HIMA

SMART SAFETY.

Handbuch

Automation Security

HIMA Security

Kontakt

HIMA Paul Hildebrandt GmbH

Postfach 1261

68777 Brühl

Tel.: +49 6202 709-0

Fax: +49 6202 709-107

E-Mail: info@hima.com

Revisions-index	Änderungen	Art der Änderung	
		technisch	redaktionell
1.00	Erstausgabe des Handbuchs		
2.00	Überarbeitete, modernisierte Version	X	X
2.01	Kapitel 3.2.1.3: Info ergänzt	X	X

Inhaltsverzeichnis

1 Einleitung

HIMA Safety-Produkte verfügen über wesentliche technische Eigenschaften die das Security-Risiko in Anlagen deutlich reduzieren können. Das gilt insbesondere, wenn die HIMA Safety-Produkte richtig eingesetzt werden. Dies bezieht sich auf die Netzwerkstruktur, Parametrierung und die Programmierung der HIMA Safety-Produkte. Das vorliegende Handbuch beschreibt die Aspekte der Automation-Security, welche beim Einsatz der HIMA Safety-Produkte zu berücksichtigen sind.

Insbesondere werden HIMax, HIQuad X und HIMatrix Systeme beschrieben.
Es wird ein praxistauglicher Aufbau empfohlen. Dieser ist typischerweise individuell an das betreiberseitige Gesamtkonzept angepasst werden.

Der vorgeschlagene Aufbau ersetzt die Risikoanalyse nicht.

Sollte eine individuell durchgeführte Risikoanalyse ein anderes Konzept ergeben, so ist dem Ergebnis der Risikoanalyse zu folgen.

Zusätzlich können weitere externe risikoreduzierende Maßnahmen eingesetzt werden. In diesem Handbuch werden jedoch keine Empfehlungen für den Einsatz von Drittprodukten, wie z. B. Infrastrukturkomponenten, gegeben. Werden Produkte erwähnt, so ist deren Nennung beispielhaft zu verstehen, ohne dass eine Nennung einen empfehlenden Charakter hat.

1.1 Aufbau und Gebrauch des Handbuchs

Das Handbuch ist in folgende Hauptkapitel gegliedert:

- Einleitung.
- Einführung Sicherheit.
- Produkteigenschaften zur Unterstützung der Security.
- Weitere Informationsquellen.

Das aktuelle Handbuch kann über die E-Mail-Adresse documentation@hima.com angefragt werden. Für registrierte Kunden stellt HIMA die Dokumentationen im Download-Bereich https://www.hima.com/de/downloads/ zur Verfügung. Hier können sich die Kunden auch für den Dokumenten Info Service (DIS) anmelden, um Informationen zu aktualisierten Dokumenten zu erhalten.

Anhand des Revisionsindex in der Fußzeile kann die Aktualität bereits vorhandener Handbücher mit der Internetausgabe verglichen werden.

1.2 Zielgruppe

Dieses Dokument wendet sich an Planer, Projekteure und Programmierer von Automatisierungsanlagen sowie Personen, die zu Inbetriebnahme, Betrieb und Wartung der Geräte und Systeme berechtigt sind.

HIMA bietet zum Thema Security eine Schulung an. Informationen hierzu befinden sich auf der HIMA Webseite unter:
https://www.hima.com/de/produkte-services/seminarangebot/ (→ Weitere Schulungen)

Kontakt

Bei Fragen zur Security wenden Sie sich an support@hima.com oder security@hima.com. Wir sind ständig um die Verbesserung unserer Produkte bemüht. Wir freuen uns über Rückmeldungen, insbesondere wenn Ihnen etwas nicht klar verständlich ist, Sie Verbesserungsvorschläge haben oder wenn Sie ein Verhalten an ihrer Anlage beobachten, das Ihnen nicht plausibel erscheint.

Aktuelle Informationen zu Security finden Sie auf der HIMA Webseite unter:
https://www.hima.com/de/branchen-loesungen/cybersecurity/.

1.3 Darstellungskonventionen

Zur besseren Lesbarkeit und zur Verdeutlichung gelten in diesem Dokument folgende Schreibweisen:

Fett	Hervorhebung wichtiger Textteile. Bezeichnungen von Schaltflächen, Menüpunkten und Registern im Programmierwerkzeug, die angeklickt werden können.
Kursiv	Parameter und Systemvariablen, Referenzen.
`Courier`	Wörtliche Benutzereingaben.
RUN	Bezeichnungen von Betriebszuständen (Großbuchstaben).
Kap. 1.2.3	Querverweise sind Hyperlinks, auch wenn sie nicht besonders gekennzeichnet sind. Im elektronischen Dokument (PDF): Wird der Mauszeiger auf einen Hyperlink positioniert, verändert er seine Gestalt. Bei einem Klick springt das Dokument zur betreffenden Stelle.

Sicherheits- und Gebrauchshinweise sind besonders gekennzeichnet.

1.3.1 Sicherheitshinweise

Um ein möglichst geringes Risiko zu gewährleisten, sind die Sicherheitshinweise unbedingt zu befolgen.

Die Sicherheitshinweise im Dokument sind wie folgt dargestellt.

- Signalwort: Warnung, Vorsicht, Hinweis.
- Art und Quelle des Risikos.
- Folgen bei Nichtbeachtung.
- Vermeidung des Risikos.

Die Bedeutung der Signalworte ist:

- Warnung: Bei Missachtung droht schwere Körperverletzung bis Tod.
- Vorsicht: Bei Missachtung droht leichte Körperverletzung.
- Hinweis: Bei Missachtung droht Sachschaden.

⚠ SIGNALWORT

Art und Quelle des Risikos!
Folgen bei Nichtbeachtung.
Vermeidung des Risikos.

HINWEIS

Art und Quelle des Schadens!
Vermeidung des Schadens.

1.3.2 Gebrauchshinweise

Zusatzinformationen sind nach folgendem Beispiel aufgebaut:

i	An dieser Stelle steht der Text der Zusatzinformation.

Nützliche Tipps und Tricks erscheinen in der Form:

TIPP	An dieser Stelle steht der Text des Tipps.

2 Einführung in die Sicherheit

2.1 Unterscheidung zwischen Safety und Security

Sicherheit bezeichnet den Zustand der Freiheit von unvertretbaren Risiken.

Neben den technischen Maßnahmen zur Risikoreduzierung sind immer auch organisatorische Maßnahmen zu berücksichtigen.

2.1.1 Safety (Funktionale Sicherheit)

Funktionale Sicherheit bezeichnet den Teil der Sicherheit eines Systems, der von der korrekten Funktion des sicherheitsbezogenen Systems und anderer risikomindernder Maßnahmen abhängt.

Hierbei geht es um die Vermeidung von systematischen Fehlern (Management der funktionalen Sicherheit) sowie die Reduzierung und Beherrschung zufälliger Fehler (Bauteilfehler - Dies wird durch fehlersicheres Design, der Schaffung von Hardware- Fehlertoleranzen und der Nutzung von Diagnosen erreicht).

HIMA entwickelt, produziert und liefert Safety-Steuerungen, welche zur Erhöhung der Anlagensicherheit eingesetzt werden. Dabei helfen unseren Steuerungen die Risiken von Prozessen auf ein tolerierbares Maß zu reduzieren.

2.1.2 Security (Automation Security, IT-Sicherheit oder Cyber Security)

Security beschreibt die Sicherheit bezüglich der Vertraulichkeit von Daten, deren Integrität, und Verfügbarkeit. Im Gegensatz zur Safety ist bei Security von gezielten externen Einflüssen (z. B. Hackern) auszugehen.

Safety kann nur auf der Basis korrekter Daten sichergestellt werden. Somit können die Bedingungen für Safety nur dann gewährleistet werden, wenn entsprechende Security-Maßnahmen umgesetzt wurden.

Die Priorität der oben genannten Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit ist abhängig von der Anwendung.

In der Informationstechnik (IT) hat meist die Vertraulichkeit von Daten höchste Priorität, in der Automatisierungstechnik (OT) meist die Verfügbarkeit. Für die Erfüllung der Anforderungen an Safety ist meist die Integrität der Daten von größter Bedeutung.

Es gilt für alle zu schützenden Systeme, dass eine individuelle Betrachtung nötig ist.

Weitere (untergeordnete) Schutzziele sind Authentifizierung, Autorisierung und Nicht-Abstreitbarkeit.

Organisatorische Schutz-Maßnahmen werden durch technische Maßnahmen unterstützt. Technische Maßnahmen allein sind nicht ausreichend.

i Dies gilt nicht nur für programmierbare Systeme, sondern auch für alle technischen Systeme im gesamten Lebenszyklus. So kann z. B. die Modifikation von Konstruktionsunterlagen zu erheblichen Risiken führen.

2.2 Bedrohung der Security

Automatisierungskomponenten litten bereits vor längerer Zeit unter den Folgen von Schadsoftware. Diese war oft nicht auf die Automation gezielt. Mittlerweile sind jedoch gezielte Angriffe auf Automatisierungssysteme bekannt. Stuxnet ist die erste bekannte Schadsoftware, die gezielt die Funktion von Automatisierungskomponenten störte. (Ausführliche Informationen z. B. unter https://www.langner.com/wp-content/uploads/2017/08/Stuxnet-und-die-Folgen.pdf) Mittlerweile gab es mit TRITON auch einen Angriff auf ein Safety-System.
(Weitere Informationen unter https://www.hima.com/de/unternehmen/news/artikel/hima-security-advisory-trisistriton-1/).

Daraus ist zu erkennen, dass sich sowohl die Bedrohung (das Interesse) als auch die Verwundbarkeit (bekannte, nutzbare Lücken) von Systemen ständig ändert. Der erreichte Grad an Security kann demzufolge immer nur für einen gewissen Zeitraum erhalten werden.

2.3 Maßnahmen zum Erhalt der Security

2.3.1 Awareness

Normen und Publikationen zur Security befassen sich ausführlich mit dem Thema Sicherheitsbewusstsein. Dies ist die Basis für Sicherheit. Alle technischen Maßnahmen können nur dann funktionieren, wenn das nötige Bewusstsein (Awareness) für die Security in der Belegschaft geprägt ist. Dies gilt von der Planung über die Inbetriebnahme bis in den Betrieb und die Außerbetriebnahme.

2.3.2 Good Engineering Practice

Security hat viel mit der Denkweise der Beteiligten zu tun. Aus diesem Grund seien hier als gutes Beispiel Grundprinzipien der Security von Viega und McGraw genannt. Diese 2002 zusammengestellte Liste ist auch heute noch gültig. Die gezeigten Prinzipien sollen kein 100 %iger Schutz sein. Sie sollen helfen, mit 20 % des Aufwands 80 % der möglichen Risikoreduzierung zu erreichen.

