Bundesamt
für Sicherheit in der
Informationstechnik

SYS.4.3 Eingebettete Systeme

1. Beschreibung

1.1. Einleitung

Eingebettete Systeme sind informationsverarbeitende Systeme, die in ein größeres System oder Produkt integriert sind. Sie übernehmen Steuerungs-, Regelungs- und Datenverarbeitungsaufgaben und werden dabei oft nicht direkt von den Benutzenden wahrgenommen. Eingebettete Systeme finden sich sowohl im Bereich der Hochtechnologie wie z. B. der Luft- und Raumfahrt, der Medizintechnik, der Telekommunikation und der Automobiltechnik als auch im Consumer- und Haushaltsgerätebereich.

Ein eingebettetes System bildet aus Soft- und Hardware eine funktionale Einheit, die nur eine definierte Aufgabe erfüllt. Die Software eingebetteter Systeme wird als Firmware bezeichnet und ist zumeist in einem Flash-Speicher, einem EPROM, EEPROM oder ROM gespeichert und durch Anwendende nicht oder nur mit speziellen Mitteln oder Funktionen austauschbar. Sie besteht im Wesentlichen aus dem Bootloader, dem Betriebssystem und der Anwendung. Spezialisierte Systeme können auch auf ein Betriebssystem verzichten. Eingebettete Systeme sind zwar spezialisierte Geräte, aber im Gegensatz zur reinen Hardwareimplementierung (ASIC) universelle Rechner. Als Plattformen kommen unterschiedliche CPU-Architekturen oder flexible hochintegrierte Field-Programmable-Gate-Array-Bausteine (FPGA) infrage.

Eingebettete Systeme haben entweder keine Bedienschnittstelle oder nutzen Spezialperipherie wie z. B. funktionelle Tasten, Drehschalter und auf den jeweiligen Einsatzzweck hin konzipierte Anzeigen. Das Spektrum an Ausgabeeinheiten reicht von einer einfachen Signallampe über LCDs bis hin zu komplexen Cockpit-Anzeigen. Eingebettete Systeme kommunizieren häufig über Datenbusse, die in komplexen Systemen heterogen vernetzt sind. Zusätzlich können über mehrere unterschiedliche und mehrkanalige Ein-/Ausgabeports auch zusätzlich Peripheriekomponenten wie Sensoren und Aktoren angebunden sein. Einige Arten eingebetteter Systeme verfügen darüber hinaus auch über ein Webinterface, über das sie per Browser konfiguriert werden können.

1.2. Zielsetzung

Ziel dieses Bausteins ist es, über typische Gefährdungen für eingebettete Systeme zu informieren sowie aufzuzeigen, wie diese Systeme sicher in Institutionen eingesetzt werden können.

1.3. Abgrenzung und Modellierung

Der Baustein SYS.4.3 *Eingebettete Systeme* ist auf jedes eingebettete System im Informationsverbund einmal anzuwenden.

Dieser Baustein beschäftigt sich allgemein mit eingebetteten Systemen. Er ist für ein großes Spektrum unterschiedlicher eingebetteter Systeme anwendbar. Auf dedizierte Sicherheitseigenschaften, etwa von Bedien- und Anzeigesystemen oder spezifische Hard- und Software-Architekturen, wird nicht näher eingegangen. Ebenso wird nicht speziell auf Sicherheitsaspekte von eingebetteten Systemen eingegangen, die in der industriellen Steuerung eingesetzt werden. Hierfür sind zusätzlich die Bausteine der Schicht IND *Industrielle IT* heranzuziehen. Spezifische Sicherheitsaspekte von IoT-Geräten sind ebenfalls nicht Gegenstand des vorliegenden Bausteins. Als vernetzte Geräte oder Gegenstände mit zusätzlichen smarten Funktionen werden IoT-Geräte im Gegensatz zu eingebetteten Systemen nicht in ein größeres System oder Produkt integriert. Auf Grund ihrer drahtlosen Verbindung zu Datennetzen bestehen hier andere Sicherheitsanforderungen. Sie werden in SYS.4.4 *Allgemeines IoT-Gerät* behandelt.

