prometo
Embedded Systems • IT • Safeguard

System-Design | Hardware | Software

Kombi-Lehrgang: Safety & Security

Kombi-Lehrgang!
Einzigartig in Deutschland!
Safety & Security-Experte

Modul 1 (Grundlagen) > **Funktionale Sicherheit trifft auf IT-Sicherheit**

Modul 2 (Systementwurf) > **Safety & Security Design**

Modul 3 (Software-Entwicklung) > **Sichere Programmierung**

Modul 4 (Hardware- Entwicklung) > **Safety & Security für Hardware-Entwickler**

Safety & Security

Gesetzliche Vorgaben, Wirtschaftlichkeit, Sicherheitskonzepte

prometo
Embedded Systems • IT • Safeguard

- **Für Führungskräfte und System-Entwickler**
- **Für Hardware-Entwickler**
- **Für Software-Entwickler**

Werden Sie Safety und Security-Experte in einem Ausbildungslehrgang!
Wir sind wohl die ersten, die einen geschlossenen und praxisnahen Kurs anbieten.

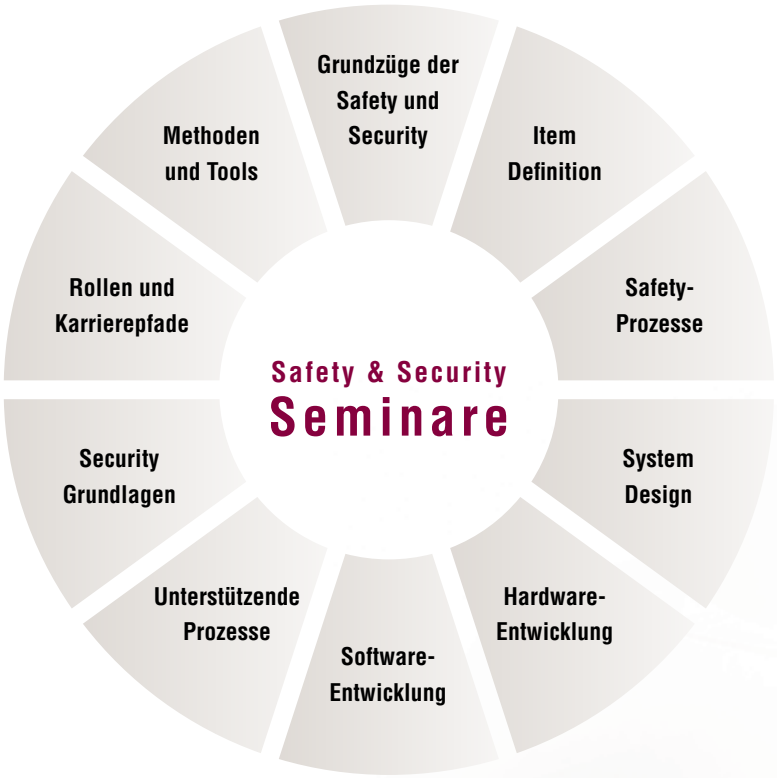
Wenn ein Fahrzeughersteller 1,4 Mio. Autos in die Werkstätten ruft, weil Hacker aus der Ferne die Kontrolle über Bremsen und Lenkung übernehmen können, wird deutlich, dass Hacking eine Bedrohung für Leib und Leben darstellen kann. Folglich gilt es, Produkte in den Markt zu bringen, die eine hohe Funktionssicherheit haben und gleichzeitig genügend Schutz vor Hackern bieten.

Die Seminarreihe richtet sich sowohl an Entwickler als auch an Führungskräfte. Der Schwerpunkt liegt auf bewährten Konstruktionsprinzipien, die funktionale Sicherheit für Leib und Leben bieten und es gleichzeitig Hackern schwer machen, in Systeme einzudringen. Häufig wird die Illusion geweckt, dass Sicherheit mit einer einzigen IEC-, EN- oder ISO-Norm wie der IEC 61508, ISO 26262, EN 50128 o.ä. vollständig beschrieben ist. Tatsächlich kommen in einem Projekt 50 bis 500 unterschiedliche Normen und Vorschriften zum Tragen. Wir schaffen einen Gesamtüberblick und gehen auf industriespezifische Normenaspekte ein.

Funktionssicherheit (Safety) behandelt die Abwehr von Gefahren für Leib und Leben, die von technischen Gegenständen ausgehen. Dem gegenüber ist Security der Grad des Schutzes gegen Beschädigungen, Verlust sowie gegen kriminelle Aktivitäten. Mit der Vernetzung mit dem Internet bleibt die Funktionssicherheit weiterhin die Hauptanforderung an unsere Produkte. Einzig ändert sich das Augenmerk auf den Erhalt der Integrität der Systeme und der Software.

PROMETO bietet ein einzigartiges Kurrikulum an. Es besteht aus 10 Themengebieten, die je nach Erfahrung und geplanter Rolle auf unterschiedliche Trainings-Ausgangsprofile abzielen.

Die 10 Themengebiete unseres Safety- und Security-Kurrikulums:



PROMETO GmbH • Elsener Straße 92-94 • 33102 Paderborn • www.prometo.de • Telefon: 05251 1485160

Seminartermine

prometo
Embedded Systems • IT • Safeguard

Übersicht: Seminarangebot 2017

Unsere Seminare fangen frühestens Montagmittag an, so dass eine Anreise am Montag möglich ist.

Die Veranstaltungen enden spätestens Freitagmittag, so dass eine Abreise am Freitag möglich ist.

Sie schließen den Kombi-Lehrgang mit dem Besuch aller vier Seminare ab. Gerne können Sie die Seminare auch einzeln buchen.

