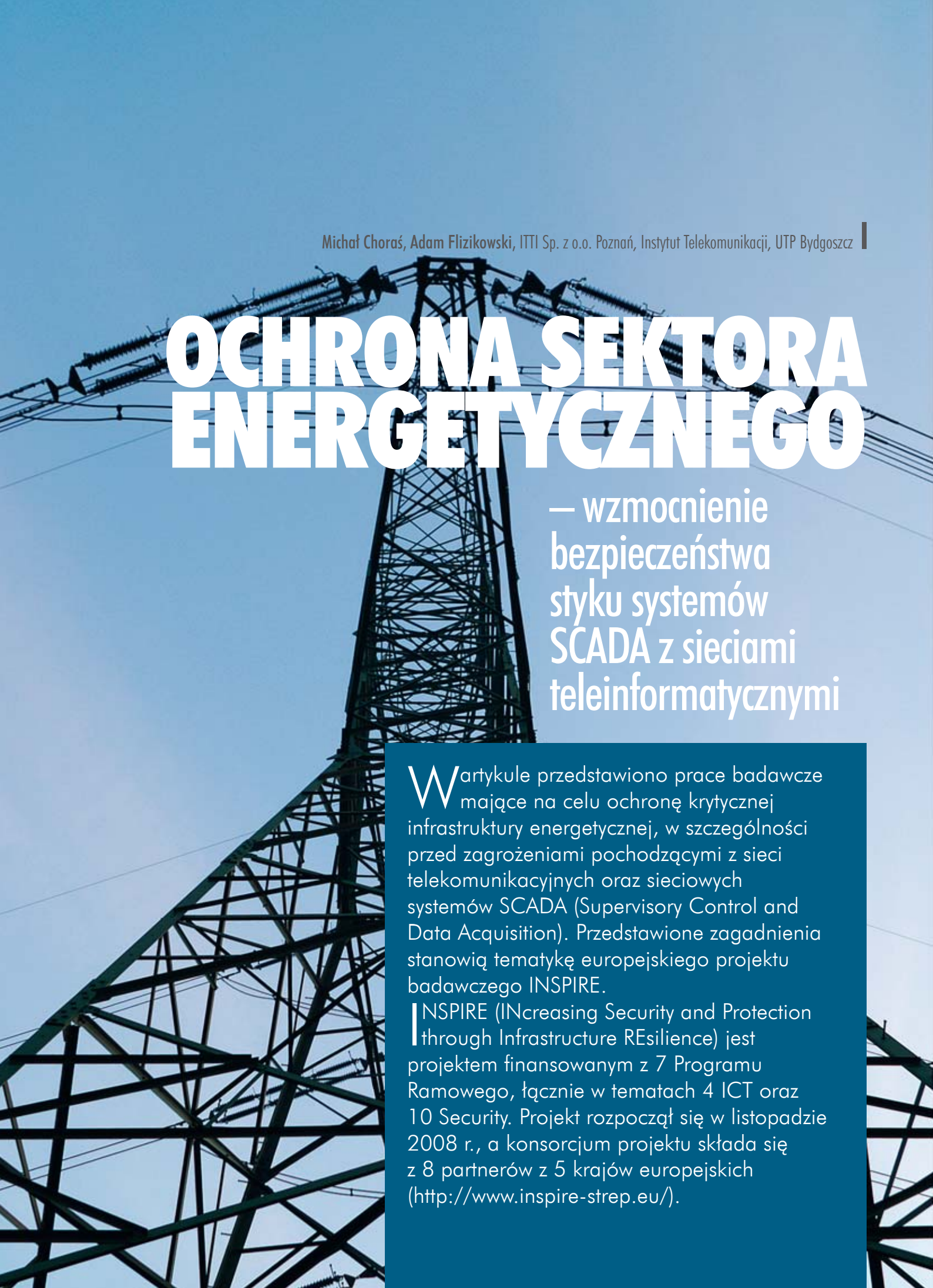
Michał Choraś, Adam Flizikowski, ITTI Sp. z o.o. Poznań, Instytut Telekomunikacji, UTP Bydgoszcz