Eine besondere Anwendung eines eingebetteten Systems sind Chipkarten. Die Karten besitzen in der Regel einen Prozessor, Arbeitsspeicher und I/O-Interfaces. Auch für Chipkarten gilt, dass zwar grundsätzliche Sicherheitsaspekte in diesem Baustein angesprochen werden, allerdings keine spezifischen Aspekte betrachtet werden.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein SYS.4.3 *Eingebettete Systeme* von besonderer Bedeutung:

2.1. Unzureichende Sicherheitsanforderungen bei der Entwicklung von eingebetteten Systemen

Aus Kostengründen spielt die Informationssicherheit bei der Entwicklung von eingebetteten Systemen häufig eine weniger wichtige Rolle als z. B. die Performance oder Zuverlässigkeit. Werden jedoch Sicherheitsanforderungen in einer oder mehreren Entwicklungsphasen nicht ausreichend berücksichtigt, können die eingebetteten Systeme schwerwiegende Schwachstellen aufweisen.

2.2. Ungesicherte Ein- und Ausgabe-Schnittstellen bei eingebetteten Systemen

Die Schnittstellen eingebetteter Systeme sind potenzielle Angriffspunkte. Das betrifft Schnittstellen auf allen Ebenen des OSI-Schichtenmodells und alle eingesetzten Übertragungsmedien. Wird der Zugang über die Schnittstellen nicht kontrolliert oder sind die Kontrollmechanismen zu schwach, könnte bei einem Angriff in das System eingedrungen werden, unbefugt Daten gelesen und manipuliert sowie Folgeangriffe eingeleitet werden. So könnten unbemerkt Spionage- oder Sabotagegeräte angeschlossen werden, z. B. miniaturisierte Steuerungen oder Datenlogger.

Auf Mikrocontroller-Ebene könnten bei Anschluss der Systeme an die I/O-Ports über die I/O-Leitungen Signale in die I/O-Register eingespielt werden oder es könnten Ausgangssignale aufgezeichnet werden.

Ist ein Reset-Eingang vorhanden, könnten Angreifende diesen ansteuern und temporär das System außer Betrieb setzen.

2.3. Unzureichende physische Absicherung bei eingebetteten Systemen

Sind eingebettete Systeme physisch leicht zugänglich, könnten Angreifende die Systeme zerstören oder beschädigen, z. B. durch mechanische Gewalt, Kurzschlüsse oder Überspannungen. Auch könnten sie auf die elektronischen Komponenten zugreifen, z. B. IC-Pins oder Kontaktierungen, und so die elektrischen Signale mit entsprechenden Mess- und Analysewerkzeugen unbemerkt aufzeichnen sowie selbst Signale einspeisen. Gelangen sie in den Besitz eines eingebetteten Systems, können sie mittels physischer Verfahren Daten lesen und manipulieren oder auf nicht sicher gelöschte Daten zugreifen. Das kann dann dazu führen, dass die Vertraulichkeit, Integrität und Verfügbarkeit der auf dem eingebetteten System gespeicherten Informationen verletzt werden.

2.4. Hardwareausfall und Hardwarefehler bei eingebetteten Systemen

Umgebungseinflüsse wie elektromagnetische Interferenz, Temperaturschwankungen, eine instabile Spannungsversorgung, herstellungsbedingte Materialfehler und Fertigungsstreuung können dazu führen, dass eingebettete Systeme ausfallen. Auch ein normaler oder vorzeitiger Verschleiß, der z. B. durch raue Umgebungseinflüsse wie Staub, Sand oder Verschmutzungen entstehen kann, kann einen Ausfall der Systeme zur Folge haben. Auch könnten hierdurch die umgebenden Systeme stark beeinträchtigen werden.

2.5. Einspielen (Flashen) von manipulierten Software-Updates bei eingebetteten Systemen

Viele eingebettete Systeme speichern ihre Software auf Flash-Speichern und EEPROMs und bieten die Möglichkeit, ihre Firmware mit einem Programmiergerät zu aktualisieren, das über eine Datenschnittstelle oder über eine Netzverbindung angeschlossen wird. Darüber können allerdings auch Angreifende manipulierte Software-Updates einspielen und so die Funktion des Systems modifizieren. In der Folge können die ursprünglichen Aufgaben des Systems unterbrochen oder manipuliert werden.

2.6. Seitenkanalangriffe auf eingebettete Kryptosysteme

Angreifende könnten mittels eines Seitenkanalangriffs Verschlüsselungen oder Signaturen brechen, indem sie dazu beobachtbare Eigenschaften der physischen Implementierung eines Kryptosystems ausnutzen. So könnten sie beispielsweise aus dem Energieverbrauch eines Mikroprozessors während kryptographischer Berechnungen Rückschlüsse auf ausgeführte Operationen und auf Schlüssel ziehen. Auch könnten sie Rechenzeitangriffe, mikroarchitekturelle Angriffe oder (semi-) invasive Angriffe durchführen. So konnten Forschende in der Vergangenheit den geheimen Schlüssel eines TLS/SSL-Servers ermitteln, der den Digital Signature Algorithm (DSA) mit Elliptischer Kurven-Kryptografie verwendet. Der Angriff beruhte auf der Tatsache, dass die benötigte Zeit für eine Multiplikation Rückschlüsse auf deren Operanden zulässt.