Funktionale Sicherheit trifft auf IT-Sicherheit
Seminar E100

27.-28.03.2017 (Mo. - Di.)
26.-27.06.2017 (Mo. - Di.)
20.-21.11.2017 (Mo. - Di.)

Safety & Security Design
Seminar E170

29.-31.03.2017 (Mi. - Fr.)
28.-30.06.2017 (Mi. - Fr.)
22.-24.11.2017 (Mi. - Fr.)

Sichere Programmierung
Seminar E120

03.-05.04.2017 (Mo. - Mi.)
03.-05.07.2017 (Mo. - Mi.)
27.-29.11.2017 (Mo. - Mi.)

Safety & Security für Hardware-Entwickler
Seminar E130

06.-07.04.2017 (Do. - Fr.)
06.-07.07.2017 (Do. - Fr.)
30.11.-01.12.2017 (Do. - Fr.)

Anreise

Voraussichtliche Reisezeiten nach Paderborn

Hamburg:	3 Stunden mit dem Auto
Hannover:	1,5 Stunden mit dem Auto
Berlin:	3,5 Stunden mit dem Zug
Frankfurt:	3 Stunden mit dem Zug
Stuttgart:	3 Stunden mit dem Flugzeug
München:	1 Stunde mit dem Flugzeug

Funktionale Sicherheit trifft auf IT-Sicherheit

Grundlagen sicherer und vernetzter Produkte

prometo
Embedded Systems • IT • Safeguard

Im Preis inbegriffen:
Schulungsunterlagen, Getränke und Mittagessen sowie Snacks in den Pausen

Herausforderung

Funktionssicherheit (Safety) behandelt die Abwehr von Gefahren für Leib und Leben, die von technischen Gegenständen ausgehen. Traditionell geht die Betrachtung der Safety von geschlossenen Systemgrenzen aus, ohne dass eine Vernetzung mit öffentlichen Netzen (Internet) Berücksichtigung findet. In der Folge tauchte der Begriff der Security überwiegend nur als unbedeutendes Randgebiet bei Safety-Betrachtungen auf. Diese Sichtweise ist heute nicht mehr zeitgemäß, denn 2015 wurden Millionen Fahrzeuge in die Werkstätten zurückgerufen, weil zuvor Hacker die Kontrolle über Bremsen und Lenkungen übernommen haben.

Bei der Vernetzung mit öffentlichen Netzen bleibt die Funktionssicherheit weiterhin die Hauptanforderung an unsere Produkte. Einzig ändert sich das Augenmerk auf den Erhalt der Integrität der Systeme und der Software. Es müssen nicht immer Hacking-Attacken sein, die die Integrität aushebeln. Software-Updates oder das Freischalten von nicht autorisierten Funktionen stellen weitere Herausforderungen an die Integrität dar.

Dieses Seminar bietet Entwicklern, Projektmanagern und Teamleitern einen Einstieg in die Welt der Safety und Security. Dazu gehören Grundlagen, bewährte Konstruktionsprinzipien und Vorgehensweisen der Safety, aber auch detaillierte Einblicke in das Vorgehen der Hacker, die Auslöser für die Rückrufaktionen waren. Die Teilnehmer sehen, wie sie Safety und Security gemeinschaftlich in der Produktentwicklung berücksichtigen können.

Daten & Fakten

Optionen:	Offenes Seminar oder Inhouse-Seminar
Zielgruppe:	Entwickler, Projektleiter, System-Architekten als Einsteiger in die Themen Safety bzw. Security
Dauer:	1,5 Tage
Kosten:	980,00 € zzgl. MwSt.
Anfrage:	www.prometo.de

Inhalte des Seminars

01: Einleitung
- Einführung in die Sicherheit
- Gemeinsamkeiten und Unterschiede der einzelnen Industrien
- Überblick über einige zentrale Gesetze, Normen und Vorschriften

02: Ein kurzer Überblick über die Entstehung sicherheitskritischer Systeme
- Funktionssicherheit auf einen Blick: Risikoanalyse, sichere Zustände und Rückwirkungsfreiheit
- Normative Zielsetzungen für die Produktentstehung

03: Ein kurzer Überblick über die IT-Datensicherheit (Security)
- Prioritätsreihenfolge in der Sicherheit
- Risiken durch Malware, Trojaner, Exploits und zero-day Lücken
- Fehlverhalten von Mitarbeitern

04: Einblick in die Techniken digitaler Einbrüche
- Überblick über das gezielte Vorgehen von Hackern
- Methoden und Werkzeuge zur Informationsbeschaffung
- Durchführung eines Hacks und Spuren verwischen

05: Typische Angriffsvektoren und Risiken
- Direkter Zugang zum Netzwerk (Ethernet, WiFi, CAN etc.)
- Man in the middle-Attacken (Internet, KFZ)
- Software-Schwachstellen (Vulnerabilities)

06: Embedded Software
- Code-Beispiele unsicherer Programmierungen
- Code-Analyse von Malware
- Design-Rules für Secure Software

07: Hardware Analyse von Embedded Devices
- Safety: zufällige Hardware-Ausfälle
- Chip-Plattformen aus Sicht der Safety bzw. Security
- Reverse Engineering Ansätze

08: Technische Lösungsansätze
- Safety und Security by Design
- Segmentierung und Isolation
- Sichere Hardware (TPM, security processor, Lockstep)
- Zertifikate und Schlüsselmanagement
- Sicherheits-Updates über den Lebenszyklus hinaus

Safety & Security Design

Durchdachte Designprozesse entwickeln

prometo
Embedded Systems • IT • Safeguard

Herausforderung

Gute Designprozesse, die von Anfang an auf Sicherheit abzielen, bilden die Basis für wirtschaftlich erfolgreiche Produkte. In diesem Seminar zeigen wir Designprinzipien aus der Safety & Security, die wir zu einem Gesamtwerk kombinieren.

