Niezawodna, bezpieczna sieć dla przemysłu oraz IoT

Komunikacja sieciowa, zdalne kontrolowanie urządzeń przemysłowych, urządzenia M2M oraz gwałtownie rosnąca liczba aplikacji IoT mają to samo, podstawowe wymaganie – muszą mieć możliwość pewnego i bezpiecznego przyłączania wielu punktów końcowych oraz umożliwiać scentralizowaną kontrolę poprzez sieć. Protokół internetowy IP stał się standardem również w sieciach przemysłowych, co postawiło nowe wymagania przed urządzeniami komunikującymi się w sieci. Podobne zagadnienia dotyczą również technologii IoT, mało tego – będą nas dotykały „bliżej" i bardziej osobiście. W artykule omówiono procesor sieciowy z LS1021A z rodziny QorIQ oraz jego wyposażenie zabezpieczające komunikację w sieciach IoT, M2M i innych.

W zakładach produkcyjnych rośnie liczba maszyn, które komunikują się za pomocą Ethernetu. Wcześniej ten standard sieciowy rozpowszechnił się w aplikacjach biurowych i ma potężne wsparcie w postaci aplikacji dla komputerów osobistych. Dzięki połączeniu sieci „biurowej" i przemysłowej kadra zarządzająca przedsiębiorstwem ma możliwość natychmiastowego podglądu danych dotyczących produkcji oraz ich wizualizacji za pomocą typowych aplikacji. Pozwala to szybciej reagować na zmiany, pozwala na zdalne zarządzanie procesami przemysłowymi i w efekcie wzrasta produktywność. Co naturalne, do takich danych nie każdy może mieć dostęp. Dlatego wspomniana funkcjonalność musi być powiązana z możliwością zapewnienia bezpieczeństwa danych transmitowanych w obrębie sieci wewnątrz przedsiębiorstwa i inne łącza.

Firma Freescale jest jednym z liderów w dostarczaniu procesorów służących do komunikacji sieciowej. Są one używane w sieciach przemysłowych oraz w lotnictwie od ponad 20 lat. Jeśli tylko projekt wymaga infrastruktury sieciowej, urządzeń służących do kontrolowania procesów przemysłowych (na przykład, bramek sieciowych czy sterowników PLC) lub wyposażenia hali produkcyjnej, to muszą być spełnione podstawowe wymagania: wyjątkowa pewność komunikacji, bezpieczeństwo transmitowanych danych, sprawne i wydajne przetwarzanie pakietów oraz wsparcie dla rozszerzonych możliwości łączeniowych.

Początkowo miejsce lidera w obszarze rozwiązań sieciowych zapewniły firmie Freescale procesory komunikacyjne bazujące na technologii Power Architecture. Bazując na wiedzy, doświadczeniach oraz innowacjach wprowadzonych sukcesywnie przez ostatnie 20 lat, firma Freescale opracowała pierwszy procesor komunikacyjny z rodziny QorIQ bazujący na ARM ISA.

Dodatkowe informacje:
Opracowano na podstawie materiałów firmy Freescale. Więcej informacji jest dostępne na stronie *www.freescale.com/QorIQ*.

Innowacyjny procesor QorIQ LS1021A jest wyposażony w dwa rdzenie ARM Cortex-A7 z dwupoziomową pamięcią cache (L1 i L2), zabezpieczoną mechanizmem korekcji błędów ECC. Pozwala to na niezawodną pracę rdzenia przy taktowaniu przebiegiem o częstotliwości 1 GHz. Dwa rdzenie ARM są zaimplementowane w strukturze o najwyższej skali integracji, dzięki czemu pobór mocy nie przekracza 3 W. Procesor LS1021A jest wyposażony w wydajne interfejsy sieciowe, włączając w to Gigabit Ethernet, PCI Express 2.0, SATA 3.0 oraz USB 3.0. Oprócz nich ma wbudowanych szereg popularnych interfejsów szeregowych, włączając w to: TDM, HDLC, UART, I²C, SPI, CAN oraz dekoder PWM/Quadric. Oprócz tego procesor ma wsparcie dla obsługi pamięci SDHC, interfejs I²S oraz zintegrowany kontroler LCD. Schemat blokowy procesora LS1021A pokazano na **rysunku 1**.