1. **Secure the weakest link** (Identifizieren und stärken Sie das schwächste Glied.)
   Angreifer suchen nach einfachen Möglichkeiten ein System zu beeinflussen und werden versuchen für Angriffe eine möglichst schwache Stelle zu finden. Daher sollte das schwächste Glied zuerst gesichert werden.
2. **Practice defense in depth** (Begegnen Sie Software-Risiken mit mehrschichtigen Security-Lösungen)
   Beim Überwinden einer Schwäche kann nicht das gesamte System, sondern nur ein Teil beeinflusst werden. Des Weiteren erhöht sich das Risiko für den Angreifer entdeckt zu werden. In der Safety wird das als *Layers of Protection* bezeichnet.
3. **Fail securely** (Stellen Sie sicher, dass das System im Fall eines Versagens auf eine secure Weise versagen wird.)
4. **Follow the principle of least privilege** (Vergeben Sie nicht mehr Rechte als nötig, und vergeben Sie Rechte nicht länger als nötig.)
   Was nicht erlaubt ist, ist verboten. Für die minimal mögliche Zeit sollen lediglich die minimal benötigten Rechte vergeben werden. Wenn ausschließlich Lesezugriff benötigt wird, so sollte auch nur dieser zur Verfügung gestellt werden.
5. **Compartmentalize** (Versuchen Sie, Fehler auf einem Teil des Systems zu begrenzen, so dass sie sich nicht auf den Rest des Systems auswirken.)
6. **Keep it simple & stupid** (KISS)
   KISS sollte in guter Balance mit *Defence in the Depth* stehen. Einfach zu durchschauen, Wiederverwendung gut getesteter Komponenten, einzelne kontrollierbare Datenkanäle schaffen (conduits).
   Security by Design. Mit den Anwendern sprechen, die es einsetzen müssen und deren Anforderungen berücksichtigen.

7. **Promote privacy** (Geben Sie keine unnötigen Informationen preis.)
   Mit Daten sollte sensibel umgegangen werden. Es schadet auch nicht, falsche Informationen zur Verfügung zu stellen.
8. **Remember that hiding secrets is hard**
   Geheimnisse sind in einem nicht offensichtlichen Format (z. B. Binär-Datei) nicht secure. Dies wird als *Security by Obscurity* bezeichnet und funktioniert nicht.
9. **Be reluctant to trust**
   Auch Hersteller von Secure-Software sind nicht unfehlbar. Sich selbst und seinem eigenen Unternehmen sollte auch nicht bedingungslos getraut werden, sondern bei Bedarf unabhängige Dritte mit einbeziehen.
10. **Use your community resources** (Beschreiben Sie, was Sie zur Security tun.)
    Wenn es einer Prüfung durch Dritte widersteht, kann davon ausgegangen werden, dass es ziemlich secure ist. Wenn Sie Sich nicht sicher sind, ob Ihr Design secure ist, dann holen Sie Hilfe.

Für weitere Informationen siehe auch:
http://searchsecurity.techtarget.com/opinion/Thirteen-principles-to-ensure-enterprise-system-security

2.4 Security als Prozess

Aufgrund ständiger Änderungen des Security-Risikos ist es nötig einen kontinuierlichen Prozess zum Erreichen und Erhalt des erforderlichen Security-Level aufzusetzen. Ähnlich wie der kontinuierliche Verbesserungsprozess im Qualitätsmanagement, oder dem Functional Safety Management muss Security aktiv und kontinuierlich aufrechterhalten werden. Dies wird am besten mit einem Managementsystem unterstützt.

Der Prozess der Security kann z. B. in folgende vier Schritte eingeteilt werden:

- **Risiko analysieren (Plan)**: Die schützenswerten Teilsysteme werden ermittelt und bewertet.
- **Schützen (Do)**: Die Teilsysteme werden bedarfsgerecht geschützt.
- **Erkennen (Check)**: Maßnahmen zum Erkennen von Lücken im System werden integriert und ausgewertet.
- **Reagieren (Act)**: Nach Erkennen einer Lücke wird sachgerecht reagiert.

Nach einem festgelegten Zeitraum, dem Bekanntwerden einer Bedrohung oder dem Erkennen eines Ereignisses, wird von vorn begonnen. Dieser Prozess wird auch als PDCA-Modell (**P**lan, **D**o, **C**heck, **A**ct) bezeichnet.

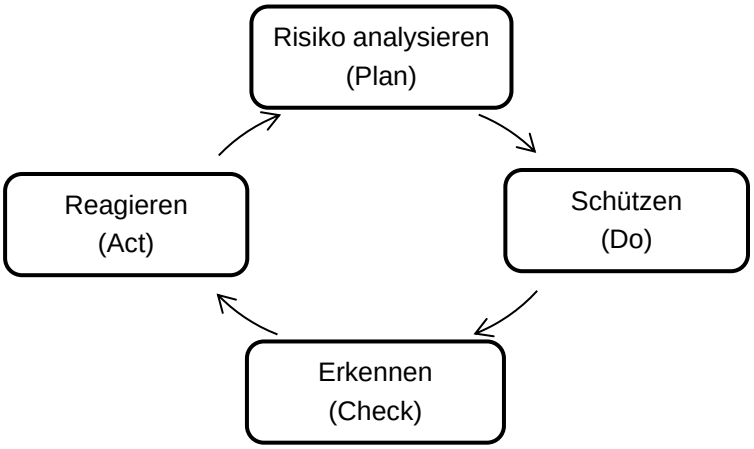


Bild 1: PDCA-Zyklus

Bei einem Änderungsmanagement müssen nicht nur Safety, sondern auch Security-Eigenschaften des Systems berücksichtigt werden.

TIPP Der gezeigte PDCA-Zyklus ist nur eine Möglichkeit. Weitergehende Informationen sind z. B. in den Standards ISO 27000 (ff), IEC 62443-2-1, VDI 2182, NIST SP 800-37 zu finden.

2.4.1 Risiko analysieren

Neben der Implementierung eines Basisschutzes sollte zur Ermittlung des Risikos eine Risikoanalyse durchgeführt werden.
Bei der Risikoanalyse wird die gesamte Anlage systematisch analysiert. Es werden mögliche Bedrohungen und Verwundbarkeiten sowie das potentielle Schadensausmaß ermittelt. Dies hilft die passenden Lösungen für individuelle Anlagen zu erstellen.

TIPP Die Risikoanalyse wird in mehreren Standards beschrieben. Hilfreich sind z. B. IEC 62443-3-2, NA163, ISO 27005, BSI 200-3.

HIMA bietet Risikoanalyse für Safety und Security als Service an.

2.4.2 Schützen

2.4.2.1 Organisatorische Maßnahmen

Eine weit verbreitete Ansicht ist, dass Sicherheitsmaßnahmen zwangsläufig mit hohen Investitionen in Sicherheitstechnik und der Beschäftigung von hoch qualifiziertem Personal verknüpft sind. Dem ist jedoch nicht so. Die wichtigsten Erfolgsfaktoren sind ein gesunder Menschenverstand, durchdachte organisatorische Regelungen sowie zuverlässige und gut informierte Mitarbeiter, die selbständig Sicherheitserfordernisse diszipliniert und routiniert beachten. Die Erstellung und Umsetzung eines wirksamen und effektiven Informationssicherheitskonzeptes muss darum nicht zwangsläufig unbezahlbar sein. Die wirksamsten Maßnahmen sind überraschend simpel und noch dazu oft kostenlos! (Quelle: BSI Leitfaden Informationssicherheit)

2.4.2.2 Technische Maßnahmen

Technische Maßnahmen unterstützen die organisatorischen Maßnahmen.

Mehrstufige Abwehrsysteme (*Defense in the Depth*) werden derzeit als die effizienteste Maßnahme zur Risikominimierung anerkannt. In industriellen Automatisierungsanlagen sollten mehrere Schutzschichten zu finden sein.

HIMA Systeme sind mit einem eigens für die Safe-Automation entwickelten Betriebssystem ausgerüstet. So kann die Safety-Steuerung die bestmögliche letzte Verteidigungslinie darstellen.

2.4.3 Erkennen

HIMA Produkte setzen umfassend auf Standardtechnologien. Programmiersysteme beruhen auf aktuellen Windows Betriebssystemen. Die angebotene Kommunikation beruht auf Standard-Ethernet. Somit können zusätzliche technische Maßnahmen, wie z. B. die Verwendung von Honeypots oder IDS helfen, Unregelmäßigkeiten im Netzwerk oder Gesamtsystem zu erkennen.

2.4.4 Reagieren

Wenn eine Unregelmäßigkeit im System erkannt wird, muss auf diese entsprechend reagiert werden. Die Ursache muss behoben werden. Es ist zu überprüfen, ob und wie zukünftig derartige Ereignisse unterbunden werden. Der Prozess beginnt von neuem.

3 Produkteigenschaften zur Unterstützung der Security

Dieses Kapitel beschreibt den Einsatz von HIMA Systemen. Als Orientierung dient Bild 2:

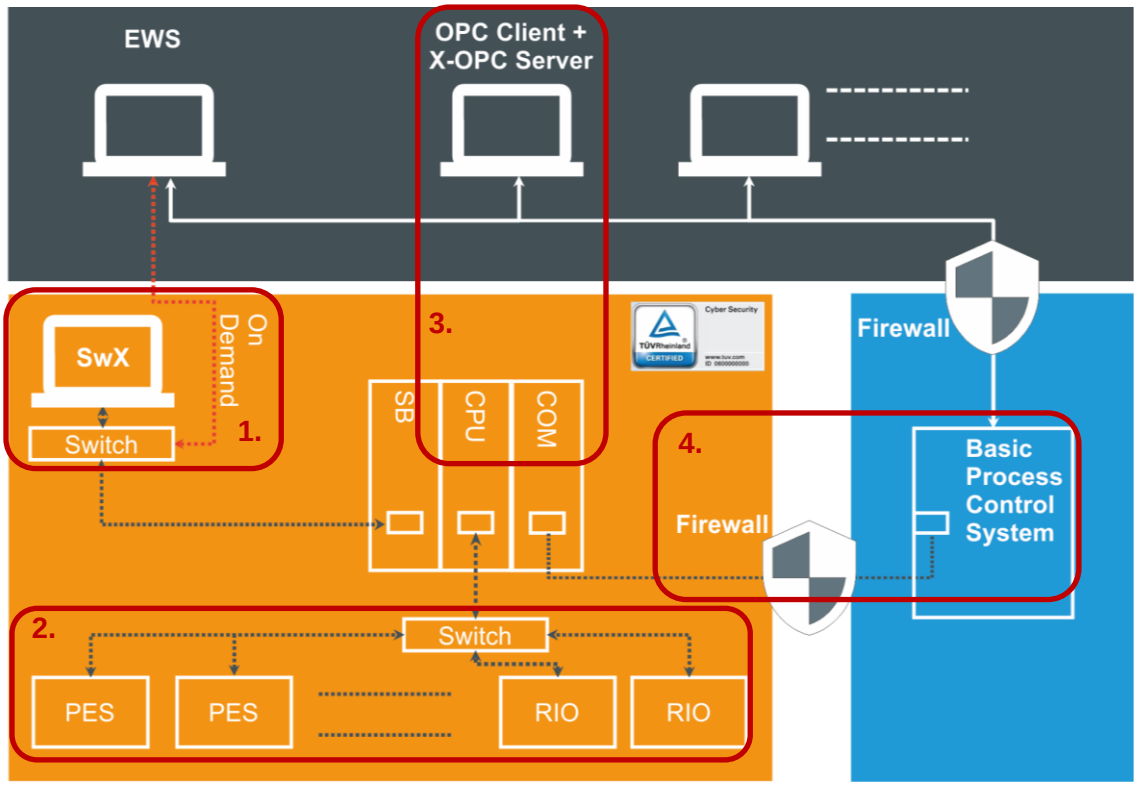


Bild 2: Übersicht Safety-Steuerung mit anderen Systemen

Erläuterung: Eine Safety-Steuerung, HIMA PES, ist (fast) immer im Kontext mit anderen Systemen zu sehen. Dies sind hauptsächlich:

1. PADT (Windows PC mit SILworX oder ELOP II).
2. Anbindung an weitere Safety-Systeme (HIMA PES und RIO).
3. Anbindung an Fremdsysteme z. B. via OPC.
4. Anbindung an ein Leitsystem (BPCS, DCS, PLS).