Die Funktionssicherheit (Safety) technischer Systeme verfolgt das Ziel der Eigensicherheit. Damit ist gemeint, dass konstruktionsbedingt nahezu keine Gefährdung für Leib und Leben existiert. In diesem Seminar präsentieren wir die Grundzüge zu den Themen Sicherheitsanforderungen, Sicherheitskonzepte und Design. Die Normen zur Funktionalen Sicherheit beschreiben hierzu bewährte Prinzipien, nach denen die Entwicklung verfahren sollte. Diese bilden die Grundlage dieses Seminars.

Auf den Grundlagen aufbauend zeigen wir die Erweiterung um Security. Dabei geht es um den Schutz vor den Angriffen von Hackern und Datendieben. Folglich ist diese Erweiterung immer dann notwendig, wenn funktionssichere Geräte mit öffentlichen Netzen verbunden werden. Beispiele hierfür sind Autos mit Internetzugang aber auch Maschinen, die per Fernwartung überwacht werden.

Das Beispiel Auto steht stellvertretend für die funktionale Veränderung, die auch unser Sicherheits-Design beeinflusst. Die Prinzipien lassen sich leicht auf andere Maschinen und Anlagen übertragen. Die Systemgrenze Auto in frühen Tagen war das Auto selbst. Erst vor wenigen vergangenen Jahren wurde es beispielsweise möglich, die Klimatisierung per Smartphone-App zu regeln oder die Türen zu verriegeln. Das führte dazu, dass die Systemgrenze sich ausdehnte auf die IT-Systeme des Fahrzeugherstellers sowie auf eine Vielzahl von Mobilgeräten, die sich einer Integritätskontrolle des Fahrzeugherstellers entziehen. Zukünftig tauschen Fahrzeuge untereinander und mit der Straße selbst Informationen aus, so dass ein sicherer Weg auch bei schlechtem Wetter und ein schnelles Vorankommen im dichten Verkehr gewährleistet wird.

In diesem Seminar gehen wir ausführlich auf die gesamte Wirkkette zwischen dem Gerät (Auto, Maschine), öffentlichen Netzwerken, IT-Systemen und Endgeräten ein. Wir zeigen das Zusammenwirken dieser Elemente und gehen dann im Detail auf die Besonderheiten der einzelnen Elemente ein. Neben den funktionalen Aspekten greift das Seminar auch den Aspekt der Lebenszyklen der einzelnen Elementen auf, denn das Design muss ein Lebenszyklus eines Smartphones von 2 Jahren mit dem Lebenszyklus des Autos oder der Anlage von 15 Jahren übereinander bringen. Hierin liegt eine besondere Herausforderung, nicht nur in Hinblick auf die IT-Sicherheit und die hierfür erforderlichen Updates.

Daten & Fakten

Optionen:	Offenes Seminar
Zielgruppe:	System-Architekten, Prozess-Experten, Safety Manager bzw. Assessoren, Projektleiter
Vorkenntnisse:	Ausgeprägte Kenntnisse im Bereich Produktentstehung
Dauer:	2,5 Tage
Kosten:	1.980,00 € zzgl. MwSt.
Anfrage:	www.prometo.de

Detaillierte Inhalte des Seminars auf der folgenden Seite

Safety & Security Design

Durchdachte Designprozesse entwickeln

prometo
Embedded Systems • IT • Safeguard

Im Preis inbegriffen:
Tablet, Schulungsunterlagen, Getränke und Mittagessen sowie Snacks in den Pausen

Inhalte des Seminars

Tag 1: Safety

01: Einleitung
- Einführung in die Sicherheit
- Gemeinsamkeiten und Unterschiede der einzelnen Industrien
- Überblick über einige zentrale Gesetze, Normen und Vorschriften

02: Entstehung sicherheitskritischer Systeme
- Normative Zielsetzungen für die Produktentstehung
- Gefahren- und Risikoanalyse
- Sichere Zustände und Rückwirkungsfreiheit
- Sicherheitsanforderungen
- Sicherheitskonzepte
- Hardware- und Softwareentwicklung

03: Designelemente für sicherheitsgerichtete Systeme
- Aufbau von Wirkketten
- Zeitliche Abläufe
- System Basic Chips
- Lockstep und Safety Units
- ECC Speicherschutz

Tag 2: Security

04: Ein kurzer Überblick über die IT-Datensicherheit (Security)
- Prioritätsreihenfolge in der Sicherheit
- Malware, Trojaner, Exploits und zero-day Lücken kurz erklärt
- Überblick über das gezielte Vorgehen von Hackern
- Fehlverhalten von Mitarbeitern

05: Typische Angriffsvektoren und Risiken
- Direkter Zugang zum Netzwerk (Ethernet, WiFi, CAN etc.)
- Hacks über das User Interface
- Man in the middle-Attacken (Internet, KFZ)
- Software-Schwachstellen (Vulnerabilities)

06: Hardware Hacking von Embedded Devices
- Ziel: Kontrolle übernehmen
- Hardware-Analyse
- Debug- und Programmierschnittstellen
- Speicher auslesen
- Software reverse engineering
- Netzwerk-Analyse

07: Hacking von PCs und Mobilgeräten
- Ziel 1: Identitäten der Eigentümer übernehmen
- Ziel 2: Informationen beschaffen
- Hacking von PCs
- Hacking von Mobil-Geräten
- Hacking mit Mobil-Geräten

