YASKAWA

HMI

TP-smart | HA1-A1A41-0 | Handbuch

HB160 | TP-smart | HA1-A1A41-0 | de | 24-40

smartPanel - TP410-SM

YASKAWA Europe GmbH
Philipp-Reis-Str. 6
65795 Hattersheim
Deutschland
Tel.: +49 6196 569-300
Fax: +49 6196 569-398
E-Mail: info@yaskawa.eu
Internet: www.yaskawa.eu.com

HA1-A1A41-0_000_TP410-SM,1,DE -

Inhaltsverzeichnis

1 Allgemein. 5
1.1 Copyright © YASKAWA Europe GmbH. 5
1.2 Über dieses Handbuch. 6
1.3 Sicherheitshinweise. 7
2 Hardwarebeschreibung. 9
2.1 Sicherheitshinweis für den Benutzer. 9
2.2 Leistungsmerkmale. 9
2.2.1 HMI - Ersatzteile. 10
2.3 Aufbau. 11
2.3.1 Übersicht. 11
2.3.2 Schnittstellen. 11
2.3.3 Speichermanagement. 14
2.4 Maße. 14
2.5 Allgemeine Daten für das smartPanel. 15
2.6 Einsatz unter erschwerten Betriebsbedingungen. 16
2.7 Technische Daten. 17
3 Einsatz 20
3.1 Montage. 20
3.2 Inbetriebnahme. 21
3.3 System Settings. 23
3.3.1 Übersicht. 23
3.3.2 Lokalisierung. 23
3.3.3 System. 24
3.3.4 Log. 24
3.3.5 Datum & Uhrzeit. 24
3.3.6 Netzwerk. 24
3.3.7 Sicherheit. 25
3.3.8 Anwendungen. 25
3.3.9 Dienste. 25
3.3.10 Verwaltung. 27
3.3.11 Anzeige. 27
3.3.12 Schriftarten. 27
3.3.13 Authentifizierung. 27
3.3.14 Neu starten. 28
3.4 Startup Sequence. 28
3.5 Tap-Tap Menü. 28
3.6 Firmwareupdate. 29
3.7 Anbindung an ein SPS-System. 31

3.8 Integrierte Server. 32
3.8.1 FTP-Server. 32
3.8.2 VNC-Server. 33
3.8.3 Web-Server. 33
4 Industrielle Sicherheit und Aufbaurichtlinien. 34
4.1 Industrielle Sicherheit in der Informationstechnologie. 34
4.1.1 Absicherung von Hardware und Applikationen. 35
4.1.2 Absicherung von PC-basierter Software. 36
4.2 Aufbaurichtlinien. 36

1 Allgemein

1.1 Copyright © YASKAWA Europe GmbH

EU-Konformitätserklärung

Hiermit erklärt YASKAWA Europe GmbH, dass die Produkte und Systeme mit den grundlegenden Anforderungen und den anderen relevanten Vorschriften übereinstimmen. Die Übereinstimmung ist durch CE-Zeichen gekennzeichnet.

Informationen zur Konformitätserklärung

Für weitere Informationen zur CE-Kennzeichnung und Konformitätserklärung wenden Sie sich bitte an Ihre Landesvertretung der YASKAWA Europe GmbH.

Warenzeichen

Linux ist ein eingetragenes Warenzeichen von Linus Torvalds.

Alle anderen erwähnten Firmennamen und Logos sowie Marken- oder Produktnamen sind Warenzeichen oder eingetragene Warenzeichen ihrer jeweiligen Eigentümer.

Allgemeine Nutzungsbedingungen

Es wurden alle Anstrengungen unternommen, um sicherzustellen, dass die in diesem Dokument enthaltenen Informationen zum Zeitpunkt der Veröffentlichung vollständig und richtig sind. Fehlerfreiheit kann nicht garantiert werden, das Recht auf Änderungen der Informationen bleibt jederzeit vorbehalten. Eine Informationspflicht gegenüber dem Kunden über etwaige Änderungen besteht nicht. Der Kunde ist aufgefordert, seine Dokumente aktiv aktuell zu halten. Der Einsatz der Produkte mit zugehöriger Dokumentation hat immer in Eigenverantwortung des Kunden unter Berücksichtigung der geltenden Richtlinien und Normen zu erfolgen.
Die vorliegende Dokumentation beschreibt alle heute bekannten Hard- und Software-Einheiten und Funktionen. Es ist möglich, dass Einheiten beschrieben sind, die beim Kunden nicht vorhanden sind. Der genaue Lieferumfang ist im jeweiligen Kaufvertrag beschrieben.

Dokument-Support

Wenden Sie sich an Ihre Landesvertretung der YASKAWA Europe GmbH, wenn Sie Fehler anzeigen oder inhaltliche Fragen zu diesem Dokument stellen möchten. Sie können YASKAWA Europe GmbH über folgenden Kontakt erreichen:

E-Mail: Documentation.HER@yaskawa.eu

Technischer Support

Wenden Sie sich an Ihre Landesvertretung der YASKAWA Europe GmbH, wenn Sie Probleme mit dem Produkt haben oder Fragen zum Produkt stellen möchten. Ist eine solche Stelle nicht erreichbar, können Sie den Yaskawa Kundenservice über folgenden Kontakt erreichen:

YASKAWA Europe GmbH,
European Headquarters, Philipp-Reis-Str. 6, 65795 Hattersheim, Deutschland
Tel.: +49 6196 569 500 (Hotline)
E-Mail: support@yaskawa.eu

1.2 Über dieses Handbuch

Zielsetzung und Inhalt

Das Handbuch beschreibt das smartPanel HA1-A1A41-0.

- Beschrieben wird Aufbau, Projektierung und Anwendung.
- Das Handbuch ist geschrieben für Anwender mit Grundkenntnissen in der Automatisierungstechnik.
- Das Handbuch ist in Kapitel gegliedert. Jedes Kapitel beschreibt eine abgeschlossene Thematik.
- Als Orientierungshilfe stehen im Handbuch zur Verfügung:
  - Gesamt-Inhaltsverzeichnis am Anfang des Handbuchs.
  - Verweise mit Seitenangabe.

Gültigkeit der Dokumentation

Produkt	Best.-Nr.	ab Version	
TP 410-SM	HA1-A1A41-0	HW: 01	Board Support Package (BSP): V3.1.403

Piktogramme und Signalwörter

Wichtige Textteile sind mit folgenden Piktogrammen und Signalwörtern hervorgehoben:

GEFAHR
Unmittelbare oder drohende Gefahr. Personenschäden sind möglich.

VORSICHT
Bei Nichtbefolgen sind Sachschäden möglich.

Zusätzliche Informationen und nützliche Tipps.

1.3 Sicherheitshinweise

Bestimmungsgemäße Verwendung

- Es liegt in der Verantwortung des Kunden, die Konformität mit allen Standards, Vorschriften oder Bestimmungen zu erfüllen, die gelten, wenn das Yaskawa-Produkt in Kombination mit anderen Produkten verwendet wird.
- Der Kunde muss sich vergewissern, dass das Yaskawa-Produkt für die vom Kunden verwendeten Anlagen, Maschinen und Geräte geeignet ist.
- Wenn das Yaskawa-Produkt auf eine Art und Weise verwendet wird, welche nicht in diesem Handbuch beschrieben ist, kann der durch das Yaskawa-Produkt gebotene Schutz beeinträchtigt werden.
- Wenden Sie sich an Yaskawa, um festzustellen, ob der Einsatz in den folgenden Anwendungen zulässig ist. Ist der Einsatz in der jeweiligen Anwendung zulässig, so ist das Yaskawa-Produkt mit zusätzlichen Toleranzen in den Nennwerten und Spezifikationen zu verwenden, und es sind Sicherheitsmaßnahmen vorzusehen, um die Gefahren im Fehlerfall zu minimieren.
  - Verwendung im Freien, Verwendung mit möglicher chemischer Verunreinigung oder elektrischer Störung oder Verwendung unter Bedingungen oder in Umgebungen, welche nicht in Produktkatalogen oder Handbüchern beschrieben sind
  - Steuerungssysteme für Kernenergie, Verbrennungssysteme, Eisenbahnsysteme, Luftfahrtsysteme, Fahrzeugsysteme, medizinische Geräte, Vergnügungsmaschinen und Anlagen, welche gesonderten Industrie- oder Regierungsvorschriften unterliegen
  - Systeme, Maschinen und Geräte, die eine Gefahr für Leben oder Eigentum darstellen können
  - Systeme, die ein hohes Maß an Zuverlässigkeit erfordern, wie z. B. Systeme zur Gas-, Wasser- oder Stromversorgung oder Systeme, die 24 Stunden am Tag in Betrieb sind
  - Andere Systeme, die ein ähnlich hohes Maß an Sicherheit erfordern
- Verwenden Sie das Yaskawa-Produkt niemals für eine Anwendung, die eine ernsthafte Gefahr für Leben oder Eigentum darstellt, ohne vorher sicherzustellen, dass das System so ausgelegt ist, dass es das erforderliche Sicherheitsniveau mit Risikowarnungen und Redundanz gewährleistet und dass das Yaskawa-Produkt ordnungsgemäß ausgelegt und installiert ist.
- Die in den Produktkatalogen und Handbüchern beschriebenen Schaltungsbeispiele und sonstigen Anwendungsbeispiele dienen als Referenz. Überprüfen Sie die Funktionalität und Sicherheit der tatsächlich zu verwendenden Geräte und Anlagen, bevor Sie das Yaskawa-Produkt einsetzen.
- Lesen und verstehen Sie alle Verwendungsverbote und Vorsichtsmaßnahmen, und bedienen Sie das Yaskawa-Produkt korrekt, um versehentliche Schäden an Dritten zu vermeiden.