Anhand dieser Darstellung wird der typische Einsatz der HIMA Produkte im Folgenden erläutert. Alle Informationen stehen auch in anderen HIMA Dokumenten zur Verfügung. In diesem Dokument sind die relevanten für Security aller HIMA Systeme zusammengefasst.

3.1 Übersicht HIMA Systeme

Dieses Dokument bezieht sich auf die aktuell in der Preisliste befindlichen Produkte.

3.1.1 Verbindungsprogrammierte Steuerung (VPS, Planar 4 Systeme)

Bei hoher Anforderung an Safety (SIL 4) und die Security ist das Planar 4 System in Betracht zu ziehen. Planar 4 Systeme erhalten ihre Funktion mittels Hardware-Verdrahtung. Diese Art der Programmierung ist extrem robust und **immun** gegen jegliche Schadsoftware.

3.1.2 HIQuad

HIQuad ist ein programmierbares System, das in einer Zeit entstanden ist, zu der keine Security-Betrachtungen in der Automatisierungstechnik durchgeführt wurden. Es wird mit dem Programmierwerkzeug ELOP II programmiert. Das System verfügt über keine expliziten Security-Eigenschaften. Es ist jedoch sehr stabil im Betrieb und kann über entsprechende Organisatorische und applikative Maßnahmen secure betrieben werden. Vor allem der Zugriffschutz (separate Netzwerke, abschließbare Schaltschränke, Betrieb ohne angeschlossenes PADT …) sind hier elementar.

i Anlagen, die mit HIQuad ausgerüstet sind, sollten mittels HIQuad X Systemen modernisiert werden, wenn mittlerweile Ansprüche an Security bestehen.

Damit stehen die neusten HIMA Technologien zur Verfügung.

3.1.3 HIMatrix Remote I/Os

HIMatrix Remote I/Os sind nicht-programmierbare safety Eingangs- und Ausgangsmodule, die an HIMax, HIQuad X und HIMatrix Systeme angeschlossen werden können. Die Konfiguration ist im Programmierwerkzeug vorzunehmen und wird beim Start von den PES übertragen.

i HIMatrix Remote I/Os für ELOP II Factory sind in der Lebensphase *Legacy*. Sollen die PES aufgerüstet werden, so sollten die HIMatrix Remote I/Os mittels Update des Betriebssystems auf SILworX Kompatibilität modernisiert werden.

3.1.4 HIMatrix F*02

Dieses programmierbare elektronische System ist in der Lebensphase *Legacy*. Es verfügt über grundlegende Security-Mechanismen wie ein Benutzermanagement. Das System wird jedoch nicht weiter gepflegt.

i Anlagen, die mit HIMatrix ELOP II Factory ausgerüstet sind, sollten mittels aktueller HIMatrix SILworX Systemen modernisiert werden, wenn mittlerweile Ansprüche an Security bestehen.

Damit stehen die neusten HIMA Technologien zur Verfügung.

3.1.5 HIMax, HIQuad X, HIMatrix F*03

HIMA Produkte unterstützen die Vermeidung systematische Fehler. Deren hohe Qualität unterstützt den Schutz von Anlagen auch im Sinne der Security.

Die Berücksichtigung von Security-Aspekten ist integraler Bestandteil der Entwicklung dieser programmierbaren elektronischen Systeme. So werden alle PES in jedem Ausgabestand auf ihr Verhalten im Falle eines Angriffs überprüft.

3.2 Maßnahmen der Absicherung

Das folgende Kapitel beschreibt Funktionalitäten zur Erhöhung der Security der HIMA Systeme. Die Betrachtung erfolgt dabei von der Netzwerk-Ebene über Switch und Steuerung zum Programmierwerkzeug (PADT, SILworX) und der Anbindung von Fremdsystemen.

3.2.1 Schutz auf Netzwerkebene

3.2.1.1 HIMatrix Remote I/Os

Die Remote I/Os sind für einfache Punkt zu Punkt Verbindungen entwickelt worden. Bei hoher Netzwerklast können die Remote I/Os zum Reboot gebracht werden. Daher sind speziell HIMatrix Remote I/Os vor zu hoher Netzwerklast zu schützen. Dies kann durch die Trennung der Systeme von möglichen Störquellen erfolgen (siehe Kapitel 0).

3.2.1.2 Ethernet-Schnittstelle

Nicht verwendete Ethernet-Schnittstellen sollten mittels eines physikalischen Schutzes blockiert werden. Dies verhindert versehentliche Benutzung. Verschlüsse gibt es mit Schlüssel (z. B. von Tyco Electronics) oder als Kunststoffkappen mit Spezialwerkzeug zum Öffnen (z. B. von Panduit oder Lindy).

Dies gilt für alle Geräte mit Ethernet-Ports.

3.2.1.3 Ethernet-Einstellungen

1. Default Gateway

   Dieses steht als Standard auf 0.0.0.0. Somit kann kein Routing durchgeführt werden.

2. ARP-Aging und MAC Learning

   Ist *MAC-Learning* auf *tolerant* eingestellt, werden neue Adressen sofort gelernt und können auch durch Angreifer leicht überschrieben werden.
   Daher ist die Standardeinstellung von *MAC-Learning konservativ*. Wenn sich im ARP-Cache bereits MAC-Adressen von Kommunikationspartnern befinden, so sind diese Einträge für die Dauer von 1 … 2 mal *ARP Aging Time* verriegelt und können nicht durch andere MAC-Adressen ersetzt werden.

3. ICMP Mode

   Die Standardeinstellung ist *Echo Response*. Dies ist die bevorzugte Einstellung wenn das Gerät auf Kommunikationsfähigkeit überwacht werden soll. Die Einstellung ist ein guter Kompromiss aus Bedienbarkeit und Security. Wird bevorzugt, Geräte im Netzwerk zu verstecken, sollte dieser Parameter auf *keine ICMP-Antworten* eingestellt werden.

Gilt für	HIMax	HIQuad X	HIMatrix PES	HIMatrix RIO
CPU	X	X	X	X
COM	X	X	X	

i Bei einem DoS-Angriff kann es passieren, dass das PES kurzzeitig nicht auf ARP- oder ICMP-Anfragen reagiert.

Die Funktionalität des PES ist davon unberührt.

3.2.1.4 Netzwerktrennung und physikalisches VLAN

Die Bildung von Zonen und die damit verbundene Trennung von Netzwerken ist die Basis für das *Defence-in-the-Depth*-Konzept. Dieses wird durchgehend als wichtiges Security-Konzept verstanden. Die IEC 62443 gibt dieses Konzept explizit vor. Bild 3 zeigt einen Vorschlag für den sinnvollen Aufbau von Zonen. Es ist deutlich zu erkennen, dass die einzelnen Zonen (orange: safety, blau: control, grau: IT) nur an jeweils einer explizit festgelegten Stelle Übergänge in die anderen Zonen ermöglichen. Diese Übergänge sind klar definiert und können demzufolge gut geschützt werden.