Tag 3: Design-Regeln Safety & Security

08: Betrachtung des Lebenszyklus des Gerätes
- Gerätelebenszyklus
- Sicherheitsupdates
- Lebenszyklus von elektronischen Bauteilen

09: Anti-Tamper
- Hardware fälschungssicherer gestalten
- Speicher vor Auslesen schützen
- Debug- und Programmier-Schnittstellen vermeiden

10: Verschlüsselung von Speichern
- Schlüssel und Zertifikate
- Crypto-Chips
- Secure Boot bei Embedded-Systemen

11: Kommunikation
- Netzwerk-Topologien aus Sicht der Sicherheit
- Verschlüsselung der Netzwerk-Verbindungen
- Authentifikation des Senders

12: Mobilgeräte, PCs und Cloud-Services
- Passwortsicherheit
- Schutz des Speichers
- Verhindern von Überbrückungen
- Zwei-Faktor-Authentifizierung

13: Modellbasierte Entwurfstechniken
- SysML / UML
- Timing-Modelle
- Modellierung menschlichen Verhaltens

Sichere Programmierung

Prinzipien und Stolperfallen

prometo
Embedded Systems • IT • Safeguard

Herausforderung

Wenn Sie Software für Geräte entwickeln, die sicherheitskritisch sind und sich ggf. mit dem Internet verbinden, dann unterstützt Sie dieses Seminar bei der Erkennung und Behebung von Sicherheitslücken. Neben Safety-Aspekten geben wir auch einen Einblick in die Taktiken von Hackern. Programmieren und auch Hacken lernt man nicht alleine mit Theorie, sondern mit viel Praxis. Aber was genau macht Funktionssicherheit aus und wie genau funktioniert die Magie der Hacker?

Es gibt Sicherheitslücken in nahezu jeder Software, die uns umgibt und von dem unser Leben täglich abhängig ist. Während sich Sicherheitslücken im Sinne der Safety durch zufällige Ausfälle offenbaren, warten die Sicherheitslücken im Sinne der Security nur darauf, von Hackern entdeckt zu werden. Ob sie ausgenutzt oder nur geschlossen werden, hängt von menschlichen Faktoren ab.

Hacker sind innovative Geister und haben tiefgreifende Kenntnisse der Technologie. Sie sind Meister darin, Sicherheitslücken zu finden. Folglich müssen wir uns in diesem Seminar mit der durchaus aufwändigen Suche nach Sicherheitslücken beschäftigen. Neben Reverse-Engineering-Techniken sehen wir aber auch viele andere Ansätze der Informationsbeschaffung.

Der Satz „Software funktioniert genau so, wie sie programmiert wurde“ ist ein zentraler Satz, denn wir müssen zwischen dem tatsächlichen Verhalten und dem beabsichtigten Verhalten der Software unterscheiden. Oft übersehen Programmierer, dass ihre Software anders verwendet werden könnte als eigentlich vorgesehen. Hacker als innovative Geister verwenden gezielt Software anders als eigentlich gewollt. Eine Sicherheitslücke ist dann entdeckt, wenn Hacker zeigen, wie sie diesen Umstand ausnutzen.

Security lässt sich in drei Bereiche zusammenfassen: Programmierung, Vernetzung, Kryptographie. Eine Entsprechung in der Safety lautet: Programmierung, Dissimilarität, Determinismus. Das, was auf den ersten Blick wie zwei unterschiedliche Welten zu sein scheint, entpuppt sich in Wirklichkeit als eine Zweckgemeinschaft, die sich gegenseitig stützt. Daher geht es im Seminar auch um die Synergien zwischen Safety und Security.

Skriptkiddies versuchen trotz mangelnder Grundlagenkenntnisse in fremde Computersysteme einzudringen. Der Hauptunterschied zwischen einem Skriptkiddie und einem Hacker liegt darin, dass der eine lediglich die Werkzeuge anderer Leute einsetzt und der andere die passenden Werkzeuge selbst programmiert. Wir werden uns daher auch intensiv mit der Programmierung von Werkzeugen beschäftigen. Das hört sich komplizierter an als es ist. Es gibt gute Frameworks, mit dessen Hilfe und etwas Python sich schnell wirkungsvolle Werkzeuge bauen lassen.

Inhalte des Seminars auf der folgenden Seite:

Daten & Fakten

Optionen:	Offenes Seminar oder Inhouse-Seminar
Zielgruppe:	Software-Entwickler, System-Architekten, Safety Manager bzw. Assessoren, Projektleiter
Vorkenntnisse:	Programmierkenntnisse
Dauer:	2,5 Tage
Kosten:	1.980,00 € zzgl. MwSt.
Anfrage:	www.prometo.de

Im Seminar ist ein Laptop für jeden Teilnehmer inklusive!

PROMETO GmbH • Elsener Straße 92-94 • 33102 Paderborn • www.prometo.de • Telefon: 05251 1485160

Sichere Programmierung

Prinzipien und Stolperfallen

prometo
Embedded Systems • IT • Safeguard

Im Preis inbegriffen:
Hackbook, Schulungsunterlagen, Getränke und Mittagessen sowie Snacks in den Pausen

Inhalte des Seminars

Tag 1: Schwerpunkt Safety

01: Einleitung
- Illusion sicherer Software
- Einführung in die Sicherheit
- Gemeinsamkeiten und Unterschiede der einzelnen Industrien
- Überblick über einige zentrale Gesetze, Normen und Vorschriften

02: Lebenszyklus sicherheitskritischer Systeme
- Funktionssicherheit auf einen Blick: Risikoanalyse, sichere Zustände und Rückwirkungsfreiheit
- Normative Zielsetzungen für die Produktentstehung
- Systementwurf sicherheitskritischer Systeme
- Realisierung in Hardware und Software
- Aspekte in Hinblick auf die Fertigung
- Betrieb, Service und Entsorgung

03: Software-Entwicklung sicherheitskritischer Systeme
- Ziel: Rückwirkungsfreiheit
- Einfluss der Safety Integrity Level (SIL bzw. ASIL) auf die Methoden der Entwicklung
- Bewährte Methoden und zweifelhafte Forderungen entlang des V-Modells
- Nutzen von Code-Analysen (MISRA etc.)