Einsatzbereich

Das System ist konstruiert und gefertigt für:

- Kommunikation und Prozesskontrolle
- Allgemeine Steuerungs- und Automatisierungsaufgaben
- den industriellen Einsatz
- den Betrieb innerhalb der in den technischen Daten spezifizierten Umgebungsbedingungen
- den Einbau in einen Schaltschrank

GEFAHR

Das Gerät ist nicht zugelassen für den Einsatz

- in explosionsgefährdeten Umgebungen (EX-Zone)

Haftungsausschluss

- Das Yaskawa-Produkt eignet sich nicht für den Einsatz in lebenserhaltenden Maschinen bzw. System.
- Wenden Sie sich an einen Yaskawa-Vertreter oder an Ihren Yaskawa-Vertriebsmitarbeiter, wenn Sie die Anwendung des Yaskawa-Produkts für spezielle Zwecke in Betracht ziehen, wie z.B. für Maschinen oder Systeme, welche in Personenkraftwagen, in der Medizin, in Flugzeugen und in der Luft- und Raumfahrt eingesetzt werden, für die Energieversorgung von Netzen, für die elektrische Energieversorgung oder für die Schaltung von Unterwasserrelais.

GEFAHR

Wenn Sie dieses Yaskawa-Produkt in Anwendungen einsetzen, bei denen ein Versagen des Geräts zum Verlust von Menschenleben, zu einem schweren Unfall oder zu körperlichen Verletzungen führen kann, müssen Sie entsprechende Sicherheitsvorrichtungen installieren.

- Wenn Sie die Sicherheitsvorrichtungen nicht ordnungsgemäß installieren, kann dies zu schweren Verletzungen oder zum Tod führen.

Entsorgung

Zur Entsorgung des Geräts nationale Vorschriften beachten!

Dokumentation

Das Handbuch ist zugänglich zu machen für alle Mitarbeiter in:

- Projektierung
- Installation
- Inbetriebnahme
- Betrieb

VORSICHT

Vor Inbetriebnahme und Betrieb der in diesem Handbuch beschriebenen Komponenten unbedingt beachten:

- Änderungen am Automatisierungssystem nur im spannungslosen Zustand vornehmen!
- Anschluss und Änderung nur durch ausgebildetes Elektro-Fachpersonal
- Nationale Vorschriften und Richtlinien im jeweiligen Verwenderland beachten und einhalten (Installation, Schutzmaßnahmen, EMV ...)

2 Hardwarebeschreibung

2.1 Sicherheitshinweis für den Benutzer

Handhabung elektrostatisch gefährdeter Baugruppen

Die Baugruppen sind mit hochintegrierten Bauelementen in MOS-Technik bestückt. Diese Bauelemente sind hoch empfindlich gegenüber Überspannungen, die z.B. bei elektrostatischer Entladung entstehen. Zur Kennzeichnung dieser gefährdeten Baugruppen wird nachfolgendes Symbol verwendet:

Das Symbol befindet sich auf Baugruppen, Baugruppenträgern oder auf Verpackungen und weist so auf elektrostatisch gefährdete Baugruppen hin. Elektrostatisch gefährdete Baugruppen können durch Energien und Spannungen zerstört werden, die weit unterhalb der Wahrnehmungsgrenze des Menschen liegen. Hantiert eine Person, die nicht elektrisch entladen ist, mit elektrostatisch gefährdeten Baugruppen, können Spannungen auftreten und zur Beschädigung von Bauelementen führen und so die Funktionsweise der Baugruppen beeinträchtigen oder die Baugruppe unbrauchbar machen. Auf diese Weise beschädigte Baugruppen werden in den wenigsten Fällen sofort als fehlerhaft erkannt. Der Fehler kann sich erst nach längerem Betrieb einstellen. Durch statische Entladung beschädigte Bauelemente können bei Temperaturänderungen, Erschütterungen oder Lastwechseln zeitweilige Fehler zeigen. Nur durch konsequente Anwendung von Schutzeinrichtungen und verantwortungsbewusste Beachtung der Handhabungsregeln lassen sich Funktionsstörungen und Ausfälle an elektrostatisch gefährdeten Baugruppen wirksam vermeiden.

Versenden von Baugruppen

Verwenden Sie für den Versand immer die Originalverpackung.

Messen und Ändern von elektrostatisch gefährdeten Baugruppen

Bei Messungen an elektrostatisch gefährdeten Baugruppen sind folgende Dinge zu beachten:

- Potenzialfreie Messgeräte sind kurzzeitig zu entladen.
- Verwendete Messgeräte sind zu erden.

Bei Änderungen an elektrostatisch gefährdeten Baugruppen ist darauf zu achten, dass ein geerdeter Lötkolben verwendet wird.

VORSICHT

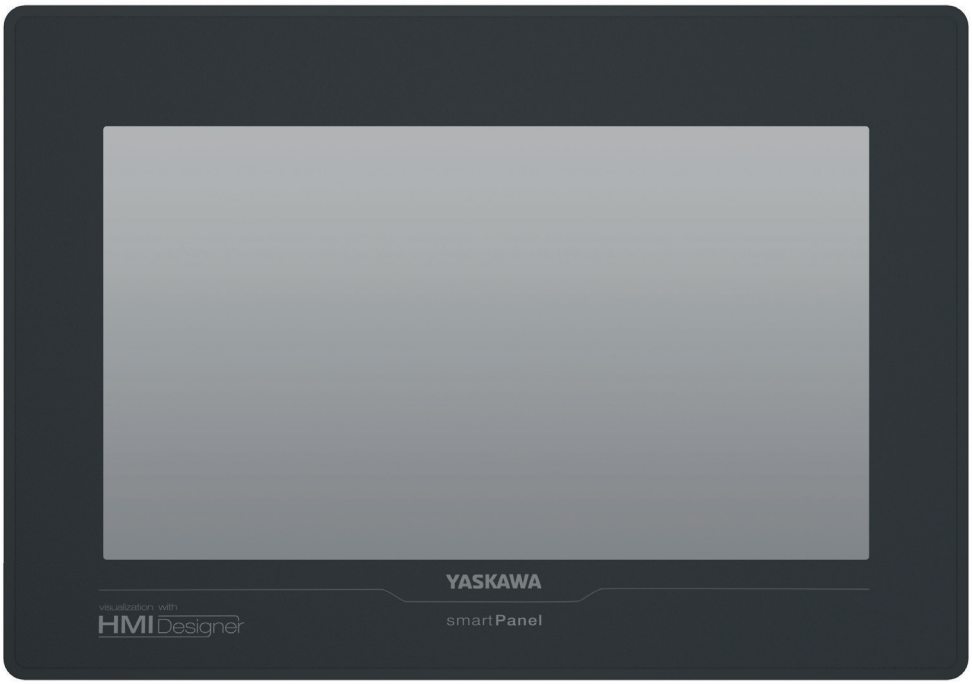
Bei Arbeiten mit und an elektrostatisch gefährdeten Baugruppen ist auf ausreichende Erdung des Menschen und der Arbeitsmittel zu achten.