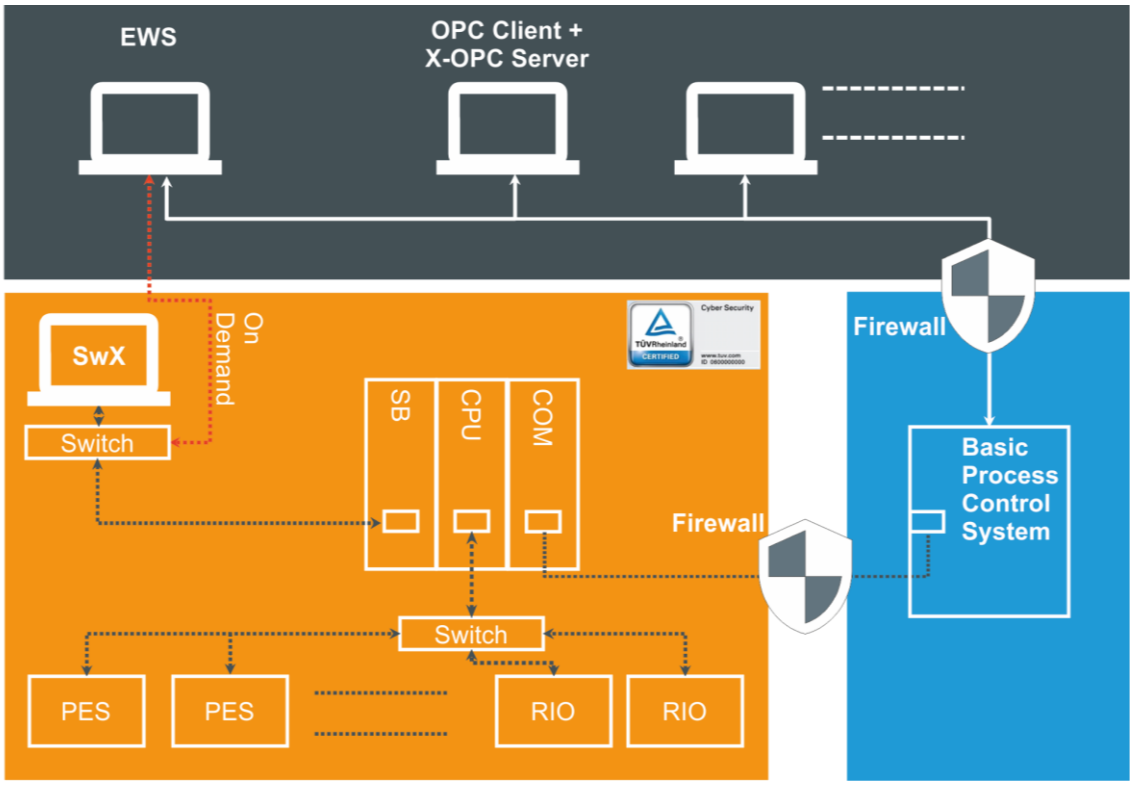


Bild 3: Beispiel für den Aufbau von Zonen

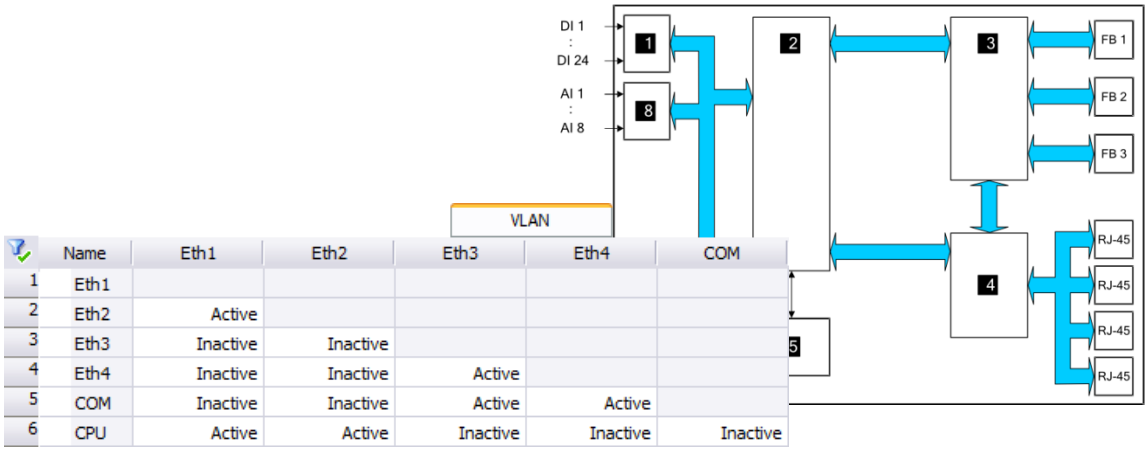
HIMax und HIQuad X: CPU und COM kommunizieren über den Rückwandbus miteinander. Die COM hat keinen direkten Zugriff auf die CPU. Sie ist lediglich in der Lage, Daten aus einem Speicher der COM zu lesen und zu beschreiben. Die CPU greift über den Systembus auf diesen Speicher lesend und schreibend zu.

Um mit der Außenwelt zu kommunizieren, verfügen CPU und COM jeweils über einen Ethernet Switch. Diese Switche sind vollständig unabhängig voneinander.

Ein Teilnehmer (z. B. BPCS), der an einem COM-Modul angeschlossen ist, kann lesend und schreibend auf diese COM zugreifen. Der Zugriff auf die CPU oder an die CPU angeschlossene Geräte bleibt dem BPCS jedoch verwehrt.

TIPP HIMA empfiehlt, diese Systemeigenschaft für die Reduzierung von Security-Risiken zu nutzen. Es sollte ein Safety-Netzwerk über die CPU aufgebaut werden und ein davon getrenntes Netz für den Anschluss von nicht Safety-Komponenten wie das BPCS.

HIMatrix PES: Intern verfügt auch HIMatrix über eine CPU (2) und eine COM (3). Diese sind direkt und über den intern verbauten Switch (4) miteinander verbunden.



	Name	Eth1	Eth2	Eth3	Eth4	COM
1	Eth1					
2	Eth2	Active				
3	Eth3	Inactive	Inactive			
4	Eth4	Inactive	Inactive	Active		
5	COM	Inactive	Inactive	Active	Active	
6	CPU	Active	Active	Inactive	Inactive	Inactive

Bild 4: Netzwerktrennung bei HIMatrix

Bei diesem Switch kann die Verbindung von jedem Port zu jedem anderen Port über die VLAN-Settings konfiguriert werden. Wie in der Matrix dargestellt, kann der Switch also in 2 getrennte Switches aufgeteilt werden. Auch so ist der direkte Zugriff von Geräten, die an der COM angeschlossen sind, auf die Geräte, die an der CPU angeschlossen sind, verwehrt.

TIPP HIMA empfiehlt, die nicht genutzten Ports der HIMatrix zu schließen.

ACHTUNG: Wenn alle Ports geschlossen werden, kann das System erst nach Initialisierung wieder erreicht werden.

Gilt für	HIMax	HIQuad X	HIMatrix PES	HIMatrix RIO
CPU	X	X	X	-
COM	X	X	X	

TIPP Zusätzlich können Infrastrukturkomponenten eingesetzt werden, bei denen nicht verwendete physikalische Ports geschlossen werden können. So werden Zugangsmöglichkeiten für unbefugte Nutzer eingeschränkt und das Risiko reduziert.

3.2.1.5 Verwendung von safe**ethernet**

safe**ethernet** dient der Safety-Kommunikation zwischen HIMA Safety-Systemen. Dieses sollte in einem getrennten Netzwerk, unabhängig von der nicht Safety-Kommunikation, über die CPU betrieben werden. Aus Sicht der Security wird durch diese Maßnahme eine gute physikalische Trennung erreicht. Soll aus Gründen der Verfügbarkeit die Belastung der CPU weiter reduziert werden, ist es möglich zusätzliche COM(s) ausschließlich für safe**ethernet** einzusetzen.

3.2.1.6 Verwendung von OPC

PES-SERVER-Verbindung

Zum Anschluss des OPC-Servers wird ebenfalls safe**ethernet** verwendet. Auch wenn die Kommunikation dadurch nicht safe wird (der PC, auf dem der OPC läuft, ist kein Safety-Gerät) so wird trotzdem die Zuverlässigkeit von safe**ethernet** genutzt. Zur Trennung vom Safety-Teil sollte der Anschluss immer über eine COM erfolgen. Bei Zonentrennung wird empfohlen, in diese Verbindung eine Firewall einzubauen.

CLIENT-SERVER-Verbindung

Hier wird gemäß Spezifikation der OPC Foundation DCOM verwendet. Bei erhöhtem Schutzbedarf wird empfohlen, hier eine zusätzliche Firewall einzusetzen. Hierfür gibt es spezielle Firewalls, die in der Lage sind der DCOM Kommunikation zu folgen.

3.2.1.7 Systembus-Modul (HIMax X-SB)

Der PADT-Anschluss des Moduls ist für die Verbindung zum Programmiersystem geeignet. Alle anderen Anschlüsse (UP, DOWN und DIAG) dürfen ausschließlich zur Anbindung an andere HIMax X-SB verwendet werden. Jegliche externe Einflüsse sind zu vermeiden. HIMA empfiehlt den mechanischen Schutz von nicht verwendeten Anschlüssen. Die Möglichkeiten des Aufbaus in Linien- und Netzstruktur sind im Systemhandbuch der HIMax beschrieben.

3.2.1.8 Verwendung von nicht Safety-Protokollen

ETHERNET

Nicht Safety-Protokolle wie Modbus TCP sollten immer über COM angeschlossen werden. Dadurch wird eine Trennung vom Safety-Netz ermöglicht.

FELDBUS

Im Allgemeinen ist die Manipulation von Feldbussen genauso möglich wie die von Ethernet Protokollen. Bei erhöhtem Schutzbedarf sollte erwogen werden auch hier Schutzmaßnahmen zu ergreifen.

HART

Bei der Verwendung von HART kann das Schreiben von Parametern unterbunden werden. So können Feldgeräte von zentraler Stelle verwaltet werden. Eine Manipulation der Feldgeräten ist jedoch nicht möglich.

⚠ WARNUNG

Mittels HART-Handheld kann bei direktem Anschluss an die Leitung das HART Gerät umprogrammiert und so z. B. Parameter verstellt werden, die für eine Abschaltung nötig wären. Das kann schon rein elektrisch von der Steuerung nicht unterbunden, sondern lediglich im Anwenderprogramm erkannt werden. Um die Endgeräte auch davor zu schützen, muss das Beschreiben im Feldgerät selbst mit einem Schreibschutz versehen werden.

ALLGEMEIN

Es können nur definierte Lesevariablen gelesen und definierte Schreibvariablen beschrieben werden. Anfragen auf nicht explizit beschriebene Variablenbereiche werden abgelehnt.

Es ist generell sinnvoll, Werte die über nicht Safety-Protokolle in das HIMA System geschrieben werden auf Plausibilität zu überprüfen, z. B.:

- Ist ein Eingabewert außerhalb der sinnvollen Grenzen, könnte es sich um einen Angriffsversuch handeln.
- Ändert sich ein Wert in einer Zeiteinheit deutlich schneller als vom Prozess zu erwarten ist, könnte es sich um eine Umparametrierung eines Sensors handeln.
- Stimmt die Korrelation zwischen 2 Prozessparametern nicht mehr, könnte es sich um eine Manipulation handeln

3.2.1.9 Fernzugriffe auf das PES

Fernwartungssysteme sollten in Verbindung mit Safety-Systemen grundsätzlich nicht genutzt werden.

Ein Fernwartungssystem für eine Safety-Steuerung sollte lediglich im Falle eines begründeten Bedarfes und nach der Durchführung einer gewissenhaften Risikoanalyse eingesetzt werden.

Für Safety-Kommunikation über nicht vertrauenswürdige Netzwerke gilt dasselbe. Muss ein nicht ausreichend getrenntes Netzwerk oder eine Wireless-Strecke überwunden oder gar öffentliches Netz (z. B. Internet) genutzt werden, ist für ausreichenden Schutz zu sorgen. Dieser Schutz hat mindestens dem Stand der Technik zu entsprechen.

3.2.1.10 Link Layer Discovery Protocol (LLDP)

LLDP ist ein Protokoll, das den Austausch von Informationen zwischen Nachbargeräten ermöglicht. LLDP wird in HIMA Produkten ausschließlich für des Legacy-Protokoll PROFINET verwendet. Es sollte ansonsten abgeschaltet bleiben. Dies entspricht der Standardeinstellung.

Gilt für	HIMax	HIQuad X	HIMatrix PES	HIMatrix RIO
CPU	X	n.a.	X	n.a.
COM	X	n.a.	n.a.	

3.2.1.11 Mirroring

Switches leiten im Gegensatz zu Hubs den Datenverkehr ausschließlich an den Ziel-Port weiter. Um den Datenverkehr (z. B. mit Wireshark) analysieren zu können, muss dieser an einen anderen Port weiter geleitet werden. Dieses wird mit *Mirroring* ermöglicht. *Mirroring* ist in der Standardeinstellung aus, kann aber zur Netzwerküberwachung oder Fehlersuche eingeschaltet werden. Nach der Überwachung/Fehlersuche sollte *Mirroring* **deaktiviert** werden.