04: Die Brücke zwischen Safety und Security
- Bei Hackern beliebte Fehler der Entwickler
- Safety: Zahlenüberläufe und Security: Buffer-Overflow
- Safety: Grenzwertbetrachtungen und Security: Fencepost error

Tag 2: Schwerpunkt Security

05: Überblick über die IT-Security
- Prioritätsreihenfolge in der Sicherheit
- IT und industrielle Systeme: Gemeinsamkeiten und Unterschiede
- Erfolgreiche Attacken auf technische Einrichtungen
- Tätergruppen organisierte Kriminalität, Geheimdienste und Innentäter
- Risiken durch Malware, Trojaner, Exploits und zero-day Lücken
- Fehlverhalten von Mitarbeitern
- Statistiken und finanzielle Schadensbilanzen

06: Die Magie der Hacker entmystifiziert
- Überblick über das gezielte Vorgehen von Hackern
- Methoden und Werkzeuge zur Informationsbeschaffung
- Durchführung eines Hacks und Spuren verwischen
- Automotive Hacking
- Hacking von IoT (Haushaltsgeräte, Beleuchtung etc.)

07: Netzwerk-Sicherheit
- CAN Netzwerke analysieren
- CAN Netzwerke gezielt kompromittieren
- Man in the middle-Attacken auf Ethernet
- WLAN-Hacking

08: Passwort-Sicherheit
- Techniken zum Gewinnen von Passwörtern
- Passwort-Sicherheit
- Techniken zum Umgehen von Passwörtern
- Verschlüsselung von Daten
- Daten entschlüsseln

09: Hardware Analyse von Embedded Devices
- Chip-Plattform aus Sicht der Safety bzw. Security
- Reverse Engineering Ansätze
- Embedded Speicher auslesen

Tag 3: Realisierung sicherer Software und Systeme

10: Safety und Security by Design
- Segmentierung
- Isolation
- Sichere Zustände für Safety und Security
- Sichere Hardware

11: Entwurfsregeln sicherer Software
- Verzahnung zwischen Hardware und Software
- Trusted Zones
- Gestaltung Software Design Guide
- Gestaltung Code-Styleguide
- Safety und Vulnerability Assessment

12: Organisatorische Maßnahmen
- Notfallpläne
- Qualifizierung für Mitarbeiter

13: Capture the flag
- Sie erhalten einen Prototyp und sind aufgefordert, die Sicherheit dieses Embedded Systems zu beurteilen

Safety & Security für Hardware-Entwickler

Grundlagen sicherer und vernetzter Produkte

prometo
Embedded Systems • IT • Safeguard

Im Preis inbegriffen:
Schulungsunterlagen, Getränke und Mittagessen sowie Snacks in den Pausen

Herausforderung

Hacker haben gezeigt, wie sie die Kontrolle über Bremsen und Lenkung von Autos übernehmen, einen Hochofen zerstören oder gar gezielt die Ausbeute von Produktionsanlagen beeinflussen. Für die Hersteller und Betreiber sind diese Ereignisse mehr als ärgerlich, denn zusätzlich zu den finanziellen Folgen sind die juristischen Konsequenzen und der Imageverlust nicht zu unterschätzen.

Dabei kann gerade die Hardware einen entscheidenden Beitrag zur Systemsicherheit leisten. Wir zeigen die klassischen Elemente der Funktionssicherheit und erweitern diese um Hardware-Security-Elemente. Für Kunden bedeutet Sicherheit der Schutz vor Manipulation oder anderen kriminellen Aktivitäten. Für Hersteller bedeutet Sicherheit der Schutz des geistigen Eigentums und Geschäftsmodelle. Anhand vieler Beispiele und Übungen zeigen wir Wege, wie Unternehmen ihren Schutz stärken können.

Dieses Seminar führt zunächst in den Entwurf sicherheitskritischer Hardware ein. Im zweiten Schritt zeigen wir das Vorgehen der Hacker und Datendiebe und gehen dabei insbesondere auf den Hardware-Teardown ein. Dabei geht es um die genaue Analyse einer Hardware, so dass sowohl der Aufbau genauestens bekannt ist, als auch Zugänge über CAN, Ethernet oder andere Bussysteme sowie über Debug-Schnittstellen geschaffen werden. Daraus werden mögliche Abwehrmaßnahmen zum Erhalt der Sicherheit und zum Schutz des geistigen Eigentums abgeleitet. Im Mittelpunkt steht das Kraftfahrzeug. Wir übertragen die Erkenntnisse auch auf IoT und industrielle Anwendungen.

