

O standaryzacji Internetu rzeczy i jego zastosowań

„Normy to nie tylko kwestia techniczna. Określają technologię, która wdroży Społeczeństwo Informacyjne, a w konsekwencji sposób, w jaki skorzystają z niego przemysł, użytkownicy, konsumenci i administracja”. Ten cytat przekazuje dwa ważne spostrzeżenia, które zbyt często są pomijane. Po pierwsze, systemy technologii informacyjno-komunikacyjnych (ICT) po prostu nie działałyby bez podstawowych standardów. Po drugie, dzisiejsze standardy ICT to technologia jutra. Oznacza to, że ci, którzy obecnie przewodzą inicjatywom normalizacyjnym, prawdopodobnie będą sterować, jeśli chodzi o faktyczny rozwój i wdrażanie technologii. W każdym systemie teleinformatycznym wdrażanych jest wiele standardów, od najbardziej złożonej infrastruktury międzynarodowej po skromny komputer PC na biurku w domu. Istnieją standardy dotyczące systemów operacyjnych, języków programowania, interfejsów użytkownika, protokołów komunikacyjnych, napędów dysków, kabli i złączy i tak dalej. Biddle i inni stwierdzili, że co najmniej 251 standardów interoperacyjności jest wdrażanych w laptopie; uważają, że łączna liczba norm dotyczących takiego urządzenia jest znacznie wyższa. W dzisiejszych czasach ekonomiczne znaczenie norm nie jest już kwestionowane. Swann przedstawia bardzo dokładny przegląd odpowiedniej literatury. W raportowanych ustaleniach można znaleźć m.in. tak samo jak patenty na wzrost gospodarczy. Badania z różnych części świata pokazują, że wkład norm do tempa wzrostu produktu krajowego brutto (PKB) wynosi około 0,9% w Niemczech, 0,8% w Australii, 0,3% w Wielkiej Brytanii i 0,2% w Kanadzie. W wartościach bezwzględnych oznacza to, że korzyści ekonomiczne wynikające z obecnego zbioru norm np. dla Niemiec wynoszą prawie 17 miliardów euro rocznie. Ponadto istnieje wiele studiów przypadku, które podkreślają korzyści ekonomiczne norm zarówno dla państw narodowych, jak i firm. W szczególności normy często (choć niekoniecznie) mają pozytywny wpływ na innowacyjność. Na przykład Blind twierdzi, że istnieje kilka sposobów, w jakie normy mogą promować innowacyjność. Dotyczy to zwłaszcza sektora ICT, gdzie standardy kompatybilności są główną podstawą innowacji. Rzeczywiście, standardy platformy GSM (Global System for Mobile Communications) były na przykład podstawą wielu oferowanych obecnie usług mobilnych. Wreszcie, normy są również przedmiotem dużego zainteresowania decydentów politycznych. Na przykład w Europie normy zharmonizowane w dużym stopniu przyczyniły się do stworzenia jednolitego rynku europejskiego – pomagają usuwać bariery techniczne w handlu oraz umożliwiają swobodniejsze przemieszczanie się ludzi, usług, towarów i kapitału. Powyższe dotyczy ogólnie standardów, a w szczególności ICT i Internetu rzeczy (IoT). Jednak standaryzacja IoT wiąże się z dodatkowymi wyzwaniami. Z definicji IoT opiera się na standardowych protokołach komunikacyjnych, aby łączyć unikalnie adresowalne obiekty. Jednak „przedmiot” to bardzo szerokie pojęcie; może to być czujnik lub komputer typu mainframe. Najważniejszą cechą większości węzłów IoT będzie „ograniczenie mocy”. Infrastruktura komunikacyjna musi uwzględniać to ograniczenie poprzez np. odpowiednie modyfikacje istniejących protokołów i/lub dedykowane nowe protokoły. W swojej obecnej formie większość standardów jest zbyt skomplikowana dla ograniczonych urządzeń w IoT. Co gorsza, wiele z tych urządzeń obsługuje zastrzeżone protokoły, tworząc w ten sposób izolowane silosy danych. Ta zwiększona różnorodność oznacza również, że interoperacyjność będzie jeszcze trudniejsza do osiągnięcia niż w innych obszarach sektora ICT. Rzeczywiście, Jari Arkko, przewodniczący grupy zadaniowej ds. inżynierii internetowej (IETF), nie może wymyślić lepszego przykładu tego, gdzie interoperacyjność jest ważna niż Internet rzeczy. Standardy interoperacyjności są warunkiem sine qua non zarówno dla IoT, jak i różnych „inteligentnych” aplikacji, które będą na nim oparte. Ponadto standaryzacja Internetu Rzeczy będzie często wymagać współpracy multidyscyplinarnej, przynajmniej między następującymi elementami:

* Inżynierowie elektrycy, którzy budują - często ograniczone - węzły zasilania i określają związane z nimi wymagania dotyczące, na przykład, systemu operacyjnego oraz oprogramowania i protokołów komunikacyjnych.

* Informatyków/Inżynierów Telekomunikacji, którzy projektują m.in. protokoły komunikacyjne.

* Inżynierowie oprogramowania, którzy opracowują np. system operacyjny i dbają o jego integrację z oprogramowaniem komunikacyjnym.