Gilt für	HIMax	HIQuad X	HIMatrix PES	HIMatrix RIO
CPU	X	X	X	-
COM	X	X	X	

3.2.1.12 Simple Network Time Protocol (SNTP)

SNTP ist ein einfaches Protokoll zur Zeitübertragung und Zeitsynchronisation von Geräten. Es wird in einer Client-Server-Struktur angewandt.

HIMax, HIQuad X und HIMatrix verwenden SNTP für die Synchronisation mit HIMatrix Remote I/Os. Dies kann nicht abgeschaltet werden.

Des Weiteren können HIMax, HIQuad X und HIMatrix eine Zeitsynchronisation z. B. mit einem GPS-Zeitserver durchführen. Die genannten Steuerungen können auch selbst Zeitserver sein. Sowohl SNTP Server als auch SNTP Client können ein- und ausgeschaltet werden. In der Standardeinstellung sind sie aus.

Gilt für	HIMax	HIQuad X	HIMatrix PES	HIMatrix RIO
CPU	X	X	X	X
COM	X	X	X	

3.2.1.13 Verwendete Ethernet-Ports

HIMA Produkte basieren auf Standard Ethernet Protokollen, die mit jeder Firewall verwendet werden können. Auch die Safety-Kommunikation via safe**ethernet** nutzt den gewöhnlichen Ethernet UDP Rahmen und kann somit in jeder Firewall je nach Bedarf durchgelassen oder blockiert werden.

	HIMax, HIQuad X, HIMatrix PES SILworX	**HIQuad ELOP II**	**HIMatrix PES ELOP II Factory**	**PADT**
HIMax HIQuad X HIMatrix PES (SILworX)	**UDP 6010**	**UDP 6010**	UDP 6010	**UDP 8000**
HIQuad	**UDP 6010**	**UDP 6005 UDP 6010 UDP 6012**		**TCP 6034**
HIMatrix PES (E2F)	UDP 6010		UDP 6010	UDP 8000
HIMatrix Remote I/O	**UDP 6010 UDP 8004 UDP 123**		UDP 6010 UDP 8001 UDP 123	**UDP 8000**
(X-)OPC Server DA	**←UDP 15138 (var) → UDP 6010**	**UDP 6005 UDP 6010 UDP 6012**	UDP 6005 UDP 6010 UDP 6012	**←UDP 25138 (var) → UDP 6010**
(X-)OPC Server A&E	**←UDP 15138 (var) → UDP 6010**	**TCP 502**		**←UDP 25138 (var) → UDP 6010**
Modbus	**TCP 502 UDP 502 (var)**	**TCP 502 TCP 8896**	TCP 502 UDP 502 (var)	
HART over IP (nur HIMax)	**UDP 5094 TCP 5094 (var)**			
Send Receive	**TCP (var)**		TCP (var)	
CUT	**TCP (var) UDP (var)**		TCP (var) UDP (var)	
SNTP	**UDP (var)**		UDP (var)	
ISOfast	**UDP (var) ***			
COMeth		**UDP 6011 UDP 6031 UDP 6032**		
safe**ethernet Token**		UDP 6005 UDP 6010 UDP 6012	UDP 6005 UDP 6010 UDP 6012	
PROFINET	UDP 49152 UDP 49153 UDP 34964		UDP 49152 UDP 49153 UDP 34964	
EtherNet/IP			TCP 44818 UDP 44818 UDP 2222	

Tabelle 1: Von HIMA Produkten verwendete Ethernet-Ports

Informationen zur Tabelle:

- An den Schnittstellen der Matrix sind die verwendeten Ports vermerkt, z. B. HIMax zu X-OPC verwendet UDP 15138, X-OPC zu HIMax verwendet UDP 6010. HIMatrix PES (SILworX) zu HIMatrix Remote I/O verwendet UDP 6010, UDP 8004 und UDP 123 in beide Richtungen.
- (var) … Ports sind variabel einstellbar.
- Auf einem PC können mehrere OPC Server laufen. Daher sind die Ports konfigurierbar. Es wird der Standardwert dokumentiert.
- Alle Ethernet-basierten Kommunikationen benötigen ARP.
- DCOM für Datenaustausch zwischen (X-)OPC Server und OPC Client benötigt UDP 135 ff.
- Der Port UDP 8001 wird für das Suchen per MAC benötigt.

* ISOfast steht lediglich in HIMatrix zur Verfügung. Der gewünschte UDP Port ist frei konfigurierbar. Wird ISOfast nicht verwendet ist kein Port dafür geöffnet.

i Die oben dargestellte Matrix ist eine vollständige Liste der zur Verfügung stehenden Ports. Es werden keine weiteren Dienste wie DHCP, DNS, Priorität, FTP etc. angeboten.

i Ein PC mit SILworX (PADT) hat keinen bestimmten Source-Port, sondern wählt diesen selbständig aus.

3.2.1.14 Firewalls regeln den Datenverkehr

Die HIMA (Kommunikation) stützt sich immer auf Standards. Daher können Standard-Security-Maßnahmen (wie z. B. Firewalls) verwendet werden. Firewalls dienen zur Trennung von (internen und externen) Netzwerken und reduzieren den Datenverkehr auf den gewünschten, konfigurierten Zugriff.

Der Funktionsumfang variiert und kann z. B. folgendes beinhalten:

- Das geschützte Netzwerkes soll entlastet werden.
- Nur bestimmte Ports (Protokolle) dürfen verwendet werden.
- Ausschließlich die konfigurierte Kommunikation von einem bestimmten Teilnehmer zu einem bestimmten anderen Teilnehmer wird zugelassen.
- Nur Antworten auf Anfragen in das externe Netz dürfen beantwortet werden.
- Bekannte Protokolle können untersucht und nach bestimmten Regeln gefiltert werden.

Meist werden auch Vorgänge, wie z. B. die Anfrage einer nicht autorisierten Kommunikation, mitgeloggt und einem zentralen Management zur Verfügung gestellt.

Gilt für	HIMax	HIQuad X	HIMatrix PES	HIMatrix RIO
CPU	X	X	X	X
COM	X	X	X	

3.2.2 Interne Schutzmechanismen

3.2.2.1 Betriebssystemstand

HIMA empfiehlt, die Betriebssysteme der PES auf dem aktuellen Stand zu halten.
Bei redundanten Systemen ist ein Update des Betriebssystems im laufenden Betrieb möglich.

Gilt für	HIMax	HIQuad X	HIMatrix PES	HIMatrix RIO
CPU	X	X	X	X
COM	X	X	X	

3.2.2.2 Zugriffseinschränkungen

Zum Schutz des Anwenderprogramms sollten folgende Systemvariable verwendet werden:

- *Force-Deaktivierung*
- *Read-only in RUN*
- *Reload-Deaktivierung*

Dieser Schutz sollte im täglichen Gebrauch aktiv sein. So wird direkter Einfluss auf das Programm und das PES verhindert. HIMA empfiehlt, einen Schlüsselschalter an einen Eingang anzuschließen und diesen auf einer Systemvariablen abzubilden. Es ist eine gute Lösung, die Systemvariable *Force-Deaktivierung* auf einen und *Read-only in RUN* und *Reload-Deaktivierung* auf einen anderen Schlüsselschalter zu legen.

Gilt für	HIMax	HIQuad X	HIMatrix PES	HIMatrix RIO
	X	X	X	n.a.

TIPP HIMA empfiehlt, 0 V als logische 1 für die Systemvariablen zu verwenden. Dies bedeutet, dass das System im Falle eines Drahtbruches geschützt ist.

Um einen „vergessenen“ Schlüsselschalter auszuschließen, sollte ein entsprechendes Programm geschrieben werden. Die steigende Flanke des Eingangssignals (Schlüsselschalters) sollte ein Zeitglied triggern, das die Systemvariablen für eine angemessene Zeit auf 0 setzt. (z. B. 1 Arbeitstag, 8 h). So könnte auch für unterschiedliche Anwender mit unterschiedlichen Schlüsselschaltern unterschiedliche Zeiten gewährt werden.

Schlüsselschalter in Verbindung mit der Benutzerverwaltung helfen das Konzept „least privilege“ durchzusetzen.

HIMA empfiehlt, die Stellung des Schlüsselschalters in der Leitwarte (hart verdrahtet) anzuzeigen. So kann dort überwacht werden, ob Änderungen an der Safety-Steuerung durchgeführt werden können.

3.2.2.3 Rücklesen und Änderungen von Teilen des Programmes

Für einen Reload Vorgang wird das vollständige, originale SILworX Projekt benötigt. Dieses sollte nur einem eingeschränkten Anwenderkreis zugänglich sein. Somit kann das Konzept des „least privilege“ unterstützt werden. Sollte ein Angreifer in der Lage sein, Zugriff auf das PES zu erlangen, so ist es unmöglich das Programm auszulesen oder nur Teile nachzuladen. Beides wird vom System nicht unterstützt.

3.2.2.4 PES-Benutzerverwaltung

PES Passwörter sind vor Abnahme zum letzten Mal zu ändern. Andernfalls hat dies eine Änderung des CRCs zur Folge. HIMA Passwörter werden verschlüsselt übertragen und abgelegt. (Die Grundeinstellung ist User: *Administrator*, Passwort: *Administrator*)

⚠ WARNUNG

Für den Secure-Betrieb ist eine Änderung der Passwörter unbedingt durchzuführen.

Standard-Passwörter sollten weder in der Inbetriebnahme und schon gar nicht im laufenden Betrieb verwendet werden. Optimaler Weise werden Passwörter direkt bei der ersten Kontaktaufnahme mit dem PES verändert.

Die für den Betrieb benötigten Passwörter sollten vom Endanwender eingestellt werden. (siehe Kapitel 3.2.3.10)

Benutzerkonten, die nicht mehr benötigt werden, sollten entfernt werden.

i Sollte sich der Anwender aus dem PES aussperren, so ist ein erneuter Zugriff ausschließlich durch Ausschalten und Einschalten der Steuerung (oder der Remote I/O) möglich. Dazu gilt während des Bootens für die verschiedenen HIMA Systeme:

- HIMatrix: der Reset-Taster unter der Gehäuseoberseite muss betätigt sein.
- HIQuad X CPU: der Mode-Schalter auf der Rückseite der Frontplatte muss auf INIT stehen.
- HIMax CPU: der Mode-Schalter auf der Frontseite muss auf INIT stehen.

3.2.2.5 Systemüberwachung

Mittels Systemvariablen kann der erste Zyklus nach einem Download oder Kaltstart (*Start-Zyklus*) oder nach einem Reload (*Reload-Zyklus*) erkannt werden. Auch die CRCs werden in Variablen abgebildet.

Beides kann mittels Reload geändert werden, sofern das richtige Projekt verfügbar ist. Werden die eigenen Projekte und Ladevorgänge auf diese Variable überwacht, so ist erkenntbar, ob ein Programm modifiziert wurde, denn eine Zielvariable kann nur an einer Stelle überschrieben werden.