Daten & Fakten

Optionen:	Offenes Seminar
Zielgruppe:	Hardware-Entwickler System-Ingenieure
Grundlagen:	Hardware-Entwicklung
Dauer:	1,5 Tage
Kosten:	980,00 € zzgl. MwSt.
Anfrage:	www.prometo.de

Inhalte des Seminars

01: Einleitung
- Illusion sicherer Hardware
- Wertschöpfung durch Hacking
- Problem eines langen Lebenszyklus
- Risikoquelle Remote Access
- Rechtliche Aspekte

02: Ein kurzer Überblick über die Entstehung sicherheitskritischer Systeme
- Funktionssicherheit auf einen Blick: Risikoanalyse, sichere Zustände und Rückwirkungsfreiheit
- Normative Zielsetzungen für die Produktentstehung
- Gemeinsamkeiten und Unterschiede der einzelnen Industrien
- Überblick über einige zentrale Gesetze, Normen und Vorschriften in der Hardware-Entwicklung

03: Anwendung der Normen - Beispiel ISO 26262
- Inhalt der Norm ISO 26262-Teil 5
- Hürden bei der Anwendung in der Praxis
- Zusätzlich notwendige Normen und Vorschriften
- Durchführung von Safety-Projekten
- Hardware-Safety-Anforderungen

04: Hardware-Entwicklung
- Hardware-Software-Interface Spezifikation
- Hardware Design
- FMEA
- FMEDA
- FTA
- Hardware Integration und Test

05: Crashkurs Hacking
- Prioritätsreihenfolge in der Sicherheit von Büro-IT gegenüber industriellen Anlagen und IoT
- Überblick über das gezielte Vorgehen von Hackern
- Menschliche Faktoren Illusion / Ignoranz / Irrglaube
- Methoden und Werkzeuge zur Informationsbeschaffung
- Bussysteme und andere Zugänge zum Zielsystem

06: Hardware Analyse von Embedded Devices
- Safety: zufällige Hardware-Ausfälle
- Chip-Plattformen aus Sicht der Safety bzw. Security
- Reverse Engineering Ansätze

07: Technische Lösungsansätze
- Safety und Security by Design
- Segmentierung und Isolation
- Sichere Hardware (TPM, security processor, Lockstep)
- Zertifikate und Schlüsselmanagement
- Sicherheits-Updates über den Lebenszyklus hinaus

Anmeldung Seminare 2017*

prometo
Embedded Systems • IT • Safeguard

Was können wir für Sie tun?

SENDEN

Vorname:		Name:	
Firma:		Abteilung:	
Straße:		PLZ/Ort:	
Telefon:		E-Mail:	

Ihre Seminartermine: Bitte tragen Sie je Seminar nur einen Termin ein.

Funktionale Sicherheit trifft auf IT-Sicherheit
Seminar E100

- ☐ 27.-28.03.2017 (Mo. - Di.)
- ☐ 26.-27.06.2017 (Mo. - Di.)
- ☐ 20.-21.11.2017 (Mo. - Di.)
- ☐ Anfrage Inhouse-Schulung, bitte kontaktieren Sie uns.

Safety & Security Design
Seminar E170

- ☐ 29.-31.03.2017 (Mi. - Fr.)
- ☐ 28.-30.06.2017 (Mi. - Fr.)
- ☐ 22.-24.11.2017 (Mi. - Fr.)
- ☐ Anfrage Inhouse-Schulung, bitte kontaktieren Sie uns.

Sichere Programmierung
Seminar E120

- ☐ 03.-05.04.2017 (Mo. - Mi.)
- ☐ 03.-05.07.2017 (Mo. - Mi.)
- ☐ 27.-29.11.2017 (Mo. - Mi.)
- ☐ Anfrage Inhouse-Schulung, bitte kontaktieren Sie uns.

Safety & Security für Hardware-Entwickler
Seminar E130

- ☐ 06.-07.04.2017 (Do. - Fr.)
- ☐ 06.-07.07.2017 (Do. - Fr.)
- ☐ 30.11.-01.12.2017 (Do. - Fr.)
- ☐ Anfrage Inhouse-Schulung, bitte kontaktieren Sie uns.

☐ **Hiermit widerrufe(n) ich/wir den von mir/uns abgeschlossenen Vertrag über die Teilnahme an der Veranstaltung/ den Veranstaltungen:**

Seminarnummer(n): Veranstaltungstermin(e):

☐ Ich erkenne / wir erkennen die AGB der PROMETO GmbH an. Ferner erkläre ich mich / erklären wir uns einverstanden, dass meine / unsere oben gemachten persönlichen Daten für die Veranstaltungsorganisation elektronisch verarbeitet und gespeichert werden dürfen.

☐ Ich möchte gerne zukünftig per E-Mail über Seminare, Veranstaltungen und sonstige Angebote informiert werden. Diese Einverständniserklärung kann jederzeit schriftlich widerrufen werden.

PROMETO GmbH • Elsener Straße 92-94 • 33102 Paderborn • www.prometo.de • Telefon: 05251 1485160

* Bei gleichzeitiger Buchung aller 4 Seminare erhalten Sie ein 1,5 Tagesseminar gratis!

Allgemeine Geschäftsbedingungen der PROMETO GmbH (Stand 04.09.2015)

1. Geltungsbereich

Die folgenden Allgemeinen Geschäftsbedingungen regeln alle Vertragsverhältnisse, die zwischen dem Teilnehmer an Konferenzen, Kursen und Seminaren (im Folgenden „Veranstaltung" genannt) und der PROMETO GmbH (im Folgenden „PROMETO" genannt) zustande kommen können.

Abweichende Allgemeine Geschäftsbedingungen des Teilnehmers haben keine Gültigkeit.

2. Anmeldung/Anmeldebestätigung

Die Anmeldung kann über Internet, Brief, Telefax, E-Mail oder telefonisch erfolgen.

Die Anmeldung wird erst durch unsere schriftliche Bestätigung, welche ebenfalls über Internet, Brief, Telefax oder E-Mail erfolgen kann, rechtsverbindlich.

3. Teilnahmebeitrag

Der Teilnahmebetrag versteht sich pro Person und Veranstaltungstermin zzgl. gesetzlicher Umsatzsteuer.