Ta potrzeba współpracy multidyscyplinarnej dotyczy jeszcze bardziej systemów cyberfizycznych (CPS), a zwłaszcza różnych obszarów zastosowań IoT. W tym rozdziale przyjrzymy się rozwojowi w ciągu ostatnich 20 lat jednostek normalizacyjnych dla IoT i inteligentnych systemów transportowych (ITS), Smart Manufacturing (SM), Smart Grid (SG) i Smart Cities (SC) oraz powiązań między nimi. Czyli to, ma na celu spojrzenie w przyszłość normalizacji w tych sektorach w oparciu o wydarzenia z przeszłości. Jest to pierwszy krok w kierunku odpowiedzi na pytanie: Jak powinno wyglądać środowisko standaryzacyjne dla (e)łączenia aplikacji w przyszłości? To z kolei powinno pomóc przemysłowi, decydentom i organizacjom ustanawiającym standardy (SSO) w optymalnym pozycjonowaniu się, gdy dedykowane działania normalizacyjne dotyczące (e)łączenia aplikacji w końcu naprawdę ruszą z miejsca.

Aktualny stan

Szereg SSO rozpoczęło działalność w zakresie standaryzacji IoT i opracowało już znaczną liczbę norm. Organizacje te w większości opracowują to, co nie tylko Sherif nazywa „standardami antycypacyjnymi”; są one zazwyczaj określane przy wprowadzaniu technologii i mają kluczowe znaczenie dla interoperacyjnych systemów komunikacyjnych. Standardy antycypacyjne kontrastują ze standardami „partycypacyjnymi” i „responsywnymi”. Te pierwsze działają równolegle z implementacjami, umożliwiając w ten sposób testowanie specyfikacji przed ich przyjęciem. Ten ostatni w zasadzie stempluje istniejące, udane specyfikacje. Według Międzynarodowej Organizacji Normalizacyjnej (ISO) pod koniec 2016 r. istniało ponad 900 norm związanych z IoT. Spośród nich około 140 pochodzi z Instytutu Inżynierów Elektryków i Elektroników (IEEE), 200 z Międzynarodowego Związku Telekomunikacyjnego (ITU) i 300 ze wspólnego komitetu ds. normalizacji ICT ISO i Międzynarodowego Komitetu Elektrotechnicznego (IEC; ISO/ IEC JTC1). Chociaż większość z nich to raczej bardziej ogólne standardy w dziedzinie systemów komunikacji bezprzewodowej, które niekoniecznie zostały opracowane specjalnie dla IoT, mogą być również przez niego wdrażane. Cyberbezpieczeństwo i prywatność to inne ważne dziedziny ustanawiania standardów, w których aktywny jest szeroki wachlarz SSO (w tym ITU, ISO, IEC, CEN, ETSI, W3C, OASIS i IETF). Ponownie, standardy te niekoniecznie są unikalne dla IoT.

Standaryzacja Internetu Rzeczy

Specyficzne standardy związane z Internetem Rzeczy dla infrastruktury komunikacyjnej zostały opracowane głównie dla dziedziny urządzeń o ograniczonej mocy. Odpowiednie działania w tym zakresie są prowadzone na przykład w oneM2M, gdzie opracowywane są standardy dla wspólnej warstwy usług M2M (Machine-to-Machine). W ramach Europejskiego Instytutu Norm Telekomunikacyjnych (ETSI) nad interfejsem między warstwą usługową a warstwą aplikacji pracuje komitet „Smart M2M Communications”. Inne komitety techniczne (TC) ETSI oraz grupy w IEEE, ITU i kilku innych SSO pracują nad aplikacjami bezprzewodowymi. W ramach IETF kilka Grup Roboczych (WG) skupia się na urządzeniach z ograniczeniami. ITU określił „Listę organizacji związanych z Internetem rzeczy (IoT) i fora.” Aktualizacja i dostosowanie tej listy, tak aby obejmowała tylko organizacje i podmioty, które opracowują natywne standardy IoT (w przeciwieństwie do tych, które opracowują bardziej ogólne standardy, które mogą być również wdrażane przez IoT) daje listę SSO pokazaną w Tabeli 7.1; bez roszczenia o kompletność. Powiązania istniejące między tymi (i innymi) SSO zostaną omówione później. Liczba podmiotów, które poświęcają się standaryzacji danej technologii, może być postrzegana jako wskaźnik rosnącego postrzeganego (rynkowego) znaczenia tej technologii.

W przypadku Internetu Rzeczy liczba ta gwałtownie wzrosła w ciągu ostatnich 8 lat. Warstwa IoT zapewnia warstwie aplikacji funkcje specyficzne dla IoT (np. zarządzanie danymi, bezpieczeństwo, prywatność). Skupiamy się tutaj na standaryzacji w dużej mierze na poziomie architektonicznym. Istniejące standardy komunikacji mogą zostać ponownie wykorzystane do wdrożenia w warstwie sieciowej. Wysiłki związane z IoT w tej warstwie dotyczą przede wszystkim problemów związanych z ograniczeniem mocy wielu urządzeń IoT (np. czujników). Dedykowane wymagania pojawią się w niektórych obszarach zastosowań i będą wymagały nowych lub dostosowanych protokołów komunikacyjnych, pomyśl na przykład o autonomicznej jeździe).