OCHRONA SEKTORA ENERGETYCZNEGO

– wzmocnienie bezpieczeństwa styku systemów SCADA z sieciami teleinformatycznymi

W artykule przedstawiono prace badawcze mające na celu ochronę krytycznej infrastruktury energetycznej, w szczególności przed zagrożeniami pochodzącymi z sieci telekomunikacyjnych oraz sieciowych systemów SCADA (Supervisory Control and Data Acquisition). Przedstawione zagadnienia stanowią tematykę europejskiego projektu badawczego INSPIRE.

INSPIRE (INcreasing Security and Protection through Infrastructure REsilience) jest projektem finansowanym z 7 Programu Ramowego, łącznie w tematach 4 ICT oraz 10 Security. Projekt rozpoczął się w listopadzie 2008 r., a konsorcjum projektu składa się z 8 partnerów z 5 krajów europejskich (http://www.inspire-strep.eu/).

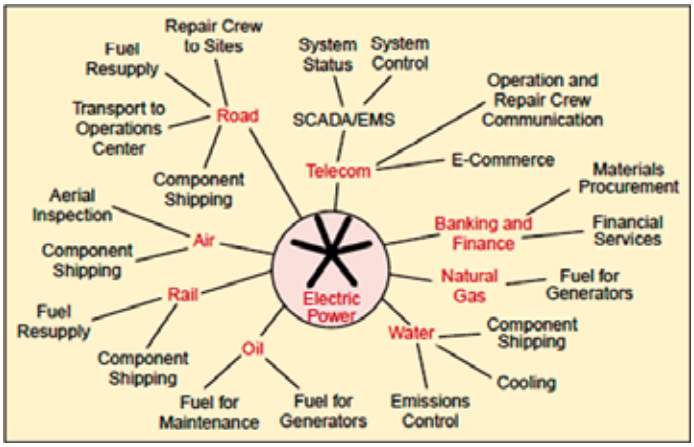
Infrastruktury krytyczne to sektory gospodarki, dostarczające towary i usługi w społeczeństwie na szeroką skalę, uważane za kluczowe i najbardziej znaczące. Jedną z kluczowych dziedzin gospodarki zaliczanych do infrastruktur krytycznych jest sektor energetyczny.

Cechą charakterystyczną sektorów zaliczanych do infrastruktury krytycznej jest to, że awarie, uszkodzenia czy inne negatywne sytuacje, jakie mogą wystąpić w danym sektorze mogą wpłynąć na wiele innych sektorów, oddziałując na część lub nawet całe społeczeństwo. Dlatego też, współzależności pomiędzy sektorami prowadzą do tego, że złożone awarie w sektorze infrastruktury krytycznej (np. w sektorze energetycznym), mogą stanowić poważne zagrożenie, powodując uszkodzenia w części bądź skrajnie w całej Europie. Rys. 1 przedstawia przykład współzależności sektora energii elektrycznej z innymi sektorami zaliczanymi do infrastruktury krytycznej [1].

Przykłady awarii w sektorze energetycznym to m.in. awaria nad kanałem Dortmund-Ems (4 listopada 2006), która spowodowała brak prądu w 15 mln gospodarstw domowych, powodując szkodę szacowaną na 200 mln euro. oraz atak na infrastrukturę komputerową elektrowni jądrowej Davis-Besse w Ohio przez robaka komputerowego „Slammer worm" w styczniu 2003 r.

Wymienione przykłady awarii prezentują, jak znaczący może mieć wpływ stosunkowo niewielka awaria na funkcjonowanie całego sektora lub sektorów, a co za tym idzie jak znaczące mogą być straty finansowe. Przykłady te uwidaczniają także, jak duże zagrożenia mogą płynąć z podatności sieci telekomunikacyjnej oraz sieciowych systemów SCADA.