Er beinhaltet Tagungsunterlagen, die nach Wahl von PROMETO digital oder in Papierform zur Verfügung gestellt werden. Darüber hinaus gehende Leistungen werden gesondert zu den jeweiligen Veranstaltungen genannt.

4. Fälligkeit und Zahlung, Aufrechnung

Der Teilnahmebetrag ist bei Erhalt der Rechnung fällig und innerhalb von 10 Tagen nach Erhalt der Rechnung auf das Konto von PROMETO zu zahlen.

Eine Aufrechnung mit einer Forderung des Teilnehmers ist nur zulässig, wenn PROMETO die Forderung schriftlich anerkannt hat, oder diese rechtskräftig gerichtlich festgestellt wurde.

5. Leistung

PROMETO bemüht sich, einen reibungslosen Ablauf der Veranstaltung zu organisieren. Hierfür verpflichtet sich PROMETO, bei eventuell auftretenden Störungen der Veranstaltung, alles Zumutbare zu unternehmen, um zu einer Behebung oder Begrenzung der Störung beizutragen.

PROMETO behält sich vor, angekündigte Referenten durch andere zu ersetzen und notwendige Änderungen des Veranstaltungsprogramms unter Wahrung des Gesamtcharakters derselben vorzunehmen.

Ist die Durchführung der Veranstaltung aufgrund höherer Gewalt, wegen Verhinderung eines Referenten, wegen Störungen am Veranstaltungsort oder aufgrund zu geringer Teilnehmerzahl nicht möglich, werden die Teilnehmer umgehend informiert. Die Absage wegen zu geringer Teilnehmerzahl erfolgt nicht später als zwei Wochen vor der Veranstaltung. Die Veranstaltungsgebühr wird in diesen Fällen erstattet.

6. Stornierung

Eine Stornierung ist bis 30 Kalendertage vor Veranstaltungsbeginn kostenlos möglich; danach wird die Hälfte des Teilnahmebetrages erhoben.

Die Stornierung muss schriftlich erfolgen.

Bei Nichterscheinen oder Stornierung am Veranstaltungstag ist der gesamte Teilnahmebetrag zu zahlen.

PROMETO akzeptiert, ohne zusätzliche Kosten zu erheben, die Stellung eines Ersatzteilnehmers.

7. Urheberrechte

Sämtliche Tagungsunterlagen sind urheberrechtlich geschützt. Eine Vervielfältigung, Weitergabe oder anderweitige Nutzung ist nur mit ausdrücklicher schriftlicher Zustimmung von PROMETO gestattet.

8. Haftung

Die Inhalte der Veranstaltungen werden von qualifizierten Referenten sorgfältig vorbereitet und durchgeführt und unterliegen der alleinigen Verantwortung der Referenten. PROMETO übernimmt keine Haftung für die Aktualität, Richtigkeit und Vollständigkeit in Bezug auf die Tagungsunterlagen und die Durchführung der Veranstaltung.

Im Falle des Ausfalls der Veranstaltung nach Punkt 5 haftet PROMETO nicht. Insbesondere ist ein Anspruch auf Ersatz von Reise- und Übernachtungskosten sowie Arbeitsausfall ausgeschlossen. Dies gilt nicht, wenn solche Kosten aufgrund grob fahrlässigen oder vorsätzlichen Verhaltens seitens PROMETO entstehen.

9. Widerrufsrecht

Widerrufsbelehrung:

Widerrufsrecht

Sie haben das Recht, binnen vierzehn Tagen ohne Angabe von Gründen diesen Vertrag zu widerrufen. Die Widerrufsfrist beträgt vierzehn Tage ab dem Tag des Vertragsabschlusses. Um Ihr Widerrufsrecht auszuüben, müssen Sie uns (PROMETO GmbH, Geschäftsführer: Jürgen Belz, Elsener Str. 92-94, 33102 Paderborn; info@prometo.de; Fax: 05251 / 148 51 61) mittels einer eindeutigen Erklärung (z.B. ein mit der Post versandter Brief, Telefax oder E-Mail) über Ihren Entschluss, diesen Vertrag zu widerrufen, informieren.

Sie können dafür das beigefügte Muster-Widerrufsformular verwenden, das jedoch nicht vorgeschrieben ist. Zur Wahrung der Widerrufsfrist reicht es aus, dass Sie die Mitteilung über die Ausübung des Widerrufsrechts vor Ablauf der Widerrufsfrist absenden.

Folgen des Widerrufs

Wenn Sie diesen Vertrag widerrufen, haben wir Ihnen alle Zahlungen, die wir von Ihnen erhalten haben, einschließlich der Lieferkosten (mit Ausnahme der zusätzlichen Kosten, die sich daraus ergeben, dass Sie eine andere Art der Lieferung als die von uns angebotene, günstigste Standardlieferung gewählt haben), unverzüglich und spätestens binnen vierzehn Tagen ab dem Tag zurückzuzahlen, an dem die Mitteilung über Ihren Widerruf dieses Vertrags bei uns eingegangen ist. Für diese Rückzahlung verwenden wir dasselbe Zahlungsmittel, das Sie bei der ursprünglichen Transaktion eingesetzt haben, es sei denn, mit Ihnen wurde ausdrücklich etwas anderes vereinbart; in keinem Fall werden Ihnen wegen dieser Rückzahlung Entgelte berechnet.

Besondere Hinweise:

Ihr Widerrufsrecht erlischt vorzeitig, wenn der Vertrag von beiden Seiten auf Ihren ausdrücklichen Wunsch vollständig erfüllt ist, bevor Sie Ihr Widerrufsrecht ausgeübt haben.