Aplikacje oparte na IoT

Połączenie wcześniej odrębnych technologii jest trendem trwającym od kilku lat. Prawie ukończona integracja technologii (tele)komunikacyjnych i informatycznych doprowadziła do powstania technologii informacyjno-komunikacyjnych. Nowsze przykłady (e)łączenie technologii obejmują m.in. inteligentne systemy transportowe (ITS; obejmujące telematycję transportu, inżynierię ruchu, energetycję, motoryzację, ICT), inteligentną produkcję (SM; inżynieria produkcji, robotyka, automatyka, ICT), smart grid (SG; energetyka, ICT). Inteligentne miasta to w zasadzie nadzbiór pozostałych trzech, plus kilka innych. Jedną wspólną cechą tych technologii jest wiodąca rola ICT. W rzeczywistości integracja ICT z „tradycyjnymi” technologiami (transport, produkcja, dystrybucja energii) ma decydujące znaczenie; umożliwia bit „inteligentny”. I chociaż kompatybilność i interoperacyjność są ważnymi aspektami w wielu technologiach, są one warunkiem sine qua non IoT. To z kolei oznacza, że standardy (kompatybilność/interoperacyjność) odgrywają kluczową rolę. Bez nich inteligentne technologie po prostu się nie zmaterializują. Można zidentyfikować znaczną liczbę (e)łączących się „inteligentnych” obszarów zastosowań. Uzupełniają to wyniki ankiety z literatury akademickiej. Wszystkie one identyfikują inteligentną produkcję, e-zdrowie, ITS i inteligentną infrastrukturę (energetyczną), z innymi obszarami zastosowań zidentyfikowanymi na podstawie podzbioru uwzględnionych raportów i dokumentów. Każdy z tych obszarów zastosowań jest z natury multidyscyplinarny. Jedną z ich wspólnych cech jest poleganie na Inżynierii Telekomunikacyjnej i Informatyce.

Bezpieczeństwo i prywatność

Bezpieczeństwo obejmuje zestaw usług, w tym uwierzytelnianie, autoryzację, integralność i poufność. Ponadto należy zagwarantować prywatność, a najlepiej byłoby zapewnić mechanizmy wspierające rozwój pewnego poziomu zaufania między stronami. W rzeczywistości powszechnie postrzegany brak bezpieczeństwa i prywatności może być potencjalną przeszkodą dla IoT i jego aplikacji. Jest bardzo prawdopodobne, że ludzie będą się im opierać, jeśli nie ma pewności, że nie spowodują poważnych zagrożeń dla prywatności. Podobnie, praktycznie wszystkie obszary zastosowań mają silne wymagania bezpieczeństwa; w związku z tym obawy przemysłu również bardzo skupiają się na tym aspekcie. Te problemy również muszą zostać rozwiązane poprzez standaryzację. Ponieważ takie obawy nie dotyczą wyłącznie Internetu Rzeczy, istnieje już duża liczba protokołów zapewniających bezpieczeństwo i prywatność. W związku z tym można pokusić się o stwierdzenie, że nie ma realnej potrzeby projektowania nowych, dedykowanych protokołów bezpieczeństwa dla IoT. Jednak głównym problemem, który stoi na drodze do jednokrotnego przyjęcia istniejących protokołów, jest – ponownie – ograniczenie mocy wbudowanych „inteligentnych” urządzeń (takich jak czujniki i siłowniki), które będą reprezentować zdecydowaną większość węzłów IoT. W konsekwencji konieczne będzie podjęcie dodatkowych wysiłków w celu dostosowania istniejących protokołów do ich ograniczonych możliwości urządzenia. Może to sprowadzać się do opracowania dedykowanych, specyficznych dla IoT mechanizmów bezpieczeństwa. Pomimo ich kluczowego znaczenia, standaryzacja bezpieczeństwa i prywatności nie będzie brana pod uwagę w tym rozdziale. Po pierwsze, ich włączenie wykraczałoby

poza jego zakres; szczegółowe omówienie powiązanych aspektów technicznych i bieżących działań normalizacyjnych znajduje się w. Co więcej, społeczno-ekonomiczne i polityczne konsekwencje tego tematu są w rzeczywistości zbyt ważne, aby można je było ukryć w ogólnej części dotyczącej normalizacji IoT.

