P6 – Temat 6: Infrastruktura komunikacyjna [C]

Podrozdziały tematu

A. Sieć i architektura „Electronic Highway”
B. Wymiana danych w czasie rzeczywistym
C. Wymiana plików przy wykorzystaniu serwera FTP
D. Poczta elektroniczna e-mail poprzez „Electronic Highway”
E. Komunikacja poza „Electronic Highway”

Wstęp

Unia dla Koordynacji Przesyłu Energii Elektrycznej (UCTE) (Union for the Co-ordination of Transmission of Electricity) ustanowiła sieć komunikacyjną, która dostarcza wymaganą infrastrukturę do wspierania wymiany danych pomiędzy OSP. Dokument ten opisuje minimalne wymagania, zasady wdrożenia, czynności związane z rozszerzeniem i utrzymaniem sieci komunikacyjnej Europejskich Operatorów Systemów Przesyłowych - European Transmission System Operators (Electronic Highway-EH) oraz główne usługi aplikacyjne.

Same zastosowania razem ze specyfikacją Zastosowanie Wymiany Danych (Application Data for Exchange) są opisane w odpowiednim Dokumencie „Instrukcji pracy systemów połączonych UCTE” (UCTE Operation Handbook). Każda istotna wymiana danych pomiędzy OSP powinna być przekazywana za pomocą usług aplikacyjnych EH. Jeśli wymagane są dodatkowe usługi aplikacyjne, UCTE zdecyduje jaka będzie ich konstrukcja oraz jak należy je obsługiwać i konserwować.

EH jest siecią prywatną dedykowaną do wymiany danych pomiędzy OSP. Odpowiedzialność za pracę sieci spoczywa na członkowskich OSP, a zarządzanie siecią na dwóch Sieciowych Centrach Operacyjnych UCTE (Network Operation Centres) – NOCs (podstawowe (pNOC) oraz dodatkowe (sNOC)). Rozszerzenie EH do kolejnych OSP jest także brane pod uwagę.

Informacje sensytywne pod względem technologicznym i technicznym są zebrane w oddzielnym dokumencie Poradnik Techniczny Electronic Highway (Electronic Highway Technical Reference Manual), utrzymywanym przez pNOC. Poradnik Techniczny Electronic Highway jest oznaczony jako dokument poufny UCTE i jest wyłącznie udostępniony partycypującym OSP.

Historia zmian

v.0.8	***aktualizowano 16.11.2004 EH Core Team***	***ostateczna korekta***
v.0.7	***aktualizowano 14.09.2004 EH Core Team***	***na konsultacje zewnętrzne***

Stan obecny

Niniejszy dokument podsumowuje obecne zalecenia UCTE związane z architekturą, działaniem, konserwacją, rozszerzeniem oraz wykorzystaniem Electronic Highway na potrzeby wymiany danych. Po szczegółowe definicje terminów używanych w niniejszym

Temacie proszę odnieść się do Słownika terminologicznego „Instrukcji pracy systemów połączonych UCTE" (UCTE Operation Handbook) (patrz G).

Niniejszy dokument bazuje na dokumentacji EH opracowanej przez Grupę Zadaniową 6 SGEH w ETSO (ETSO Task Force 6 SGEH) jako dokument UCTE. Dokument ten łączy w sobie wszystkie poprzednie dokumenty UCTE odnoszące się do infrastruktury komunikacyjnej. Niniejsza wersja dokumentu (wersja 0.8, poziom C, datowany 16.11.2004) ma status „ostateczna korekta".

A. Sieć i architektura „Electronic Highway”

[Załącznik A6 – A. Sieć i architektura „Electronic Highway”]

Wstęp

Prywatna sieć kratowa służąca do komunikacji pomiędzy OSP dostarcza niezbędną infrastrukturę, która wspomaga i wspiera wymianę danych pomiędzy OSP. Niniejsza część dokumentu opisuje niezbędną strukturę dla wdrożenia, działania, rozszerzenia oraz utrzymania sieci komunikacyjnej Europejskich Operatorów Systemów Przesyłowych - European Transmission System Operators (Electronic Highway - EH).

EH jest siecią prywatną dedykowaną do wymiany danych pomiędzy OSP. Odpowiedzialność za pracę sieci spoczywa na członkowskich OSP, a zarządzanie siecią na dwóch Centrach Operacyjnych UCTE (Network Operation Centres) – NOCs.

Podstawowym zakresem Electronic Highway jest wymiana danych w czasie rzeczywistym, która zwiększa bezpieczeństwo prowadzenia ruchu.

W związku z powyższym, ruch generowany przez dane czasu rzeczywistego ma najwyższy priorytet spośród wszystkich wymienianych danych.

Kryteria

C1. Dostępność EH. Wyrażony w procentach okres czasu kiedy EH była dostępna. Obliczana jest na podstawie MTBF / (MTBF + MTTR) dla każdego komponentu pomiędzy dwoma bramkami EH włączając w to połączenia rezerwowe, zalecana dostępność powinna być wyższa niż 99,8%. Uważa się, że EH powinna mieć taki sam stopień dostępności jak SCADA i oczekuje się, że będzie działać w każdych warunkach.

C2. Niezawodność EH. Wszystkie wymieniane dane muszą być przesyłane za pomocą EH od nadawcy do odbiorcy bez uszkodzeń, kolejno oraz na czas. Otrzymanie przez odbiorcę niepoprawnych danych (nie skorygowanych na poziomie sieci), utrata danych czy też dane przesłane wielokrotnie zmniejszają niezawodność EH. Uszkodzenie danych jest niedopuszczalne.

