

Bezpieczeństwo dla systemów IoT i embedded w oprogramowaniu ARM KEIL

Warunkiem wprowadzenia na rynek wielu produktów, w branżach takich jak: AGD, motoryzacja, przemysł czy medycyna, jest spełnienie wymogów prawnych potwierdzających ich zgodność z normami bezpieczeństwa funkcjonalnego. Jednym z elementów procesu certyfikacji jest zabezpieczenie kodu urządzenia przed wykonaniem niewłaściwej operacji, jak również blokowanie dostępu przed nieautoryzowaną próbą przejęcia jego kontroli. Bezpieczeństwo w działaniu aplikacji wbudowanych jest więc kluczowym tematem podczas certyfikowania produktów.

W szczególności w ostatnim czasie, gdyż rosnąca liczba urządzeń IoT wprowadzanych na rynek wymusza działania również w tym zakresie. Rządy krajów zaczynają więc prace nad ustandaryzowaniem zabezpieczeń, a także nad określeniem wymogów, które będą spełniały aplikacje

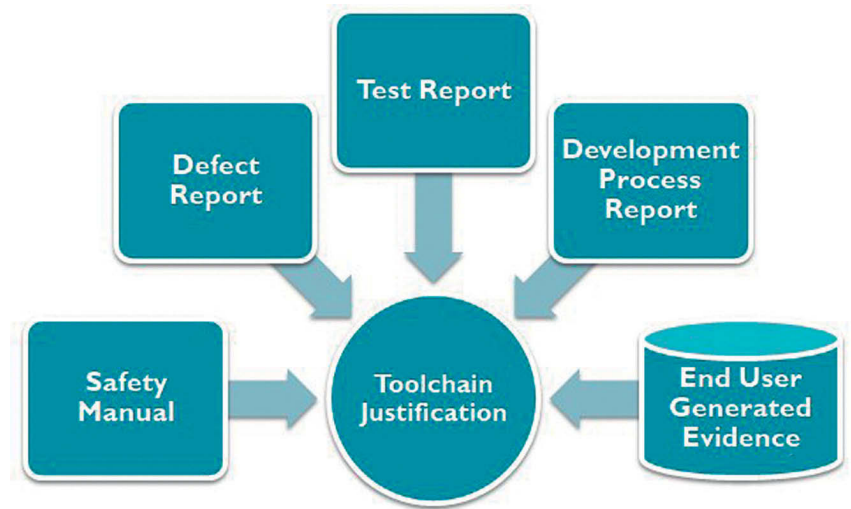
IoT. Informacje zaczynają napływać ze Stanów Zjednoczonych, o „rozsądnych zabezpieczeniach” i potrzebie ich stosowania w urządzeniach wykorzystywanych przez instytucje rządowe. Jednak takie działania pozwala przypuszczać, że podobne rozwiązania zostaną wprowadzone także w innych krajach i będą do-

tyczyły zarówno przemysłu, jak również rynku konsumenckiego.

Bezpieczeństwo w aplikacjach IoT

IoT, czyli Internet Rzeczy oznacza system oraz sieć połączonych urządzeń elektronicznych zdolnych do wymia-

ny informacji pomiędzy sobą w sposób automatyczny. Urządzenia IoT pozwalają na gromadzenie danych oraz udostępnianie ich użytkownikom, jak również na komunikację przez Internet. Dlatego ważnym aspektem jest ochrona informacji, jak również prawidłowa praca sprzętu podczas całego czasu użytkowania. W celu osiągnięcia tej funkcjonalności przydatna może być technologia TrustZone korzystająca z rozwiązania SoC (System on Chip) i podejście do bezpieczeństwa obejmujące cały system. Technologia TrustZone dla procesorów Arm Cortex-M zapewnia wysoki poziom ochrony. Zmniejsza także ryzyko ataku, izolując krytyczne oprogramowanie sprzętowe, zasoby i prywatne informacje od reszty aplikacji. Stanowi doskonały punkt wyjścia dla urządzenia w oparciu o wytyczne Platform Security Architecture (PSA). Do urządzeń IoT możemy zaliczyć między innymi inteligentne urządzenia typu „smart home”. Nietrudno zauważyć, że takie rozwiązania, choć bardzo przydatne człowiekowi, jak np. otwieranie bramy domu przy użyciu smartfonu, umożliwiają działa-