Środowisko normalizacyjne

Większość sektorów przemysłu ma dość proste środowisko normalizacyjne. Szereg krajowych organizacji normalizacyjnych (NSO) uczestniczy w pracach ISO i IEC na poziomie międzynarodowym. Dodatkowy poziom regionalny został utworzony w Europie za pośrednictwem Europejskich Organizacji Normalizacyjnych (ESO). Inaczej sytuacja wygląda w sektorze ICT (w szczególności w telekomunikacji). Sektor ten charakteryzuje się wieloma organami krajowymi/regionalnymi, a w szczególności ogromną liczbą (ponad 200) prywatnych konsorcjów ustanawiających standardy. Rozmnażanie się tych konsorcjów rozpoczęło się pod koniec lat 80. XX wieku i było spowodowane przede wszystkim szybkim rozwojem technologii ICT oraz szeroko postrzeganym spowolnieniem i brakiem reakcji na potrzeby użytkowników po stronie SDO. Liczba konsorcjów i złożone powiązania między nimi a SDO tworzą niemal nieprzenikloną sieć SSO. Ogólnie rzecz biorąc, takie powiązanie reprezentuje pewien poziom formalnej współpracy. Taka współpraca może przybrać formę wymiany informacji o planowanych nowych elementach pracy, wspólnego opracowywania wspólnych standardów lub czegokolwiek pomiędzy. Wobec braku centralnego podmiotu koordynującego powiązania te stanowią obecnie najważniejszy (rozproszony) mechanizm koordynacji w ustanawianiu norm. Istnieje więcej powiązań między konsorcjami a „formalnymi” SDO; na przykład konsorcja mogą przedłożyć swoje specyfikacje dla SDO dla (międzynarodowej) normalizacji („normalizacja reaktywna). SSO aktywni w normalizacji telekomunikacji. Ich liczba jest porównywalnie ograniczona, a powiązania między nimi są stosunkowo silne. Na przykład 3GPP i oneM2M to wspólne inicjatywy kilku regionalnych SSO. W szczególności oneM2M opracowuje standardy komunikacji maszyna-maszyna (M2M) oraz IoT. Global Standards Collaboration (GSC) to mniej formalna forma współpracy między regionalnymi SSO a ITU. Krajobraz normalizacji IT to najgęściej zaludniona i najbardziej złożona część środowiska normalizacji ICT. Tutaj również istnieją porównywalnie silne powiązania między poszczególnymi graczami. Ważną kwestią pozostaje koordynacja różnych działań normalizacyjnych. Brak koordynacji, ostatecznie skutkujący opracowaniem funkcjonalnie równoważnych (a tym samym konkurencyjnych) standardów, zmniejszy przejrzystość rynku, zmniejszy interoperacyjność i łatwość użytkowania, rozdrobni rynek i zwiększy koszty transakcyjne. Rzeczywiście, z biegiem czasu opracowano różne mechanizmy koordynacji, od wysoce sformalizowanych dokumentów regulacyjnych wysokiego szczebla po bardzo nieformalną koordynację przez osoby, które przyczyniają się do pracy wielu SSO. Rysunek 7.3 przedstawia niektóre z istniejących formalnych mechanizmów koordynacji między niektórymi głównymi graczami globalnymi. W każdym razie wszelkie formy koordynacji będą miały szczególne znaczenie w złożonym świecie standaryzacji IoT.

Standaryzacja w wybranych obszarach zastosowań

W tej sekcji przyjrzymy się środowisku czterech typowych obszarów zastosowań IoT. Należą do nich inteligentne systemy transportowe (ITS), inteligentna produkcja (SM), inteligentna sieć (SG) i inteligentne miasta (SC). Obszary te reprezentują jedną porównywalnie dojrzałą dziedzinę (ITS), dwie nowsze zmiany, w tym trend w prywatnym sektorze produkcyjnym (SM) i typowo prywatne narzędzie, które jest jednak kluczową częścią infrastruktury publicznej (SC) i wreszcie nadrzędną a może nawet nieco futurystyczną koncepcją inteligentnych miast (SC).

Inteligentne systemy transportowe (sektor motoryzacyjny)

ITS wynikają z integracji ICT z pojazdami i infrastrukturą transportową w celu poprawy wyników ekonomicznych, bezpieczeństwa, mobilności i zrównoważenia środowiskowego. Krajobraz standaryzacji ITS obejmuje trzy różne typy podmiotów. Po pierwsze, są te z „tradycyjnego” sektora motoryzacyjnego. Ich główną wspólną cechą jest porównywalnie podeszły wiek (oczywiście według standardów ICT). Można je dalej podzielić na wyspecjalizowane podmioty, które zajmują się wyłącznie kwestiami motoryzacyjnymi/transportowymi, oraz na bardziej ogólne SSO, które od dłuższego czasu zajmują się aspektami związanymi z transportem. Zazwyczaj tematy związane z ITS dodawały do swojego portfolio dopiero niedawno, albo poprzez dedykowane grupy, albo poprzez rozszerzenie zasięgu istniejących grup (np. IEC). Prywatne konsorcja, które koncentrują się wyłącznie na tematach ITS, tworzą trzecią grupę. Większość członków tej grupy powstała dopiero w tym tysiącleciu, na przykład CAR2CAR, Car Connectivity Consortium (CCC) i Open Automotive Alliance (OAA). ITS stały się popularne dopiero na przełomie lat 80. i 90. XX wieku. Obecnie środowisko stało się znacznie bardziej złożone, a wielu dodatkowych graczy tworzy znacznie bardziej rozbudowaną sieć z różnymi rodzajami powiązań między nimi. Z jednej strony jest to zgodne z ogólną tendencją norm zmierzającą do ściślejszej współpracy. Z drugiej strony rysunek pokazuje również, że powiązania między prywatnymi konsorcjami są nadal bardzo ograniczone; dla wielu nie udało się zidentyfikować powiązań z innymi SSO aktywnymi w tym samym sektorze⁸. Taką sytuację można również zaobserwować w innych częściach uniwersum normalizacji. Jak wspomniano powyżej, idea ITS pojawiła się pod koniec lat 80-tych. Na początku lat 90. pierwsze podmioty związane z normalizacją, które powstały (w 1991 r.), nie były SSO, ale raczej podmiotami związanymi z polityką. Następnie ustanowiono stowarzyszone komitety techniczne (TC) głównych międzynarodowych i europejskich SDO. Druga „fala” organów normalizacyjnych rozpoczęła się prawie 10 lat później, ponownie kierowana przez organizację niebędącą SSO (EasyWay, program prowadzony przez europejskich zarządców dróg i władze oraz Komisję Europejską). W latach 2002-2010 powstały duże wyspecjalizowane konsorcja (Car2Car, Autosar) oraz Grupy Robocze w sektorze telekomunikacyjnym skupiające się na wsparciu komunikacyjnym usług i aplikacji ITS. Rozwój ten był spowodowany nie tylko rozpowszechnieniem się i coraz bardziej zaawansowanymi funkcjami oferowanymi przez systemy komunikacji mobilnej. Podsumowując, wydaje się, że można bezpiecznie powiedzieć, że sektor ITS jest już dość dojrzały. Chociaż z pewnością można by poprawić koordynację między SSO, istnieje sporo dość dobrze ugruntowanych powiązań i mechanizmów koordynacji.