2.2 Leistungsmerkmale

Allgemeines

Mit dem smartPanel können Sie Betriebszustände und aktuelle Prozesswerte einer angekoppelten SPS ausgeben und verändern. Das smartPanel ist ein auf Linux® basierender "Embedded PC" in kompakter und modularer Bauform. Neben den umfangreichen Linux® Funktionen besitzt das smartPanel vielfältige Kommunikationsmöglichkeiten wie VNC und Web Server. Hiermit können Sie auf einfache Weise Ihr smartPanel konfigurieren, steuern und fernwarten. Das smartPanel eignet sich besonders zur Überwachung und Steuerung von Prozessabläufen. Zur Projektierung ist der HMI Designer zu verwenden.

TP 410-SM



- Linux®
- Projektierung mit dem HMI Designer
- Prozessor ARM Cortex A8 1GHz
- Flash Speicher 4GB, RAM 512MB DDR
- RS232/RS422/RS485, USB-A- und Ethernet-Schnittstelle
- Robustes Kunststoffgehäuse
- Displayauflösung 600 x 1024 / 1024 x 600, 64K Farben
- Uhr gepuffert (Goldcap)
- Resistiver Touchscreen
- Einfachste Montage über Montageclips
- Schutzart IP66, Typ 2 und 4X (Frontseite) / IP20 (Rückseite)

Bestelldaten

Typ	Bestellnummer	Beschreibung
TP 410-SM	HA1-A1A41-0	10,1" TFT color, RS232/RS422/RS485, USB-A, Ethernet RJ45

2.2.1 HMI - Ersatzteile

Ersatzteile

Für das smartPanel erhalten Sie folgende Ersatzteile:

Ersatzteil	Best.-Nr.	Beschreibung	Verpackungs-einheit
	692-9AX00	3-fach Steckverbinder für Spannungsversorgung smartPanel.	20 Stück

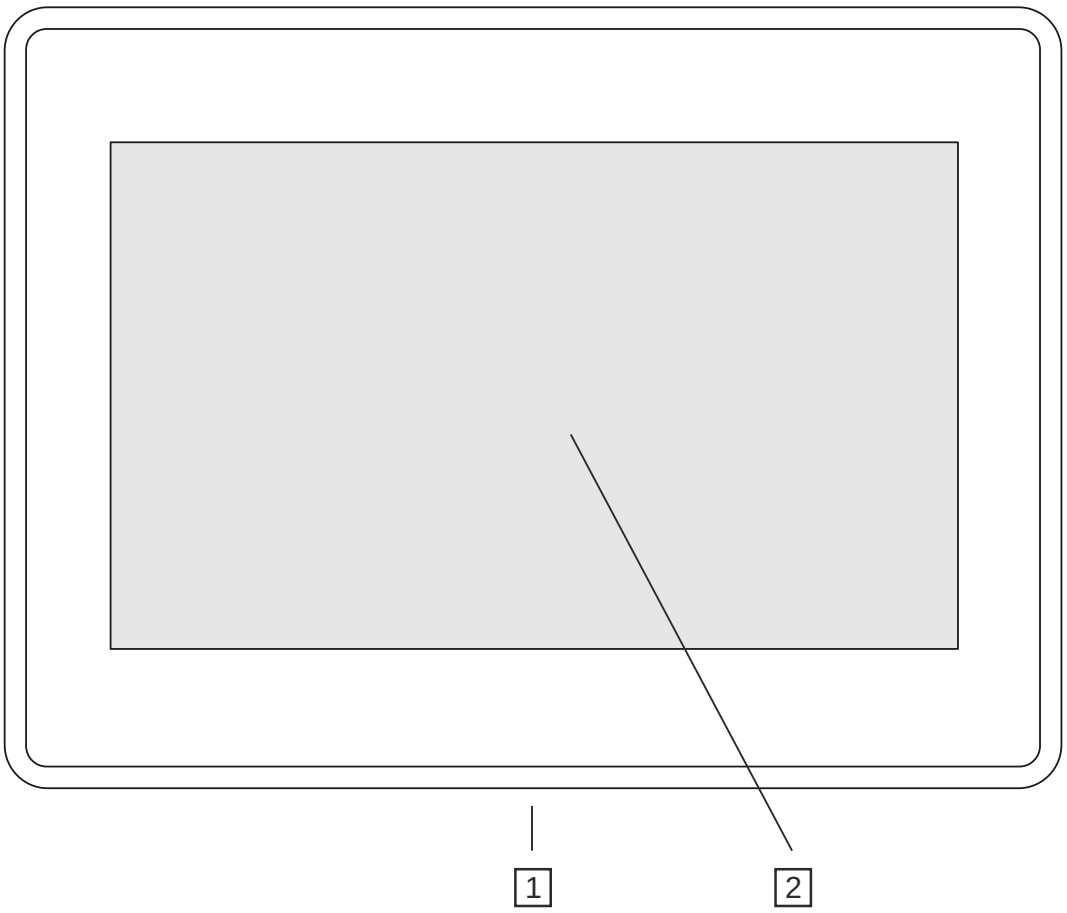
VORSICHT

Bitte beachten Sie, dass Sie die Ersatzteile ausschließlich mit Yaskawa-Modulen einsetzen dürfen. Der Einsatz mit Modulen von Fremdherstellern ist nicht zulässig!

2.3 Aufbau

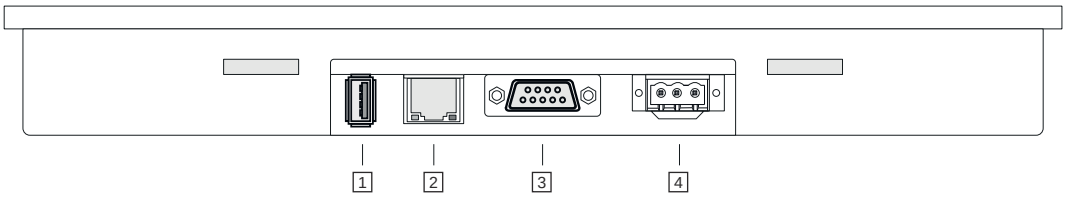
2.3.1 Übersicht

Frontansicht



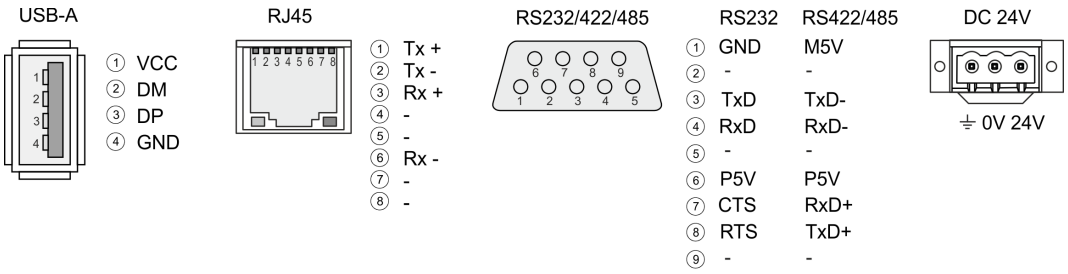
1 Schnittstellen
2 Display mit berührempfindlichem Bereich (Touch-Screen)

Ansicht von unten



1 USB-A-Schnittstelle USB 2.0
2 RJ45-Buchse für Ethernet-Kommunikation LAN
3 RS232/RS422/RS485-Schnittstelle COM
4 Anschluss für DC 24V Spannungsversorgung

2.3.2 Schnittstellen



"Host"-USB-A

Über die "Host"-USB-A-Schnittstelle haben Sie die Möglichkeit USB-Maus, -Tastatur, -Stick oder -Festplatte anzuschließen.