2.7. Eindringen und Manipulation über die Kommunikationsschnittstelle von eingebetteten Systemen

Eingebettete Systeme sind oft hinsichtlich Codegröße, Zeitverhalten, Energieverbrauch, Kosten sowie Größe und Gewicht eingeschränkt. Sie sind daher häufig nicht mit ausreichenden Sicherheitsfunktionen, wie z. B. starker Kryptografie, ausgestattet. Moderne eingebettete Systeme sind zunehmend durch weitverbreitete Techniken und Protokolle vernetzt und somit potenziell angreifbar.

Bei einem Angriff könnte versucht werden, Daten oder Software auf einem eingebetteten System zu manipulieren, indem versucht wird, die standardmäßig vorgesehenen Kommunikationsschnittstellen und -protokolle für eigene Zwecke zu missbrauchen. Sind z. B. die IP-Kommunikation oder Ethernet-, WLAN-, Bluetooth- und Mobil- oder Digitalfunk-Schnittstellen nicht ausreichend gesichert, können Angreifende Verbindungen übernehmen, Nachrichten fälschen oder in ein System eindringen und Folgeangriffe durchführen. Weiterhin kann ebenso versucht werden, mittels anderer verfügbarer Kommunikationsschnittstellen, z. B. USB-Ports, in das System einzudringen.

2.8. Einsatz gefälschter Komponenten

Im Produktionsprozess oder wenn im Servicefall Komponenten ausgetauscht werden, kann es passieren, dass gefälschte Komponenten in eingebettete Systeme eingebaut werden. Da für viele Bauteile Fälschungen im Umlauf sind, kann dies auch unabsichtlich geschehen. Gefälschte Bauteile arbeiten oft unzuverlässiger als die originalen Bauteile. Hierdurch könnten Funktionen ausfallen oder nur fehlerhaft arbeiten. Angreifende können auch gezielt ein Gerät oder Bauteil entwickeln, das genauso aussieht wie das Original, aber dessen Funktion manipuliert ist. Durch eine derartige Komponente könnten beispielsweise Hintertüren eingebaut, einzelne Funktionen manipuliert oder die Verfügbarkeit eingeschränkt werden.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins SYS.4.3 *Eingebettete Systeme* aufgeführt. Der oder die ISB ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Planende, Beschaffungsstelle, Entwickelnde

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

SYS.4.3.A1 Regelungen zum Umgang mit eingebetteten Systemen (B)

Alle Benutzenden und Administrierende MÜSSEN über Verhaltensregeln und Meldewege bei Ausfällen, Fehlfunktionen oder bei Verdacht auf einen Sicherheitsvorfall informiert sein.

Alle eingebetteten Systeme inklusive Schnittstellen MÜSSEN erfasst werden. Die eingebetteten Systeme MÜSSEN sicher vorkonfiguriert werden. Die vorgenommene Konfiguration SOLLTE dokumentiert sein. Weiterhin SOLLTEN Regelungen festgelegt werden, um die Integrität und Funktionsfähigkeit der eingebetteten Systeme zu testen.

SYS.4.3.A2 Deaktivieren nicht benutzter Schnittstellen und Dienste bei eingebetteten Systemen (B)

Es MUSS sichergestellt werden, dass nur auf benötigte Schnittstellen zugegriffen werden kann. Alle anderen Schnittstellen MÜSSEN deaktiviert werden. Zudem DÜRFEN NUR benötigte Dienste aktiviert sein. Der Zugang zu Anwendungsschnittstellen MUSS durch sichere Authentisierung geschützt sein.

