Robotyzacja w usługach bezpieczeństwa

TECHNOLOGIA WPŁYWAŁA NA MIEJSCA PRACY NA PRZESTRZENI DZIEJÓW. WYNALAZKI TAKIE JAK ELEKTRYCZNOŚĆ I KOMPUTERY CAŁKOWICIE ZMIENIŁY SPOSÓB W JAKI PRACUJEMY. NIE INACZEJ JEST DZISIAJ. POJAZDY AUTONOMICZNE, ROBOTYKA, SZTUCZNA INTELIGENCJA (AI) I AUTOMATYZACJA WPŁYWAJĄ NA SPOSÓB I EFEKTY NASZEJ PRACY.

Jan T. Grusznic

R&D Manager w Securitas Polska, pomysłodawca i projektant systemów automatyzujących pracę ochrony. Inżynier elektronicznych systemów zabezpieczeń, z branżą związany od 2004 r.

Securitas

Słyszymy o coraz śmielszych wdrożeniach robotów w różnych sferach naszego życia, które dotychczas rezerwowaliśmy dla ludzi: wydawanie posiłków, obsługa gości czy usługi transportowe. Tak, to jest możliwe! Przykładem mogą być usługi taksówkarskie w San Francisco realizowane przez autonomiczne pojazdy. Od pewnego czasu następuje również wielowymiarowa robotyzacja usług ochrony, której zadaniem jest zwiększanie efektywności, redukcja liczby błędów oraz oszczędność czasu i pieniędzy.

Kiedy firma Knightscope w 2015 roku zaprezentowała swojego pierwszego robota stróżującego, zachwytom nie było końca. Z biegiem lat liczba incydentów z udziałem maszyn zmniejszyła entuzjazm w branży bezpieczeństwa. Również zasada działania została zweryfikowana – autonomiczne maszyny mają na celu uzupełnienie składu ochrony, powiadamiają pracowników o podejrzanej aktywności, ale same nie interweniują bezpośrednio. Prawdą jest, że właściwe wdrożenie robotów i rozwiązań automatyzujących procesy wpływa na znacząco niższe wskaźniki incydentów w obszarach nadzorowanych przez takie systemy, a to przekłada się na zwiększone poczucie bezpieczeństwa oraz na wyższy komfort użytkowników obiektu. Nie zawsze jednak automatyzacja przekłada się na takie wyniki. Osiągnięcie sukcesu w tej sferze wymaga uprzednio wykonania solidnej analizy procesów, ich opisania i zmapowania (przypisanie poszczególnych etapów do właściwych użytkowników, określenie czasu trwania etapu, zdefiniowania wyjątków, itp.). Dopiero w kolejnym kroku możliwe jest rozpoczęcie prac nad przygotowaniem algorytmu, który będzie odpowiedzialny za nadzorowanie każdego etapu procesu, komunikację i zarządzanie wyjątkami. Takie podejście zagwarantowało sukces wdrożenia systemu Securitas smartGATE (automatyzujący ruch kołowy w zakładach produkcyjnych i logistycznych) i Securitas smartIN (automatyzujący proces obsługi gościa w budynkach biurowych).

Od czego zacząć?

Kluczowe jest określenie obszarów wymagających poprawy w obecnych procesach. Warto zastanowić się co jest wyzwaniem dla użytkowników, gdzie są punkty bólu i jaki jest pożądany efekt docelowy. Na tym etapie Klientów potrafi ponieść wyobraźnia i przypisują robotom funkcjonalności, o których nie śniło się jeszcze nawet inżynierom. Z drugiej strony obciążeniem jest sposób działania obecnego procesu, od którego wad trudno się uwolnić, i które mimowolnie przenoszone są do nowo tworzonego modelu. W Securitas panuje zasada: im więcej wiemy, tym bardziej możemy być pomocni. Warto jest stworzyć listę co jest „koniecznością", co jest „potrzebą", a co po prostu jest „fajnie mieć". Często okazuje się, że po wielu dialogach „musi" było tak naprawdę „fajnie mieć" i na odwrót.

Współpraca i komunikacja są kluczowe w osiągnięciu celu w każdym projekcie. Kiedy cel zadania i oczekiwania wobec rozwiązania zostaną odpowiednio wcześnie ustalone, wdrożenie przebiega bez problemów. Warto pamiętać, że każda organizacja jest inna, dlatego nie zawsze rozwiązania, które funkcjonują w firmie X będą efektywne w firmie Y. Składową sukcesu jest prowadzenie ciągłej i jasnej komunikacji oraz wspólne wprowadzanie ulepszeń, a w wielu przypadkach to sam Klient, bez konsultacji z zespołem, oczekuje znaczących zmian.

W przypadku wdrożeń takich jak roboty czy automatyzacja procesów, trzeba określić

źródło finansowania. Usługi ochrony zasilane są na ogół z budżetu przeznaczonego na bezpieczeństwo. Gdy jednak chodzi o wdrażanie innowacyjnych usług, opcji jest wiele i koszty mogą być alokowane w budżecie obiektu, budżecie IT lub budżecie przeznaczonym na innowacje. Warto jest wiedzieć, kto jest sponsorem, a także kto będzie zaangażowany w proces podejmowania decyzji. O ile dyrektor ds. bezpieczeństwa decyduje, że potrzebne są nowe kamery i taka decyzja nie wymaga szerszych konsultacji, to w przypadku np. 200-kilogramowego, w pełni autonomicznego robota, patrolującego siedzibę 24/7/365, prawdopodobnie w proces decyzyjny będzie zaangażowanych więcej osób. Nie inaczej jest z rozwiązaniami automatyzującymi procesy. Tylko Securitas smartGATE wymaga zaangażowania osób z 7 działów: bezpieczeństwa, produkcji, logistyki, bhp, IT, finansów i zarządzania obiektem na różnym etapie projektu.