Inteligentna produkcja

Idea „inteligentnej produkcji” pojawiła się pod koniec lat 80., stała się bardziej popularna jako temat badawczy pod koniec lat 90. i wystartowała wraz z nadejściem niemieckiej inicjatywy „Industrie 4.0” w 2013 r. (GTAI, 2014). Inteligentna produkcja wykorzystuje technologie informacyjno-komunikacyjne do optymalizacji wykorzystania siły roboczej, materiałów i energii w celu wytwarzania dostosowanych, wysokiej jakości produktów, które są dostarczane na czas oraz aby móc szybko reagować na zmiany w wymaganiach rynku i łańcuchach dostaw. Dla 1996 roku środowisko wyznaczające standardy dla inteligentnej produkcji nie różni się zbytnio od tego w sektorze ITS – stosunkowo niewielkiej liczbie podmiotów o bardzo ograniczonych powiązaniach między nimi. Również tutaj sytuacja dzisiaj bardzo różni się od tej, która miała miejsce wtedy. Liczba ważnych graczy prawie się potroiła i ustanowiono szereg różnych rodzajów powiązań (zob. Rysunek 7.7). Prawie wszystkie prywatne konsorcja i sojusze (z wyjątkiem eCl@ss) skupiają się na aspektach komunikacyjnych. Wyjaśnieniem może być to, że inteligentna produkcja po prostu nie nastąpi bez odpowiedniej podstawowej infrastruktury komunikacyjnej, która musi spełniać specjalne wymagania dotyczące na przykład opóźnienia, odporności, niezawodności i przewidywalności (zob. na przykład Fettweis i in. (2014)). W związku z tym standardy dla tej infrastruktury będą znacznie szersze stosowane niż te dla aplikacji znajdujących się na jej szczycie. Przynajmniej we wczesnych dniach rozwoju, stanowią więc znacznie bardziej

lukratywną dziedzinę niż standardy aplikacji. Jednak SSO z sektora telekomunikacyjnego (ITU, ETSI, oneM2M) wydają się być odizolowane od innych podmiotów. To trochę niespodzianka, ponieważ dziś łańcuchy dostaw stają się globalne i tego samego można oczekiwać w przypadku przyszłej produkcji (IEC, 2015). Na tym tle potrzeba globalnych usług komunikacyjnych wydaje się oczywista. Patrząc ponownie na ós czasu, niektóre starsze jednostki (ISO/TC184 i IEC TC65 oraz ich europejski lustrzany podmiot, CENELEC TC65X, pracujące nad automatyzacją procesów) są znacznie starsze (patrz Rysunek 7.8). W połowie lat 90. pojawiło się wiele podmiotów, z których większość określiła i opracowała produkty do komunikacji halowej. Wiele ich specyfikacji znalazło się w procesie IEC i ostatecznie zostało formalnie znormalizowanych. W niedalekiej przeszłości wiele SDO założyło TC lub inne grupy, które w szczególności skupiają się na inteligentnej produkcji. Aglomeracja nowo powstałych podmiotów w latach 2013-2015 jest dość znacząca i podkreśla rosnące w ostatnim czasie znaczenie, jakie przywiązują się do inteligentnej produkcji.