Ethernet-Anschluss

Über die RJ45-Buchse haben Sie einen Twisted-Pair-Anschluss an Ethernet. Die Ethernet-Schnittstelle verfügt über zwei LEDs zur Statusanzeige

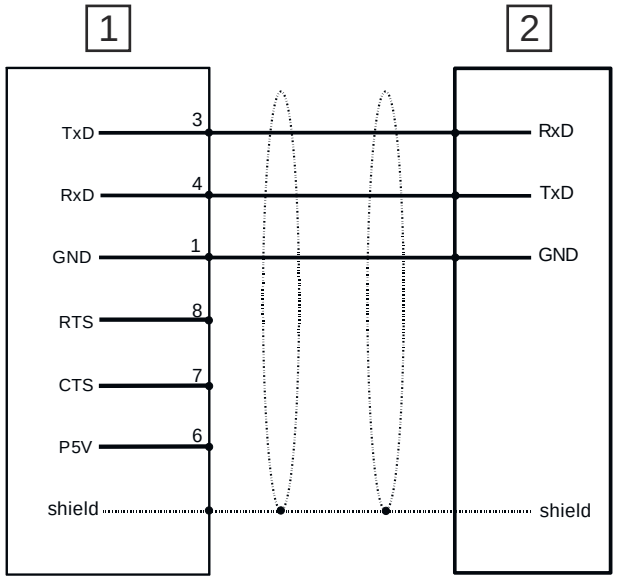
LEDs

grün	gelb	Beschreibung
an	aus	keine Verbindung
blinkt	an	100Mbit/s Verbindung
blinkt	aus	10Mbit/s Verbindung

RS232-Schnittstelle

9poliger SubD-Stecker

- Schnittstelle ist kompatibel zur COM Schnittstelle eines PC
- Logische Zustände als Spannungspegel
- Punkt-zu-Punkt-Kopplung mit serieller Vollduplex-Übertragung in 2-Draht-Technik bis zu einer Entfernung von 15m
- Datenübertragungsrate bis 115,2kBit/s

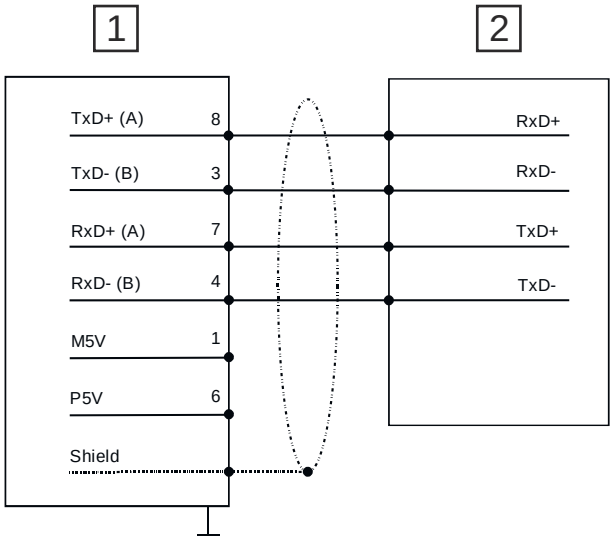


1 RS232-Schnittstelle
2 Peripherie

RS422/485-Schnittstelle

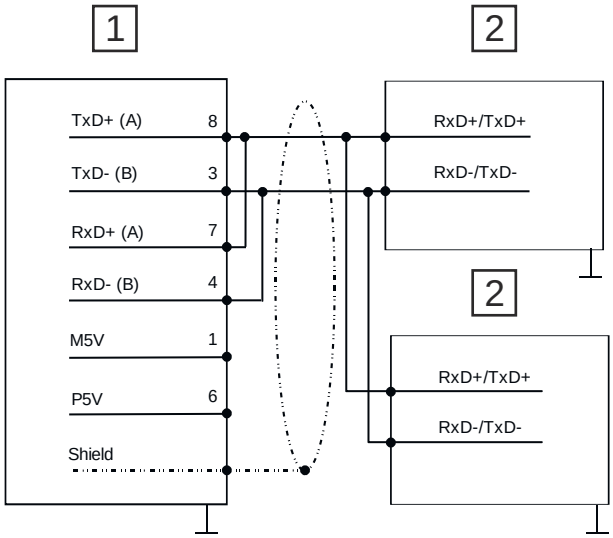
9polige SubD-Buchse

- Logische Zustände als Spannungsdifferenz zwischen 4 verdrillten Adern
- Serielle Busverbindung in 4-Drahttechnik im Vollduplex-Verfahren
- Datenübertragung bis 500m Entfernung
- Datenübertragungsrate bis 115,2kBaud



1 Betrieb als RS422-Schnittstelle
2 Peripherie

- Serielle Busverbindung in 2-Drahttechnik im Halbduplex-Verfahren



1 Betrieb als RS485-Schnittstelle
2 Peripherie

Spannungsversorgung

Das smartPanel besitzt ein eingebautes Netzteil. Das Netzteil ist mit DC 24V (10 ... 32 VDC) zu versorgen. Hierzu befindet sich an der Unterseite ein DC 24V Anschluss ➥ *"Versorgungsspannung anschließen" ...Seite 21*.

2.3.3 Speichermanagement

Übersicht

Dem smartPanel stehen folgende Speichersysteme zur Verfügung:

- 512MB Arbeitsspeicher (RAM)
- 4GB Anwenderspeicher (Flash)
- USB-Speichermedium über "Host"-USB-A-Schnittstelle

Arbeitsspeicher (RAM)

Das smartPanel besitzt einen 512MB großen Arbeitsspeicher. Der Arbeitsspeicher ist ungepuffert und wird nach dem Ausschalten gelöscht.

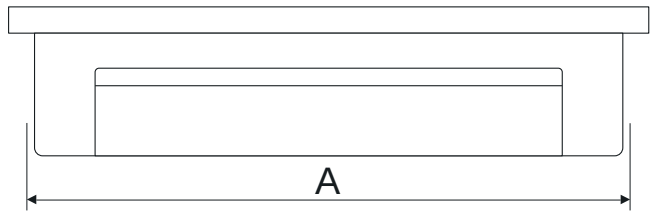
Anwenderspeicher (Flash)

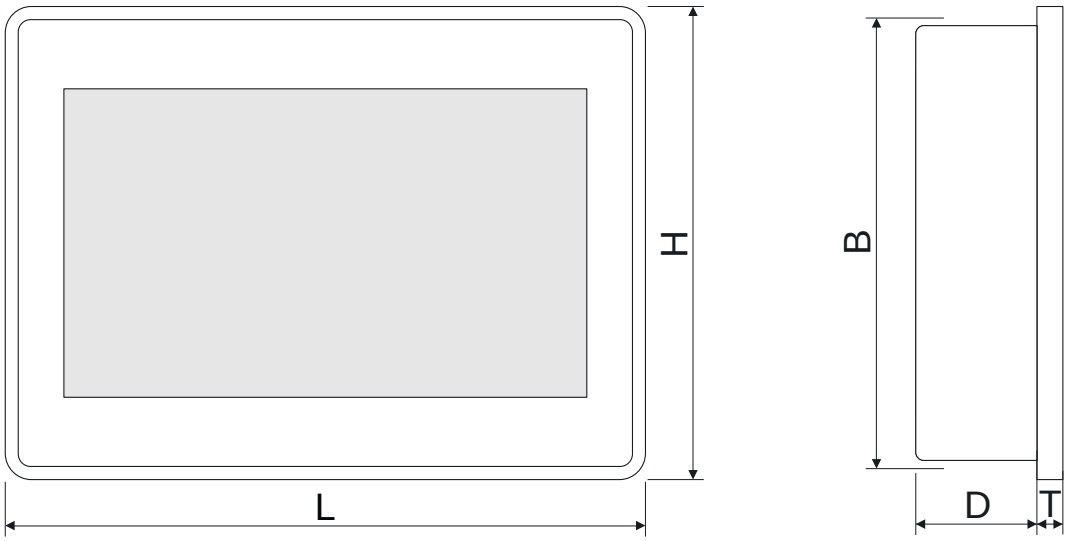
Als internes permanentes Speichermedium besitzt das smartPanel einen 4GB Flash-Speicher.

USB-Speichermedium (USB 2.0)

Das smartPanel unterstützt die Anbindung von USB-Sticks und USB-Laufwerken über die "Host"-USB-A-Schnittstelle. Nach dem Anstecken wird das Speichermedium als *USB Hard Disk* unter *My Device* aufgelistet.