Wird Multitasking verwendet, so wird pro Anwenderprogramm eine individuelle Prüfsumme erstellt.

Als zusätzliche Maßnahme kann im Anwenderprogramm eine Variable erstellt werden, die bei jedem Reload erhöht wird. Dafür steht eine Systemvariable zur Verfügung (*Reload-Zyklus*), die während des ersten Zyklus nach Reload aktiv ist. Diese ist für das gesamte System und für jedes einzelne Anwenderprogramm verfügbar.

3.2.2.6 Absicherung der Betriebssysteme

Alle Safety-CRC und MD5 (eine secure Prüfsumme) werden in der TÜV Versionsliste zur Verfügung gestellt. So kann sichergestellt werden, dass beim Download die richtigen Betriebssysteme verwendet werden.

3.2.3 Schutz beim Anschluss des PC für Programmierung

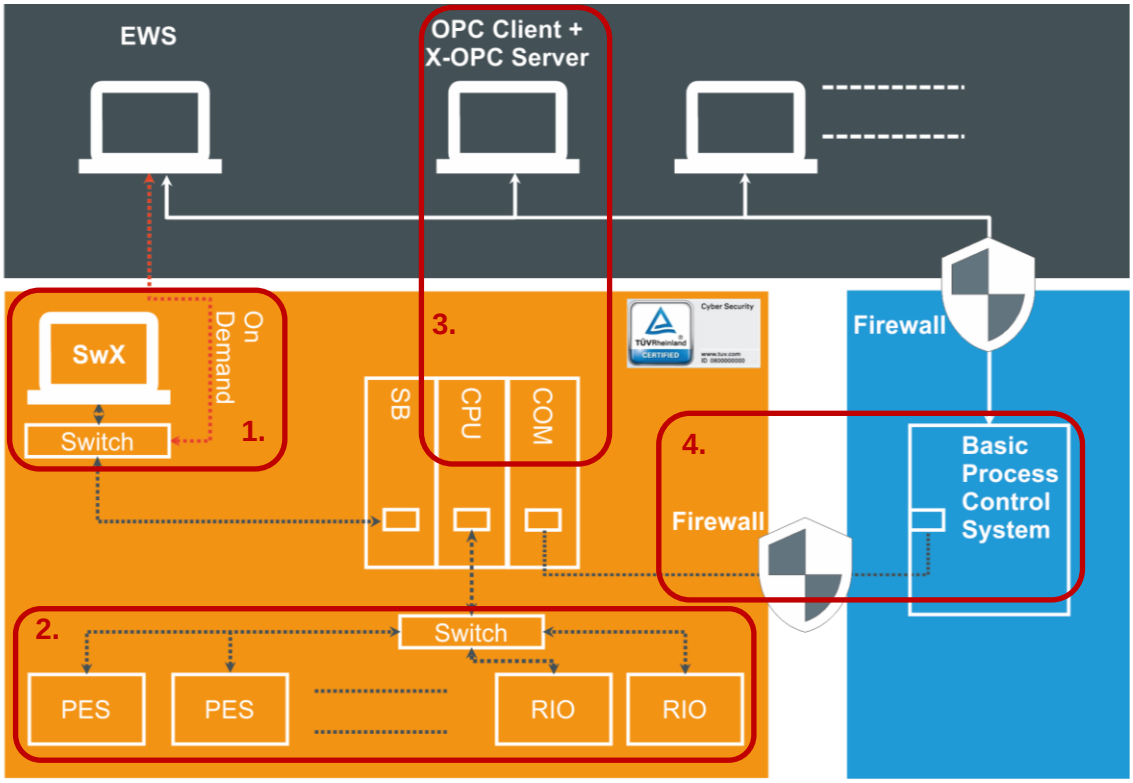


Bild 5: PADT an der Safety-Steuerung

Nr. 1 in dieser Übersicht.

3.2.3.1 Installation (SILworX)

Die MD5 Prüfsumme der Installationsdatei (setup.exe) ist auf der HIMA DVD im Verzeichnis der Installationsdatei mit aufgeführt und ist auch in der TÜV Versionsliste dokumentiert. So kann sichergestellt werden, dass eine korrekte Installation verwendet wird.

Abhängig von seiner individuellen Installation, kann der Anwender eine kryptographische Prüfsumme erstellen. Um Modifikationen der SILworX Installation festzustellen, kann diese Prüfsumme in regelmäßigen Abständen überprüft werden. Alternativ kann dies auch mit einem Application Whitelisting Programm automatisiert durchgeführt werden (siehe auch Kapitel 3.2.5.6).

3.2.3.2 SILworX PADT

Bei der SILworX Entwicklung wurde streng darauf geachtet, möglichst unabhängig vom Windows Betriebssystem zu bleiben.

Dies bedeutet insbesondere, dass die Safety der damit erstellten Anwenderprogramme NICHT vom benutzten Windows Betriebssystem abhängt oder von diesem beeinflusst wird.

Update-Zyklen von HIMA Software unterliegen aufgrund der nötigen TÜV-Zertifizierungen gewisser zeitlicher Beschränkungen. Daher ist es nicht möglich, den immer kürzer werdenden Windows-Betriebssystemzyklen zu folgen und alle Windows-Versionen, Varianten und Kombinationen von Hardware und Software zu testen. HIMA hat sehr positive Erfahrung mit Windows Updates. Alle Service und Engineering-Mitarbeiter arbeiten mit aktuellen Windows Betriebssystemen und testen somit HIMA Software im realen Umfeld. Durch einfache Tests lässt sich für das individuelle Umfeld die einwandfreie Funktionalität bestätigen:

1. Installation (wenn nicht schon geschehen).
2. Lizenz-Aktivierung (wenn nicht schon geschehen).
3. Öffnen der Online-Hilfe.
4. Erstellen oder Öffnen eines Projektes.
5. Code-Generierung (am Test Projekt!).
6. Aufbau der Verbindung zur Steuerung.

HIMA empfiehlt, den PADT-PC ausschließlich für den Zweck der Programmierung und Wartung des Safety-Systems einzusetzen.

Wird ein OPC Server verwendet, so sollte dieser auf einem anderen PC betrieben werden.

TIPP HIMA PES sind autarke Systeme. HIMA empfiehlt dringend, diese ohne angeschlossenes PADT zu betreiben. Der Anschluss des PADT sollte ausschließlich erfolgen, wenn es wirklich benötigt wird, z. B. Inbetriebnahme oder Wartung.

3.2.3.3 SILworX Benutzerverwaltung

Für den Schutz des SILworX Projektes und den Zugriff auf das PES sollte das angebotene Benutzermanagement verwendet werden.

⚠ WARNUNG

Für den Secure-Betrieb sollten unbedingt Passwörter eingerichtet werden.

Optimaler Weise wird direkt bei Projekterstellung ein Benutzermanagement eingerichtet.

Die für den Betrieb benötigten Passwörter sollten vom Endanwender eingestellt werden (siehe auch Kapitel 3.2.3.10).

i Unabhängig von den Benutzerrechten kann jeweils nur ein SILworX schreibend mit einem HIMA PES verbunden sein. Jedes weitere SILworX, das sich mit dem PES verbindet, kann lediglich lesend zugreifen.

SILworX Passwörter können jederzeit vom Security-Manager verändert werden, ohne Einfluss auf das Projekt in der Steuerung oder auf die Prüfsummen zu nehmen. Diese Passwörter sollten gemäß individueller Passwort-Richtlinie geändert werden, spätestens jedoch beim Ausscheiden eines Mitarbeiters.

SILworX Projekte können für das Öffnen mit SILworX mittels Passwort geschützt werden. Soll höheren Security-Ansprüchen genügt werden, so kann die Projektdatei (*.e3) kryptographisch mit einem entsprechenden Tool (z. B. veracrypt) verschlüsselt werden.

Der Verschluss dieser Projektdatei ist nicht nur für den Know-How Schutz wichtig. HIMA PES können im laufenden Betrieb, ohne Stopp, ein neues Anwenderprogramm erhalten. Dieser Vorgang wird Reload genannt. Ein Programm, das per Reload in die Steuerung geladen werden kann, muss auf der Version beruhen, die in der Steuerung ist. Steht diese Vorgängerversion nicht zur Verfügung, so kann kein Reload durchgeführt werden. Die Steuerung muss dann erst angehalten werden, was ggf. mittels vorhandener Überwachung im Betrieb festgestellt werden kann.

3.2.3.4 Backup-Recovery-Strategie

SILworX Projekte werden in Datenbanken gespeichert (eine Datei pro Projekt). Von dieser Projektdatei sollte zu gegebenem Anlass ein Backup erstellt werden. Es ist auch möglich, bei jedem Download automatisch eine Kopie des Projektes zu speichern.

HIMA empfiehlt, neben der Projektdatei auch die SILworX und OPC Installation, sowie alle verwendeten Betriebssysteme der Steuerungen zu sichern.

Liefert HIMA im Rahmen eines Projektes PCs aus, so werden Recovery-CD, SILworX und der von HIMA gelieferte Stand des Projektes zur Verfügung gestellt.

i Vollständige Backups sind an einem sicheren Ort zu verwahren (Sicher vor Feuer, Wasser, Fremdzugriff). Zugriff auf diese Backups sollte im Notfall schnell möglich sein.

3.2.3.5 SILworX Codevergleicher

SILworX stellt einen Codevergleicher zum Überprüfen der Änderungen zweier Projektversionen zur Verfügung. Es ist sicherzustellen, dass beim Einspielen eines neuen Anwenderprogrammes ausschließlich bewusste Änderungen durchgeführt wurden.

3.2.3.6 Know-How-Schutz

HIMA empfiehlt, für den Know-How Schutz die relevanten Funktionsbausteine zu verschließen. SILworX unterstützt hierfür 2 Möglichkeiten:

1. Funktionsbausteine können gegen Modifikation geschützt werden (*read only* in den Eigenschaften).
2. Der Zugriff auf Funktionsbausteine kann komplett blockiert werden (*Know-How Protection* in den Eigenschaften).

⚠ WARNUNG

Wird der Know-How-Schutz genutzt, so ist der Zugriff auf diesen Funktionsbaustein nicht mehr möglich. Auch HIMA verfügt nicht über die Möglichkeit einen lesbaren Funktionsbaustein aus diesem Code zu erzeugen. Eine spätere Modifikation ist somit nicht möglich. Der Anwender muss dafür sorgen, dass ein Backup des nicht geschützten Funktionsbausteins zur Verfügung steht.

