embedded-software engineer
Fachwissen für Software-Professionals

Mit komponentenbasiertem Software-Design zur Security-Zertifizierung für IoT-Geräte

28.11.18 | Autor / Redakteur: Sergey Tverdyshev * / Sebastian Gerstl

Für unterschiedliche Arten von IoT-Anwendungen existieren auch unterschiedliche Sicherheitsstandards. Ob Sie nun die Common Criteria for Information Technology Security (ISO 15408), die IEC 62443 für Industrial Control Systems, EDSA (Embedded Device Security Analysis) oder J3061 im Automobilbereich erfüllen wollen: Wir zeigen, wie Sie mit komponentenbasiertem Softwaredesign schnell alle notwendigen Ansprüche erfüllen können. (Bild: gemeinfrei/ CC0)

Der Erfolg von IoT-Ansätzen liegt darin, dass mit Hilfe von offenen Standards und offenen Protokollen eingebettete kommerziell verfügbare Off-the-Shelf-Komponenten vergleichsweise lose verknüpft werden. Diese Modularität spiegelt sich auch in den Zertifizierungsstandards wider. Wir zeigen auf, wo und wie ein Komponenten-basiertes Softwaredesign es signifikant erleichtert, Zertifizierungsanforderungen zu genügen.

Im Internet der Dinge wird die klassische IT-Sicherheit immer mehr auf eingebettete Komponenten ausgeweitet. Charakteristisch für die Sicherheitsanforderungen vieler IoT-Systeme ist, dass Integrität und Verfügbarkeit in stärkerem Fokus stehen. Dies schlägt sich auch in Zertifizierungsstandards nieder: die klassischen Common Criteria for Information Technology Security (ISO 15408) werden durch domänenspezifische Sicherheitsstandards ergänzt, wie z.B. IEC 62443 für Industrial Control Systems, EDSA (Embedded Device Security Analysis) oder J3061 im Automobilbereich, die von einem starken Fokus von „Security for Safety“ geprägt sind.

Das Internet der Dinge (Internet of Things, IoT]) ist extrem heterogen, sehr dynamisch, immer verfügbar, damit jederzeit angreifbar. Das IoT besteht aus IoT-Komponenten als modularen Bausteinen (siehe auch I. Yaqoob, E. Ahmed, I. Hashem, A. Ahmed, A. Gani, M. Imran und M. Guizani, „Internet of Things Architecture: Recent Advances, Taxonomy, Requirements, and Open Challenges,“).

Auch Sicherheit ist in der Regel modular

Bild 1 zeigt das Sicherheitsmodell nach Teil 1 der Common Criteria (CC) (Abschnitt 7.1), das ebenfalls von IEC 62443-1-1 (Abschnitt 5.1) explizit aufgegriffen wird. Diese Abbildung stellt alle Assets, Bedrohungen und Gegenmaßnahmen als jeweils eine Box dar. Bei genauerer

Betrachtung sieht unserer Erfahrung nach das Bild hingegen oft eher aus wie in Bild 2. Die folgende Tabelle zeigt ein Beispiel für eine denkbare Belegung mit zwei Assets:

Nummer/Farbe	Asset	Bedrohung	Gegenmaßnahme
1/rot	Motorsteuerung	Verzögerung in Hinderniserkennung → Personenschaden	Echtzeitgarantien, Separierung
2/grün	Performancelogger	Verlust von Operational HistoryPerformanceloggerVerlust von Operational History	Passwort in der Webschnittstelle

Im oben gezeigten Beispiel sind die Assets und ihre Bedrohungen von sehr unterschiedlicher Kritikalität. Anhand der konkreten Belegung in Bild 2 wird auch klar, dass eine weitere Bedrohung darin besteht, dass der Angreifer versucht, die Gegenmaßnahmen zu umgehen („will try to bypass“), z.B. könnte ein Ethernet-Zugriff auf den Performancelogger dazu missbraucht werden, auch die Motorsteuerung anzugreifen. Ein Mittel, um komplexe IT-Systeme und insbesondere IoT-Komponenten unterschiedlicher Kritikalität auf einer angemessenen Abstraktionsebene zu beherrschen, ist die Aufteilung in Sicherheitdomänen („teile und herrsche“). Eine Sicherheitsdomäne ist eine Zone, in der alle Objekte derselben Sicherheitspolitik unterliegen. Die Grenzen von Sicherheitsdomänen werden auch „trust boundaries“ genannt.