SYS.4.3.A3 Protokollierung sicherheitsrelevanter Ereignisse bei eingebetteten Systemen (B)

Sicherheitsverstöße MÜSSEN protokolliert werden (siehe OPS.1.1.5 *Protokollierung*). Ist eine elektronische Protokollierung nicht oder nur sehr begrenzt realisierbar, SOLLTEN alternative, organisatorische Regelungen geschaffen und umgesetzt werden.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

SYS.4.3.A4 Erstellung von Beschaffungskriterien für eingebettete Systeme (S) [Beschaffungsstelle]

Bevor eingebettete Systeme beschafft werden, SOLLTE eine Anforderungsliste erstellt werden, anhand derer die infrage kommenden Systeme oder Komponenten bewertet werden. Die Anforderungsliste SOLLTE mindestens folgende sicherheitsrelevante Aspekte umfassen:

- Aspekte der materiellen Sicherheit,
- Anforderungen an die Sicherheitseigenschaften der Hardware,
- Anforderungen an die Sicherheitseigenschaften der Software,
- Unterstützung eines Trusted Plattform Module (TPM) durch das Betriebssystem,
- Sicherheitsaspekte der Entwicklungsumgebung sowie
- organisatorische Sicherheitsaspekte.

SYS.4.3.A5 Schutz vor schädigenden Umwelteinflüssen bei eingebetteten Systemen (S) [Entwickelnde, Planende]

Es SOLLTE sichergestellt werden, dass eingebettete Systeme entsprechend ihrer vorgesehenen Einsatzart und des vorgesehenen Einsatzorts angemessen vor schädigenden Umwelteinflüssen geschützt sind. Die Anforderungen hierfür SOLLTEN bereits bei der Planung analysiert werden. Zudem SOLLTE sichergestellt werden, dass die Vorkehrungen, um einzelne Komponenten vor Staub, Hitze, Nässe und Verschmutzung zu schützen, keine Probleme mit den Anforderungen des übergeordneten Systems verursachen.

SYS.4.3.A6 Verhindern von Debugging-Möglichkeiten bei eingebetteten Systemen (S) [Entwickelnde]

Eventuelle Debugging-Möglichkeiten SOLLTEN möglichst vollständig aus eingebetteten Systemen entfernt werden. Wird On-Chip-Debugging genutzt, MUSS sichergestellt werden, dass Debugging-Funktionen nicht unberechtigt genutzt oder aktiviert werden können.

Weiterhin SOLLTE sichergestellt werden, dass keine Eingabeschnittstellen für Testsignale und Messpunkte zum Anschluss von Analysatoren aktiviert und für Unberechtigte nutzbar sind. Zudem SOLLTEN alle Hardware-Debugging-Schnittstellen deaktiviert sein.

SYS.4.3.A7 Hardware-Realisierung von Funktionen eingebetteter Systeme (S) [Entwickelnde, Planende, Beschaffungsstelle]

Werden eingebettete Systeme selbst entwickelt, SOLLTEN bei der Designentscheidung zur Hardware- und Software-Realisierung Sicherheitsaspekte berücksichtigt werden. Auch bei der Entscheidung, eine bestimmte Hardware-Technik zu implementieren, SOLLTEN Sicherheitsaspekte berücksichtigt werden.

SYS.4.3.A8 Einsatz eines sicheren Betriebssystems für eingebettete Systeme (S) [Entwickelnde, Planende, Beschaffungsstelle]

Das eingesetzte Betriebssystem und die Konfiguration des eingebetteten Systems SOLLTEN für den vorgesehenen Betrieb geeignet sein. So SOLLTE das Betriebssystem für die vorgesehene Aufgabe über ausreichende Sicherheitsmechanismen verfügen. Die benötigten Dienste und Funktionen SOLLTEN aktiviert sein. Das Betriebssystem SOLLTE es unterstützen, ein Trusted Plattform Module (TPM) zu nutzen.

SYS.4.3.A9 Einsatz kryptografischer Prozessoren bzw. Koprozessoren bei eingebetteten Systemen (S) [Entwickelnde, Planende, Beschaffungsstelle]

Wird ein zusätzlicher Mikrocontroller für die kryptografischen Berechnungen verwendet, SOLLTE dessen Kommunikation mit dem System-Mikrocontroller ausreichend abgesichert sein. Für das eingebettete System SOLLTEN die nötigen Vertrauensanker realisiert werden. Auch SOLLTE eine Vertrauenskette (Chain of Trust) implementiert sein.

SYS.4.3.A10 Wiederherstellung von eingebetteten Systemen (S)

Eingebettete Systeme SOLLTEN über Rollback-Fähigkeiten verfügen.