3.2.3.7 Bevorzugter Anschluss des PADT

Die Auswahl des Anschluss eines PADT (PC mit Programmierwerkzeug SILworX) ist gezielt zu entscheiden. Abhängig davon, welche Gesamtkonstellation zur Verfügung steht, gilt folgende Reihenfolge:

HIMax	HIQuad X und HIMatrix
Ein PADT-Port einer X-SB, die nicht *Responsible* ist.	Ethernet-Port einer COM
Ethernet-Port einer COM	Ethernet-Port einer CPU
Ethernet-Port einer CPU	
Ein PADT-Port einer X-SB, die *Responsible* ist.	

Tabelle 2: Priorität zum Anschluss des PADT

Bei HIMatrix sollte für die Trennung VLAN gemäß Kapitel 0 eingestellt sein.

i Das PADT sollte in der gleichen Security-Zone wie das PES sein.

3.2.3.8 SILworX Diagnose

Mit SILworX ist es möglich, Diagnose-Informationen aus der Steuerung auszulesen. Diese Informationen können nicht vom PES gelöscht werden. Daher stehen Informationen, wie das Einloggen in das PES oder das Ändern sicherheitsrelevanter Parameter, dauerhaft zur Verfügung. Diese Informationen sind zur Nachvollziehbarkeit mit einem Zeitstempel versehen.

3.2.3.9 Fernzugriff auf das PADT

Ein Fernzugriff auf das PADT entspricht einem direkten Zugang auf das PES und ist daher zu vermeiden (siehe auch Kapitel 3.2.1.9).

3.2.3.10 Passwörter

Grundsätzlich gilt, dass geeignete Passwörter zu verwenden sind. Diese bestehen aus mehr als 12 Zeichen und enthalten Ziffern, Sonderzeichen, Groß- und Kleinbuchstaben.
Für die Trennung von Rollen sind individuelle Passwörter zu vergeben.

HIMA empfiehlt, für die Verwaltung von vielen Passwörtern einen Passwortmanager einzusetzen.

3.2.4 Schutz beim Anschluss des OPC-Servers

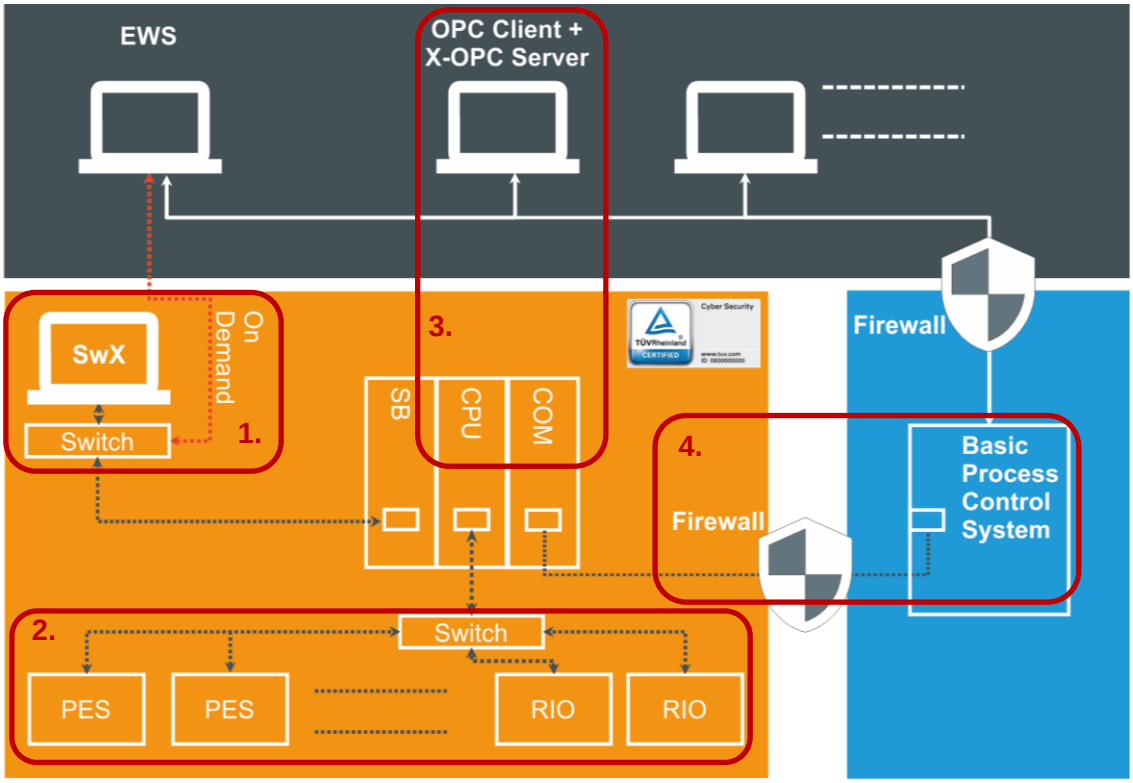


Bild 6: OPC-Server an der Safety-Steuerung

Je nach dem wo der OPC Server abläuft Nr. 3 oder Nr.4 in dieser Übersicht.

Die MD5 Prüfsumme der Installationsdatei (setup.exe) ist auf der HIMA DVD im Verzeichnis der Installationsdatei mit aufgeführt und in der TÜV-Versionsliste dokumentiert. Somit kann sichergestellt werden, dass eine korrekte Installation verwendet wird.

Der X-OPC Server für SILworX programmierte Systeme (HIMax, HIQuad X und HIMatrix) läuft als Service. Das bietet den Vorteil, dass der X-OPC Server aktiv ist, ohne dass ein Anwender eingeloggt ist. Selbst Änderungen können mittels SILworX vorgenommen werden, ohne dass eine Anmeldung in Windows benötigt wird.

Bei erhöhtem Schutzbedarf sollte zwischen X-OPC-Server und HIMA PES zusätzlich eine Firewall eingebaut werden, die ausschließlich die benötigten Ports für diese Kommunikation öffnet.

TIPP Der PC für den OPC-Server sollte nicht als Programmierstation eingesetzt werden. Zum einen kann somit die Programmierstation meist ausgeschaltet sein, was die Möglichkeit der Angriffe schon durch die zeitliche Einschränkung reduziert. Zum anderen ist der OPC typischerweise an ein übergeordnetes Netz mit größerer Gefährdung angeschlossen.

3.2.5 Konfiguration von PCs

HIMA bietet einen gehärteten PC an, der dem aktuellen Stand der Technik zur Absicherung entspricht.

Dieses Kapitel gibt Hinweise, wie die Konfiguration eines PC secure gestaltet werden kann. Die Erfahrung zeigt, dass Windows Systeme selten genau gleich sind. Daher können nur typische Merkmale beschrieben werden.

PCs in der Automatisierungstechnik ändern sich typischerweise im laufenden Betrieb nicht. Es muss keine Software zusätzlich installiert werden. Wenn doch, so ist das sehr selten der Fall. Des Weiteren wird davon ausgegangen, dass regelmäßige Updates sehr schwierig sind. Tägliche Updates von Virensignaturen können in den seltensten Fällen in Betracht gezogen werden. HIMA empfiehlt, ein mehrstufiges Schutzkonzept einzurichten, siehe auch Kapitel 2.3.2.

- BIOS-Passwortschutz.
- Schutz der Schnittstellen.
- Reduzierung der Windows-Rechte auf minimale Anforderungen.
- Reduzieren der Programme auf ein Minimum.
- Einsatz von Schutzsoftware.
- Projektschutz.
- Recovery Strategie.

3.2.5.1 BIOS-Einstellungen

Falls möglich, sollten BIOS Passwörter verwendet werden.

Die Boot-Reihenfolge ist derart einzustellen, dass als erstes die interne Festplatte und anschließend weitere Medien verwendet werden.

Falls es der Arbeitsablauf ermöglicht, sind alle nicht benötigten Schnittstellen (wireless, USB, Firewire, …) im BIOS auszuschalten.

3.2.5.2 Schutz der Schnittstellen

Ist ein Abschalten der Schnittstellen im BIOS nicht möglich, sind diese im Betriebssystem durch geeignete Maßnahmen zu schließen.

Für den Schutz der Schnittstellen ist die Windows Firewall zu aktivieren. Windows ist so weit zu verschließen, dass der Zugriff auf externe Medien nur mit Administrator-Rechten möglich ist. Der Administrator hat alle Medien vor Anschluss mit einem aktuellen Virenscanner zu überprüfen.

USB-Schnittstellen sind über das BIOS auszuschalten oder durch Software zu schützen. Hierzu können USB-Blocker verwendet werden, die nur den Zugriff auf zugelassene USB-Geräte erlauben.

3.2.5.3 Reduzierung von Rechten (Least Privilege)

Eine Grundidee der Absicherung ist es, die Angriffsfläche so weit wie möglich zu verringern. Die von Windows angebotenen Rechte sind auf ein Minimum zu beschränken.

Seit SILworX V4.X können sowohl Softlock als auch Hardlock betrieben werden. Administratorrechte sind lediglich für die Installation nötig. HIMA empfiehlt, im alltäglichen Gebrauch Windows mit Anwenderrechten zu betreiben.

Grundsätzlich kann jede Software eine Schwachstelle bilden, die potentiell als Einfallstor in das System verwendet werden kann. Es ist daher aus Gründen der Security ratsam, keine weitere Software auf dem verwendeten PC zu installieren. HIMA verbietet die Installation weiterer Software nicht, kann aber für deren Verhalten, speziell auch bezüglich der Security, keine Aussage treffen.

Die weitere Absicherung von Windows PC kann den individuellen Bedürfnissen angepasst werden. Es ist z. B. möglich, dem PC alle USB Schnittstellen abzuschalten, SILworX mit einem

Softlock zu Betreiben und PS2 Maus und Tastatur zu verwenden. HIMA empfiehlt, den Bildschirmschoner nach Zeit und die Windows Firewall einzurichten und zu aktivieren.

⚠ VORSICHT

Die Windows-Firewall-Einstellungen können durch das Einspielen von Patches beeinflusst werden. Der Schutz könnte dadurch gefährdet sein. Nach einem Patch oder Update sind die Firewall-Einstellungen zu kontrollieren.

Als weiterer Schutz kann der Windows Bildschirmschoner mit Passwort eingesetzt werden. Je nach individuellen Bedürfnissen sollten die Mitarbeiter angewiesen werden, beim Verlassen des PC diesen zu sperren (Tastenkombination Windows + L) oder auch das Projekt zu verlassen.

Die Passwortverwaltung der Active Domain (AD) kann prinzipiell für den Zugriff auf den PC verwendet werden. SILworX kann jedoch nicht an die AD angebunden werden. Des Weiteren ist eine AD in der Security-Zone für Safety nur in Ausnahmefällen sinnvoll.

3.2.5.4 Patches

HIMA Software ist Plattform-unabhängig entwickelt. HIMA Software kann jedoch nicht auf allen Plattformen mit allen möglichen Fremd-Software und deren Kombinationen getestet werden.

Zudem ist bei den meisten Schutzprodukten (Antiviren-Software) ein regelmäßiges (Offline) Update (Patches) erforderlich. Dies kann zur Änderung der Plattform und damit zu einem veränderten Verhalten des Systems führen (z. B. verringerte Geschwindigkeit oder Blockieren von Funktionen).