Aufbauen einer Sicherheitsarchitektur für eine Common-Criteria-Zertifizierung

Bei der Common Criteria for Information Technology Security Evaluation (CC) arbeitet ein Hersteller zusammen mit einer Prüfstelle an der Evaluierung eines vom Hersteller vorgeschlagenen IT-Produktes. Das Produkt kann aus Software oder Software und Hardware bestehen, IoT-Komponenten sind also ausdrücklich enthalten. Ist die Evaluierung erfolgreich, so erteilt die Zertifizierungsstelle, in Deutschland das BSI (Bundesamt für Informationstechnik), ein Zertifikat.

Die Common Criteria fordern vom Entwickler als zentralen Bestandteil der der Prüfstelle vorzulegenden Dokumentation eine Designdokumentation, in der, je nach angestrebter Evaluierungsstufe, eine ein- oder zweistufige Unterteilung in Subsysteme (einstufig) oder Subsysteme und Module (zweistufig) vorgenommen werden muss. Die Eigenschaften von Subsystemen und Module und ihre Interaktionen müssen beschrieben werden. Die Designdokumentation beschreibt auch inwiefern die Schnittstellen von Subsystemen und Modulen für den Angreifer direkt oder indirekt zugänglich sind.

Eine Sicherheitsarchitektur ist ein Mittel, die Sicherheitseigenschaften eines Systems in Hinblick auf seine Sicherheitsdomänen zu analysieren und zu dokumentieren.

Eine Sicherheitsarchitektur (ADV_ARC) nach Common Criteria hat die folgenden Punkte zu erklären:

- welche Sicherheitsdomänen hat das System? Inwieweit sind diese Sicherheitsdomäne vollständig getrennt oder dürfen sie miteinander (kontrolliert) kommunizieren? In unserem Beispiel wären der Performancelogger und die Motorsteuerung verschiedene Domänen.
- wie wird das System initialisiert?
- wie schützt sich das System selber dagegen, dass ein Angreifer versucht, es anzugreifen?
- wie schützt sich das System dagegen, dass es umgangen wird (in unserem Beispiel: der Webzugriff auf den Perfomancelogger kann die Motorsteuerung nicht umgehen)?

Sicherheitsarchitektur nach IEC 62443

IEC 62443 ist ein Standard für die Sicherheit von industriellen Steuerungsanlagen als Ganze (insbesondere Teile 3-1 bis 3-3) und deren Komponenten (insbesondere Teile 4-1 und 4-2). IEC 62443 wird vom Safety-Standard IEC 61508 für Security referenziert (IEC 61508 Teil 1-1 Abschnitt 7.5.2.2: „If security threats have been identified, then a vulnerability analysis shall be undertaken in order to identify security requirements. Note: Guidance is given in the 62443 series"). IEC 62443 ist zum großen Teil noch in (fortgeschrittener) Entwicklung unter dem Dach von IsaSecure.

In IEC 62443 heißen die Sicherheitsdomänen „Zonen" und das System soll die Partitionierung in Zonen unterstützen (IEC 62443 Teil 3-3 Abschnitt SR 5.4), sowie ein Ressourcenmanagement betreiben welches robust gegenüber Angreifern ist (IEC 62443 Teil 3-3 Abschnitte SR 7.1 und SR 7.2 und IEC Teil 4-2 Abschnitte CR 7.1 und CR 7.2), also z.B. gegenüber Denial-of-Service.

In Hinblick auf Entwicklungsprozess fordert IEC 62443 Teil 4-1 SR-2 die Erstellung eines Bedrohungsmodells mit Trust boundaries, welches auch behandelt, wie Informationen über diese Trust boundaries fließen. Es wird ein Defense-in-depth-Design empfohlen (IEC 62443 Teil 4-2 SD-2). IEC 62443 Teil 4-1 SD-6 fordert darüber hinaus, dass es ein Designziel sein muss, die Angriffsfläche zu minimieren.