Akceleratory komunikacyjne

W automatyzacji procesów oraz w aplikacjach służących do kontroli produkcji, sieć musi być zawsze dostępna, bezawaryjna, niezawodna

i bezpieczna. Procesory sieciowe powinny być wyposażone w inteligentne opcje, które pozwalają przedsiębiorstwu na wykorzystanie zalet przepływu informacji dostępnych w obrębie ich sieci korporacyjnej.

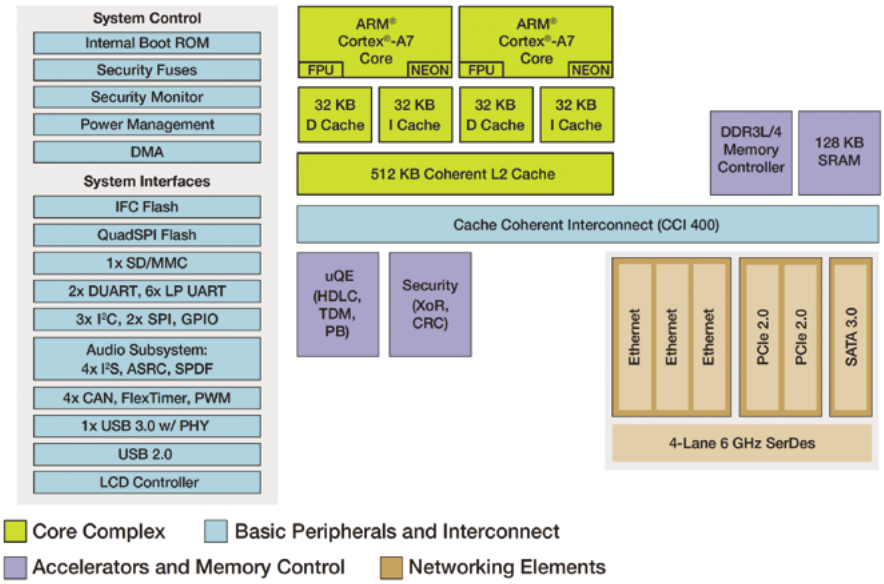
Aby zapewnić najwyższą niezawodność oraz bezpieczeństwo procesory sieciowe Freescale integrują wiodące technologie służące do przyśpieszenia pracy sieci oraz jej zabezpieczenia. Wśród niech można wymienić programowaną jednostkę QUICC, która obsługuje protokoły FieldBus oraz RS485, takie jak PROFIBUS (w trybach *master* i *slave*). Oprócz niej zastosowano kontroler Ethernet o potrójnej prędkości (VeTSEC), zapewniający sprzętowe wsparcie dla znaczników czasu (*timestamp*) zgodnie z normą IEEE 1588, zarówno dla danych wysyłanych, jak i odbieranych. Ten kontroler umożliwia również programowe zarządzanie kolejkowaniem. Dzięki parsowaniu aż do warstwy 4 modelu ISO danych odbieranych oraz sprzętowemu ustalaniu priorytetów dla danych wysyłanych, algorytm kolejkowania jest łatwy do wykonania, a przy tym efektywny.

Te wypróbowane w wielu zastosowaniach kontrolery Ethernet są dostępne we wszystkich procesorach Freescale przeznaczonych do aplikacji przemysłowych oraz mają wsparcie w postaci dużej liczby sprawdzonych, „dojrzałych" driverów programowych, włączając w to stosy dla Ethernetu przemysłowego (EtherCAT Master), PROFINET (RT), EtherNet/IP oraz PRP.

Niezawodność w sieciach korporacyjnych

Procesor LS1021A z rodziny QorIQ został zbudowany w taki sposób, aby spełniać restrykcyjne wymagania aplikacji sieciowych. Zostało to osiągnięte dzięki zaimplementowaniu timerów watchdog oraz mechanizmu detekcji i korekcji błędów (ECC) we wszystkich pamięciach, włączając w to cache (L1 i L2), SRAM oraz zewnętrzną pamięć DDR. Uzupełnieniem niezawodności uzyskiwanej za pomocą ECC jest wsparcie dla wielu mechanizmów zabezpieczających, włączając w to autentykację i szyfrowanie, preloader zapewniający bezpieczny start systemu (*secure boot*), mechanizm *ARM TustZone* oraz ochronę własności intelektualnej (również w postaci obrazów pamięci). Wszystkie te opcje umożliwiają uzyskanie najwyższego poziomu bezpieczeństwa urządzenia pracującego pod kontrolą procesora QorIQ.