C3. Wydajność EH. W normalnych warunkach, opóźnienie danych przesyłanych przez EH, dla danych czasu rzeczywistego o określonym rozmiarze i obustronnie uzgodnionych, pomiędzy dwoma bramkami nie powinno przekraczać 2 sekund. System musi posiadać odpowiednią szerokość pasma tak aby spełnione były wymagania dotyczące wydajności dla określonych rozmiarów przesyłanych danych. Sugerowana szerokość pasma podana jest w późniejszym rozdziale.

C4. Redundancja. EH powinna musi zachować redundancje aby umożliwić pracę w przypadku pojedynczej usterki. Dotyczy to zarówno komponentów sieciowych jak też transmisyjnych.

C5. Konserwacja. Usterki EH powinny być traktowane przez OSP w ten sam sposób jak SCADA. Procedura usuwania błędów podana jest w Poradnik Techniczny Electronic Highway.

C6. Linia jest fizycznym połączeniem pomiędzy dwoma lokalizacjami OSP za pomocą dedykowanej infrastruktury komunikacyjnej.

C7. Łącze jest logicznym połączeniem pomiędzy dwoma OSP za pomocą jednej lub więcej linii. Linie te mogą lub nie bezpośrednio łączyć dwóch OSP.

Wymagania

R1. Sieć prywatna. Electronic Highway:

R1.1. jest dedykowana dla sektora elektroenergetycznego do użytku tylko przez OSP.

R1.2. Przesyła tylko dane operacyjne zatwierdzone przez UCTE oraz dane rynkowe pomiędzy OSP. Tylko zatwierdzone wymiany danych pomiędzy OSP i NOCs są przesyłane przez EH.

R1.3. Powinna używać tylko protokołów i formatów zatwierdzonych przez odpowiednie ciało UCTE.

R1.4. Nie ma bezpośredniego połączenia z Internetem.

R2. Sieć dedykowana do wymiany danych. EH jest medium komunikacyjnym dla OSP dla wymiany danych powiązanych z prowadzeniem ruchu oraz rynkiem.

R3. Sieciowe Centra Operacyjne. Dwa Sieciowe Centra Operacyjne UCTE pracują w odpowiednich Centrach Koordynacyjnych UCTE. NOCs wykonują monitoring pracy EH praz udostępniają wsparcie techniczne dla OSP. Obydwa NOCs są reprezentowane w strukturze organizacyjnej UCTE.

R4. Wzajemne połączenia EH.

R4.1. Połączenia OSP. Przynajmniej dwa niezależne fizyczne łącza punk-punkt z innym OSP muszą być wdrożone w taki sposób aby zapewnić redundancje sieci szkieletowej EH. Aby zwiększyć poziom redundancji oraz wydajność zaleca się aby każdy OSP posiadał dodatkowe fizyczne linie do sąsiednich OSP.

R4.2. Sieć szkieletowa EH. Sieć szkieletowa EH składa się ze wszystkich połączeń wzajemnych które przekraczają granice OSP.

R4.3. Szerokość pasma połączenia. Zalecana szybkość łącza to 2 Mbps dla wszystkich łączy sieci, obowiązkowa jest minimalna szybkość na poziomie 64 kbps. Przepustowość niższa niż 2 Mbps powinna być używana tylko jako tymczasowe rozwiązanie.

R4.4. Rozszerzenia sieci. Budowa, modyfikacja oraz minimalny standard techniczny komponentów musi być uzgodniony przez odpowiednie ciała UCTE.

R5. Połączenia EH w krajach o więcej niż jednym OSP.

R5.1. W krajach gdzie więcej niż jeden OSP jest aktywny, OSP w danym kraju muszą opracować rozwiązanie zgodnie z niniejszym dokumentem.

R5.2. Przynajmniej operator bloku regulacyjnego UCTE powinien być bezpośrednio połączony do EH.

R6. Infrastruktura OSP. Każdy OSP musi zbudować, obsługiwać i konserwować część sieci EH zlokalizowanej w swoim obszarze regulacyjnym oraz ponosić odpowiednie koszty związane z inwestycją, konserwacją i udoskonalaniem.

R7. OSP dopuszczenia do połączenia do EH

R7.1. Każdy członek UCTE powinien być podłączony do EH. OSP planujący przyłączenie do UCTE powinni skontaktować się z pNOC celem uzyskania procedur do przyłączenia do Electronic Highway.

R7.2. OSP nie należący do UCTE, a przyłączeni do synchronicznej sieci przesyłowej UCTE oraz wszyscy członkowie ETSO mogą być przyłączeni do EH po zatwierdzeniu przez UCTE.

R7.3. Przedsiębiorstwa, które wypełniają zadania OSP z ramienia jednego OSP lub grupy OSP zgodnie z R7.1 i R7.2 oraz są własnością jednego lub więcej OSP mogą być przyłączeni do EH po zatwierdzeniu przez UCTE.

R8. Odpowiedzialność OSP. OSP muszą:

R8.1. Zapewnić bezpieczeństwo pracy EH.

R8.2. Podjąć odpowiednie kroki dla ochrony Electronic Highway i każdego przyłączonego OSP przed dwoma następującymi głównymi niebezpieczeństwami:

R8.2.1 Przerwanie pracy lub zniszczenie danych

R8.2.2 Ujawnienie danych uznanych za poufne przez prawo, urząd regulacji lub bilateralne umowy.

