpieczeństwa wskazuje dwa kluczowe czynniki wpływające na bezpieczeństwo kolei, tj. motywacja i morale. Te czynniki są związane z innymi podstawowymi czynnikami, tj: szkoleniem, odpowiednimi procedurami, instrukcjami, harmonogramami pracy, stylem zarządzania i zasadami organizacyjnymi.

Pierwszym wyzwaniem dla Organizacji powinno być określenie „Odporności" *(resilience)* systemu, tj. *naturalnej zdolności układu do regulacji jego działania (przed lub po zakłóceniu) tak, że może on utrzymywać operacyjność po wystąpieniu uszkodzenia czy też działać poprawnie w czasie trwania zakłócania*. W początkowej fazie działania Organizacji istnieje mała wiedza dotycząca niespo-

dziewanych incydentów i w związku z tym powinien być przeprowadzony proces oceny ryzyka, w którym powinny być zdefiniowane:
1. Główne zagrożenia – czynniki techniczne, organizacyjne czy ludzkie?
2. Działania zmniejszające ryzyko i poprawę odporności na ryzyko usterki lub uszkodzenia.
3. Warunki poprawy zdolności do uczenia się w sposób aktywny, przez zainteresowane „byty".

Organizacja powinna osiągnąć poprawę bezpieczeństwa przez działania badawcze i wspólne działania (spotkania / konferencję) uczestników w zakresie:
1. Diagnozowania (identyfikacja ryzyka).
2. Planowania działań (ocena ryzyka i działania łagodzące).
3. Podejmowania działań (wykonanie).
4. Oceny (ocena realizacji i wiedzy / świadomości).
5. Pozyskania wiedzy.

Podstawowym zadaniem Organizacji powinno być opracowanie strategii „Odporności systemu" w zakresie poprawy bezpieczeństwa. W złożonych systemach, a takim jest system GSM-R, ta strategia jest opisana przez elastyczne zasady, których kluczowe słowa to:
- redundancja, aby móc przeprowadzić kontrolowaną degradację systemu oraz możliwość „odbicia" lub odzyskania zdolności operacyjnej (elastyczność systemu),
- umiejętność zarządzania redundancją,
- zdolność do utrzymania w Organizacji wspólnych koncepcji bezpieczeństwa.

Zasady bezpieczeństwa przedstawione w strategii powinny być zaimplementowane w technologii, organizacji i zespole ludzkim. Podczas eksploatacji systemu GSM-R mogą wystąpić różne niepożądane sytuacje. Do kluczowych niepożądanych sytuacji można zaliczyć:
- błąd techniczny w systemie GSM-R, utratę połączeń w systemie GSM-R (słaba odporność infrastruktury technicznej),
- nieprzewidziane błędy ludzkie ze względu na słabe wyszkolenie i brak dostatecznej wiedzy – zbyt mało dobrze wyszkolonych pracowników (słaba odporność na ryzyko w Organizacji),
- brak dobrej komunikacji między poszczególnymi bytami w Organizacji – mentalnie różna ocena ryzyka,
- słabą zdolność do obsługi sytuacji kryzysowych (słaba odporność) z powodu złego szkolenia kryzysowego.

W związku z tym należy przewidzieć działania łagodzące, które powinny przyczynić się do zmniejszenia skutków niepożądanych sytuacji. Kluczowe działania łagodzące są następujące:

1. Redundancja w systemie GSM-R w celu poprawy odporności technicznej.
2. Poprawa organizacyjnej odporności, gdy zawiedzie system GSM-R, przez stworzenie lepszych procedur w całej Organizacji (administracja, przewoźnicy, operatorzy infrastruktury).
3. Zwiększenie liczby odpowiednio przeszkolonych pracowników zajmujących się bezpieczeństwem w celu poprawy odporności w Organizacji.
4. Organizacja narad między najważniejszymi podmiotami (administracja, przewoźnicy, operatorzy infrastruktury) w celu poprawy przewidywalności usterek.
5. Modernizacja scenariuszy szkolenia w zakresie przewidywanych sytuacji kryzysowych, których celem będzie poprawa odporności.

3. Zakończenie

System GSM-R jest składnikiem systemu ERTMS, który stanowi o bezpiecznym prowadzeniu ruchu pociągów, dlatego musi być systemem bezpiecznie i pewnie działającym w zakresie przesyłania informacji (dane i głos), a jego pewność i działanie powinna być większa niż w publicznym systemie GSM. Pewność działania powinna być zapewniona przez dodatkowe środki (redundancja sprzętu, odpowiednie pokrycie pola elektromagnetycznego), jak również odpowiednią eksploatację systemu. Ponadto system GSM-R powinien być odporny na nieuprawniony dostęp i poufność przesyłanych informacji. System powinien realizować połączenia, przełączenia i przesyłanie danych w założonych reżimach czasowych. Do spełnienia wymienionych wymagań ważna jest nie tylko radiowa część systemu GSM-R, ale również część łączności przewodowej, bez której zarówno system GSM-R, jak i system ERTMS nie mógłby poprawnie pracować. Dlatego koniecznym jest stosowanie teletransmisyjnych struktur samonaprawialnych, zapewnienie rezerwowych dróg transmisyjnych, synchronizacji, zintegrowanego systemu zarządzania, kontroli dostępu itd. Tylko kompleksowe działania mogą zapewnić bezpieczeństwo systemu GSM-R, a tym samym zwiększyć bezpieczeństwo systemu ERTMS. Istotną sprawą jest też świadomość, fachowość i odpowiedzialność administracji, przewoźników i operatora infrastruktury w zakresie znajomości i implementacji procedur i systemów utrzymania bezpieczeństwa i niezawodności sieci GSM-R. Są to elementy tak zwanej kultury bezpieczeństwa, której wdrożenie i utrzymanie na określonym poziomie powinno być priorytetem dla wszystkich decydentów, odpowiedzialnych za szeroko rozumiane bezpieczeństwo ruchu na kolei.