2.4 Maße





Einbaumaße

Frontseite (L x H)	282 x 197 mm
Tiefe (D+T)	29 + 6 mm
Einbauausschnitt (A x B)	271 x 186 mm

Die Schutzarten für Wasser- und Staubschutz werden nur dann gewährleistet, wenn folgendes eingehalten wird:

- *Materialdicke für den Einbauausschnitt: 1,5 ... 6mm*
- *Abweichung des Einbauausschnitts von der Ebenheit, bezogen auf die Außenabmessungen des Bediengeräts: ≤ 0,5mm*
- *Zulässige Oberflächenrauhigkeit im Bereich der Einbaudichtung: ≤ 120µm (Rz 120)*

2.5 Allgemeine Daten für das smartPanel

Konformität und Approbation		
Konformität		
CE	2014/30/EU	EMV-Richtlinie
RoHS (EU)	2011/65/EU	Richtlinie zur Beschränkung der Verwendung bestimmter gefährlicher Stoffe in Elektro- und Elektronikgeräten
UKCA	2016 No. 1101	Electrical Equipment (Safety) Regulations
	2016 No. 1091	Electromagnetic Compatibility Regulations
RoHS (UK)	2012 No. 3032	Use of Certain Hazardous Substances
Approbation		
Zertifizierungen	-	Siehe technische Daten

Personenschutz und Geräteschutz		
Schutzart	-	Rückseite: IP20; Front: IP66, NEMA Typ 2 und Typ 4x
Potenzialtrennung		
Zum Feldbus	-	Galvanisch entkoppelt
Zur Prozessebene	-	Galvanisch entkoppelt
Isolationsfestigkeit		-
Isolationsspannung gegen Bezugserde		
Eingänge / Ausgänge	-	AC / DC 50V, bei Prüfspannung AC 500V
Schutzmaßnahmen	-	gegen Kurzschluss

Umgebungsbedingungen gemäß EN 61131-2		
Klimatisch		
Lagerung /Transport	EN 60068-2-14	-20…+70°C
Betrieb		
Horizontaler Einbau	EN 61131-2	0…+40°C
Vertikaler Einbau	EN 61131-2	0…+50°C
Luftfeuchtigkeit	EN 60068-2-30	RH1 (ohne Betauung, relative Feuchte 5 … 85%)
Verschmutzung	EN 61131-2	Verschmutzungsgrad 2
Mechanisch		
Schwingung	EN 60068-2-6	1g, 9Hz ... 150Hz
Schock	EN 60068-2-27	15g, 11ms

Montagebedingungen		
Einbauort	-	Im Schaltschrank
Einbaulage	-	Horizontal und vertikal

EMV	Norm		Bemerkungen
Störaussendung	EN 61000-6-4		Class A (Industriebereich)
Störfestigkeit	EN 61000-6-2		Industriebereich
Zone B		EN 61000-4-2	ESD 8kV bei Luftentladung (Schärfegrad 3), 4kV bei Kontaktentladung (Schärfegrad 2)
		EN 61000-4-3	HF-Einstrahlung (Gehäuse) 80MHz … 1000MHz, 10V/m, 80% AM (1kHz) 1,4GHz ... 2,0GHz, 3V/m, 80% AM (1kHz) 2GHz ... 2,7GHz, 1V/m, 80% AM (1kHz)
		EN 61000-4-6	HF-Leitungsgeführt 150kHz … 80MHz, 10V, 80% AM (1kHz)
		EN 61000-4-4	Burst
		EN 61000-4-5	Surge[1]

1) Aufgrund der energiereichen Einzelimpulse ist bei Surge eine angemessene externe Beschaltung mit Blitzschutzelementen wie z.B. Blitzstromableitern und Überspannungsableitern erforderlich.

2.6 Einsatz unter erschwerten Betriebsbedingungen

Ohne zusätzlich schützende Maßnahmen dürfen die Produkte nicht an Orten mit erschwerten Betriebsbedingungen; z.B. durch:

- *Staubentwicklung*
- *chemisch aktive Substanzen (ätzende Dämpfe oder Gase)*
- *starke elektrische oder magnetische Felder*

eingesetzt werden!

2.7 Technische Daten

Artikelnr.	HA1-A1A41-0
Bezeichnung	smartPanel TP410-SM
Display	
Displaygröße (diagonal)	10,1 "
Displaygröße (Breite)	224 mm
Displaygröße (Höhe)	128 mm
Auflösung	1024 x 600 / 600 x 1024
Seitenverhältnis	16:9
Displaytyp	TFT color (64K Farben)
MTBF Hintergrundbeleuchtung (bei 25°C)	20000 h
Systemeigenschaften	
Prozessor	Cortex-A8 1GHz
Betriebssystem	Linux 4.14.94
Anwendungssoftware	HMI Runtime
Arbeitsspeicher	512 MB
Anwenderspeicher	4 GB
Nutzbarer Speicher (Anwenderdaten)	60 MB
SD/MMC Slot	-
CF Card Slot Typ II	-
CFast Slot	-
Uhrzeit	
Uhr gepuffert	✓
Uhr Pufferungsdauer (min.)	2 w
Art der Pufferung	Goldcap
Ladezeit für 50% Pufferungsdauer	5 h
Ladezeit für 100% Pufferungsdauer	10 h
Genauigkeit (max. Abweichung je Tag)	8 s
Bedienelemente	
Touchscreen	resistiv
Touchfunktion	Single Touch
Tastatur	extern via USB
Maus	extern via USB
Schnittstellen	
MPI, PROFIBUS-DP	-
MPI, PROFIBUS-DP Anschluss	-
Seriell, COM1	RS232 / RS422 / RS485
COM1 Anschluss	9 poliger SubD Stecker

Artikelnr.	HA1-A1A41-0
Seriell, COM2	-
COM2 Anschluss	-
Anzahl USB-A Anschlüsse	1
USB-A Anschluss	USB-A (Host)
Anzahl USB-B Anschlüsse	-
USB-B Anschluss	-
Anzahl Ethernet Anschlüsse	1
Ethernet	Ethernet 10/100 MBit
Ethernet Anschluss	RJ45
Integrierter Ethernet-Switch	-
Videoanschlüsse	-
Audioanschlüsse	-
Technische Daten Stromversorgung	
Versorgungsspannung (Nennwert)	DC 24 V
Versorgungsspannung (zulässiger Bereich)	10 - 32 VDC
Verpolschutz	✓
Stromaufnahme (im Leerlauf)	0,1 A
Stromaufnahme (Nennwert)	0,38 A
Einschaltstrom	47 A
I^2t	0,7 A^2s
Verlustleistung	9 W
Status, Alarm, Diagnosen	
Statusanzeige	keine
Versorgungsspannungsanzeige	keine
Mechanische Daten	
Gehäuse / Schutzklasse	
Material	PC + ABS
Befestigung	Montageclips
Schutzklasse IP Frontseite	IP 66
Schutzklasse IP Rückseite	IP 20
Schutzklasse NEMA Frontseite	Type 2, 4X
Schutzklasse NEMA Rückseite	-
Abmessungen	
Frontseite	282 mm x 197 mm x 6 mm
Rückseite	268 mm x 183 mm x 29 mm
Einbau-Ausschnitt	
Breite	271 mm
Höhe	186 mm

Artikelnr.	HA1-A1A41-0
Minimale Fronttafeldicke	1,5 mm
Maximale Fronttafeldicke	6 mm
Gewicht Netto	893 g
Gewicht inklusive Zubehör	1033 g
Gewicht Brutto	1519 g
Umgebungsbedingungen	
Betriebstemperatur	0 °C bis 50 °C
Lagertemperatur	-20 °C bis 70 °C
Zertifizierungen	
Zertifizierung nach UL	ja
Zertifizierung nach KC	-
Zertifizierung nach UKCA	ja
Zertifizierung nach ChinaRoHS	in Vorbereitung
Zertifizierung nach DNV	in Vorbereitung
Zertifizierung nach EU MR	in Vorbereitung

3 Einsatz

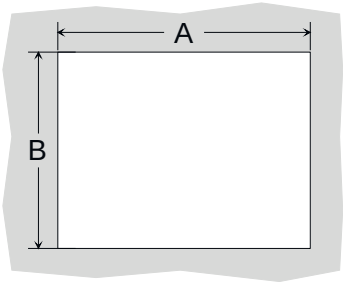
3.1 Montage

Übersicht

Das smartPanel ist geeignet zum Einbau in Bedientableaus und Schaltschrankfronten. Die Montage erfolgt von der Rückseite. Hierzu besitzt das smartPanel eine Befestigungsmechanik, welche eine einfache Montage mittels eines Kreuzschlitz-Schraubendrehers erlaubt. Ein schneller Geräteaustausch ist dadurch jederzeit möglich.