Ende der Widerrufsbelehrung

10. Datenschutz

PROMETO bemüht sich um größtmöglichen Schutz Ihrer personenbezogenen Daten und sichert zu, die vom Besteller überlassenen Daten vertraulich zu behandeln.

Die Daten werden, sowohl zum Zweck der Durchführung unserer Leistungen als auch für die Möglichkeit, Ihnen postalisch und per E-Mail Informationen zukommen zu lassen, gespeichert.

Soweit sich die Teilnehmer nicht dagegen aussprechen, sind diese mit der Zusendung von Information zu Angebote von uns und unseren Partnerunternehmen, die den vorher von Ihnen genutzten Leistungen ähnlich sind, einverstanden. Bei der Erhebung der Daten fragt PROMETO nach Ihrer Einwilligung, ob PROMETO Sie über verschiedenste Angebote von sich und von Partnerunternehmen per E-Mail informieren darf. Sie können der Nutzung Ihrer Daten für Zwecke der Werbung oder der Ansprache per E-Mail oder per Post jederzeit gegenüber der PROMETO widersprechen.

Das Internet ist für eine Vertraulichkeit des Nachrichteninhalts ohne Verschlüsselung ungeeignet. Wir gehen davon aus, dass wir Ihre unverschlüsselte Anfrage auch unverschlüsselt beantworten dürfen und können.

11. Schlussbestimmungen

Änderungen und Ergänzungen dieser Bedingungen bedürfen der Schriftform. Dies gilt auch für die Aufhebung des Schriftformerfordernisses.

Sollte eine oder mehrere Bestimmung/en dieses Vertrages ganz oder teilweise rechtsunwirksam sein, so wird dadurch die Gültigkeit der übrigen Bestimmungen nicht berührt. An die Stelle der unwirksamen Bestimmungen tritt rückwirkend eine inhaltlich, möglichst gleiche Regelung, die dem Zweck der gewollten Regelung am nächsten kommt.

Es gilt ausschließlich das Recht der Bundesrepublik Deutschland. Soweit Sie in Ausübung Ihrer gewerblichen oder selbstständigen Tätigkeit handeln, wird als Erfüllungsort und Gerichtsstand Paderborn vereinbart. Die Vertragssprache ist Deutsch.

PROMETO:
Sicherheit und Kollaboration

Unser Leistungsspektrum

prometo
Embedded Systems • IT • Safeguard

Wir, die PROMETO GmbH, arbeiten seit vielen Jahren in den Entwicklungs- und IT-Abteilungen namhafter Hersteller von elektronischen und mechatronischen Systemen und bringen dort Prozesse, Methoden und Tools ein. Unsere Stärke liegt darin, wirtschaftlich sinnvolle Lösungen mit Kunden zu erarbeiten. Dabei sindwir sehr gewandt darin, unterschiedliche oder auch konträre Interessen aufzulösen, um ein gemeinsames Ziel zu erreichen. Auch sind wir sehr erfahren darin, neue Technologien in Unternehmen einzubringen.

→ Unser Wertangebot ›Safety & Security‹

Etliche Führungskräfte und sehr viele Entwickler sind nicht sonderlich mit Sicherheit vertraut. Wir zeigen sehr praxisnah, wie Hacker Autos aus der Ferne übernehmen und in die Netzwerke von Unternehmen, Fertigungsanlagen oder von Privatpersonen eindringen.

Wir bieten Know-how in Form von Beratung und Seminaren und liefern Werkzeuge zur Überprüfung der Sicherheit. Das ist unser Beitrag zur Sicherheit von Produkten.

→ Unsere Besonderheiten

Unsere Kunden schätzen vor allem unsere extreme Praxisnähe, also den Blick für das Erforderliche und wirtschaftlich Machbare.

Gegenüber unseren Wettbewerbern erscheinen wir deshalb pragmatisch und zielführend, weil wir geschickt Safety mit Security sowie technische Realisierung mit normativen und juristischen Aspekten kombinieren.

→ Ihr Nutzen

Mit unseren Beratungsleistungen bringen wir gezielt das Thema Sicherheit in die Entwicklung elektronischer Systeme und den Betrieb von IT ein. Als Kunde bekommen Sie das noch fehlende Know-how schnell und kostengünstig.

Die Teilnehmer an unseren Seminaren verfeinern ihre Fertigkeiten durch eine Vielzahl von Praxisbeispielen. So können Entwickler sichere Produkte entwickeln und Manager ihre persönlichen Haftungsrisiken senken. Unsere Software und Hardware sind praxiserprobt sowie schnell und ohne großen Aufwand einsetzbar.

Fakten zu Industrie 4.0 – Autoelektronik – Smart Home – Internet of Things

1. Diese Begriffe sind vor allem Inbegriff für massive Veränderung von Kundenbedürfnissen und Geschäftsmodellen
2. Kern der Veränderung ist die Vernetzung von mobilen Geräten und Fabriken mit dem Internet, um eine einfache und komfortable Art des Umgangs mit den individuellen Bedürfnissen der Kunden zu schaffen
3. Verbraucher wie Unternehmen werden beharrlich die Benutzerfreundlichkeit der Sicherheit vorziehen
4. Fehlende Sicherheit bei den Produkten sorgt für immense Kosten und Image-Verluste
5. Hacken hat sich vom Kiddie-Zeitvertreib zum industriell betriebenen Geschäft gewandelt
6. Die vernetzte Welt eröffnet neue Angriffsmöglichkeiten, denn die Systeme bieten hohe Rechenleistung und ständige Verfügbarkeit im Internet bei vergleichsweise geringem Schutz

PROMETO GmbH • Elsener Straße 92-94 • 33102 Paderborn • www.prometo.de • Telefon: 05251 1485160