POZNAN UNIVERSITY OF TECHNOLOGY ACADEMIC JOURNALS
No 105 Electrical Engineering 2020

DOI 10.21008/j.1897-0737.2020.105.0006

Grzegorz TRZMIEL*, Jakub KWACZ

WYBRANE SYSTEMY OCHRONY TECHNICZNEJ DLA STACJI ELEKTROENERGETYCZNYCH

W pracy przedstawiono specyfikacje poszczególnych elementów systemów ochrony technicznej będących zabezpieczeniami stacji elektroenergetycznej, a także zaproponowano koncepcję systemu zabezpieczeń. Opisano również sposoby integracji realizowanych systemów na stacjach elektroenergetycznych. Przedstawiono skrótowo metodologię doboru podstawowych parametrów niezbędnych do użytkowania systemów.

SŁOWA KLUCZOWE: systemy ochrony technicznej, stacja elektroenergetyczna.

1. WSTĘP

Zagrożenie mienia i obiektów to jeden z bardziej nurtujących problemów całego społeczeństwa. Poprawa warunków życia oraz zamożności ludzi wiąże ze sobą chęć zabezpieczenia konkretnej nieruchomości przez człowieka. Spowodowane jest to m.in. pojawiającymi się wiadomościami w mediach o globalnym wzroście zagrożenia atakami terrorystycznymi, które wymierzone są bezpośrednio w instytucje użyteczności publicznej czy nawet w mniejsze obiekty. Te pierwsze jednak traktuje się jako obiekty budowlane należące do grupy będącej tzw. Infrastrukturą Krytyczną.

Systemy objęte ochroną techniczną na terenie mienia, mniejszych obiektów czy firm są monitorowane przez specjalne firmy ochroniarskie i zobligowane są do interwencji w określonym przedziale czasowym. W przypadku zabezpieczenia Infrastruktury Krytycznej monitoring zdarzeń realizowany jest przez Centra Nadzoru (np. RCN – Radiowe Centra Nadawcze w przypadku stacji elektroenergetycznych). Posiadają one całodobowy dyżur operatorski, a w chwili zanotowania konkretnego zdarzenia realizują procedury poprzez Centra Zarządzania Kryzysowego. Systemy Sygnalizacji Pożaru pełnią rolę systemów zabezpieczenia życia. Te muszą być nadzorowane zarówno lokalnie jak i terytorialnie poprzez jednostki straży pożarnej.

* Politechnika Poznańska

2. WYBRANE ELEMENTY OCHRONY TECHNICZNEJ

Systemów wchodzących w skład SOT (systemu ochrony technicznej) wyróżnić można kilka. Firmy, które je realizują poprzez projekt bądź budowę, prześcigają się w ich nazewnictwie. Wszystko po to, aby klienta zainteresować, zachęcić, uzmysłowić, że na danym terenie będzie on niezbędny. I tak często System Sygnalizacji Włamania i Napadu rozbija się, tworząc System Ochrony Obwodowej. Wybór elementów ostatecznie implementowanych często zależy od możliwości finansowych kontrahentów. Na takim rynku najlepiej odnajdą się zatem średnie i duże przedsiębiorstwa, a już na pewno właściciel sieci najwyższych napięć w Polsce. Kompleksowe zabezpieczenie obiektów uzupełnia się o ich integrację i odpowiednią wizualizację na monitorach pracowników ochrony, co oczywiście poprzedzane jest kursami i szkoleniami. W poniższym artykule przedstawiono główne systemy zabezpieczeń stosowanych na stacjach elektroenergetycznych.

2.1. System Sygnalizacji Pożaru

Niezwykle istotnym systemem, który powinien znaleźć się wewnątrz każdej stacji elektroenergetycznej jest System Sygnalizacji Pożaru (SSP). Odpowiedzialny jest on za wykrywanie i sygnalizację pojawiających się zjawisk fizycznych, które są wynikiem powstawania pożaru. Budynki na terenie stacji muszą zostać całkowicie ochronione przed powyższymi zjawiskami w związku z ich przeznaczeniem i charakterystyką.

Sposób podłączenia elementów SSP realizowany jest dwojako. Większość elementów systemu połączonych jest ze sobą pętlowo. Do tzw. linii sygnałowych central zaś podłącza się wyłącznie sygnalizatory optyczne i akustyczne. Przy większej liczbie central w zależności od konfiguracji i lokalizacji urządzeń wykorzystuje się obecnie połączenia optotelekomunikacyjne, czyli światłowody.