Wymienione opcje są podstawowym wymaganiem dla aplikacji IoT, w których wiele urządzeń sieciowych oraz sensorów przesyła specyficzne dane użytkownika pomiędzy węzłami lub do punktu centralnego. W związku z tym, że te dane mogą być odniesione lub powiązane bezpośrednio z konkretną osobą, to jest oczywiste, że muszą być chronione. W niedalekiej przyszłości z całą pewnością



Rysunek 1. Schemat blokowy procesora LS1021A

pojawią się odpowiednie regulacje prawne, a aplikacje IoT będą musiały być certyfikowane i dopuszczone do użytku. Nieuniknioną konsekwencją będzie wymaganie, aby procesory używane do komunikacji w aplikacjach M2M oraz IoT miały możliwość wykonywania operacji kryptograficznych, takich jak haszowanie, podpisywanie oraz kodowanie danych oraz bezpieczne i zgodne z wymaganiami prawnymi przechowywanie klucza kryptograficznego.

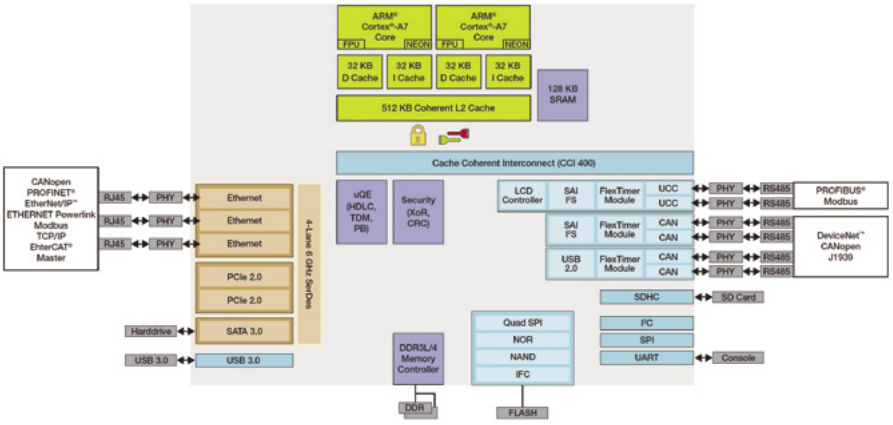
Połączenia w sieci przedsiębiorstwa również muszą być zabezpieczone, nie tylko przed „podsłuchiwaniem" danych, ale również przed nieautoryzowanym przejęciem kontroli nad wyposażeniem, co może skutkować takimi kosztownymi zdarzeniami, jak dla przykładu zatrzymanie linii produkcyjnej. Nawet jeśli dane przesyłane poprzez łącze sieciowe są szyfrowane, to urządzenie fizyczne musi być odporne na atak poprzez nieautoryzowaną modyfikację oprogramowania. Dlatego gotowy produkt musi zapewniać nie tylko bezpieczną komunikację, ale również pracować jako bezpieczny (zaufany) węzeł. Jednym zdaniem, użytkownik mieć pewność, że dane są chronione oraz że urządzenie pracuje pod kontrolą właściwego, autentycznego oprogramowania utworzonego przez użytkownika lub na jego zamówienie.

W świecie rzeczywistym zazwyczaj ufamy informacjom, które docierają do nas od współpracowników i typowo to zaufanie jest w naturalny sposób przenoszone do świata cyfrowego. Jeśli w sieci otrzymujemy informacje (dane lub komendy) z jakiegoś urządzenia, to spodziewamy się, że są to pewne, ważne informacje. Problem pojawia się, jeśli do naszej sieci zostanie dołączone coś pracujące na naszą szkodę. Dlatego do urządzeń sieciowych wprowadza się mechanizmy zabezpieczające tworząc tzw. zaufane źródła danych.