Derzeit können alle bekannten Schutzprogramme (z. B. Antiviren-Software) eingesetzt werden.

HIMA empfiehlt, (Offline) Updates in unkritischen Situationen durchzuführen, da Patches und Signaturen immer zu verändertem Verhalten führen können. Wechselwirkungen im Sinne der Verfügbarkeit können nicht vollständig ausgeschlossen werden.

HIMA verwendet in der eigenen Engineering-Abteilung und im eigenen Service immer alle aktuellen Patches und Signaturen.

Die Notwendigkeit eines Anschlusses an das Internet sollte trotz aller Schutzmaßnahmen wohl überlegt sein. War ein PC am Internet angeschlossen, so wird ein kompletter Virenscan empfohlen.

i Die Safety wird durch Patches und neue Signaturen nicht beeinflusst.

3.2.5.5 Antiviren-Software

HIMA empfiehlt den Einsatz von Schutzsoftware in PCs entsprechend der kundeneigenen Security-Policy. Üblich ist hier die Verwendung von Antiviren-Software. Diese kann mithilfe von Signaturen und Heuristik bekannte Schadsoftware erkennen.

TIPP HIMA gibt keine spezielle Antiviren-Software vor. Im direkten Safety-Umfeld sollte kein direkter Internet Zugang bestehen. Es ist also darauf zu achten, dass ein Offline Update von Signaturen (z. B. mittels CD) möglich ist.

3.2.5.6 Application Whitelisting

Einige HIMA Kunden haben Application Whitelisiting (AWL) bereits erfolgreich im Einsatz.

Gerade in einem Umfeld, in dem Updates nicht oder nur schwer möglich oder sinnvoll sind, sollte über Alternativen oder Ergänzungen zur gängigen Antiviren-Software nachgedacht werden. Zusätzlich zu den Zugriffsbeschränkungen im Betriebssystem kann Application Whitelisting schützen.

Mittlerweile wird Application Whitelisting als gleichwertig zu Antivirensoftware anerkannt.

3.2.5.7 Allgemeine Beschreibungen zum Schutz von PC

Absicherung eines PC mit Windows

Beschreibungen zum Schutz von Windows 7 sind z. B. in folgenden Quellen zu finden:

- BSI, Anleitung zur Installation und Minimierung eines Arbeitsplatz-PCs mit Windows 7:
  https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Internetsicherheit/isi-client-Anleitung_Windows-7.pdf?__blob=publicationFile
- c‘t 2011/Heft 3, *Der öffentliche PC*:
  http://www.heise.de/artikel-archiv/ct/2011/03/114_Der-oeffentliche-PC

Absicherung eines PC mit Windows 10

Eine Beschreibung zum Schutz von Windows 10 ist z. B. in folgender Quelle zu finden:

- BSI, IT-Grundschutz:
  https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/SYS/SYS_2_2_3_Clients_unter_Windows_10.html

3.2.6 Weitere Schutzmaßnahmen

HIMA Systeme verwenden in weiten Teilen Standard Technologien und können mit Standard Mitteln ihrer Wahl abgesichert werden. Z. B. ist neben dem Vermeiden von Gefahren das Erkennen von Gefahren ein wichtiger Bestandteil der Bekämpfung von Schadsoftware. Wichtig ist dann ein Plan, welche Aktion auf das Erkennen einer Gefahr zu folgen hat.

- Der Einsatz von Honeypots kann sinnvoll sein, ist relativ einfach im Einsatz und bietet gute Erkennungsraten. Hier bietet z. B. die Firma secXtreme eine industrietaugliche Lösung namens honeyBox an.
- Der Einsatz von Intrusion Detection und Intrusion Prevention Systemen kann sehr sinnvoll sein, erfordert derzeit jedoch Expertenwissen.

3.2.7 Tests durch eine unabhängige Stelle

HIMA Systeme müssen aufgrund der Anforderungen an die Safety einen hohen Anspruch an Qualität erfüllen. Die hochwertigen Implementierungen führen zu einer hohen Stabilität und damit zu geringer Anfälligkeit gegen Cyber Attacken. Dies wurde mit HIMax seit 2009 mehrfach mit Achilles Zertifikaten nachgewiesen.

Eine Basis ist, dass ausschließlich geplante Funktionen implementiert sind, also z. B. keine Backdoors. Das kann während der Security-Zertifizierung vom TÜV überprüft werden.

Für HIMax und HIMatrix F35 03 wurden exemplarisch eine Zertifizierung nach IEC 62443-4-1 und IEC 62443-4-2 für SL1 durchgeführt. Demzufolge sind entsprechende Entwicklungsprozesse und Funktionalitäten im Produkt berücksichtigt.

4 Weiteres

4.1 HIMA Information

Gerade bei Security-Themen ist es wichtig, auf dem aktuellen Stand der Information zu sein. HIMA empfiehlt, sich bei unserem DIS, dem Dokumenten Info Service, anzumelden. Der DIS informiert dann in gewünschten Intervallen über neue Dokumentationen (also auch neue Versionen dieses Handbuchs). Die Anmeldung erfolgt unter:
https://www.hima.com/de/downloads/

4.2 Externe Informationsquellen

Im Folgenden ist eine Liste an möglichen Informationsquellen und Standards zum Thema Security zu finden. Diese soll aufgrund der dynamischen Veränderungen, der örtlichen Gegebenheiten und aufgrund der Unterschiedlichkeit der Anwendungen als Hinweis für weitere Recherchen verstanden werden.

- **IEC 27000 ff** *Information technology — Security techniques*:
  Dies ist der allgemein und international anerkannte Standard für die Office-IT. Beschrieben wird ein ISMS (Informationssicherheitsmanagementsystem). Sektorspezifische Erweiterungen sind im Entstehen. So wurde 2013 der Teil ISO 27019 für die Energiewirtschaft verabschiedet.
- **IEC 62443-Familie**: In enger Kooperation mit der ISA 99 (hauptsächlich aus den USA getrieben) entsteht der internationaler Standard IEC 62443 (derzeit 13 Teile).
- **IEC 63074** *Security aspects related to functional safety of safety-related control systems*
  IEC TR 63069 *Industrial-process measurement, control and automation-framework for functional safety and security*
  Beschreiben das Zusammenwirken von Safety und Security.
- **VDI/VDE 2182**: *Informationssicherheit in der industriellen Automatisierung*
  Diese Richtlinie wurde vom GMA-Fachausschuss erarbeitet. Im ersten Teil wird ein generisches Vorgehensmodel vorgestellt. Die folgenden 3 Blätter mit jeweils 2 Teilen sind Beispielblätter für unterschiedliche Anwendungsbereiche. Aus Sicht von Herstellern, Integratoren und Endanwendern wird die Richtlinie jeweils in der Prozess- und Fabrikautomation angewandt. Blatt 4 ist derzeit in Arbeit und stellt eine „Roadmap“ dar.
- **NAMUR** hat ein Namur-Arbeitsblatt NA 163 *IT-Risikobeurteilung von PLT-Sicherheitseinrichtungen* für die Betrachtung von Safety-Systemen erstellet.
- Das **BSI** ist seit ca. 2013 im Umfeld der industriellen IT-Sicherheit aktiv. Hier existieren mehrere Veröffentlichungen, die von der Homepage des BSI bezogen werden können.
  https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/ICS/Empfehlungen/ICS/empfehlungen_node.html
- Das Department of Homeland Security und NIST sind sehr aktiv und bieten kostenfrei sehr gute Dokumente zum Download an, z. B. *Seven Steps to Effectively Defend Industrial Control Systems*.

Eine vollständige Liste wäre bei weitem zu umfangreich.
Eine solche Liste wird hier gepflegt: https://www.security-standards.de/ITSecurityGrid.html.

Anhang

Glossar

Begriff	Beschreibung
ARP	Address Resolution Protocol, Netzwerkprotokoll zur Zuordnung von Netzwerkadressen zu Hardwareadressen
AWL	Application Whitelisting
BSI	Bundesamt für Sicherheit in der Informationstechnik
BPCS	Basic Process Control System, Leitsystem
COM	Kommunikationsmodul
CRC	Cyclic Redundancy Check, Prüfsumme
CVSS	Common Vulnerability Scoring System, Industriestandard zur Beschreibung des Schweregrades von Sicherheitslücken in Computer-Systemen
DCS	Distributed Control System, Prozessleitsystem
DMZ	Demilitarisierte Zone
DoS	Denial of Service
EN	Europäische Normen
EWS	Engineering Workstation (siehe auch PADT)
FAT	Factory Acceptance Test, Werksabnahme, Funktionsprüfung einer Anlage beim Hersteller
ICMP	Internet Control Message Protocol: Netzwerkprotokoll für Status- und Fehlermeldungen
ICS	Industrial Control System, Automatisierungssystem
IDS	Intrusion Detection System, System zur Erkennung von Angriffen
IEC	International Electrotechnical Commission, Normungsgremium für Elektrotechnik
IP	Internet Protocol
ISMS	Informationssicherheitsmanagementsystem
IT	Informationstechnik
LLDP	Link Layer Discovery Protocol
MAC-Adresse	Hardware-Adresse eines Netzwerkanschlusses (Media Access Control)
NAT	Network Address Translation: Sammelbegriff für Verfahren, die automatisiert Adressinformationen in Datenpaketen durch andere ersetzen, um verschiedene Netze zu verbinden. Kommt typischerweise auf Routern zum Einsatz.
OPC	OLE for Process Control: Standard für den Daten- und Informationsaustausch von Software-Komponenten
OT	Operational Technology
PADT	Programming and Debugging Tool (nach IEC 61131-3), PC mit SILworX oder ELOP II Factory
PES	Programmierbares Elektronisches System
PLS	Prozessleitsystem
RIO	Remote IO (Erweiterungsgerät mit Ein und Ausgängen)
SIEM	Sicherheitsinformations- und Ereignis-Management
SIL	Safety Integrity Level (nach IEC 61508)
SNTP	Simple Network Time Protocol (RFC 1769)
SQL	Structured Query Language, Datenbanksprache
SwX	SILworX, (siehe PADT)
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VPS	Verbindungsprogrammierte Steuerung
XSS	Cross-Site-Scripting: Website-übergreifendes Scripting

Abbildungsverzeichnis

Tabellenverzeichnis

HANDBUCH
Automation Security
HI 801 372 D

Für weitere Informationen kontaktieren Sie:

HIMA Paul Hildebrandt GmbH
Albert-Bassermann-Str. 28
68782 Brühl, Germany

Telefon +49 6202 709-0
Fax +49 6202 709-107
E-Mail security@hima.com

Erfahren Sie online mehr über HIMA Lösungen:

www.hima.com/de/branchen-loesungen/cybersecurity/

www.hima.com