Sicherheitsarchitektur nach IsaSecure EDSA / SDLA / SSA

In den Standards SDLA (Prozesse), EDSA (funktionale Anlagen für Komponenten) und SSA (funktionale Anforderungen für ganze Anlagen) hat IsaSecure ein konkretes Zertifizierungsschema für die IEC 62443-Reihe entwickelt, in das auch Anregungen aus NIST 800-53 eingeflossen sind. So stellt z.B. EDSA-311 auf funktioneller Ebene die in der folgenden Tabelle gezeigten Anforderungen:

FSA-RDF-1	**The IACS embedded device shall provide means to enforce assigned authorizations for controlling the flow of information outside the embedded controller zone and between interconnected systems in accordance with user specific policy.**
FSA-RDF-2	The IACS embedded device shall separate data acquisition services, from management functionality.
FSA-RDF-3	The IACS embedded device shall isolate security functions from non-security functions by means of partitions, domains, etc., including control of access to and integrity of, the hardware, software, and firmware that perform those security functions.
	The IACS embedded device shall prevent unauthorized and unintended

FSA-RDF-4 information transfer via shared system resources where it supports connection sessions from users with different levels of access.

Ebenso wie in IEC 62443 Teil 4-1 fordert SDLA-312 auf der Prozessebene ein modulares Design (SDLA-DSD-1.*) und die klare Identifizierung von Trust Boundaries und Angriffsflächen (SDLA-SAD-*).

Sicherheitsarchitektur in J3061

J3061 von SAE ist der jüngste der Standards, die wir betrachten und wir beziehen uns auf den veröffentlichten Entwurf von 2016. Das Erstellen einer Softwarearchitektur beginnt hier mit „Refine Functional Cybersecurity Concept into Technical Cybersecurity Concept“ (Abschnitt 8.4.3), und wiederum ist dabei die Isolation spezifischer Funktionen wichtig. Als Beispiel wird genannt: „Isolation/partitioning of systems that have external access (e.g. Wi-Fi,

Bluetooth, OBD) from safety-critical systems and systems that can have important impacts on the operation of the vehicle.” Die Softwarearchitektur wird dann einer Bedrohungsanlayse in Hinblick auf Vertraulichkeit, Integrität und Verfügbarkeit (Abschnitt 8.6.3) untezogen und auf Verwundbarkeit und Bedrohungen untersucht Abschnitt 8.6.4 nennt STRIDE, ASF, und DREAD als mögliche Hilfsmittel zur Bedrohungskategorisierung.

Gemeinsamkeiten und Ausblick

Mit der Betrachtung von Anforderungen zur Softwarearchitektur haben wir uns hier hauptsächlich auf die Sicherheitsheitsarchitektur im linken Ast des V-Modells beschränkt. Es ist klar, dass die Erfüllung dieser Anforderungen nicht nur das Design, sondern auch das Testen / Vulnerability Analyse vereinfacht.

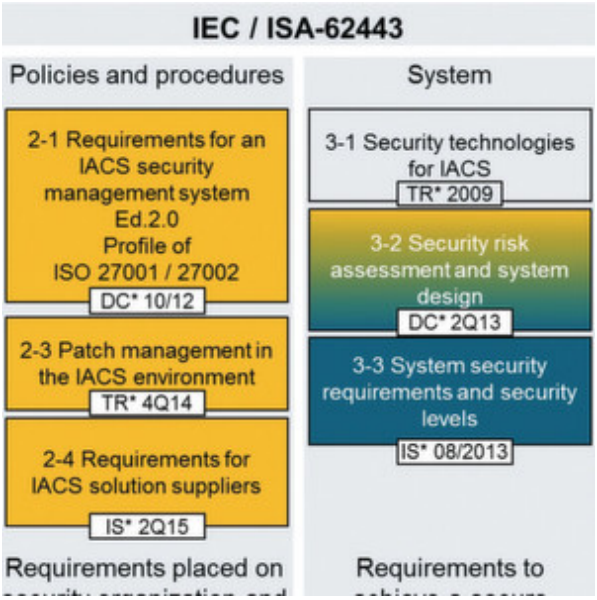
Wir haben gesehen, dass alle untersuchten IoT-relevanten Standards (Common Criteria/ISO 15408, IEC 62443, EDSA/SDLA/SSA und J3061) eine Sicherheitsarchitektur einfordern, die Isolierung, Ressourcenmanagement und Informationsflusskontrolle zwischen Sicherheitsdomänen (auch „Zonen“ oder „Partitionen“ genannt) bereitstellt.