R8.3. Chronić przed nieautoryzowanym dostępem do EH.

R8.4. Przeprowadzać kontrolę na obecność wirusów i robaków. Podstawową odpowiedzialnością każdego OSP jest dbanie o własne dane wejściowe aby zapewnić, że tylko prawidłowe, skanowane programem antywirusowym pliki są wysyłane do innych OSP.

R8.5. Monitorować i zapewnić dostępność i niezawodność komponentów EH w ich obszarze.

R8.6. Zapewnić, że koncepcja ich lokalnej sieci EH jest zgodna z wymaganiami EH co podlega akceptacji przez NOCs.

R9. OSP powinni sprawdzać redundancje fizycznych łączy i połączeń SCADA poprzez testy i raportować te działania i ich rezultaty do odpowiednich ciał UCTE i NOCs. Działania te należy to koordynować pomiędzy sąsiednimi OSP.

Standardy

S1. Sieć rozległa WAN w EH. Sieć rozległa WAN w EH bazuje na TCP/IP. Schemat przydzielania adresów IP zdefiniowany jest w Poradniku Technicznym Electronic Highway.

S2. Konfiguracja o wysokim poziomie dostępności. Komponenty sieciowe i bramki muszą być skonfigurowane w taki sposób (np. obsługa stanu gotowości do przejęcia przetwarzania (hot standby) lub systemu równoważącego obciążenia (load sharing configuration)), że w przypadku uszkodzenia jednego komponentu jego funkcjonalność jest automatycznie pokrywana przez pozostałe komponenty w redundantnym systemie.

S3. Wielozadaniowość użytkowania. Zadaniem Electronic Highway jest wymiana:

- Informacji czasu rzeczywistego na potrzeby zdalnego sterowania (TEASE2 lub ELCOM90);
- Usług nie wymagających czasu rzeczywistego jak przesyłanie plików na potrzeby grafików wymiany, modeli sieciowych, danych planistycznych czy statystyk (FTP);
- E-mail dla specjalnych zastosowań (SMTP).

Procedury

P1. Zarządzanie siecią. Zarządzanie siecią jest realizowane przez podstawowe (pNOC) i dodatkowe (sNOC) Sieciowe Centrum Operacyjne.

P2. Działalność zarządcza OSP: każde przedsiębiorstwo zarządza własną częścią sieci (routery, bramki, etc.). Wewnątrz sieci nie stosuje się pułapek.

P2.1. SNMP. Każdy musi zapewnić dostęp do odczytu przez SNMP do własnych routerów z obydwu Sieciowych Centrów Operacyjnych.

P2.2. Raporty. Wszystkie uszkodzenia łączy trwające dłużej niż 60 minut powinny być raportowane do NOCs. Dodatkowo dostępność łącza na poziomie niższym niż 99,5 %, wyłączając planowe wyłączenia w raportowanym okresie (jeden rok), także powinny być raportowane.

P2.3. Czas odpowiedzi na uszkodzenia: Analizy dla wszystkich uszkodzeń łącza powinny rozpocząć się w ciągu 60 minut. Przynajmniej jedna linia powinna roztać przywrócona aby zapewnić działanie łącza. Przywrócenie linii redundantnej powinno odbyć się tak szybko jak to możliwe.

P2.4. Monitorowanie linii/łącza. Wszyscy OSP odpowiadają za monitoring i konserwację własnych linii/łączy do swoich sąsiadów.

P2.5. Hasła. Hasło pełnego dostępu jest znane tylko właścicielowi routera. Hasła routera (login / zezwolenie) są kwestią lokalną i nie będą udostępnione żadnemu z partnerów.

P2.6. Właściwości. Wszystkie routery muszą zaimplementować obsługę Management Information Base (MIB) II, zdalne monitorowanie (RMON) nie będzie wykorzystywane. Protokół kontrolny Internet Control Message Protocol ICMP (PING) musi być dostępny dla każdego. Baza danych MIB nie będzie zaimplementowana w ramkach.

P3. Działalność Sieciowych Centrów Operacyjnych: Sieciowe Centra Operacyjne muszą wypełnić przynajmniej poniższe zadania i wymagania:

P3.1. Rozdzielić adresy sieciowe (pNOC)

P3.2. Stworzyć i konserwować podstawowy DNS (pNOC)

P3.3. Być dostępnym operacyjnie 7 dni w tygodniu przez 24 godziny na dobę

P3.4. Reagować na uszkodzenie w czasie krótszym niż 1 godzina

P3.5. Nadzorować spójność sieci (pNOC)

P3.6. Odpowiadać za numerowanie serii (fizyczych) linii sieci (pNOC)

P3.7. Koordynować realizację I modyfikację struktury sieci

P3.8. Wdrożyć rozwiązania zdefiniowane przez odpowiednie ciała UCTE w odpowiedzi na wymagania użytkowników

P3.9. Utrzymywać dokumentację opisującą sieć (adresy, nazwy, prędkość I topologię) (pNOC) I udostępnić ją dla wszystkich użytkowników EH

P3.10. Stworzyć status I raport z działalności dla odpowiednich ciał UCTE

P3.11. Jeśli wymagane - udostępnić wsparcie techniczne dla innych OSP odnośnie lokalnej konfiguracji

P3.12. Utrzymywać statystyki zakłóceń

P3.13. Monitorować stan łącza

P3.14. Gromadzić i udostępniać wymagane informacje dotyczące personelu do kontaktu w przypadku niesprawności, konserwacji i modyfikacji.

