Sicherheits-Vorkehrungen

Teilsicherheitskonzept – CONBOTICS MalerRoboter

Inhalt

Einleitung

Das Testen der Schnittstellen eines Cobots (kollaborativer Roboter) ist ein Hochrisiko-Unterfangen, da du direkt in die Steuerungs- und Sicherheitslogik eingreifst. Normale IT-Sicherheitstests reichen hier nicht aus, da ein Fehler nicht nur zu einem Datenverlust, sondern zu unkontrollierten Bewegungen und damit zu einer ernsten Gefahr für Personen und Ausrüstung führen kann.

Hier sind die essenziellen Sicherheitsvorkehrungen, gegliedert in organisatorische, physische und systemtechnische Maßnahmen.

A. Organisatorische Sicherheitsvorkehrungen (Vor Beginn der Tests)

Noch bevor ein Kabel eingesteckt wird, muss die Basis stimmen.

1. Schriftliche Freigabe und Verantwortlichkeit:

- **Holen Sie eine ausdrückliche, schriftliche Freigabe von der Betriebsleitung oder dem Systemverantwortlichen ein.**
- **Definieren Sie klar, wer für die Tests verantwortlich ist und wer die Tests durchführt.**

2. Detaillierte Risikobewertung (Das Wichtigste!):

- **Führen Sie für jeden geplanten Test eine Risikobewertung durch. Fragen Sie sich: "Was ist das schlimmstmögliche Szenario?"**
  - **Beispiel USB-Test: "Ein BadUSB-Angriff injiziert einen Befehl, der eine maximale, unkontrollierte Achsenbewegung auslöst."**
  - **Beispiel CAN-Test: "Ein Denial-of-Service-Angriff auf den CAN-Bus legt den Controller für den Not-Aus lahm."**
- **Bewerten Sie die Wahrscheinlichkeit und das mögliche Schadensausmaß.**

3. Benennung eines Sicherheitsverantwortlichen:

- **Bestimmen Sie eine Person, deren einzige Aufgabe während des gesamten Tests darin besteht, den Cobot zu beobachten und im**

Notfall sofort den Not-Aus zu betätigen. Diese Person führt keine Tests durch.

4. Studium der Dokumentation:

- **Lesen Sie das Handbuch des Cobot-Herstellers, insbesondere die Kapitel zu Sicherheit, Not-Aus-Kreisen und den Schnittstellen.**
- **Machen Sie sich mit der Position aller Not-Aus-Schalter vertraut (am Teach Pendant, am Schaltschrank etc.).**

5. Erstellung eines detaillierten Testplans:

- **Arbeiten Sie nicht improvisiert. Erstellen Sie einen schriftlichen Plan, der genau festlegt, welcher Test wann, wie und mit welchem Ziel durchgeführt wird.**

B. Physische Sicherheitsvorkehrungen (Die Testumgebung)

Hier geht es um die unmittelbare Umgebung und den Zustand des Cobots.

1. Isolierte und abgesperrte Testzone:

- **Führen Sie die Tests in einem Bereich durch, der deutlich sichtbar mit Flatterband oder Sicherheitsgittern abgesperrt ist.**
- **Unbeteiligte Personen dürfen den Bereich unter keinen Umständen betreten. Warnschilder sind Pflicht.**

2. Not-Aus-Schalter in unmittelbarer Reichweite:

- **Der benannte Sicherheitsverantwortliche muss den Haupt-Not-Aus-Schalter jederzeit sofort erreichen können (nicht nur den auf der Bedienkonsole).**

3. Maximale Reduzierung von Geschwindigkeit und Kraft:

- **Versetzen Sie den Cobot vor Beginn der Tests in den langsamsten verfügbaren Modus (oft "T1" oder ein reduzierter manueller Modus).**
- **Reduzieren Sie die Geschwindigkeits-, Beschleunigungs- und Krafteinstellungen in der Software auf das absolute Minimum (z.B. 10 %).**

4. Keine Werkzeuge oder Lasten am Roboter:

- **Demontieren Sie jegliche Werkzeuge (Greifer, Schweißbrenner etc.) vom Flansch des Cobots. Ein unkontrolliert schwingender Greifer ist eine erhebliche zusätzliche Gefahr. Testen Sie den "nackten" Roboter.**

5. Persönliche Schutzausrüstung (PSA):

- **Das Tragen von Schutzbrillen ist für alle anwesenden Personen das absolute Minimum.**

C. System- und Datensicherheitsvorkehrungen (Schutz des Cobots)

Diese Maßnahmen schützen den Cobot vor permanenten Schäden und verhindern, dass Angriffe auf andere Systeme übergreifen.

1. Erstellung eines vollständigen System-Backups:

- **Erstellen Sie ein komplettes Image der Festplatte oder des Speichers der Robotersteuerung. Dies ist Ihre "Rückversicherung", falls ein Test das Betriebssystem oder die Konfiguration irreparabel beschädigt.**

2. Vollständige Netzwerk-Isolation:

- **Der Cobot und der für die Tests verwendete Laptop müssen sich in einem physisch getrennten, isolierten Netzwerk ("Air Gap") befinden.**
- **Es darf keinerlei Verbindung zum produktiven Firmennetzwerk (LAN oder WLAN) bestehen. Dies verhindert, dass durch einen Test eingeschleuste Malware (z.B. über Bluetooth oder USB) sich im Unternehmen ausbreitet.**

3. Passive Tests zuerst:

- **Beginnen Sie immer mit passiven Tests (zuhören), bevor Sie aktiv Daten senden.**
  - **CAN: Erst candump laufen lassen, um den Verkehr zu verstehen.**
  - **Bluetooth: Erst die Umgebung scannen und Dienste analysieren.**
  - **USB: Erst mit dmesg und lsusb beobachten, wie das System ein harmloses Gerät erkennt.**

4. Keine destruktiven Werkzeuge an produktiver Hardware:

- **Verwenden Sie einen USB-Killer niemals an der Steuerung des eigentlichen Cobots. Solche Tests dürfen nur an einer dedizierten, entbehrlichen Ersatz-Hardware durchgeführt werden.**

Durch die konsequente Einhaltung dieser dreistufigen Sicherheitsvorkehrungen können Sie die Risiken bei Schnittstellentests an Cobots systematisch minimieren und sowohl die Sicherheit der Menschen als auch die Integrität der Maschine gewährleisten.