W obiektach, w których może dochodzić do fałszywych alarmów związanych z czynnikami tj. zakłócenia elektromagnetyczne bądź duże zapylenie, wprowadza się tzw. dwustopniową organizację alarmowania. Często łączy się czujki w jedną strefę dozorową i programuje się odpowiedni wariant alarmowania. Taka koincydencja nie likwiduje, ale pozwala w znacznym stopniu eliminować nieuzasadnione zadziałanie czujek w budynku.

Przykładowy scenariusz pożarowy zakłada, że podczas wystąpienia alarmu I. stopnia, a więc podczas zadziałania jednej z czujek pożarowych, powiadomiony zostanie personel, który zdalnie powinien zidentyfikować miejsce, w którym ów alarm się pojawił. Dodatkowo powinien zrobić to w ustalonym z użytkownikiem czasie. Gdy alarm okaże się fałszywy, pracownik stacji sprawdza na obiekcie stan systemu. W przeciwnym wypadku inicjuje on zawiadomienie odpowiednich służb ratunkowych i technicznych, zdalnie – jeśli nie ma go na obiekcie lub wciskając najbliższy ręczny ostrzegacz pożarowy. Uruchomiony zostaje II stopień alarmu.

Może się on również pojawić w centrali pożarowej, gdy przekroczony zostanie określony czas, zadziałają naraz dwa lub więcej detektorów albo zasygnalizują to zamontowane urządzenia kontrolno-sterujące lub inne urządzenia przeciwpożarowe.

Głównymi funkcjami central pożarowych są: sygnalizacja akustyczna i optyczna stanów na centrali, uruchomienie sygnalizacji pożarowej na obiekcie, określenie miejsca zagrożonego pożarem, wysterowanie wyjść kontroli dostępu, wyłączenie klimatyzacji i wentylatorów w miejscu pożaru, przekazanie informacji o pożarze do Regionalnego Centrum Nadzoru oraz Systemu Sterowania i Nadzoru.

Nieodłącznym elementem każdej instalacji przeciwpożarowej jest czujka pożarowa. Jej rodzajów jest wiele, gdyż tyle może być jej różnych zastosowań. Dobierając ten element do konkretnego pomieszczenia należy uwzględnić jego wysokość, warunki otoczenia, a przede wszystkim założyć co może być przyczyną rozprzestrzeniania się pożaru w początkowym etapie.

Dla małej prędkości spalania skutkiem pożaru jest duża ilość dymu – zastosować należy optyczną rozproszeniową czujkę dymu. Ma to jednak istotną wadę. Wszelkie aerozole, kurz bądź para wodna (np. z urządzeń kuchennych) interpretowane będą przez nią jako dym, a to prowadzić może często do fałszywych alarmów. Gdy zaś założenia projektowe wykażą dużą prędkość spalania w danym miejscu, spodziewać się można ciepła, dymu oraz płomienia. W takim przypadku wybór odpowiedniej czujki jest trudny. Najczęściej stosuje się wtedy czujki jonizacyjne lub wielodetektorowe (dualne). Wszystkie powyższe to tzw. czujki punktowe.

Innym rozwiązaniem, często stosowanym w pomieszczeniach, gdzie, z powodu dużej powierzchni pomieszczenia, wystąpiłaby potrzeba zainstalowania dużej liczby punktowych czujek dymu, jest czujka liniowa. Jej rola to analiza przezroczystości optycznej powietrza w przestrzeni między czujką, a zainstalowanym po drugiej stronie reflektorem pryzmowym. Podobnie jak w odpowiednikach punktowych ustawiany jest określony próg czułości decydujący o wejściu w stan alarmowania. Zwykle posiada nadajnik i odbiornik promieniowania podczerwonego, dzięki któremu strumień powietrza, nawet w przypadku największego stężenia dymu, nigdy nie zostanie przerwany. Gdy coś zablokuje tor optyczny, automatycznie wysłany jest do centrali stan uszkodzenia [1, 2].

Ręczne ostrzegacze pożarowe montuje się w każdym budynku na stacji. W przypadku większej liczby pomieszczeń, wykonuje się je w miejscach, do których żadna osoba nie musiałaby przebywać drogi dłuższej niż 30 m, pokonując drogę ewakuacyjną, najlepiej na wysokości normatywnej od 1,2 do 1,5 m nad podłogą. Cechą charakterystyczną ręcznych ostrzegaczy pożarowych jest fakt, iż nie odblokowują one wszystkich przejść ewakuacyjnych, a wywołują jedynie alarm II stopnia. Otwarcie drzwi nastąpi tylko i wyłącznie w chwili, gdy jednocześnie zadziała czujka pożaru zainstalowana w budynku, w którym ROP został wyzwolony.