P3.15. Odpowiadać za dokumentację dotyczącą zasad adresowania I nazewnictwa EH (pNOC)

P3.16. Wydawać adresy IP dla linii komunikacyjnych (pNOC)

P3.17. Integrować nowych uczestników

P3.18. Nadzorować czy nowi członkowie są przyłączeni zgodnie ze wszystkimi zasadami i wytycznymi EH włączając w to adresy e-mail I adresy IP

P4. Publikacje. Zmiany w sieci i utrzymanie sieci razem z wyposażeniem do zarządzania powinny być publikowane ponieważ w ten sposób łatwiej jest wykryć powody niesprawności. Doświadczenie pokazuje, ze wiele niesprawności występuje z powodu nieskoordynowanych zmian lub pomyłek podczas wykonywania zmian w sieci. Publikacje mogą być prezentowane na stronie Web (patrz następna procedura) lub wykorzystując strone FTP poprzez EH.

P5. Raportowanie. Dla potrzeb administratorów w EH zostanie wdrożona strona Web / FTP. Każdy uczestnik powinien raportować niesprawności na wspomnianych stronach. Raporty z bieżącej praktyki także będą publikowane na ww. stronie Web/FTP. Raporty te będą uwzględniać zachowanie sprzętu jak również pomiary ruchu sieciowego oraz wykryte wąskie gardła.

P6. Wymiana informacji. Wszystkie wymagane informacje, jeśli to możliwe, będą wysyłane do administratorów. Informacje mogą być wysłane na administracyjną skrzynkę

pocztową EH lub w przypadku trudności na internetowy adres e-mail publikowany na liście kontaktowej osób z obsługi technicznej.

Środki zaradcze

M1. Monitorowanie pracy EH:

M1.1. NOCs będą monitorować stan łącza poprzez odpytywanie łączy i raportowanie statystyk do odpowiednich ciał UCTE.

M1.2. NOCs będą informować odpowiedniego OSP o każdym fakcie niezadowalającej wydajności danego łącza.

M1.3. NOCs powinny monitorować EH pod kątem:

M1.3.1 Wykrycia usterki

M1.3.2 Koordynacji naprawy niesprawności

M1.3.3 Wykrycia wąskich gardeł

M1.4. pNOC ma za zadanie utrzymywanie i aktualizację schematu EH zgodnie z informacją przesłaną przez OSP. Schemat powinien przedstawiać nie tylko konfigurację EH lecz także adresy, nazwy interfejsów oraz przepustowość linii komunikacyjnych.

M1.5. pNOC ma za zadanie utrzymywanie i aktualizację numerów telefonów i adresów poczty elektronicznej email personelu odpowiedzialnego za działanie EH w oddzielnym dokumencie „Personel Techniczny - kontakty".

M1.6. Za pomocą samej EH odpowiedzialny personel IT może być osiągalny poprzez email wykorzystując adres email admin@skrót_nazwy_OSP.etso. Personel odpowiedzialny za IT w Sieciowym Centrum Operacyjnym może być osiągalny wykorzystując adres email admin@noc1.etso.

M1.7. Wszyscy OSP są odpowiedzialni za monitorowanie i konserwacje łączy EH oraz linii do swoich sąsiadów.

M2. Odpowiednie ciało UCTE powinno oszacować wydajność EH oraz wszystkich strat łączy trwających dłużej niż 60 minut, zebrać i raportować do NOCs.

M3. Odpowiednie ciało UCTE powinno raportować wszystkie łącza, których dostępność jest poniżej 99,5 %, wyłączając planowe wyłączenia. Okres raportowania powinien wynosić jeden rok lub krócej.

M4. Modemowe połączenia ISDN są dopuszczalne jako tymczasowe rozwiązanie. Powinny być przeniesione na stałe linie tak szybko jak to możliwe. W takim wypadku ze względów bezpieczeństwa stosowana jest identyfikacja linii dzwoniącego.

M5. Zasady postępowania w przypadku awarii.

M5.1. Każdy lokalny OSP odpowiada za własne urządzenia podczas gdy Sieciowe Centra Operacyjne (NOCs) odpowiadają za wszystkie zadania zbiegające się w czasie. W przypadku nakładających się awarii takich jak wyłączenie linii odpowiedzialność będzie spoczywać w pierwszej kolejności na dwóch OSP połączonych daną linią.

M5.2. Jeśli to tylko możliwe wszystkie usterki muszą być usunięte po stronie lokalnego OSP.

M5.3. Należy zagwarantować natychmiastowe powiadamianie odpowiedzialnego personelu IT każdego centrum regulacyjnego i Sieciowego Centrum Operacyjnego.

M6. Wykrywanie niesprawności. Niesprawność ma miejsce jeśli jeden lub więcej OPS nie jest osiągalny poprzez EH w ramach jednej z funkcji. Oznacza to, że co najmniej jedna funkcja nie działa. Wykryć to można na kilka sposobów, poprzez któregokolwiek z użytkowników lub ekspertów technicznych pracujących z EH.

M7. Raportowanie i działanie w przypadku niesprawności.

M7.1. Operator w centrum regulacyjnym OSP informuje odpowiedzialny personel IT w ramach własnego centrum regulacyjnego.

M7.2. Odpowiedzialny Personel IT w centrum regulacyjnym OSP stara się zlokalizować i naprawić błąd. Jeśli to konieczne informuje personel IT odpowiedzialny na drugim końcu uszkodzonego łącza w celu pomocy w naprawie niesprawności. Jeśli to konieczne dodatkowo Sieciowe Centrum Operacyjne będzie informowane celem naprawy nakładających się niesprawności.