Literatura

1. Ding X., Chen X., Jiang W.: *The Analysis of GSM-R Redundant Network and Reliability Models on High-speed Railway*, 2010 International Conference on Electronics and Information Engineering (ICEIE 2010), Kyoto, Japan 2010.
2. Gago S.: *Niektóre problemy praktyczne występujące w układach sterowania i telekomunikacji KDP*, Konferencja Naukowa „Koleje dużych prędkości", 15 listopada, Warszawa 2011.
3. Johnsen S.O., Veen M.: *Risk Assessment and Resilience in Critical Communication of Infrastructure in Railways*, Trondheim, 2011.
4. Lehrbaum M.: *GSM-R Disaster Recovery*, GSM-R Business Operations, Warsaw, October 2009.
5. Markowski R.: *Wdrożenie systemu ERTMS (ETCS i GSM-R) w Polsce*, Seminarium PKP PLK S.A „Zakłócenia systemu GSM-R przez komórkowe systemy publiczne", Kielce, 21.06.2011.
6. Marzilli E. et alli: *ERTMS/ETCS Level 2 high speed / high capacity lines feedback on RAMS and performance parameters: experience after two years of commercial service in Italy and features of the new HS/HC Italian lines*, Rete Ferroviaria Italiana, Rome, Italy.
7. Pawlik M.: *Polski Narodowy Plan Wdrażania Europejskiego Systemu Zarządzania Ruchem Kolejowym ERTMS,* Technika Transportu Szynowego, 1/2007.
8. *Project EIRENE – Functional Requirements Specification*, International Union of Railways, 2006.
9. *Project EIRENE – System Requirements Specification*, International Union of Railways, 2006.
10. Pushparatnam L., Taylor T.: *GSM-R Implementation and Procurement Guide V 1.0*, 15.03.2009.
11. Sauthier E., Poutas L.: *Radio bearer capacity and planning for ETCS Solutions for BSS redundancy*, 10th December 2003.
12. Siergiejczyk M., Gago S.: *Problemy zapewnienia bezpieczeństwa informacyjnego w sieci GSM-R*, K
13. Siergiejczyk M., Gago S.: *Zagadnienia bezpieczeństwa systemu GSM-R w aspekcie wspomagania transportu kolejowego,* Logistyka nr 6/2012. Wyd. ILiM, Poznań 2012.
14. Simon A., Walczyk M.: *Sieci komórkowe GSM/GPRS. Usługi i bezpieczeństwo*. Wydawnictwo: Xylab, Kraków 2002.
15. Urbanek A.: *Komunikacja kolejowa GSM-R*, Networld nr 1. IDG, Warszawa 2005.

16. *Uzupełnienie Studium Wykonalności w zakresie systemu cyfrowej łączności radiowej GSM-R, łączności technologicznej i systemów teleinformatycznych związanych z prowadzeniem ruchu na projektowanej linii kolejowej Pomorskiej Kolei Metropolitarnej*, Opracowanie WT PW pod kierownictwem M. Siergiejczyka, Warszawa, 2011.
17. Winter P.: *International Union of Railways, compendium on ERTMS*, Eurail Press, Hamburg, 2009.
18. Yuan C.: *Reliability Analysis of CTCS Based on Two GSM-R Double Layers Networks Structures Communications and Mobile Computing*, 2009. CMC'09. WRI International Conference on 6–8 Jan. 2009.

Chosen Problems of Reliability and Safety of Information Transmission in the GSM-R System

Summary

The paper presents the selected items affecting the reliability and safety of the network of digital mobile GSM-R. In the domain of telecommunications safety are discussed selected methods and mechanisms to ensure the required level of reliability and availability of GSM-R network in both parts of radio and wired in faultless mode and emergency mode. The paper highlights the influence of the method of exploitation and maintenance on the safety of GSM-R system as well as system safety ties with the culture of safety in the administrative and the decision-making bodies.

Keywords: GSM-R system, rail transport, transmission, reliability, availability, safety culture

Избранные вопросы надёжности и безопасности передачи данных в сети GSM-R

Резюме

В разработке представлены избранные элементы, влияющие на надёжность и безопасность цифровой сети мобильной телефонной связи GSM-R. В области безопасности телекоммуникации обсуждены избранные методы и механизмы для обеспечения требуемого уровня надёжности и доступности сети GSM-R, как в части радио, так и проводной, в режиме бесперебойной работы и в аварийном режиме. В документе подчёркивается влияние метода эксплуатации и технического обслуживания на безопасность системы GSM-R, а также связи безопасности системы с культурой безопасности в административно-управленческих органах.

Ключевые слова: система GSM-R, железнодорожный транспорт, передача, надёжность, доступность, культура безопасности