Sygnalizatory optyczno-akustyczne instaluje się na zewnątrz budynku. Urządzenia te muszą charakteryzować się dużo szczelnością. Dla budynku wyniesionego sygnalizator musi zostać zasilony z certyfikowanego zasilacza i wyzwolony poprzez moduł pętlowy wejść/wyjść. Dla wewnętrznych rozwiązań można wykorzystać pętlowe sygnalizatory akustyczne, które instaluje się na linii dozorowej. Są one za jej pomocą wyzwalane oraz zasilane. W razie zaniku napięcia instaluje się rezerwowe źródło zasilania, które zapewnia pracę sygnalizatora przez przynajmniej 30 minut.

W przypadku wykrycia pożaru ważną rolę pełnią moduły. Sterują m.in. pracą klimatyzatorów, aby ogień nie rozprzestrzenił się od podmuchu powietrza lub otwierają przejścia objęte kontrolą dostępu.

W razie wystąpienia awarii zasilania głównego, niezbędne jest zastosowanie rezerwowego w postaci akumulatorów. Ich pojemność powinna umożliwić utrzymanie instalacji w stanie pracy przez co najmniej 72 godziny, po czym musi zapewnić alarmowanie jeszcze co najmniej 30 minut.

Bilans prądowy liczy się ze wzoru [1, 2, 3]:

$$Q = 1,25 \cdot \left(I_d \cdot T_d + I_a \cdot T_a \right) \tag{2.1}$$

gdzie:

Q – pojemność akumulatora [Ah], I_d – prąd pobierany przez urządzenia w stanie dozoru [A], T_d – czas dozoru = 72 h, I_a – prąd pobierany przez urządzenia w stanie alarmu [A], T_a – czas alarmowania – 0,5 h.

2.2. System Sygnalizacji Włamania i Napadu

System alarmowy SSWiN najczęściej realizowany jest w oparciu o poniższe założenia:

- ochrona wybranych pomieszczeń za pomocą wielosensorowych czujek ruchu,
- kontaktrony drzwiowe na wszystkich drzwiach zewnętrznych oraz szafach teleinformatycznych,
- ochrona obwodowa kluczowych budynków stacji w tym m.in. Budynku Nastawni przy wykorzystaniu barier podczerwieni,
- koincydencja całego systemu z ochroną obwodową naokoło terenu stacji.

Centrala alarmowa posiada konstrukcję mikroprocesorową. Pozwala to na podział systemu na tzw. strefy dozorowe. Moduł, do którego podłączony jest czujnik, nie identyfikuje go z konkretnym podsystemem. O przynależności decyduje sposób zaprogramowania centrali. Tworzy to zjawisko funkcjonalności, ponieważ wyłączenie z dozoru może obejmować tylko te pomieszczenia w budynkach, w których wykonywana jest praca. Pozostała część systemu pozostaje w stanie czuwania.

Wszystkie urządzenia użyte w opisywanym systemie muszą posiadać tzw. ochronę sabotażową. Każdy brak komunikacji z modułami, każda usterka czy

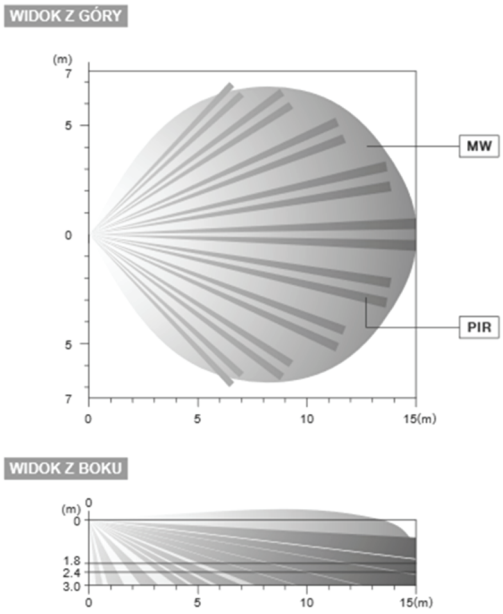
otwarcie którejś obudowy powinien wywołać w systemie alarm. Ponadto nadzorowana powinna być ciągłość sygnalizatorów. System zatem musi rozpoznawać cztery stany: usterki – gdy wystąpi zwarcie w obwodzie, alarmu – gdy linia będzie otwarta, a czujka zostanie naruszona, sabotażu – następuje przerwa w obwodzie, a obudowa została otwarta i normalny – gdy linia będzie zamknięta, a czujka nie została naruszona.