Einbaumaße

Zum Einbau in Bedientableaus und Schaltschrankfronten ist für das smartPanel folgender Frontplattenausschnitt erforderlich:

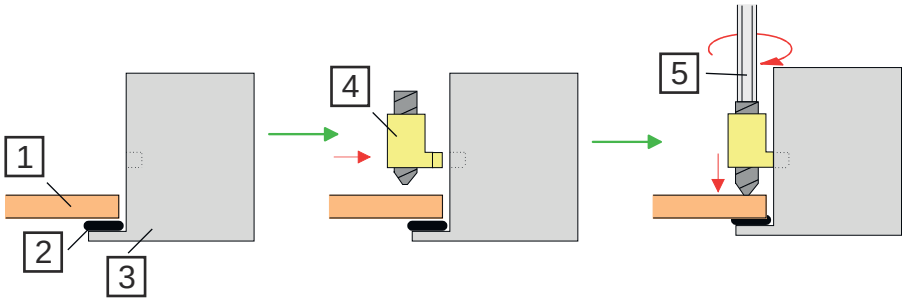


smartPanel	A x B in mm
HA1-A1A41-0	271 x 186 mm

Montage

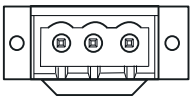
Zur Befestigung des smartPanel befinden sich Montageclips im Lieferumfang. Für die Montage ist ein kleiner Kreuzschlitz-Schraubendreher erforderlich.

1. Stecken Sie Ihr smartPanel [3] von der Frontseite durch den Frontplattenausschnitt [1], bis dieses mit der Dichtung [2] aufliegt.
2. Stecken Sie nun an allen vier Seiten des smartPanel die Montageclips [4] in die dafür vorgesehenen Öffnungen, so dass die Spitze der Schraube in Richtung Frontplatte zeigt.
3. Schrauben Sie die Schrauben mit dem Kreuzschlitz-Schraubendreher [5] fest.



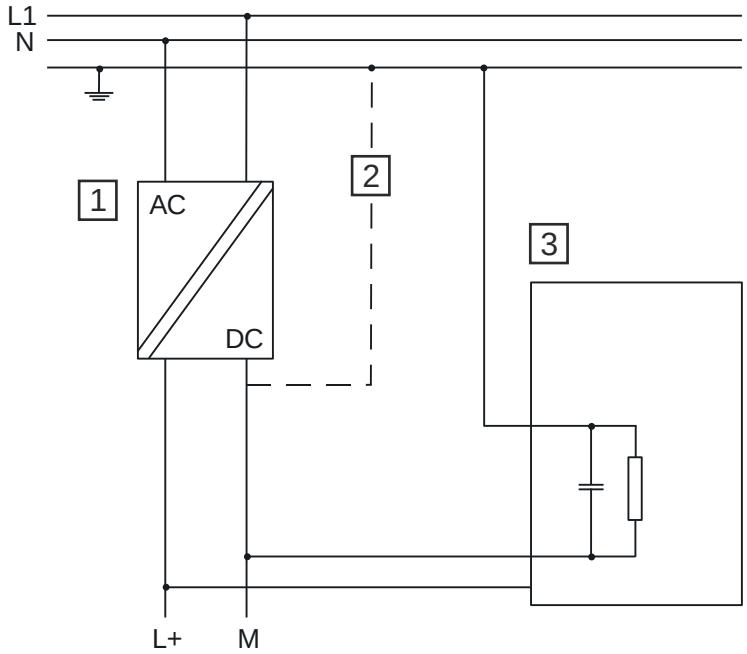
[1] Frontplattenausschnitt
[2] Dichtung
[3] smartPanel
[4] Montageclip
[5] Kreuzschlitz-Schraubendreher

Versorgungsspannung anschließen



⏚ 0V 24V

- Für die Verdrahtung der DC 24V Spannungsversorgung (DC 10 ... 32V) wird ein 3-fach Steckverbinder mit Schraubkontakten eingesetzt, welcher sich im Lieferumfang befindet. Die zugehörige Beschriftung befindet sich auf der Rückseite des smartPanel.
- Das smartPanel muss immer geerdet sein. Dies vermindert die Auswirkungen von elektromagnetischen Störungen.
- Verwenden Sie zur Erdung die mit ⏚ bezeichnete Klemme des Netzteils.
- Die Beschaltung zur Spannungsversorgung kann potentialfrei oder geerdet sein.
  - Bei potentialfreier Beschaltung ist zu beachten, das beim smartPanel intern über einen 1MΩ Widerstand parallel zu einem 4,7nF Kondensator eine Verbindung zwischen Stromversorgung und Erde besteht.
  - Bei Erdung verbinden Sie die Stromversorgung mit der Erde, wie in der nachfolgenden Abbildung unter 2 dargestellt.



1 Spannungsversorgung
2 Bei geerdeter Beschaltung der Spannungsversorgung
3 smartPanel

3.2 Inbetriebnahme

VORSICHT

- Vor Inbetriebnahme ist das Gerät der Raumtemperatur anzugleichen.
- Bei Betauung darf das Gerät erst eingeschaltet werden, nachdem es absolut trocken ist.
- Vermeiden sie den Einsatz in direktem Sonnenlicht.
- Nach Öffnen des Schaltschrankes oder -Pultes sind Teile des Systems zugänglich, die unter gefährlicher Spannung stehen können.
- Für alle Signalverbindungen sind nur geschirmte Leitungen zulässig.
- Signalleitungen dürfen nicht mit Starkstromleitungen im selben Kabelschacht geführt werden.

IP-Adresse

Im Auslieferungszustand besitzt das smartPanel folgende IP-Adresse:

- 192.168.1.100

Eine gültige IP-Adresse erhalten Sie von Ihrem Systemadministrator. Diese können Sie in den "System Settings" über Netzwerk vorgeben.
➥ Kap. 3.3.6 "Netzwerk" ...Seite 24

Projekttransfer

Das smartPanel kann ausschließlich mit dem HMI Designer projektiert werden. Hierbei werden die Daten über Ethernet mittels der IP-Adresse in das smartPanel übertragen. Näheres hierzu finden Sie in der Dokumentation zum HMI Designer.

1. Montieren und verdrahten Sie Ihr smartPanel.
   ➥ Kap. 3.1 "Montage" ...Seite 20
2. Stellen Sie eine Ethernet-Verbindung zu Ihrem smartPanel her und schalten Sie dieses ein.
3. Starten Sie den HMI Designer mit Ihrem Projekt und öffnen Sie den Dialog für die Projektübertragung.
4. Geben Sie die IP-Adresse des smartPanel an bzw. lassen Sie diese suchen.
5. Übertragen Sie Ihr Projekt in das smartPanel.
   ➥ Nach der Übertragung startet das smartPanel mit Ihrem Projekt.

Runtime

Das smartPanel wird ohne eine Laufzeitumgebung, im folgenden "Runtime" genannt, ausgeliefert. Das smartPanel kann ausschließlich mit dem HMI Designer konfiguriert werden. Sobald Sie aus dem HMI Designer ein Projekt in das smartPanel übertragen, wird automatisch die zugehörige Runtime installiert.

Startmenü

Sofern noch kein Projekt übertragen wurde, zeigt das smartPanel das *Startmenü* mit Zugriff auf:

- System Settings
- Startup Sequence

Sie können auch während des Hochlaufs mittels "Tap-Tap"-Verfahren das *"Startmenü"* aufrufen.

➥ Kap. 3.5 "Tap-Tap Menü" ...Seite 28

Zugangsdaten

Bitte beachten Sie, dass die Untermenü-Punkte innerhalb des Startmenüs durch Zugangdaten geschützt werden. Bei der Erstinbetriebnahme müssen Sie, sobald Sie einen Untermenü-Punkt aufrufen, ein Passwort vergeben. Hierbei gelten folgende Vorgaben:

- Mindestens 8 Zeichen
- Mindestens 1 Großbuchstabe (A...Z)
- Mindestens 1 Kleinbuchstabe (a...z)
- Mindestens 1 Ziffer (0...9)
- Mindestens 1 Sonderzeichen wie z.B. # ! @ ?

Nachdem Sie ein Passwort vergeben haben, wird das Startmenü angezeigt. Mit Ihrem Passwort und dem Benutzernamen *admin* haben Sie jetzt Zugriff auf die Untermenü-Punkte.

3.3 System Settings

3.3.1 Übersicht

Untermenü

Das Untermenü ist durch Zugangsdaten abgesichert.