SYS.4.3.A11 Sichere Aussonderung eines eingebetteten Systems (S)

Bevor eingebettete Systeme ausgesondert werden, SOLLTEN sämtliche Daten auf dem System sicher gelöscht werden. Ist dies nicht möglich, SOLLTE das System vernichtet werden. Die Löschung oder Vernichtung SOLLTE dokumentiert werden.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

SYS.4.3.A12 Auswahl einer vertrauenswürdigen Lieferungs- und Logistikkette sowie qualifizierte herstellende Institutionen für eingebettete Systeme (H) [Beschaffungsstelle]

Es SOLLTEN in der Logistikkette wirksame Kontrollen durchgeführt werden, sodass sichergestellt ist,

- dass eingebettete Systeme keine manipulierten, gefälschten oder getauschten Komponenten enthalten,
- die Systeme der Spezifikation entsprechen und keine verdeckten Funktionen bei der Herstellung implementiert wurden sowie
- Unbefugte nicht an vertrauliche Informationen über das eingebettete System gelangen können.

Die beteiligten Unternehmen SOLLTEN nachweisbar qualifiziert sein.

SYS.4.3.A13 Einsatz eines zertifizierten Betriebssystems (H) [Entwickelnde, Planende, Beschaffungsstelle]

Das Betriebssystem SOLLTE nach einem anerkannten Standard auf einer angemessenen Stufe evaluiert sein.

SYS.4.3.A14 Abgesicherter und authentisierter Bootprozess bei eingebetteten Systemen (H) [Entwickelnde, Planende, Beschaffungsstelle]

Der Bootprozess eines eingebetteten Systems SOLLTE abgesichert sein, indem der Bootloader die Integrität des Betriebssystems überprüft und es nur dann lädt, wenn es als korrekt eingestuft wurde. Umgekehrt SOLLTE auch das Betriebssystem die Integrität des Bootloaders prüfen.

Es SOLLTE ein mehrstufiges Boot-Konzept mit kryptografisch sicherer Überprüfung der Einzelschritte realisiert werden. Sichere Hardware-Vertrauensanker SOLLTEN verwendet werden. Bei einem ARM-basierten eingebetteten System SOLLTE ARM Secure Boot genutzt werden. Bei einem Unified Extensible Firmware Interface (UEFI) SOLLTE Secure Boot genutzt werden.

SYS.4.3.A15 Speicherschutz bei eingebetteten Systemen (H) [Entwickelnde, Planende, Beschaffungsstelle]

Bereits beim Entwurf eingebetteter Systeme SOLLTEN Speicherschutzmechanismen berücksichtigt werden. Die Art des Speicherschutzes sowie Anzahl und Größe der Schutzräume SOLLTEN für den Einsatzzweck angemessen sein.

SYS.4.3.A16 Tamper-Schutz bei eingebetteten Systemen (H) [Planende]

Für eingebettete Systeme SOLLTE ein Tamper-Schutz-Konzept entwickelt werden. Es SOLLTEN angemessene Mechanismen etabliert werden, die Tamper-Angriffe erkennen, aufzeichnen und verhindern. Schließlich SOLLTEN angemessene Vorgaben etabliert werden, wie auf einen Tamper-Angriff zu reagieren ist.

SYS.4.3.A17 Automatische Überwachung der Baugruppenfunktion (H) [Planende, Beschaffungsstelle]

Sämtliche Baugruppen eines eingebetteten Systems mit erhöhten Anforderungen an die Verfügbarkeit und Integrität SOLLTEN integrierte Selbsttesteinrichtungen (Built-in Self-Test, BIST) besitzen. Tests SOLLTEN während des Einschaltvorgangs sowie in angemessenen zeitlichen Intervallen während des Betriebs die Integrität des Systems prüfen. Soweit möglich, SOLLTEN die Selbsttestfunktionen auch Sicherheitsfunktionen und Sicherheitseigenschaften der Baugruppe überprüfen.

Regelmäßig SOLLTE die Integrität der Speicher und I/O-Komponenten im Rahmen des BIST geprüft werden. Bestehende BIST-Funktionen SOLLTEN, falls möglich, um die erforderlichen Funktionen ergänzt werden.

SYS.4.3.A18 Widerstandsfähigkeit eingebetteter Systeme gegen Seitenkanalangriffe (H) [Entwickelnde, Beschaffungsstelle]

Es SOLLTEN angemessene Vorkehrungen gegen nicht-invasive und (semi-)invasive Seitenkanalangriffe getroffen werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Das BSI gibt in seinem Dokument „ICS-Security-Kompendium - Testempfehlungen und Anforderungen für Herstellende von Komponenten“ Hilfestellungen für den Test der ICS-Komponenten und stellt Maßnahmen vor, um Schwachstellen zu vermeiden und zu erkennen.