Dla obiektów objętych tzw. Infrastrukturą Krytyczną wymagane jest zabezpieczenie w najwyższej międzynarodowej klasie Grade 3. Urządzenia tego stopnia mogą być wykorzystywane w instalacjach „wysokiego ryzyka", a więc wszystkie elementy należące do systemu SSWiN muszą posiadać odpowiednie wymagania. Centrala powinna charakteryzować się ponadto wysoką elastycznością konfiguracji i jest być przyjazna dla instalatorów.

Naruszenie strefy detekcji systemu alarmowego sygnalizuje się sygnalizatorami optyczno-akustycznymi, sygnałem akustycznym w manipulatorach, a także komunikatem na wyświetlaczu ciekłokrystalicznym.

W przypadku zarejestrowania wejścia do chronionego budynku bez użycia identyfikatora alarm zostaje uruchomiony natychmiastowo, gdy jednak użytkownik posłuży się nim, wówczas sygnał przekazany zostaje do centrali alarmowej. Załączone zostaje opóźnienie, aby dana osoba mogła wejść do budynku i rozbroić system alarmowy za pomocą jednej z dwóch klawiatur sterujących – tzw. manipulatorów.

Czujki ruchu nie mogą być przysłonięte, ani znajdować się w pobliżu otworów wentylacyjnych. Popularne stają się czujki dualne PIR+MW, które instaluje się w celu połączenia właściwości czujek mikrofalowych oraz czujek ruchu pasywnej podczerwieni. Pierwsze wykorzystują zjawisko Doppler'a – porównują częstotliwości wysyłane przez nadajnik i odbite przez obiekt ruchomy. Drugie zaś emitują fale radiowe o wysokiej częstotliwości i analizują zmiany natężenia promieniowania podczerwonego. Dzięki takiemu połączeniu minimalizuje się ryzyko powstania fałszywych alarmów, przez co zwiększa się ich wiarygodność. Zasięg działania czujki nazywany jest tzw. strefą podejścia. Jej widok przedstawiony jest na rysunku 2.1.



Rys. 2.1. Charakterystyka pracy powierzchniowej czujki ruchu CDX-DAM [4]

Na stacjach elektroenergetycznych wykorzystuje się często czujki zewnętrzne, które przeznaczone są do pracy w każdych warunkach atmosferycznych, a także posiadają funkcję wykrywania przemieszczania ludzi po terenie, ignorując przy tym poruszanie się innych obiektów, jak np. gałęzi drzew. Metoda ta nazywana jest Linear Travel Distance (LTD).

Koincydencja na obiektach będących infrastrukturą krytyczną może przyjmować różne formy. Jednak dzięki skorelowaniu dwóch niezależnych sygnałów alarmowych wybrany wariant alarmowy wywołany zostanie tylko w przypadku jednoczesnego wystąpienia ich naruszenia. Sposoby zabezpieczeń, którymi są bariery podczerwieni i kamery termowizyjne mogą być jednym z takich przykładów. Pełnią wówczas ochronę peryferyjną obiektu. W obszarach, gdzie, oprócz bariery instaluje się czujkę ruchu, również można wykorzystać ich umiejscowienie w celu zaimplementowaniu takiej koincydencji. Programuje się wówczas centralę alarmową w taki sposób, że alarm na jednym urządzeniu zasygnalizowany zostanie obsłudze, jednak dopiero koincydencja naruszenia przez oba urządzenia wywoła zadziałanie sygnalizatorów optyczno-akustycznych. Ochronę taką jednak wcześniej ustala się z użytkownikiem. [1, 2]

2.3. System Kontroli Dostępu

Wejścia do głównego budynku na stacji (np. do wspomnianego wcześniej Budynku Nastawni) oraz najważniejsze pomieszczenia najczęściej wymagają zabezpieczenia w postaci urządzeń kontroli dostępu. Obsługę tych wejść nadzoruje użytkownik stacji poprzez System Kontroli Dostępu. Dzięki połączeniu ze sobą odpowiednich elementów w danej konfiguracji oraz poprawnemu ich zaprogramowaniu, można nadać uprawnienia danej osobie bądź grupie osób, dzięki czemu budynek i/lub poszczególne w nim pomieszczenia zostaną udostępnione tylko osobom do tego upoważnionym.

Głównym urządzeniem, który scala ze sobą wszystkie elementy w systemie, jest centrala. Jego możliwościami są m.in. prezentacja stanu strefy alarmowej – odpowiedzialna za przekazanie informacji o lokalizacji wystąpienia próby wtargnięcia osoby nieupoważnionej, sterowanie nim z poziomu terminali, a także pozwala na integrację z systemem alarmowym, aby w określonych sytuacjach sygnalizować alarm.