Ciemna strona automatyzacji

Niestety nie ma systemów pracujących non stop ze skutecznością 100%. Zawsze, wcześniej czy później, pojawiają się wyjątki, którymi ktoś lub coś musi zarządzić, i należy to przewidzieć w procedurach. Zastosowanie się do wszystkich wytycznych producentów dotyczących konfiguracji urządzeń i instalacji gwarantuje nam na ogół skuteczność działania (np. analiza danych, sygnałów, procedur, itp.) na poziomie nie mniejszym niż 95%. Korzystając z doświadczenia i wiedzy eksperckiej potrafimy ten wynik, przy prawidłowej instalacji i obsłudze, podnieść do poziomu przeszło 99%. Nie oznacza to jednak, że w momencie wdrożenia system będzie działał z taką skutecznością. Poza tym to cały czas nie jest 100%. Ciemną stroną utrzymania wysokiej skuteczności algorytmów jest wzrastająca liczba wyników fałszywie pozytywnych (popularnie zwanych fałszywymi alarmami). Użyte powyżej wartości procentowe skuteczności działania algorytmu to prawdopodobieństwo wykrycia ukazujące stosunek zdarzeń wykrytych przez system do wymaganej, sumarycznej liczby zdarzeń wymagających wykrycia (tu znajduje się nasze hipotetyczne 100%). Przykładem może być system zliczania osób. W danej jednostce czasu zmierzona liczba przejść w systemie jest porównywana z wynikami zebranymi np. przez osoby zliczające. W przypadku systemów logistycznych i parkingowych liczba poprawnie odczytanych tablic rejestracyjnych pojazdów w jednostce czasu jest konfrontowana z danymi np. czujnika obecności pojazdu lub zapisem z kamer. Z kolei fałszywe alarmy oznaczają liczbę zdarzeń, które zostały odnotowane w systemie, a które nie były istotne. Liczba fałszywych alarmów jest zawsze postrzegana jako wartość krytyczna. Wyobraźmy sobie galerię handlową chronioną przez pracowników ochrony wspieranych przez elektroniczne systemy bezpieczeństwa. Jedno błędne zdarzenie przypadające na urządzenie w ciągu dnia jest do zaakceptowania. Ale gdy systemy składają się z tysięcy czujników, to duża liczba fałszywych alarmów obniża efektywność systemu, powoduje wydłużenie czasu obsługi i negatywnie wpływa na utrzymanie bezpieczeństwa.

Dokładność rozpoznawania to doskonały wskaźnik jakości oprogramowania, ale równie ważny jest wskaźnik fałszywego rozpoznania, często pomijany przez producentów.

Następny etap – świadomość operacyjna

Portfolio rozwiązań oferowanych przez dostawców elektronicznych systemów bezpieczeństwa jest bardzo szerokie. Rozwiązania typowe jak telewizja dozorowa, systemy sygnalizacji włamania i napadu, sygnalizacji pożaru i kontroli dostępu mogą być wsparte platformami integrującymi, zapewniającymi zarządzanie sygnałami z wielu systemów w jednym interfejsie, narzędziami analitycznymi, a nawet wsparciem dla aplikacji mieszanej rzeczywistości[1]. Większość z wymienionych systemów stanowi wyposażenie chronionych obiektów. Wszystkie są wykorzystywane przez pracowników ochrony. Platformy wspierające są jednak rzadkim elementem na jaki decydują się właściciele obiektów – głównie z powodu kosztów. Tymczasem takie rozwiązania stanowią istotny element w budowaniu tzw. „koncepcji świadomości operacyjnej" – podstawy skutecznego bezpieczeństwa. Polega ona m.in. na udostępnieniu intuicyjnych wizualizacji uwzględniających wszystkie informacje potrzebne do zidentyfikowania miejsca i przyczyn incydentu oraz podjęcia szybkich reakcji. Ważny jest też dostęp i integracja dużych zasobów danych: historycznych, dostarczanych w czasie rzeczywistym oraz danych predykcyjnych, ze zintegrowanych systemów, ale również z zewnętrznych źródeł danych. Takie podejście zapewnia wyższą świadomość o potencjalnych zdarzeniach. Dodając do tego złożoność obiektu, dodatkowe informacje referencyjne prezentowane na etapie weryfikacji powstałego incydentu, można udoskonalić i poprawić dokładność reakcji w sytuacji awaryjnej. To właśnie inwestycje w takie rozwiązania zapewnią zwrot z inwestycji wynikający z optymalizacji składu osobowego pracowników ochrony przy jednoczesnym zwiększeniu poziomu bezpieczeństwa.

> WSPÓŁPRACA I KOMUNIKACJA SĄ KLUCZOWE W OSIĄGNIĘCIU CELU W KAŻDYM PROJEKCIE. KIEDY CEL ZADANIA I OCZEKIWANIA WOBEC ROZWIĄZANIA ZOSTANĄ ODPOWIEDNIO WCZEŚNIE USTALONE, WDROŻENIE PRZEBIEGA BEZ PROBLEMÓW.

[1] Połączenie świata rzeczywistego i wirtualnego w celu tworzenia nowych środowisk i wizualizacji, w których obiekty fizyczne i cyfrowe współistnieją i oddziałują w czasie rzeczywistym. Rzeczywistość mieszana nie odbywa się wyłącznie w świecie fizycznym lub wirtualnym, ale jest hybrydą rzeczywistości i rzeczywistości wirtualnej.