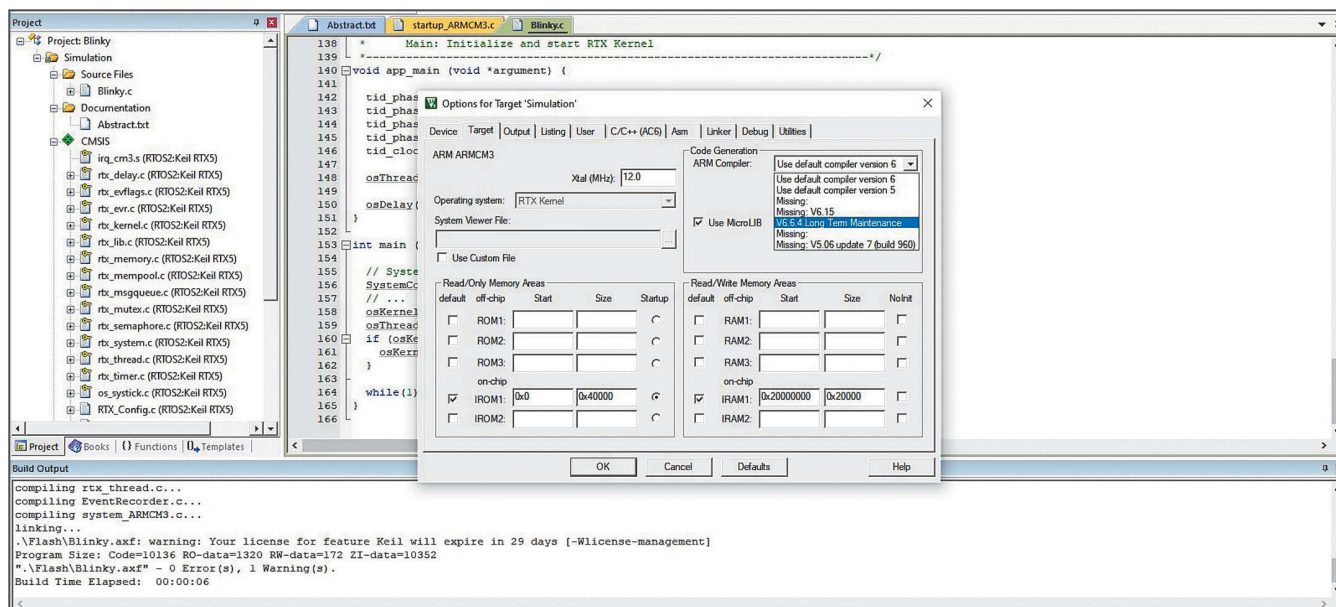


nie osobom niepożądanym np. poprzez próby włamania się do obiektu. Jeszcze poważniej sprawa wygląda w przemyśle i medycynie.

Środowisko bezpiecznych aplikacji Arm Keil MDK Professional

Biorąc pod uwagę fakt, że bezpieczeństwo programu jest istotnym ele-

mentem podczas procesu certyfikacji Functional Safety, z pomocą w tym zakresie mogą przyjść bezpieczne rozwiązania firmy Arm. Należą do nich między innymi: certyfikowane kompilatory C, C++, zestaw kwalifikacyjny (Qualification Kit), modele symulacyjne, czy optymalizacje systemu RTOS oraz technologia TrustZone. Warto dodać, że wymienione funkcjonalności



może obsługiwać jedne wspólne środowisko, którym jest μ Vision MDK Professional.

Arm Keil rozwija narzędzia programistyczne dla układów opartych na swojej architekturze, dlatego zawsze zna najnowsze rozwiązania, udostępniając je w postaci paczek do ściągnięcia w swoim zintegrowanym środowisku. Narzędzia producenta używane są przez ogromną liczbę developerów, tworzących aplikacje dla produktów w lotnictwie, bankowości, motoryzacji, transporcie, produkcji, wojsku czy telekomunikacji.