Użytkownicy mający specjalne uprawnienia mogą, dzięki posiadanej karcie magnetycznej bądź wpisaniu kodu PIN, prawnie wejść na teren chroniony. Nie zawsze jednak instaluje się je z obu stron przejścia. Wychodząc z budynku nie powinno się wymagać od obsługi ponownej weryfikacji, a więc przy takich drzwiach (od wewnątrz) instaluje się tylko przycisk. Oba warianty wysyłają sygnał do elementu nazywanego elektrozaczepem rewersyjnym. To urządzenie fizycznie blokujące przejście przed nieupoważnionym wejściem. Ważnym elementem jest także przycisk wyjścia awaryjnego, powoduje przerwanie prądu w obwodzie, a co za tym idzie zwalnia elektrozaczep.

Firmy na rynku oferują m.in. czytniki linii papilarnych wyposażone w optyczny skaner jak również w klasyczny czytnik kart zbliżeniowych. Urządzenia te działają w dwóch trybach: 1:N oraz 1:1. W tym pierwszym rozpoznają użytkownika poprzez porównanie zeskanowanego odcisku palca z wcześniej wgranymi do wewnętrznej bazy danych odciskami wzorcami. W drugim natomiast porównanie dokonuje się ze wzorem odcisku palca wczytanym z karty zbliżeniowej. Właśnie to rozwiązanie wydaje się spełniać standardy bezpieczeństwa, według których to pracownik przechowuje na własnym nośniku swoje dane biometryczne.

W obecnych czasach coraz większą rolę odgrywają techniki biometryczne ze względu na specyfikę działania. Opierają się na skonkretyzowanych cechach organizmu, charakterystycznych dla każdego człowieka. Najpopularniejsze z nich dzieli się na poszczególne podgrupy. Są to systemy oparte o rozpoznawanie [5]: linii papilarnych, geometrii dłoni, mowy, cech charakterystycznych tęczówki oka.

2.4. System Telewizji Dozorowej

Do rejestrowania obrazu na terenie stacji elektroenergetycznych, oprócz kamer termowizyjnych, które wykorzystuje się do ochrony obwodowej, wykorzystuje się System Telewizji Dozorowej. Działa on m.in. w oparciu o kamery stacjonarne czy obrotowe typu dzień/noc. Realizowany jest bardzo często w technologii IP PoE (ang. Internet Protocol - Power over Ethernet). Zewnętrzne aparaty to kamery światła białego i służą do ciągłej obserwacji transformatorów, wejść do budynków czy terenu stacji. Instaluje się je w specjalnych obudowach zewnętrznych i podłącza dzięki okablowaniu światłowodowemu w przypadku, gdy są one znacznie oddalone od budynków, w którym znajdują się rejestratory czy przełączniki sieciowe. Kamery zainstalowane na tych budynkach, bądź w nich podłączane są kablami miedzianymi.

Obsługa systemu odbywa się lokalnie z rejestratora poprzez przełącznik KVM (ang. Kernel-based Virtual Machine). Dzięki temu możliwy jest zapis cyfrowy, a co za tym idzie zapewnia to łatwość przeszukiwania archiwum, a także wielokrotne wykorzystanie nośnika danych, którym jest dysk twardy. Rejestrator zabezpiecza również archiwum przed niepożądanymi modyfikacjami. System pozwala również na przesyłanie danych przez sieć oraz bezpośrednio na inne nośniki bez straty na jakości.

Rejestrator IP powinien rejestrować obraz w trybie ciągłym – 24 godziny przez 7 dni w tygodniu w pełnej rozdzielczości. Obowiązkowo stosuje się redundantny zasilacz, a jego minimalny okres rejestracji nie powinien być mniejszy niż pełny miesiąc.

Przy doborze konkretnego urządzenia zawsze wcześniej skupia się na jego lokalizacji oraz celu, dla którego ma być on zainstalowany. Ważnymi elementami przy kamerach są warunki atmosferyczne oraz (lub też co za tym idzie) oświetlenie terenu, który ma być objęty monitoringiem. Często zapomina się także o roślinności, która może kolidować z rejestrowanym obrazem. Usuwanie drzew, które „przeszkadzają" w prawidłowej widoczności wiąże się z olbrzymimi kosztami. Nierzadko więc w zastępstwie wybiera się wariant związany z zastępczymi nasadzeniami.

Tradycyjne kamery rejestrują jedynie promieniowanie widzialne, a więc odbicie promieniowania źródła. Na terenach dobrze oświetlonych (tam, gdzie w pobliżu znajdują się latarnie) występuje doskonały obraz docierany do użytkownika. Może on łatwo rozpoznać czyjąś twarz czy zarejestrować niepokojące zachowania. Znajdują więc one zastosowanie we wnętrzach budynku lub przy wejściu do nich [5].