➦ *"Zugangsdaten" ...Seite 22*

Nach Abfrage der Zugangsdaten haben Sie über folgende Untermenü-Punkte Zugriff auf die Grundeinstellungen des smartPanel:

- Lokalisierung
- System
- Log
- Datum & Uhrzeit
- Netzwerk
- Sicherheit
- Anwendungen
- Dienste
- Verwaltung
- Anzeige
- Schriftarten
- Authentifizierung
- Neu starten

Navigation

In der Kopfzeile eines Untermenüs befinden sich folgende Elemente zur Navigation:

- springt zurück in die Übersicht der System Settings.
- öffnet den Bearbeitungsdialog, sofern verfügbar. Innerhalb des Dialogs können Sie Ihre Änderungen mit Speichern übernehmen bzw. mit Abbrechen den Dialog ohne Speichern schließen.
- aktualisiert die Ansicht.
- springt zurück in das Startmenü.

3.3.2 Lokalisierung

Sprache

Hier können Sie die Oberflächen-Sprache für das smartPanel einstellen.

Ländercode

Dieser Parameter ist für dieses smartPanel nicht relevant und sollte auf *"00..."* bleiben.

System-Tastatur-Layout

Hier können Sie das Layout für die System-Tastatur einstellen.

3.3.3 System

Info

Hier erhalten Sie Informationen zum Betriebssystem, zur Serien- und Artikelnummer, zum verfügbaren Arbeitsspeicher (RAM) des smartPanel und haben Zugriff auf das Lizenz-Infopaket.

- Das smartPanel arbeitet mit einem Linux-Betriebssystem.
- Lizenzinformationen zu den einzelnen Linux-Paketen können Sie hier über die Schaltfläche *"Abruf des Lizenz-Infopakets"* abrufen.
- Jede Open Source Software, die im Produkt verwendet wird, unterliegt den jeweiligen Lizenzbestimmungen, die von den Yaskawa-Software-Lizenzbedingungen (Software License Terms - SLT) für das Produkt nicht berührt werden.
- Der Lizenznehmer kann die jeweilige Open Source Software entsprechend den geltenden Lizenzbestimmungen ändern.

Status

Hier erhalten Sie Informationen über den aktuellen Gerätestatus wie freier Arbeitsspeicher, Betriebszeit seit PowerON und durchschnittliche CPU-Last in verschiedenen Zeitintervallen.

Zeitmessung

Hier werden die Gesamtlaufzeit des Systems und der Hintergrundbeleuchtung angezeigt.

3.3.4 Log

Permanentes Log

Im aktivierten Zustand werden die Log-Daten dauerhaft gespeichert und stehen nach einem PowerON weiter zur Verfügung. Mit *"Speichern"* können Sie die Log-Datei auf einen angebunden PC herunterladen.

3.3.5 Datum & Uhrzeit

Hier haben Sie die Möglichkeit das Datum und die Uhrzeit des smartPanel zu ändern. Gehen Sie hierzu auf *Bearbeiten* .

Sofern *"Automatisches Update (NTP)"* nicht aktiviert ist, können Sie Datum und Uhrzeit hier einstellen.

Ist *"Automatisches Update (NTP)"* aktiviert, bekommt das smartPanel Uhrzeit und Datum von dem hier anzugebenden NTP-Server.

Durch Aktivierung von *"Slow time adjustment … "* wird bei einer Zeitabweichung nicht mehr als 1 Minute am Tag angepasst.

Ist *"NTP-Anfragen akzeptieren"* aktiviert, dient das smartPanel als Zeitserver und antwortet auf externe NTP-Anfragen.

3.3.6 Netzwerk

Hier haben Sie die Möglichkeit die Netzwerkeinstellungen des smartPanel zu ändern. Gehen Sie hierzu auf *Bearbeiten* .

Allgemeine Einstellungen

Hier können Sie einen Gerätenamen für das smartPanel vergeben.

Netzwerk Schnittstelle

Sofern *"DHCP"* nicht aktiviert ist, können Sie hier Ihre Netzwerkparameter wie IP-Adresse, Netzwerkmaske und Gateway einstellen.

Bei aktiviertem DHCP werden diese Parameter automatisch vom DHCP-Server abgerufen.

DNS

Hier können Sie einen DNS-Server für die Auflösung des Hostnamen angeben bzw. eine DNS-Domäne für die Suche. In der Regel wird ein DNS-Server vom DHCP-Server bereitgestellt.

Wiederherstellen

Hiermit werden alle Netzwerk-, Firewall- und Routereinstellungen, auf ihren Auslieferungszustand zurückgesetzt!

3.3.7 Sicherheit

Anmeldedaten

Auf diese Funktion haben Sie nur als angemeldeter Administrator Zugriff.

Der Sicherheitsbereich beinhaltet Passwörter und Zertifikate, welche für Ihre Anwendungen erforderlich sind. Sie können diese neu anlegen, löschen, importieren und exportieren.

3.3.8 Anwendungen

Hier können Sie über die Schaltfläche [App-Verwaltung] die Anwendungsprogramme auf dem smartPanel verwalten.

Ist *"Autostart"* aktiviert, wird die entsprechende Anwendung beim Einschalten des smartPanel gestartet.

Über Boot-Reihenfolge definieren Sie die Reihenfolge in der die Anwendungen gestartet werden.

3.3.9 Dienste

Auf diese Funktion haben Sie nur als angemeldeter Administrator Zugriff.

Autorun scripts from external storage

Im aktivierten Zustand kann eine Skript-Datei "autoexec.sh" von einem angebunden USB-Stick ausgeführt werden. Deaktivieren Sie diesen Dienst, wenn ein unbefugter Zugriff über die USB-Schnittstelle verhindert werden soll.

Avahi Daemon

Avahi ist ein System, das Programmen die Möglichkeit bietet, Dienste und Hosts in einem lokalen Netzwerk zu veröffentlichen und zu erkennen. Im aktivierten Zustand können Sie das smartPanel auch über den Hostnamen des Geräts (alternativ zur IP-Adresse) erreichen.

Cloud / VPN Service

Hier können Sie eine Fernwartung für Geräte einrichten, welche über Gateways mit einem zentralen Server verbunden sind.

Näheres hierzu finden im Handbuch zum HMI Designer.

DHCP Server

Hier können Sie Einstellungen für den DHCP-Server vornehmen.

Enable device restore via Tap Tap option

Im aktivierten Zustand können Sie über das *"Tap-Tap Menü"* Rücksetzen auf Werkseinstellungen durchführen wenn beispielsweise das Administrator-Passwort nicht bekannt ist.

➦ *Kap. 3.5 "Tap-Tap Menü" ...Seite 28*

Enable device restore via USB

Im aktivierten Zustand können Sie über den USB-Stick Rücksetzen auf Werkseinstellungen durchführen wenn beispielsweise das Administrator-Passwort nicht bekannt ist. Erstellen Sie hierzu im Root-Verzeichnis eine leere Datei ohne Erweiterung mit Name *"device-factory-restore"*. Nach dem Bootvorgang wird diese Datei auf dem USB-Stick erkannt und das Rücksetzen auf Werkseinstellungen durchgeführt.

Firewall Service

Hier können Sie die Firewall einstellen, indem Sie Verbindungen sperren bzw. hierfür entsprechende Regeln definieren.

Näheres hierzu finden im Handbuch zum HMI Designer.

Router / NAT / Port forwarding

Hier können Sie IP-/Port-Weiterleitungen und Netzwerkadressübersetzungen konfigurieren.

Näheres hierzu finden im Handbuch zum HMI Designer.

Show loading bar during boot

Im aktivierten Zustand wird während der Bootphase ein Ladebalken angezeigt.

SNMP Server

Im aktivierten Zustand kann der SNMP-Manager Informationen vom smartPanel mittels des SNMP-Protokolls abrufen. SNMP ist ein Netzwerkprotokoll, mit dem Netzwerkinfrastrukturen verwaltet werden können. Es wird häufig zur Überwachung von Netzwerkgeräten wie Switches, Router usw. verwendet, welche an ein LAN-Netzwerk angeschlossen sind.

Näheres hierzu finden im Handbuch zum HMI Designer.

SSH Server

Im aktivierten Zustand kann die Anmeldung mittels des Secure Shell-Protokolls erfolgen.

Näheres hierzu finden im Handbuch zum HMI Designer.

VNC Service

Im aktivierten Zustand haben Sie Remote-Zugriff auf das smartPanel mittels eine VNC-Clients.

➦ *Kap. 3.8.2 "VNC-Server" ...Seite 33*

Näheres hierzu finden im Handbuch zum HMI Designer.

Web Server

Hier können Sie die Parameter für den Webserver anpassen.