Inteligentna siatka

Pierwsze inicjatywy w kierunku bardziej inteligentnego systemu zasilania rozpoczęły się pod koniec lat 80.. Dziś smart grid to nowoczesna infrastruktura sieci elektroenergetycznej z płynną integracją odnawialnych i alternatywnych źródeł energii, poprzez zautomatyzowane sterowanie i nowoczesne ICT. W 1996 r. arena normalizacyjna związana z inteligentną siecią była jeszcze mniej zaludniona niż w dwóch powyższych przypadkach. Nic dziwnego, że w tamtych czasach istniały głównie te SSO działające w dziedzinie elektrotechniki, zajmujące się głównie dystrybucją energii. Powiązania między tymi SSO nie istniały. Ponownie, podobnie jak rozwój w pozostałych dwóch omawianych już sektorach, sieć SSO pracujących nad inteligentnymi sieciami stała się dziś znacznie bardziej złożona, angażując znacznie więcej graczy o znacznie bardziej rozbudowane sieci współpracy między nimi. W porównaniu z pozostałymi dwoma sektorami liczba prywatnych konsorcjów przyczyniających się do standaryzacji inteligentnych sieci ogranicza się do Panelu Interoperacyjności Inteligentnych Sieci (SGIP) i Konsorcjum Internetu Przemysłowego (IIC), które również zajmują się aspektami specyficznymi dla sieci, nie tylko na problemy komunikacyjne (jak w inteligentnej produkcji). W tym przypadku ustalanie standardów jest głównie wykonywane przez SDO (kierowane przez IEC), które od dziesięcioleci działają w „tradycyjnych” dziedzinach zaopatrzenia w energię, akcesoriów elektrycznych, zarządzania systemami zasilania lub systemów komunikacyjnych (patrz również Rysunek 7.10). W pewnym sensie linia czasowa powstania podmiotów pracujących nad standardami dla inteligentnej sieci jeszcze bardziej wydłuża rozwój, jaki można było zaobserwować w przypadku inteligentnej produkcji (wykres 7.8) oraz, w mniejszym stopniu, ITS (wykres 7.6). W tym drugim przypadku zakładanie nowych podmiotów było bardziej równomiernie rozłożone w czasie. W przypadku tych pierwszych można zaobserwować pewną kumulację w ciągu ostatnich 7 lat. W przypadku sieci inteligentnych ta kumulacja jest znacznie wyraźniejsza. Tutaj obserwujemy powstawanie wielu „wyspecjalizowanych” podmiotów począwszy od 2008 roku. Wcześniej omawiano tylko bardziej „ogólne” aspekty (zasilanie, komunikacja). Oznacza to, że inteligentną sieć można uznać za nowy obszar zastosowań, z pewnością pod względem powiązanej standaryzacji.

Inteligentne miasta

„Inteligentne miasta” to prawdopodobnie najszerszy obszar zastosowań. Inteligentne miasto będzie m.in. obejmować inteligentne budynki, wykorzystywać inteligentną sieć, zapewniać inteligentne obiekty transportowe i usługi e-zdrowia, a także obejmować inteligentne zakłady produkcyjne. Będzie to zatem konstrukcja szczególnie złożona. Niemniej jednak badanie przeprowadzone przez TU Vienna identyfikuje 90 „inteligentnych” miast z 300 000–1 000 000 mieszkańców i 77 ze 100 000–300 000 mieszkańców. Według Navigant istnieje wiele projektów pilotażowych i inwestycji na małą skalę, ale nie ma przykładów inteligentnego miasta na dużą skalę. Prawdziwie „inteligentnym” miastom wciąż

bliżej do science fiction niż do prawdziwego życia. Jak widać, (praktycznie) wszystkie inne aplikacje przyczyniają się do realizacji celów inteligentnych miast. W pewnym sensie inteligentne miasto reprezentuje nadzbiór „inteligentnych” aplikacji. Ponadto standardy dotyczące „inteligentnych polityk i celów” zapewniają wytyczne dla kierownictwa miasta w zakresie opracowania ogólnej strategii inteligentnego miasta, identyfikacji priorytetów, opracowania praktycznej mapy drogowej wdrażania oraz skutecznego podejścia do monitorowania i ocena postępów (BSI, 2015). Do tej pory ITU przejęło wiodącą rolę w standaryzacji inteligentnych miast (podobnie jak IEC w przypadku inteligentnej sieci). „Inteligentne miasta” to dość nowy temat dla standaryzacji. Tylko bardzo ograniczona liczba graczy jest aktywna na tym polu, a powiązania między nimi nie są ani szczególnie bliskie, ani liczne. Ponadto tylko mniejszość podmiotów w ramach poszczególnych OSM koncentruje się na faktycznych pracach normalizacji technicznej. Większość z nich jest obciążona zadaniami wysokiego poziomu, takimi jak identyfikacja wymagań, a także badania, tworzenie map drogowych i/lub działania koordynacyjne. Ta ostatnia dotyczy jednak wyłącznie koordynacji wewnętrznej w ramach jednego OSM. W połączeniu z dość młodym wiekiem działań wyjaśnia to ograniczone powiązania między podmiotami. Całkowity brak prywatnych konsorcjów standardów. Można to wytłumaczyć faktem, że standaryzacja inteligentnych miast koncentruje się bardziej na poziomie strategicznym, niż na technicznym. Wydaje się słuszne założenie, że na takich działaniach zarobi się niewiele pieniędzy, więc konsorcja trzymałyby się z dala od nich. „Inteligentne miasta” to rzeczywiście bardzo nowa dziedzina. Pierwszy podmiot, ITU-T's Joint Coordination Activity on Internet of Things and Smart Cities and Communities (JCA-IoT i SC&C; obecnie rozwiązane), został utworzony w 2011 roku. Sytuacja jest podobna do tej obserwowanej w przypadku inteligentnej produkcji i inteligentnej sieci w tym również tutaj widzimy falę nowopowstałych jednostek normalizacyjnych w ciągu ostatnich 5 lat. Jednak główną różnicą w stosunku do innych sektorów jest to, że inteligentne miasta nie mają żadnych poprzedzających technologii – wszystkie działania normalizacyjne rozpoczęły się od zera w 2010 roku.