Kamery termowizyjne skonstruowane są tak, aby wykrywać niewidzialne promieniowanie podczerwone czy temperaturę ciał. W porównaniu z kamerami tradycyjnymi nie dają one idealnego obrazu, a więc użytkownik nie wychwyci wszystkich szczegółów obserwowanego celu, jednak mają niewątpliwie wielką

zaletę. Nawet pomimo całkowitej ciemności na obrazie można obiekt dostrzec, a także odróżnić go od reszty tła. Takie kamery montuje się na dużych obszarach ze zwiększoną roślinnością i przeszkodami, za którymi może ukrywać się włamywacz.

2.5. System Sterowania i Nadzoru

Na stacjach elektroenergetycznych występuje stacyjny System Sterowania i Nadzoru (SSiN), do którego wyprowadzone są sygnały ze wszystkich systemów informujące obsługę o alarmach czy uszkodzeniach poszczególnych elementów zabezpieczających. Jest to bardzo istotne, gdyż zarówno ochrona obiektu, jak i pracownicy muszą zostać poinformowani o powstałym zdarzeniu i poprawnie je zinterpretować. Tworzy się zatem listę przekaźników, z których każdy odpowiedzialny jest za to, by zasygnalizować jedno z nich. Istotną sprawą jest, aby rozdzielić sygnały według systemów tak, aby klient mógł wiedzieć z jakim typem zjawiska ma do czynienia i w jakiej strefie występuje. W tym celu do sterownika sygnalizacji ogólnej doprowadza się kabel sterowniczy (np. typu YKSY) [2].

3. PROJEKT SYSTEMU OCHRONY TECHNICZNEJ STACJI ELEKTROENERGETYCZNEJ

Stacje elektroenergetyczne należą m.in. do tzw. Infrastruktury Krytycznej (IK) i podlegają wszelkim standardom oraz ustawom związanymi z tym terminem. Według Rządowego Centrum Bezpieczeństwa oraz ustawie o zarządzaniu kryzysowym są systemy oraz obiekty, które są kluczowe dla bezpieczeństwa obywateli oraz całego Państwa. Cel takiego podziału jest o tyle istotny, że podczas zniszczeniu bądź uszkodzeniu takiej infrastruktury zagrożone może być życie jak i mienie obywateli. Ochrona IK wiąże się z konkretnymi działaniami prowadzącymi do zapewnienia jej funkcjonalności, a także integralności. Pomoże to zapobiec wszelakim zagrożeniom czy słabym punktom takich obiektów, a także prowadzi do ograniczenia niepożądanych skutków mogących wystąpić w wyniku awarii czy ataków z zewnątrz.

Właściciele stacji elektroenergetycznych (jak np. PSE Operator) wydali wytyczne w zakresie organizacji ochrony obiektów elektroenergetycznych. Precyzują w nich m.in. zasady identyfikacji zagrożeń [2].

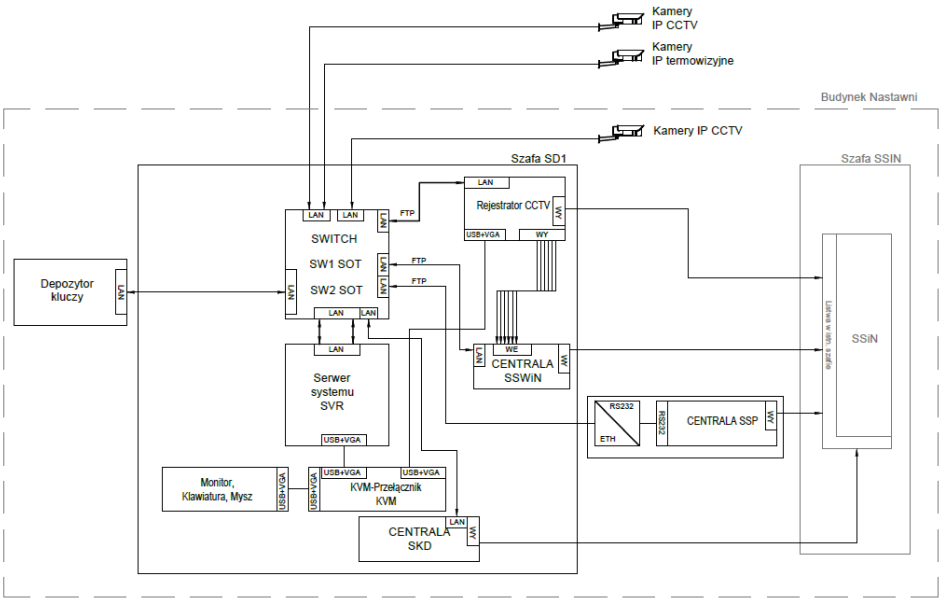
W artykule przedstawiono przykładowy szablon stacji elektroenergetycznej, na którym zaznaczone są budynki należące do obiektu wraz z doprowadzonymi do nich kanałami kablowymi. Wyrysowane zostały również istniejące słupy oświetleniowe, które wykorzystuje się do instalacji urządzeń zewnętrznych, a także ogrodzenie zewnętrzne obiektu czy nawierzchnie asfaltowe pełniące rolę przejść między budynkami.