B. Wymiana danych czasu rzeczywistego

[Załącznik A6 – B. Wymiana danych czasu rzeczywistego

Wstęp

Dla wymiany danych czasu rzeczywistego poprzez EH zalecany jest standard IEC z protokołem TASE.2. Jeśli uzgodniono to wzajemnie pomiędzy OSP tymczasowo może być używany także protokół ELCOM-90.

Rodzaj i ilość wymienianych danych w czasie rzeczywistym musi być wzajemnie uzgodniony pomiędzy zaangażowanymi OSP w ramach tematów UCTE. EH przeznaczona jest do wymiany danych, która pomaga OSP monitorować i koordynować pracę systemu. Nie zaleca się wykorzystywania danych wymienianych poprzez EH w aplikacjach do sterowania w czasie rzeczywistym. Celem niniejszej części jest spis typów danych które mogą być wymieniane w czasie rzeczywistym poprzez Electronic Highway. Lista może ulec rozszerzeniu w przyszłości.

Wymagania

R1. Dane operacyjne związane z bezpieczeństwem. Dane te dotyczą linii wysokiego napięcia, transformatorów, wyłączników, odłączników sieci przesyłowych. Są istotne dla bezpieczeństwa sieci przesyłowych, dla aplikacji EMS (Energy Management System) oraz dla obliczeń rozpływu mocy PAS (Power Aplication Software) i zawierają:

Sieć przesyłowa:

- Stan łącznika (załączony, wyłączony, pośredni)
- Moc czynna (MW) i bierna (MVar)
- Napięcie (kV)
- Obecność napięcia (obecność/brak)
- Położenie przełącznika zaczepów transformatora (stopień położenia)
- Alarmy (jeśli żądane)

Jednostki wytwórcze:

- Status bloku (w ruchu/wyłączony z ruchu)
- Moc czynna (MW) i bierna (MVar)

Dane wymieniane pomiędzy OSP muszą być uzgodnione pomiędzy zaangażowanymi OSP.

R2. Poza zakresem Electronic Highway

R2.1. Regulacja mocy i częstotliwości. Electronic Highway nie może zagwarantować opóźnień mniejszych niż 2 sekundy ze stacji elektroenergetycznej do zdalnego systemu SCADA, dlatego też uważa się, że regulacja mocy i częstotliwości jest poza jej zakresem.

R2.2. Polecenia. Wymiana poleceń dotyczących przełączeń takich jak otwarcie lub zamknięcie wyłącznika jak w systemie SCADA nie jest planowane poprzez EH. Dostępna przepustowość, rozmiar danych i różne opóźnienia czasowe w akwizycji danych, przesyłanie danych i czas odpowiedzi bramek mogą powodować nie akceptowalny poziom wydajności wymagany w aplikacjach do sterowania w czasie rzeczywistym takich jak interlocking i regulacji mocy i częstotliwości.

R3. Jakość danych. Należy umożliwić przydzielenie charakterystyczne kody jakościowe (czasem nazywane atrybutami) jak:

- Ważny/nieważny

- Wstrzymane lub nie odświeżone
- Wprowadzone ręcznie lub nadpisane
- Szacunkowe lub obliczone

R4. Maksymalne opóźnienie przesyłu. Opóźnienie przesyłu pomiędzy dwoma bramkami Electronic Highway jest to okres czasu pomiędzy:

- Czasem kiedy dane są dostępne w bramce wysyłającego;
- Czasem kiedy dane te są dostępne w miejscu odbiorcy.

Zmiana jednego obiektu danych często skutkuje zmianami kilku innych obiektów danych chwilę później. Dlatego też dobrze jest opóźnić przesył danych na krótki okres czasu (zwany okresem buforowym) tak aby zmiany kilku obiektów danych zostały uwzględnione w ramach danego okresu, zmniejszając w ten sposób ruch danych w sieci.

Opóźnienie przesyłu danych nie powinno przekraczać 2 sekund. Opóźnienie może się zwiększyć w okresie buforowym jak też podczas przetwarzania danych w bramkach i przesyłaniu ich poprzez sieć.

R5. Konfiguracje rezerwowe. Konfiguracje rezerwowe należy tak projektować aby spełniły kryteria dotyczące wydajności oraz dostępności. Przełączenie lokalnego systemu (jak SCADA, EMS) nie powinna mieć żadnego wpływu na wymianę danych z parterami. Infrastruktura EH ma być zbudowana jako system redundantny gdzie usterka pojedynczego komponentu nie wpływa ujemnie na działanie węzła danego OSP w EH.

Procedury

P1. Parametry transmisji danych. Wymagane są następujące tryby przesyłu danych:

- Okresowe;
- Na żądanie odbiorcy;
- Z inicjatywy wysyłającego;
- Spontanicznie (po zmianie wartości lub jakości);

Podczas wykorzystywania trybu spontanicznego, należy zapewnić możliwość połączenia tego trybu z powolnym okresowym przesyłem danych dla zapewnienia większej integralności danych.

Typowym wykorzystaniem trybów przesyłu danych będą:

- Dla określenia stanu: połączenie trybu spontanicznego przesyłu danych (wysyłanie tylko tych danych które uległy zmianie) z powolnym trybem okresowym przesyłu danych, np. co 5 minut.
- Dla pomiarów: okresowy przesył danych lub tryb spontanicznego przesyłania danych w przypadku zmian wielkości powyżej zdefiniowanych granic.