Dyskusja i niektóre spekulacje

Do tej pory rozdział dotyczył standaryzacji IoT oraz czterech (e) skalania obszarów aplikacji. Ich główną wspólną cechą jest konwergencja różnych technologii. Zmiany na przestrzeni czasu w odpowiednich środowiskach normalizacyjnych wykazują podobieństwa, ale także różnice. Jeśli chodzi o to pierwsze, wszystkie środowiska wyłoniły się z porównywalnie skromnych początków, począwszy od połowy lat 90., do dość złożonych sieci dzisiejszych SSO. Główną przyczyną tej zwiększonej złożoności jest pojawienie się nowych, a czasem wysoce wyspecjalizowanych SSO. Podobnie we wszystkich przypadkach formalne SDO początkowo wiodą prym; konsorcja i inne „nietradycyjne” podmioty dołączyły na późniejszym etapie (jeśli w ogóle, to do tej pory). Można argumentować, że ich pojawienie się – i rosnące znaczenie – w końcu doprowadziło do powstania wielu nowych podmiotów przez SDO. Ponadto w ciągu ostatnich 5–7 (SM, SG i SC) lub 10 lat (ITS) można zaobserwować znaczną aglomerację SSO. W przypadku SM i SG można to zinterpretować jako próbę poprawy konkurencyjności krajów uprzemysłowionych, o wysokich płacach w stosunku do gospodarek wschodzących, takich jak Chiny (inteligentna produkcja) oraz zmniejszenia ich zależności od kopalnych źródeł energii (inteligentna sieć i do stopień, ITS). Również tutaj inteligentne miasta stanowią nadzbiór tych i innych „inteligentnych” aplikacji. Porównywalnie bardziej „homogeniczny” rozwój obszaru ITS można również przypisać temu, że podmioty lobbujące i nadrzędny program unijny poprzedziły (i być może przyczyniły się do uruchomienia) pierwszej „fali” SSO na początku lat 90. XX wieku. Wydaje się, że obszar ten charakteryzuje się również najbardziej zaawansowaną integracją sektora telekomunikacyjnego, co również można uznać za oznakę większej dojrzałości. W przeciwieństwie do tego integracja ta w dużej mierze nie istnieje w SM. Warto również zwrócić uwagę na dość dominującą rolę SDO w standaryzacji inteligentnych sieci. Fakt, że jest to obszar ściśle regulowany, może być przynajmniej częścią wyjaśnienia. Inteligentne miasta to bardzo nowy rozwój bez żadnych poprzedzających technologii.