3.1. Założenia projektowe

W projekcie zaproponowano: System Sygnalizacji Pożaru (SSP), Sygnalizacji Włamania i Napadu (SSWiN), Kontroli Dostępu (SKD) oraz Telewizji Przemysłowej (CCTV). Zaproponowano również warianty alarmowania w chwili wykrycia zagrożenia przez systemy, a następnie zdefiniowano komunikaty, które docierają do ochrony obiektu.

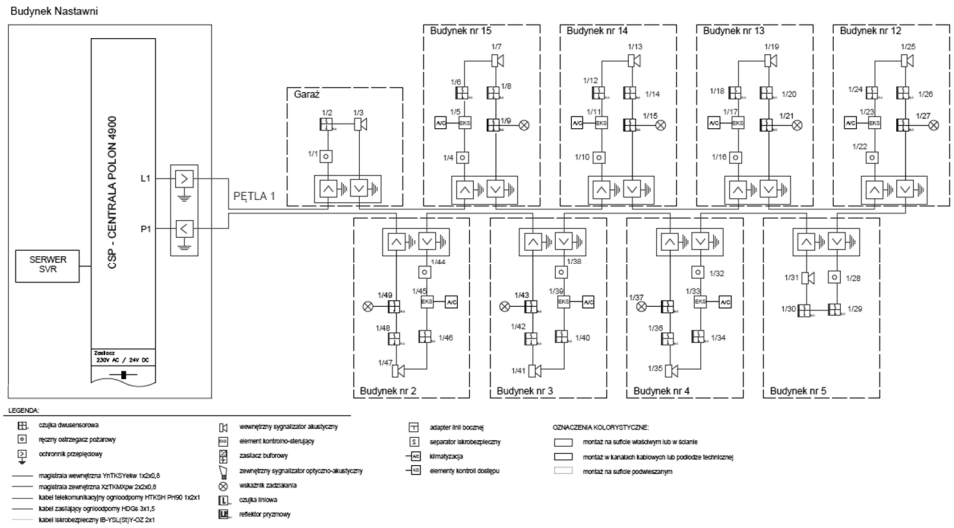
3.2. Realizacja projektu

Na rys. 3.1 przedstawiono schemat blokowy całej projektowanej instalacji systemu ochrony technicznej w budynku nastawni.



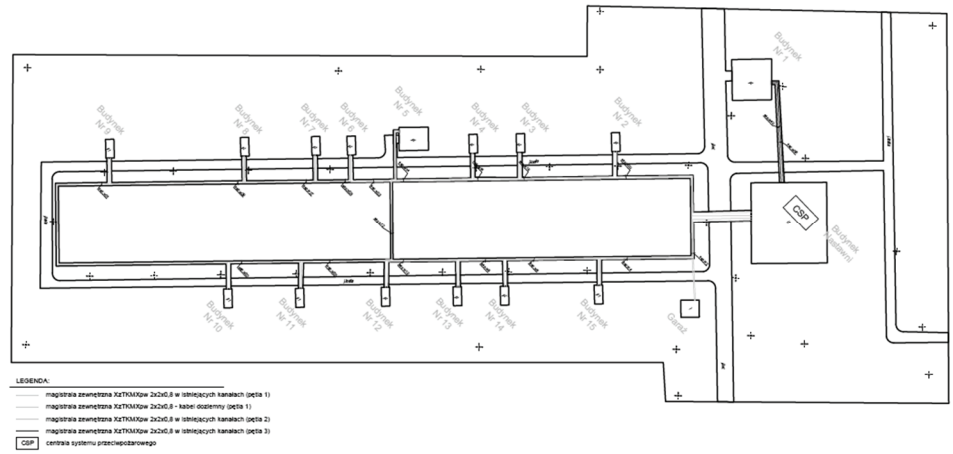
Rys. 3.1. Ogólny schemat blokowy zaprojektowanego SOT [2]

Na rys. 3.2 pokazano schemat blokowy fragmentu (pętli nr 1) systemu sygnalizacji pożaru (SSP) w rozpatrywanej stacji. Docelowo zaprojektowano 5 pętli.