Zaleca się aby partnerzy informowali się wzajemnie podczas fazy bilateralnego porozumienia jakie tryby przesyłu oraz cykle odświeżania są wykorzystywane. Umożliwi to określenie odpowiedniego trybu przesyłu we wszystkich segmentach łańcucha transmisji.

P2. Porozumienie bilateralne. Wymiana danych pomiędzy komunikującymi się partnerami jest koordynowana na bazie obustronnych uzgodnień. Partnerzy wymieniają dane na podstawie wspólnych umów.

P3. Niezależne stowarzyszenia. System komunikacyjny może utrzymywać wiele połączeń do zdalnych systemów. Aby zminimalizować liczbę przestojów spowodowanych rekonfiguracją połączenia, odpowiedzialny personel IT powinien mieć możliwość rekonfiguracji jednego z połączeń bez zakłócania pracy innych łączy. Electronic Highway powinna umożliwiać dodawać nowe połączenia z istniejącymi lub nowymi partnerami bez znaczącego wpływu na istniejące łącza komunikacyjne. W szczególności, należy zapewnić możliwość włączenia do pracy nowego połączenia bez zatrzymywania lub restartowania istniejących połączeń.

Standardy

S1. Konwencja znaku. Konwencja dotycząca znaku wskazująca kierunek przepływu energii: Znak ujemny oznacza energię wpływającą do węzła; znak dodatni oznacza energię wypływającą z danego węzła.

S2. Bloki zgodności i obiekty serwisowych wymaganych przez TASE.2. Na potrzeby wymiany danych czasu rzeczywistego poprzez Electronic Highway na bazie protokołu TASE.2 wymagane jest wykorzystanie co najmniej bloków zgodności 1 i 2. Zgodność z blokami 4 i 8 jest opcjonalna.

C. Wykorzystanie serwera FTP do wymiany danych plikowych

[Załącznik A6 – C. Wykorzystanie serwera FTP do wymiany danych plikowych

Wstęp

Niniejsza część dokumentu zawiera wytyczne dotyczące wymiany danych plikowych poprzez EH oraz implementacji serwera FTP. Jako serwer wymiany danych na potrzeby wymiany informacji i danych pomiędzy OSP przyłączonych do Electronic Highway (EH) przewiduje się wykorzystanie serwera FTP.

Kryteria

C1. Wykorzystanie serwera FTP: Serwer FTP jest zdefiniowany jako serwer wymiany danych i nie będzie wykorzystywany jako magazyn danych lub jako serwer archiwizujący dane.

Serwer FTP wykorzystywany jest jako mechanizm do wymiany danych dla bieżących potrzeb aplikacji. Każdy OSP odpowiada za archiwizację danych dostarczanych i odbieranych z serwera FTP.

Wymagania

R1. Dostępność. Dla zapewnienia wyższej dostępności należy wykorzystać dwa serwery FTP dla pracy w trybie podstawowym oraz rezerwowym. W przypadku awarii serwera podstawowego, nastąpi aktywacja serwera rezerwowego.

R2. Konserwacja systemu. Odpowiedzialność za konserwacje serwera FTP spoczywa na właścicielu serwera.

Standardy

S1. Konwencja nazewnictwa. Konwencja nazewnictwa plików powinna być zdefiniowana przez grupy użytkujące planujące wykorzystanie FTP przez EH do przesyłu danych.

S2. Pliki administracyjne. Informacje administracyjne dotyczące usług FTP są także przechowywane na serwerze FTP. Dostęp do tych plików mają tylko administratorzy.

Dodatkowo, poza obszarem administracyjnym zdefiniowany jest obszar z wolnym dostępem do dokumentacji. Obszar ten będzie dostępny dla wszystkich OSP przyłączonych do EH, dostęp do odczytu wspomnianej dokumentacji nie będzie wymagał podania hasła lub kodu dostępowego. Przykładowym sposobem wykorzystania tego obszaru będzie zarządzanie wytycznymi.

S3. Struktura danych. Struktura danych używanych na serwerze FTP jest szczegółowo zdefiniowana w Poradniku Technicznym Electronic Highway.

Procedury

P1. Typy danych. Każdy OSP może wysyłać (ang. upload) własne dane zgodnie ze zdefiniowaną strukturą i formatem. Struktura i format poszczególnych plików będzie określony i zatwierdzony przez odpowiednie ciała UCTE, które opracują jednocześnie własne zadania. W dodatku do obszarów poszczególnych OSP, niektórzy OSP mogą również tworzyć grupy w celu wymiany informacji będącej ich wzajemnym zainteresowaniem.

P2. Dostęp do danych. OSP będący źródłem danych powinien poinformować administratora FTP na temat autoryzacji wymaganej dla dostępu do danych tego typu. Dane mogą być

rozmieszczone w folderach i pod-folderach, a uprawnienia mogą być dostosowane do potrzeb poszczególnych aplikacji. Matryca autoryzacji dostępu zdefiniowana jest w Poradniku Technicznym Electronic Highway.

P3. Bezpieczeństwo i uwierzytelnienie użytkownika. Uwierzytelnienie użytkownika będzie organizowana przez administratora systemu na bazie informacji udostępnionych przez użytkowników. Uwierzytelnienie każdego użytkownika będzie utrzymywana w folderze administracyjnym. Szczegóły dotyczące bezpieczeństwa i autoryzacji są zdefiniowane w Poradniku Technicznym Electronic Highway.