Znajduje to odzwierciedlenie zarówno w osi czasu (która rozpoczyna się w 2011 r.), jak i w ich słabo zaludnionej i słabo połączonej sieci SSO. To jednak nic dziwnego. W końcu inteligentne miasta polegają na usługach dostarczanych przez inne „inteligentne” aplikacje; termin „system systemów” jest często używany do podkreślenia tej cechy (patrz na przykład IEC (2014)). Porównując te linie czasu z linią dla systemów komunikacji bezprzewodowej (najważniejszej części ich podstawowej infrastruktury), widzimy podobny obraz, ale przesunięty w lewo na linii czasu. Największa fala fundacji SSO miała miejsce w połowie/pod koniec lat 90., kiedy powstało kilka dużych podmiotów. Wyprzedził te w SM i SG o ponad 10 lat. Nie jest to aż tak wielką niespodzianką, ponieważ „inteligentne” aplikacje zależą od ugruntowanej infrastruktury teleinformatycznej. Obecnie wszystkie cztery omawiane obszary zastosowań wymagają infrastruktury komunikacji bezprzewodowej, ponieważ oferuje ona znacznie większą elastyczność niż przewodowa; oczywiście Internet nadal stanowi szkielet komunikacji. Niemniej jednak, początkowo standaryzacja w co najmniej jednym „inteligentnym” obszarze zastosowań, ITS, mogłaby najwyraźniej przebiegać bez bazowych protokołów i usług komunikacji bezprzewodowej opartych na standardach. Rozpoczęcie działań standaryzacyjnych dla komunikacji bezprzewodowej wyprzedziło ITS zaledwie o kilka lat. Oś czasu ustanowienia jednostek normalizacyjnych specyficznych dla IoT pokazuje replikację tego rozwoju. Ustanowienie zdecydowanej większości dedykowanych podmiotów ustalających standardy IoT (nowych SSO lub wyspecjalizowanych podjednostek już istniejących) miało miejsce w ciągu ostatnich 9 lat. Wystartował w 2009 roku, a szczyt przypadał na lata 2013–2014. W 2015 r. JTC1 ustanowiło WG 10 „Internet przedmiotów”. Ta grupa robocza wraz z WG 7 „Sieci czujnikowe” została przeniesiona do nowo utworzonego JTC1/SC 41 „Internet przedmiotów i technologie pokrewne”. Ta konsolidacja, a co więcej, „podniesienie” statusu podkomitetu dodatkowo podkreśla znaczenie, jakie ISO przypisuje tej dziedzinie pracy. Oznacza to, że działania normalizacyjne dla dedykowanej infrastruktury IoT rozpoczęły się mniej więcej w tym samym czasie, co standaryzacja inteligentnych miast i druga „fala” standaryzacji inteligentnej sieci i inteligentnej produkcji. Tak więc tutaj ponownie rozpoczęto standaryzację specyficzną dla aplikacji bez dedykowanej infrastruktury. Tak duża, wzajemnie niezależna standaryzacja IoT i jego zastosowań jest poniekąd niebezpieczną zmianą. Po pierwsze, dialog między światem ICT (rozwój infrastruktury opartej na IoT) a światem aplikacji (który będzie wykorzystywał tę infrastrukturę) jest kluczowy. W końcu te ostatnie muszą zapewnić wymagania dla tych pierwszych, a eksperci od strony infrastruktury muszą jasno określić wszelkie (techniczne) ograniczenia, które mogą mieć zastosowanie i potencjalnie wpływać na aplikacje. Ponadto, a także ze względu na niewystarczający poziom koordynacji pomiędzy poszczególnymi działaniami normalizacyjnymi istnieje realne ryzyko tworzenia nowych silosów. Koordynacja ma miejsce głównie w ramach poszczególnych SSO, co może prowadzić do powstania silosów specyficznych dla SSO, w których tylko normy z tego SSO mogą bezproblemowo współdziałać. Byłoby to wtedy dodatkiem do własnych silosów. Co więcej, biorąc pod uwagę samą liczbę podmiotów ustanawiających standardy, które są aktywne w domenie IoT oraz w różnych obszarach zastosowań, można pokusić się o zastanowienie, czy w ogóle można osiągnąć globalną interoperacyjność. W końcu i tak już dość znaczna liczba standardów związanych z Internetem Rzeczy może przyczynić się do problemów z interoperacyjnością w terenie (silosy). Następnym krokiem powinno być utworzenie jednostki koordynującej między operatorami SSO. Ponadto ostatecznie wymagane będą podmioty, które faktycznie próbują rozwiązać konkretne problemy związane ze stosowaniem z perspektywy multidyscyplinarnej. Zobaczymy, czy lepsza koordynacja pomogła opanować rozrost norm i specyfikacji.

Wniosek

Omówiono niektóre aspekty standaryzacji IoT i cztery jego główne obszary zastosowań. Okazało się, że w ciągu ostatnich 20 lat środowisko normalizacyjne znacznie się zmieniło. W szczególności liczba SSO

pracujących nad normami dotyczącymi Internetu Rzeczy i jego zastosowań gwałtownie wzrosła w tym okresie, podobnie jak istniejące między nimi powiązania. Bliższe przyjrzenie się osi czasu tych zmian pokazuje, że tworzenie jednostek normalizacyjnych istotnych dla IoT, ITS, inteligentnej produkcji, inteligentnej sieci i inteligentnych miast wykazuje bardzo podobny schemat. Pierwsza „fala” nowych podmiotów normalizacyjnych miała miejsce na początku - w połowie lat 90., a druga około 2010 r. na obszarach SM, SG i SC, kiedy nowe podmioty powstawały w praktycznie wybuchowym tempie. W przypadku ITS stało się to nieco wcześniej i nieco mniej wyraźne. Ten sam obraz wyłania się w przypadku systemów komunikacji mobilnej, gdzie szczyty miały miejsce odpowiednio pod koniec lat 80. i w połowie lat 90. XX wieku. W przypadku IoT linia czasowa wygląda nieco inaczej, z jedną dość masywną falą między 2008 a 2014 rokiem. We wszystkich przypadkach możemy zaobserwować spory spadek tworzenia nowych podmiotów po 2014 roku. Biorąc powyższe pod uwagę, spojrzenie w kryształową kulę sugeruje, że liczba wyspecjalizowanych jednostek normalizacyjnych (SSO, TC itp.) pracujących nad poszczególnymi aspektami (e)łączenia aplikacji i IoT będzie jeszcze przez jakiś czas rosła, choć w znacznie wolniejszym tempie (dość stromy spadek liczby nowopowstałych jednostek normalizacyjnych można zaobserwować w ciągu ostatnich 2 lat). Prawdopodobnie osiągnięte nasycenie – na dość wysokim poziomie – w niedalekiej przyszłości. Obecnie problemem jest to, że każde SSO koordynuje się wewnątrz i może otrzymywać aktualizacje od innych podmiotów poprzez mniej lub bardziej luźne kontakty. W szczególności nie istnieje koordynacja krzyżowa SSO. To po raz kolejny wzmacnia pilną potrzebę pewnego rodzaju skutecznej i wydajnej koordynacji między SSO, wykraczającej poza to, co obecnie istnieje. Dotyczy to również koordynacji między infrastrukturą opartą na IoT a wdrażającymi ją aplikacjami. Jednak okaże się, czy taka nadrzędna koordynacja zostanie faktycznie ustanowiona. Jednak jest to bardzo mało prawdopodobne w najbliższym czasie.