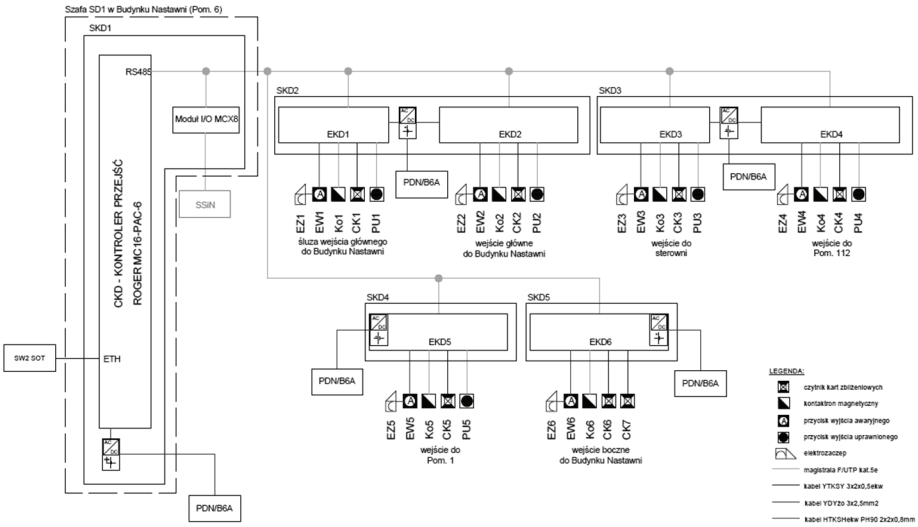
Rys. 3.2. Schemat blokowy pętli nr 1 zaprojektowanego SSP [2]

Dla wszystkich budynków stacji sporządzono plan instalacji kablowych SSP (rys. 3.3) oraz szczegółowe plany instalacji SSP w poszczególnych budynkach.



Rys. 3.3. Plan instalacji kablowych SSP na terenie stacji [2]

Analogicznie wykonano schematy instalacji dla systemów: SSWiN, SKD i CCTV. Przykładowo, na rys. 3.4 umieszczono jeden ze schematów dla zaprojektowanego SKD.



Rys. 3.4. Schemat blokowy SKD na stacji elektroenergetycznej [2]

Dodatkowo, w całym projekcie sporządzono też schematy szafek CCTV, szafek alarmowych SSWiN oraz szafki ochronników przepięciowych SSP. W sumie pełna dokumentacja projektu zawiera 44 schematy: blokowe, plany instalacji oraz projekty szafek dla wszystkich systemów.

4. PODSUMOWANIE

W artykule przedstawiono najważniejsze informacje na temat wybranych systemów ochrony technicznej przykładowej stacji elektroenergetycznej oraz pokazano wybrane elementy zaprojektowanego systemu. Artykuł stanowi wskazanie na wagę i istotę problemu ochrony technicznej stacji elektroenergetycznych. Realizacja projektu przykładowego systemu jest zagadnieniem złożonym, pracochłonnym i bardzo obszernym, aczkolwiek niezwykle ważnym w aspekcie ochrony technicznej obiektu.

LITERATURA

[1] Kastek M., Dulski R., Życzkowski M., Multisensor systems for security of critical infrastructures – Concept, data fusion, and experimental results, Proceedings of SPIE – The International Society for Optical Engineering 8193, DOI: 10.1117/12.900969, 2011.
[2] Kwacz J., Systemy ochrony technicznej dla stacji elektroenergetycznych, Praca dyplomowa, Politechnika Poznańska, 2019.
[3] Strona internetowa AVAL, http://www.aval.com.pl/index.php?zasilanie-rezerwowe, 10.02.2020.

[4] Strona internetowa NAPAD, https://www.napad.pl/karty-katalogowe/czujka-cdx-dam-karta-katalogowa.pdf, 10.02.2020.
[5] Strona internetowa BIOMETRIA, http://biometria.pl/biometria.html, 10.02.2020.

SELECTED TECHNICAL PROTECTION SYSTEMS FOR ELECTRICAL POWER STATIONS

The paper presents specifications of individual elements of technical protection systems that are power station protections, and also proposes a concept of a security system. Methods of integration of implemented systems at power stations were also described. The methodology for selecting the basic parameters necessary to use the systems is briefly presented.

(Received: 19.02.2020, revised: 07.03.2020)