P4. Monitorowanie usług. Właściciel bądź operator serwera FTP sprawdza wykorzystanie serwera FTP i sporządza zestawienia statystyczne dla zapewnienia lepszego zarządzania udostępnionymi usługami oraz główny obszar wzajemnego oddziaływania.

P5. Pojemność nośników danych i ich porządkowanie. System będzie tak zaprojektowany aby zapewnić zachowanie danych przez co najmniej 3 miesiące.

D. Poczta elektroniczna email przez Electronic Highway

[Załącznik A6 – D. Poczta elektroniczna email przez Electronic Highway

Wstęp

Poczta elektroniczna jest usługą która może służyć do asynchronicznej wymiany danych operacyjnych poprzez Electronic Highway pomiędzy osobami (person-to-person) i/lub aplikacjami (application-to-application) zlokalizowanymi u poszczególnych OSP. Każdy OSP korzystający z tej usługi musi zapewnić możliwości klienta poczty elektronicznej (zdolność do wysyłania i odbierania wiadomości) wykorzystując własny serwer pocztowy (protokół SMTP) i/lub zdalny serwer pocztowy (protokoły SMTP/POP3) u innego OSP. Format wymienianych danych jest ustalany bilateralnie lub w zależności od zastosowań, lecz powinien respektować – jeśli dotyczy – standardy UCTE jak np. ESS na bazie specyfikacji XML.

Wymagania

R1. Adresy email wykorzystywane w Electronic Highway zdefiniowane są w Poradniku Technicznym Electronic Highway. Dla serwera SMTP oraz dla klientów należy zachować stosowne wymagania bezpieczeństwa jak np. uwierzytelnienie, odseparowanie od Internetu, ochrona antywirusowa, etc.

R2. Dane użytkownika mogą być załączone do treści wiadomości i/lub wysłane jako załącznik. Do kodowania informacji o użytkowniku nie należy wykorzystywać zawartości standardowych pól wiadomości (temat, nadawca, odbiorca, etc…).

Standardy

S1. RFC 0821 Simple Mail Transfer Protocol jest obowiązkowy, natomiast standardy pokrewne są opcjonalne. Zalecane są opcjonalne standardy MIME oraz S/MIME.

S2. RFC 1939 Post Office Protocol – wersja 3 jest obowiązkowy, natomiast standardy pokrewne są opcjonalne.

Wytyczne

Email może mieć następujące zastosowania: prognoza ograniczeń sieciowych na dzień kolejny (DACF), wyniki przetargów, planowanie operacyjne, grafitowanie, zielone certyfikaty, administracja EH, etc.

E. Publikowanie Informacji przez EH za pomocą Serwera HTTP

[Załącznik A6 – E. Publikowanie Informacji przez EH za pomocą Serwera HTTP

Wstęp

Informacje operacyjne OSP mogą być publikowane poprzez EH w formacie HTML (Hypertext Markup Language) lub XML (eXtensible Markup Language). Informacje publikowane są serwerach HTTP obsługiwanych przez jednego lub kilku OSP i mogą zawierać strony tworzone statycznie bądź dynamicznie jak np. informacje dotyczące EH NOCs lub wizualizacje SCADA, a także dane grafikowe dla wymiany danych pomiarowych lub transakcji energii. Aby odczytać dane w formacie HTML każdy użytkownik OSP musi posługiwać się klientem HTTP/HTML (przeglądarka stron webowych) lub B2B (Business to business) HTTP/XML.

Wymagania

R1. Serwery http należy ulokować w Electronic Highway i odseparować od wewnętrznych sieci OSP za pomocą zapór ogniowych.

Standardy

S1. RFC2616 Hypertext Transfer Protocol – HTTP/1.1 oraz opcjonalnie pokrewne standardy jak np. HTTPS RFC 2660.

S2. RFC 2854 ‘text/html’ Media Type, który zastąpił RFC 1866 ‘Hypertext Markup Language 2.0’

S3. XML Definition. http://www.w3.org/

Wytyczne

G1. Należy wprowadzić stosowne wymagania odnośnie bezpieczeństwa jak np. uwierzytelnienie.

G2. W razie potrzeby, do przesłania informacji OSP do publikacji na serwerze należy użyć usług FTP, email lub HTTP.

F. Komunikacja poza EH

[Załącznik A6 – F. Komunikacja poza EH

Wstęp

Istotne jest aby poza infrastrukturą komunikacyjną do wymiany danych poprzez EH dla dedykowanych aplikacji, dodatkowo zapewnić komunikację za pomocą innych mediów. Poza EH mogą istnieć inne infrastruktury dla wymiany danych. Taka komunikacja pomiędzy operatorami systemów może obejmować komunikację głosową, FAX, wideo konferencje, email oraz publikowanie i prenumerowanie informacji w Internecie.

Wymagania

R1. Wymagania dotyczące komunikacji głosowej. W sytuacjach normalnych oraz awaryjnych wymagane są dedykowane linie komunikacyjne do transmisji głosu do wszystkich fizycznych sąsiadów.