Unter dem Aspekts des Materialverbrauchs (z.B. je Security-Domäne ein Steuergerät) erscheint eine solche Architektur mit klarer und vor allem nicht umgehbarer Aufgabentrennung auf den ersten Blick aufwändiger. Der Materialverbrauch kann allerdings durch Virtualisierung wie folgt kontrolliert werden:

- In Hinblick auf Netzwerkvirtualisierung sind hier vor allem neuere Entwicklungen lastbalancierender Echtzeit-Netzwerk-Standards interessant (z.B. TSN, IEEE 802.1 Qbu/Qbv), mit denen Verkabelung sicher geteilt werden kann.
- In Hinblick auf CPU-Virtualisierung findet seit einigen Jahren das ursprünglich aus der sowohl Sicherheits- wie auch Material-sensitiven Avionik stammende MILS-Konzept zunehmend Anklang.

Auf einem MILS-System sähe das eingangs in Bild 2 gezeigte Beispiel aus wie in Bild 3 zu sehen.

Bei der Realisierung durch ein MILS-System wie in Bild 3 werden die von Common Criteria, IEC 62443, EDSA, und J3061 geforderte Isolierung, Ressourcenmanagement und Informationsflusskontrolle von einem Trennungskern gestellt. Die Partitionen eines Trennungskerns sind dabei die Vorlagen für Sicherheitsdomains in IoT-Geräten, die eine MILS-Architektur verwenden.



*Dr. Inf. Sergey Tverdyshev ist Director R&T (Research & Technology) bei der SYSGO AG.

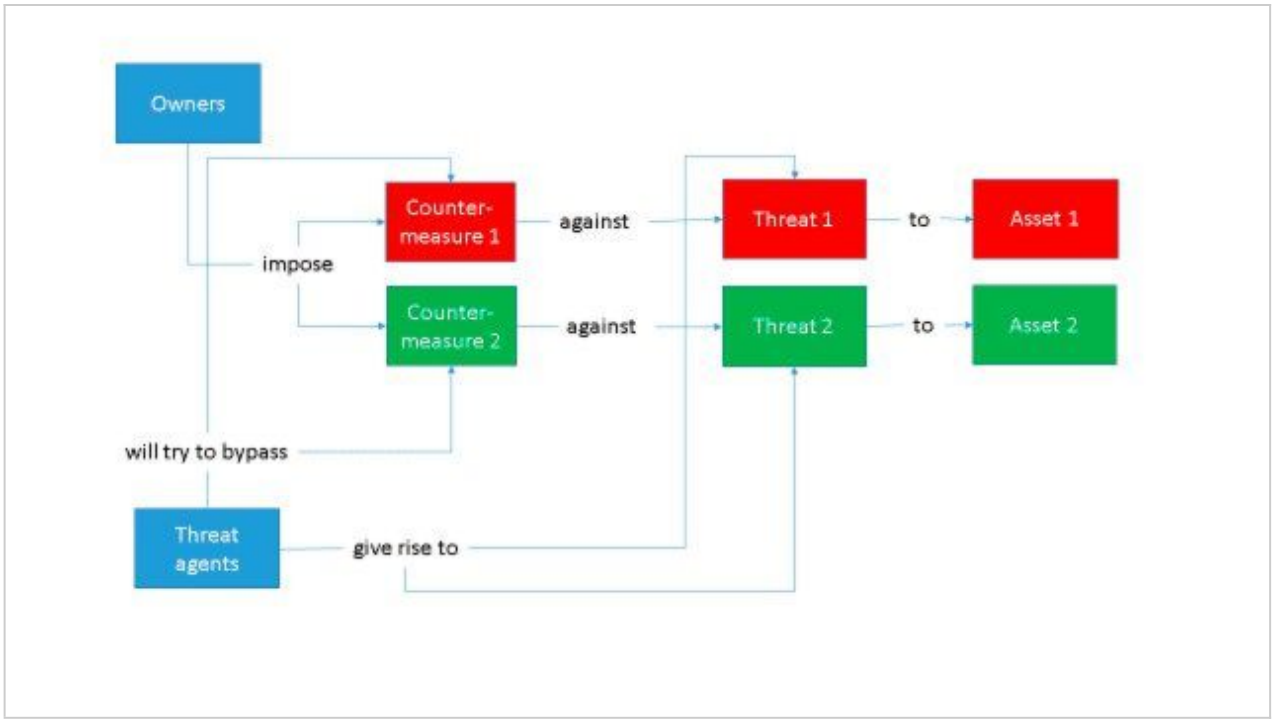


Bild 2: Sicherheitsmodell CC und IEC 62443-1-1 mit zwei Assets. (SYSGO)