Z tego powodu wzrosło w ostatnim czasie zainteresowanie zwiększeniem bezpieczeństwa sieci SCADA wykorzystywanych do monitorowania i kontroli elementów infrastruktury krytycznej. Obecnie, zarówno w Europie jak i w Polsce, systemy SCADA kontrolujące



Rys. 1. Przykład współzależności sektora energii elektrycznej z innymi infrastrukturami krytycznymi [1]

i monitorujące krytyczne infrastruktury, takie jak linie wodociągowe, energetyczne, gazowe, transport, kontrola lotnisk itp. coraz częściej korzystają i połączone są z otwartymi sieciami telekomunikacyjnymi.

Systemy SCADA

SCADA to systemy, które nadzorują i kontrolują infrastruktury rozproszone na dużym obszarze geograficznym. Zazwyczaj system SCADA składa się z rdzenia centralnego, w którym zbierane są informacje kontrolne oraz z pewnej ilości jednostek RTU (Remote Terminal Units) o ograniczonych zasobach obliczeniowych. Jednostki RTU zbierają dane i komunikują się z centrum przesyłając komunikaty w określonych interwałach czasowych.

W ostatnim czasie, wraz z presją na modernizację, integrację oraz niskie koszty, systemy SCADA z zamkniętych i dedykowanych systemów kontroli i stają się gotowymi produktami typu COTS (Components Off The Shelf), które współdzielą sieci z innymi systemami i są oparte o standardowe protokoły. Konsekwencją tych zmian jest zwiększenie podatności obecnych systemów SCADA ze względu na ich połączenie z otwartymi sieciami telekomunikacyjnymi. Dla przykładu atak przeprowadzony ze słabo zabezpieczonej sieci bezprzewodowej może sparaliżować dostarczanie wiadomości kontrolnych w czasie rzeczywistym i utratę kontroli nad fragmentem krytycznej infrastruktury. Podobnie niebezpieczne mogą być częste w otwartych sieciach IP ataki typu DoS i DDoS, mogące spowolnić bądź uniemożliwić komunikację między elementami systemu SCADA.

Projekt INSPIRE

Celem projektu INSPIRE jest zwiększenie bezpieczeństwa oraz ochrona sektora energetycznego poprzez odpowiednią konfigurację, zarządzanie i ochronę na styku sieci teleinformatycznych i rozproszonych systemów kontroli takich jak systemy SCADA. Aby osiągnąć zamierzone cele, projekt INSPIRE kieruje swoje działania na opracowanie efektywnych mechanizmów zwiększających bezpieczeństwo i odporność części telekomunikacyjnej SCADA. Ponadto zidentyfikowane i przeanalizowane zostaną podatności systemów SCADA, krytycznych infrastruktur oraz wykorzystywanych przez nie sieci telekomunikacyjnych.

Wiadomo, iż dotychczasowe awarie, zaniki oraz nagłe przerwy w działaniu krytycznych infrastruktur, takie jak awarie sieci energetycznych we Włoszech, USA, a także w Polsce (tzw. blackout) czy awarie sieci GSM (np. we Francji) wynikały z niezidentyfikowanych wcześniej podatności. Wcze-

śniejsza identyfikacja podatności pozwoliłaby na zapobieżenie zagrożeniom oraz ich skutkom.

Model komunikacji P2P

W zakresie technik zapewniających bezpieczeństwo sieciowe systemów typu SCADA rozpatrywany jest model komunikacji peer-to-peer (P2P). Oferując całkowicie zdecentralizowaną architekturę, w której każdy równorzędny węzeł może pełnić rolę i klienta i serwera, model P2P zapewnia także samoorganizację i samouzdrawianie, co może zwiększyć odporność systemów SCADA.

W zakresie zainteresowań projektu INSPIRE jest zbadanie cech P2P w celu wzmocnienia odporności systemu SCADA na ataki cybernetyczne. Architektura P2P może wesprzeć doręczanie wiadomości w czasie rzeczywistym oraz kontrolowaną replikację danych związanych z systemem SCADA, zwiększając jego odporność. W przypadku ataku lub uszkodzenia może działać jako usługa kopii zapasowej.