- **R1.1. Niezależność od PABXs**. Wspomniane linie powinny być niezależne od istniejących centrali PABX.
- **R1.2. Działanie podczas sytuacji awaryjnych.** Wspomniane linie oraz związane z nimi wyposażenie powinny mieć zabezpieczenia pozwalające na działanie w ekstremalnych warunkach systemu. (zabezpieczenia w UPS, rezerwowe wyposażenie, etc.)
- **R1.3. Rezerwowe linie.** Linia powinna być rezerwowana przez linię wewnętrzną z centrali PABX lub oddzielną linię.
- **R1.4. Dostępność telefonu komórkowego.** Podczas sytuacji awaryjnych należy zapewnić także dostęp do telefonu komórkowego lub satelitarnego. Używanie telefonu komórkowego/satelitarnego jest dopuszczalne tylko wówczas, gdy wszystkie pozostałe media nie funkcjonują, a komunikacja jest później uwierzytelniona (wytłumaczenie powodu jej użycia) pisemnym poświadczeniem.
- **R1.5. Uwierzytelnienie komunikacji głosowej.** Dla zapewnienia identyfikacji strony dzwoniącej lub odbierającej połączenie, w procedurach uzgodnionych dwustronnie, należy wprowadzić Identyfikację Dzwoniącego (Caller Identification).

R2. Wymagania dla komunikacji via FAKS

- **R2.1. Dostępność Faksu.** W Dyspozycji Mocy faks powinien być dostępny przez 24 godziny na dobę.
- **R2.2. Rozmiar papieru do Faksu.** Należy zapewnić papier przynajmniej w formacie A4.
- **R2.3. Podpis na Faksie.** Faks należy odpowiednio oznaczyć nazwiskiem nadawcy, nazwisko nadawcy powinno być czytelne.

R3. Wymagania dla poczty elektronicznej email poprzez Internet. Obsługujący personel powinien mieć zapewniony dostęp do poczty elektronicznej email.

- **R3.1. Dostępność poczty email.** Dostępność poczty elektronicznej email nie jest zależne od strony wymieniających wiadomości. Aczkolwiek należy dołożyć wszelkich starań aby poczta email dostępna była 24 godziny na dobę.
- **R3.2. Wykrywanie wirusów komputerowych w poczcie email.** Wszystkie przychodzące i wychodzące wiadomości email należy skanować na obecność wirusów.
- **R3.3. Blokowanie SPAMu oraz filtrowanie poczty.** Każdy OSP powinien zapewnić odpowiedni mechanizm do filtrowania poczty email aby zablokować niechcianą pocztę do Dyspozycji Mocy.
- **R3.4. Dopuszczalne załączniki w poczcie email.** Na potrzeby poszczególnych zastosowań należy zdefiniować typy załączników do wiadomości email. Nie

dopuszcza się używania jakichkolwiek załączników które mogłyby zagrozić bezpieczeństwu i/lub wydajności całej infrastruktury komunikacyjnej, takich jak: pliki wykonywalne, klipy dźwiękowe i wideo.

R3.5. Wymagania dotyczące uwierzytelnienia. Wymiana poczty email powinna podlegać uwierzytelnieniu i weryfikacji w inny sposób.

Standardy

S1. Standardy komunikacji głosowej. Jakość głosu powinna odpowiadać co najmniej standardom CCITT G729.

S2. Standardy transmisji Faksów. Najczęściej stosowanym standardem dla transmisji Faksów jest Standard Europejski G3 (Grupa 3).

S3. Standardy dla transmisji wideo-konferencji. Obowiązującym standardem dla wideo-konferencji jest ITU-T H.320 i H.323.

Procedury

P1. Lista osób upoważnionych. W celu zminimalizowania ryzyka związanego ze stosowaniem sieci publicznej należy wymieniać listę osób upoważnionych do używania komunikacji poza EH.

P2. Lista dostępnych urządzeń komunikacyjnych. Lista wszystkich urządzeń komunikacyjnych oraz każda ze zmian na tej liście powinna być wymieniana pomiędzy OSP wraz ze wszystkimi informacjami niezbędnymi do implementacji komunikacji.

P3. Rejestrowania komunikacji głosowej. Każda łączność pomiędzy operatorami może być rejestrowana oraz wykorzystywana zgodnie z polisami poszczególnych OSP.

S3.1. Powtórki zarejestrowanych połączeń. Kopie zarejestrowanych nagrań należy udostępnić na żądanie drugiej strony lub UCTE.

S3.2. Ochrona danych i pracowników. Wszelka łączność pomiędzy operatorami może podlegać rejestracji i wykorzystana zgodnie z odpowiednimi podstawami prawnymi w danym przedsiębiorstwie i kraju.

P4. Usuwanie usterek w sieci komunikacyjnej. Jakiekolwiek trudności związane z liniami należy zgłaszać do zaangażowanych stron, a przywrócenie/czas awarii należy traktować w ten sam sposób jak zakłócenie w systemie SCADA.

P5. Przekierowanie połączenia w przypadku awarii. W przypadku trudności z łącznością z Dyspozycją Mocy w innym OSP, łączność można zrealizować pośrednio z wykorzystaniem trzeciego OSP, który będzie przekazywał informacje i polecenia.

Wytyczne

G1. Podpis elektroniczny i szyfrowanie danych. Ogólnie rzecz biorąc, podpis elektroniczny oraz szyfrowanie danych nie są wymagane dla wymiany poczty email pomiędzy OSP. Aczkolwiek w zależności od uzgodnień dwustronnych dopuszcza się te mechanizmy pomiędzy OSP dla poczty email.

G2. Wykorzystanie i wymagania dla wideo i audio konferencji. Jeśli zachodzi taka potrzeba do dyskusji na wspólne tematy, w tym obsługi systemu, można wykorzystać wideo konferencje.