Jak wykonać zmianę do kompilatorów bezpiecznych

Posiadacz aktualnej licencji środowiska μ Vision MKD Professional ma możliwość, bez dodatkowych kosztów przejść do bezpiecznych rozwiązań. Może to wykonać korzystając z zestawu kwalifikacyjnego, który zawiera: instrukcję bezpieczeństwa, raport procesu rozwoju, raporty z testu i raport usterek. Są to narzędzia, które obejmują ponad 250 stron dokumentacji w formie wyjaśnień i potwierdzeń dotyczących zastosowań bezpiecznych kompilatora. Należy pamiętać, że żaden kompilator nie pracuje w 100% bezbłędnie, jednak Arm dokłada wszelkich starań, aby tak było. Potwierdzeniem tych prac jest wydany certyfikat przez organizację TÜV.

Aby skorzystać z narzędzi zestawu kwalifikacyjnego należy założyć profil na portalu developer.arm.com, a następnie ściągnąć narzędzia w najnowszej

wersji dla Functional Safety, czyli v6.6.4. Na stronie znajdują się kolejno do pobrania: certyfikowany kompilator, zestaw kwalifikacyjny oraz certyfikat TÜV. Istnieje również możliwość pobrania poprzednich wersji narzędzi.

Po zgraniu paczek, w środowisku μ Vision należy wejść w menu „Project-Manage-Project Items”, gdzie dodajemy nowy kompilator do listy. Z kolei w „Options for Target” możemy wybrać kompilator, z którego chcemy korzystać w projekcie. Po jego dodaniu, będzie to „v6.6.4 Long Term Maintenance”. Następnie należy skompilować projekt. Może wystąpić sytuacja, w której będzie potrzebne dostosowanie części kodu pod działanie nowego kompilatora, wtedy pomocna okaże się dokumentacja techniczna, dostępna w ściągniętej paczce.

Więcej informacji znajduje się na kanale YouTube – „ARM Keil MDK #24 – zmiana rodzaju kompilatora”.

W ofercie Arm występuje dodatkowo oprogramowanie FuSa RTS, które jest zestawem komponentów zakwalifikowanych do stosowania w najbardziej krytycznych dla bezpieczeństwa aplikacjach, w systemach motoryzacyjnych, medycznych i przemysłowych. Kolejną opcją zakupową stanowi Arm Development Studio, które zostało zaprojektowane specjalnie dla architektury Arm, zgodnie z zasadą „jeden zestaw narzędzi – dowolny projekt oparty na Arm”. Przyspiesza projektowanie, pomagając jednocześnie tworzyć solid-

ne i wydajne produkty. Licencja kompilatora Functional Safety dostępna jest dla oprogramowania Arm Development Studio w wersji Gold lub Platinum.

Wnioski

Podsumowując, rynek aplikacji IoT rośnie z roku na rok w bardzo szybkim tempie. Powstające urządzenia współpracują ze sobą, komunikując się i wymieniając dane. Takie działanie przynosi szereg korzyści użytkownikom, dostarczając informacji sprawnie, czy też umożliwiając automatyzację pracy. Jednak wdrażanie aplikacji IoT stwarza także pewne zagrożenia. Dlatego tak ważnym jest, aby zapewnić bezpieczeństwo na poziomie działania programu. Istnieje możliwość, aby usprawnić tworzenie kodu bezpiecznego, przy użyciu certyfikowanych kompilatorów. Można również pracować z dostarczoną dokumentacją i korzystać z wyników testów czy zaleceń stworzonych dla zapewnienia bezpieczeństwa funkcjonalnego. Zastosowanie rozwiązań Arm dostarczy wielu korzyści, których efektem będzie opcja zakończenia projektu dla urządzenia w krótszym czasie. Dostępność i przedłużone wsparcie produktu pozwolą także skorzystać z tych rozwiązań również w przyszłości, czyniąc pracę bardziej efektywną dla sprawdzonych rozwiązań.

Grzegorz Cuber

Computer Controls Sp. z o. o.
tel. 33 485 94 90, www.ccontrols.pl