Użycie P2P jest rozważane pod kątem korzyści, jakie może przynieść, równocześnie nie wprowadzając jednak nowych, dodatkowych podatności do systemu. Zbadania wymaga także opłacalność zastąpienia istniejących węzłów niezdolnych do komunikacji P2P nowymi bądź dodanie nowych węzłów jako dodatkowe do istniejącej struktury. Proponowane jest aktywowanie architektury P2P na żądanie (P2P on-demand) – sieć P2P byłaby aktywowana tylko w razie potrzeby, w innym razie byłaby pasywna.

Technologia MPLS

Technologia MPLS (ang. Multiprotocol Label Switching) rozważana jest w kontekście stworzenia nowych algorytmów inżynierii sieciowej, obsługujących ruch krytyczny SCADA. W MPLS wszystkie pakiety należące do tego samego strumienia danych podążają tą samą ścieżką od źródła do przeznaczenia i są trasowane zależnie od etykiety przenoszonej w nagłówku MPLS. Wykorzystanie MPLS poprawia jakość dostarczanych usług oraz pozwala na rezerwację pasma dla przypływu ruchu i umożliwia implementowanie Wirtualnych Sieci Prywatnych (ang. Virtual Private Network). Dla systemów bazujących na szybkim i niezawodnym dostarczaniu danych, kontrolujących i nadzorujących infrastruktury krytyczne, szczególnie w sektorze energetycznym, właściwości MPLS wydają się odpowiednie.

> Celem projektu INSPIRE jest zwiększenie bezpieczeństwa oraz ochrona sektora energetycznego poprzez odpowiednią konfigurację, zarządzanie i ochronę na styku sieci teleinformatycznych i rozproszonych systemów kontroli takich jak systemy SCADA

Techniki wspomagania decyzji

Kolejnym obszarem wzmacniania bezpieczeństwa systemów SCADA i ich styku z sieciami teleinformatycznymi jest zastosowanie technik wspomagania decyzji (ang. decission support systems). Zastosowanie DSS umożliwia wsparcie operatorów sieci SCADA w zakresie proaktywnego identyfikowania podatności, wynikających z nich zagrożeń oraz proponowania optymalnych w danym kontekście środków zaradczych. W celu formalizacji reprezentacji wiedzy o domenie bezpieczeństwa systemów SCADA oraz na potrzeby jej współdzielenia pomiędzy producentami oraz beneficjentami tego typu systemów, projekt INSPIRE wykorzystuje opis semantyczny wiedzy o SCADA. Jednym z realizowanych obecnie produktów projektu jest narzędzie do audytu poziomu bezpieczeństwa (DAT) wykorzystujące formalną reprezentację wiedzy eksperckiej w zakresie bezpieczeństwa SCADA w postaci reguł. Ponadto rozważana jest wizja integracji z systemami zarządzania usługami wywodzącymi się z metodyki ITIL (np. integracja z bazą konfiguracji CMDB).

Podsumowanie

W niniejszym artykule przedstawiono zakres najważniejszych działań projektu INSPIRE prowadzonego w ramach 7 Programu Ramowego UE. Projekt ma na celu zwiększenie bezpieczeństwa oraz ochronę sektora energetycznego na styku sieci teleinformatycznych i systemów nadzorujących typu SCADA. W artykule przedstawione zostały rozwiązania w tym zakresie z zastosowaniem technik takich jak P2P, MPLS czy systemów DSS. Ukazano propozycje wzmocnienia odporności i niezawodności systemów SCADA i ich połączeń z sieciami teleinformatycznymi.

Literatura

[1] S.M. Rinaldi, J.P. Peerenboom, T.K. Kelly, Critical Infrastructure Interdependencies, IEEE Control Systems Magazine, December 2001.

Acknowledgement

The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement no. 225553 (INSPIRE Project).

Fundusze otrzymane na badania prowadzące do tych wyników pochodzą z European Community's Seventh Framework Programme (FP7/2007-2013) na podstawie umowy nr 225553 (Projekt INSPIRE).

□