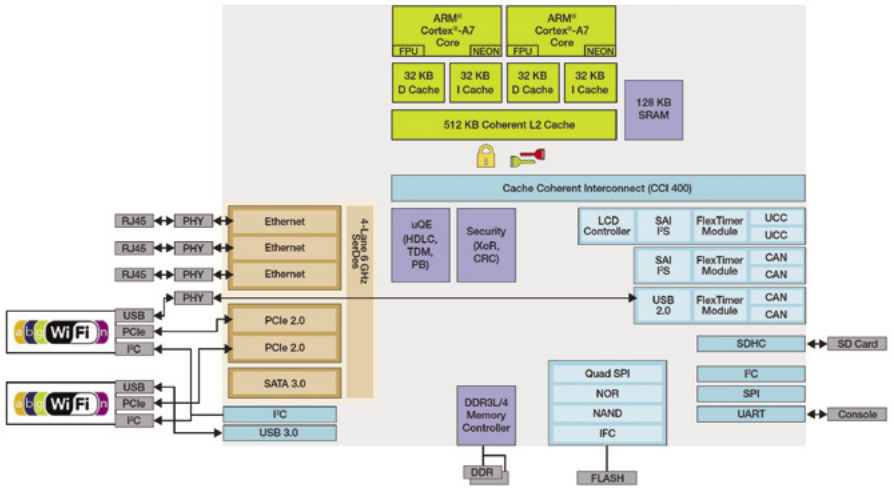
Uruchomienie zaufanego urządzenia wymaga odpowiednich mechanizmów będących „podstawami zaufania". Można je utworzyć za pomocą układu zewnętrznego (typowo – kosztownego), takiego jak FPGA lub ASIC lub mogą one być zintegrowane w SoC (system on chip), jak to zrobiono w rodzinie QorIQ LS1. W procesorze LS1021A autentykacja jest wykonywana przez wbudowany preloader, który w całości zapisano w wewnętrznej pamięci ROM. Wraz z nim jest dostarczany jednorazowy klucz przeznaczony do użycia z preloaderem programu bootloadera, który zabezpiecza przed nieautoryzowanym oprogramowaniem mogącym manipulować systemem. To zabezpieczenie jest dostępne jako opcja załączana poprzez zapisanie klucza autentykacji i włączenie bitu zezwalającego na autentykację (praca w trybie *Trust*). Ten bit jest wykonany w postaci jednorazowo ustawianego bitu bezpiecznika. Po załączeniu trybu *Trust*, obraz zewnętrznego oprogramowania (np. *bootloader*, kernel OS lub inny, „surowy" kod pracujący bez systemu operacyjnego) będzie wykonywany po pomyślnie wykonanym deszyfrowaniu oraz autentykacji za pomocą klucza preloadera. Dopiero od tego momentu odtworzony kod staje się zaufanym. To zabezpieczenie dla pierwszorzędnych lub alternatywnych (drugorzędnych), podpisanych zawartości pamięci programu (obrazów) zapewnia autentyczność kodu programu, który nie może być podmieniony przez kogoś, kto nie zna klucza szyfrowania. Co ważne, tworzone zwykle przez firmy zewnętrzne lub oddelegowane oddziały przedsiębiorstwa obrazy są szyfrowane za pomocą tego samego klucza, co zawarty w procesorze QorIQ LS1021A i dzięki temu są zabezpieczone od momentu, w którym opuszczają zespół tworzący oprogramowanie i mogą być bezpiecznie przesyłane do miejsca, w którym należy zaprogramować urządzenie czy dokonać aktualizacji firmware.

Od momentu, w którym zawartość pamięci programu zostanie autentykowana

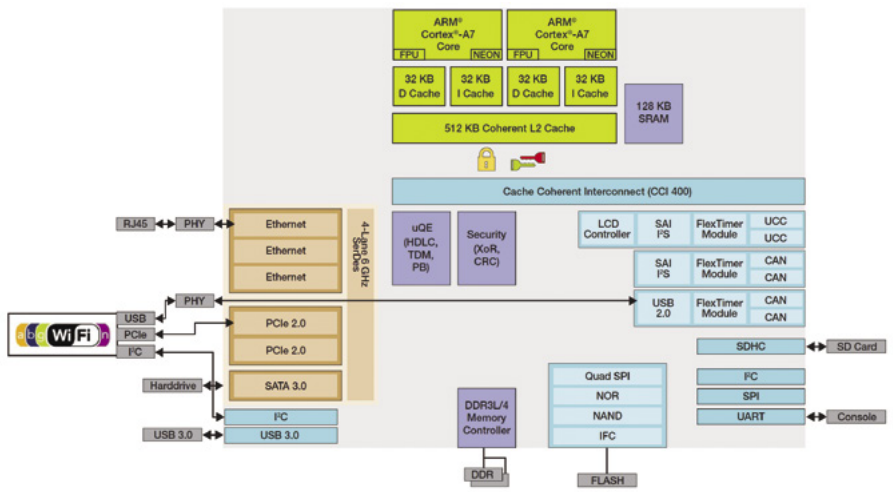
i załadowana przez procesor urządzenia, rozpoczyna ono pracę w roli zaufanego węzła. Aby zabezpieczyć ten węzeł przed próbami manipulacji, procesor ma dodatkowe możliwości wykrycia i zabezpieczenia urządzenia przed włamaniem lub manipulowaniem kodem/danymi przechowywanymi w pamięci zewnętrznej. Na przykład, kontroler trybu debuowania zapewnia dostęp do systemu przez interfejs JTAG, który może być bezwarunkowo odłączony lub dostępny w kilku różnych trybach pracy, ale dopiero po pomyślnym wykonaniu sekwencji zapytania/odpowiedzi. Wbudowana jednostka kontroli integralności systemu przeprowadza w czasie rzeczywistym periodyczną sprawdzenie predefiniowanych obszarów pamięci pod kątem wykrycia modyfikacji wykonanych przez szkodliwe lub działające wadliwie oprogramowanie. Jest to możliwe dzięki ciągłemu obliczaniu i porównywaniu sum kontrolnych predefiniowanych regionów pamięci. Procesor ma również doprowadzenie, które może być używane do wykrywania prób fizycznego dostępu do urządzenia (*tamper detection*). Na koniec, mechanizm zaimplementowany przez firmę ARM będącą konstruktorem rdzenia – *TrustZone* – umożliwia podział pamięci systemowej na obszary „bezpieczne" i „niebezpieczne" kontrolując prawa dostępu do tych obszarów.



Rysunek 2. Schemat blokowy programowanego sterownika przemysłowego PLC



Rysunek 3. Schemat blokowy bezprzewodowej, bezpiecznej bramki sieciowej



Rysunek 4. Schemat blokowy dysku sieciowego do bezpiecznego przechowywania danych

Wszystkie naruszenia bezpieczeństwa są kontrolowane przez tzw. monitor bezpieczeństwa, będący częścią pamięci nieulotnej. Użytkownik ma możliwość zaprogramowania akcji podejmowanej po próbie naruszenia integralności systemu. Może nią być na przykład automatyczne kasowanie poufnych informacji, takich jak klucz szyfrowania i powiadomienie systemu operacyjnego, który może podjąć dalszą akcję.

Innym blokiem funkcjonalnym związanym z zabezpieczeniami jest jednostka kryptograficzna, która jest również używana przez preloader, aby przyspieszyć proces deszyfrowania/autentykacji obrazu podczas bootowania. Zadaniem tego bloku jest zapewnienie wsparcia sprzętowego dla algorytmów związanych z protokołami IPSec, SSL/TLS, WiMAX i innymi. Wiele z nich jest gotowych do transmisji lub odbioru już po pojedynczym przebiegu przetwarzania. Dzięki temu dane związane np. z technologią IoT mogą być szybko przesyłane poza urządzenie.

Jednostka kryptograficzna ma budowę modularną, o skalowalnym bezpieczeństwie. Zoptymalizowano ją pod kątem wykonywania złożonych operacji kryptograficznych (np. 3DESHMAC-SHA-1) w pojedynczym przebiegu. Wśród zaimplementowanych algorytmów są dla przykładu: XOR, DES, AES i certyfikowany generator liczb pseudolosowych NIST.

Podsumowanie

Wydajna, bezpieczna komunikacja w sieci związana z kontrolą operacji przemysłowych, aplikacji M2M oraz rozwijającą się technologią IoT, wymaga spełnienia pewnych podstawowych wymagań. Urządzenie transmitujące dane musi być pewne, niezwodne, gwarantować bezpieczeństwo własne i przesyłanych danych, efektywne przetwarzanie pakietów i rozszerzone możliwości łączeniowe. Procesor QorIQ LS1021A został skonstruowany w taki sposób, aby wypełnić te wymagania, zapewniając wyjątkową niezawodność i wydajność w połączeniu z łatwością implementacji obsługi wielu protokołów komunikacyjnych oraz dużym wyborem opcji zabezpieczających zarówno dane, jak i urządzenie zbudowane w oparciu o niego. Na rysunkach pokazano schematy blokowe przykładowych aplikacji, w których zastosowano procesor QirIQ LS1021A:

- programowany sterownik przemysłowy (**rysunek 2**),
- bezpieczną bramkę sieciową (**rysunek 3**),
- dysk sieciowy do bezpiecznego przechowywania danych (**rysunek 4**).