➦ *Kap. 3.8.3 "Web-Server" ...Seite 33*

Näheres hierzu finden im Handbuch zum HMI Designer.

3.3.10 Verwaltung

Auf diese Funktion haben Sie nur als angemeldeter Administrator Zugriff.

In diesem Bereich können Sie die einzelnen Komponenten des Linux-Betriebssystems verwalten. Dies umfasst die einzelnen Betriebssystem-Komponenten und den Startbildschirm *"Splash Screen"*. Auch werden hier Information über Verwendung und Größe der jeweiligen Komponente aufgeführt.

VORSICHT

Bitte beachten Sie, dass das Arbeiten im Verwaltung-Bereich ist ein kritischer Vorgang ist. Wenn dieser nicht korrekt ausgeführt wird, kann es zu Produktschäden kommen, die eine Wartung des Produktes erforderlich machen.

Näheres hierzu finden im Handbuch zum HMI Designer

3.3.11 Anzeige

Hier können Sie mittels Schieberegler die Helligkeit des Displays und die Zeit bis zur der Abschaltung der automatischen Hintergrundbeleuchtung einstellen. Nach Ablauf der eingestellten Zeit wird die Hintergrundbeleuchtung abgeschaltet und wird durch Betätigen des Touchscreens wieder aktiviert.

Unter *"Ausrichtung"* können Sie die Panel-Ausrichtung an die eingebaut Ausrichtung anpassen. Hier können Sie zwischen 90°, 180°, 270° oder 360° wählen.

Über die Schaltfläche [Kalibrierung Touch] können Sie die Kalibrierung für den Touchscreen aufrufen. Zur Kalibrierung folgen Sie den Anweisungen auf dem Display.

3.3.12 Schriftarten

Hier können Sie die Schriftarten verwalten und ggf. weitere installieren.

3.3.13 Authentifizierung

Benutzer

Hier können Sie unter *Bearbeiten* die entsprechenden Passwörter ändern. Für das smartPanel gibt es folgende Benutzerdaten:

- Administrator
  - Benutzer: admin
  - Das Passwort ist bei der Inbetriebnahme zu definieren.
- Normaler Benutzer (default: deaktiviert)
  - Benutzer: user
  - Passwort: user

x.509 Zertifikat

Zur Verschlüsselung der Internetkommunikation über das HTTPS-Protokoll kommt im smartPanel ein generiertes Zertifikat zum Einsatz. Sie können das Zertifikat mit den Daten Ihres Unternehmens personalisieren und es von einer Zertifizierungsstelle bestätigen lassen.

Näheres hierzu finden im Handbuch zum HMI Designer.

3.3.14 Neu starten

Hier können Sie einen Neustart des smartPanel ausführen. Wählen Sie hierzu *"Main OS"* an und bestätigen Sie die Sicherheits-Abfrage.

3.4 Startup Sequence

Das Untermenü ist durch Zugangsdaten abgesichert.

➦ *"Zugangsdaten" ...Seite 22*

Hier können Sie über die Schaltfläche [App-Verwaltung] die Anwendungsprogramme auf dem smartPanel verwalten.

Ist *"Autostart"* aktiviert, wird die entsprechende Anwendung beim Einschalten des smart-Panel gestartet.

Über Boot-Reihenfolge definieren Sie die Reihenfolge in der die Anwendungen gestartet werden.

3.5 Tap-Tap Menü

Tap-Tap Menü aufrufen

Mit einer Folge von schnellen Fingertouchs auf dem Bildschirm, welche während der Einschaltphase des smartPanel ausgeführt wird, können Sie das *Tap-Tap Menü* aufrufen.

1. Schalten Sie das smartPanel ein und warten Sie, bis *"Yaskawa"* angezeigt wird.
2. Führen Sie in schneller Abfolge mehrere Fingertouchs auf dem Bildschirm durch.

“TAP-TAP DETECTED 5“
RESTART CONFIG OS
>> SYSTEM SETTINGS

➡ Sie erhalten die Meldung `TAP-TAP DETECTED` und befinde sich im Tap-Tap Menü.

Hier werden jeweils nach einem Countdown von 5s folgende Menüpunkte zur Auswahl eingeblendet:

- System Settings
- Touchscreen Calibration
- Device Restore

Die Auswahl eines Menüpunkts erfolgt durch Betätigen des Touchscreens an beliebiger Stelle und Halten von mindestens 5s.

System Settings öffnen

1. Rufen Sie wie oben gezeigt das Tap-Tap Menü auf.
2. Zum Aufruf der System Settings ist kein Betätigen des Touchscreens erforderlich. Warten Sie, bis das Tap-Tap Menü wieder verlassen und das Startmenü angezeigt wird. Von hier haben Sie Zugriff auf die *"System Settings"*.

“TAP-TAP DETECTED 5“
RESTART CONFIG OS
>> SYSTEM SETTINGS

Touchscreen-Kalibrierung aufrufen

"TAP-TAP DETECTED 5"
>> DEFAULT MODE
TOUCHSCREEN CALIBRATION

1. Rufen Sie wie oben gezeigt das Tap-Tap Menü auf.
2. Warten Sie, bis *"TOUCHSCREEN CALIBRATION"* aufgelistet wird. Zum Aufruf der Touchscreen-Kalibrierung betätigen Sie innerhalb von 5s den Touchscreen an beliebiger Stelle und halten diesen für mindestens 5s gedrückt.
   ➡ *">>"* wechselt zu TOUCHSCREEN CALIBRATION und der Zähler hinter "TAP-TAP DETECTED" startet einen Countdown von 5s.
3. Lassen Sie nach Ablauf des Countdowns das Touch los.
   ➡ Die Touchscreen-Kalibrierung wird geöffnet.
4. Zur Kalibrierung folgen Sie den Anweisungen auf dem Display.

Gerät zurücksetzen

Sofern in den ➦ *Kap. 3.3.1 "System Settings" ...Seite 23* unter *"Dienste"* aktiviert, können Sie mit dieser Funktion das Gerät auf Werkseinstellung zurücksetzen.

"TAP-TAP DETECTED 5"
>> DEFAULT MODE
DEVICE RESTORE

1. Rufen Sie wie oben gezeigt das Tap-Tap Menü auf.
2. Warten Sie, bis *"DEVICE RESTORE"* aufgelistet wird. Für das Rücksetzen auf Werkseinstellungen betätigen innerhalb von 5s den Touchscreen an beliebiger Stelle und halten diesen für mindestens 5s gedrückt.
   ➡ *">>"* wechselt zu DEVICE RESTORE und der Zähler hinter "TAP-TAP DETECTED" startet einen Countdown von 5s.
3. Lassen Sie nach Ablauf des Countdowns das Touch los.
   ➡ Das Gerät führt ein Rücksetzen auf Werkseinstellung durch und startet neu.

Bitte beachten Sie, dass beim Rücksetzen auf Werkseinstellung alle Anwendungen entfernt und alle Einstellungen auf den jeweiligen Defaultwert geändert werden!

3.6 Firmwareupdate

Übersicht

- Die aktuellsten Firmwarestände finden Sie im *"Download Center"* von www.yaskawa.eu.com unter *"Firmware HA1-A1A41-0"*.
- In den *"System Settings"* muss der Dienst *"Autorun scripts from external storage"* aktiviert sein.
- Für das Firmwareupdate ist ein leerer USB-Stick mit mindestens 1GB im FAT32-Format erforderlich.
- Die Identifikation einer Firmware-Datei auf dem USB-Stick erfolgt mittels definierter Namenskonvention.
- Das Update startet automatisch.

Firmwarestand ausgeben

Über *"System"* der *"System Settings"* können Sie Informationen zum Firmwarestand abrufen.

➦ *Kap. 3.3.1 "System Settings" ...Seite 23*

Firmwareupdate durchführen

VORSICHT

Beim Aufspielen einer neuen Firmware ist äußerste Vorsicht geboten. Unter Umständen kann Ihr smartPanel unbrauchbar werden, wenn beispielsweise während der Übertragung die Spannungsversorgung unterbrochen wird oder die Firmware-Datei fehlerhaft ist. Setzen Sie sich in diesem Fall mit unserer Hotline in Verbindung!

1. Gehen Sie in das *"Download Center"* von www.yaskawa.eu.com.
2. Laden Sie unter *"Firmware HA1-A1A41-0"* die entsprechende zip-Datei für Ihr smartPanel auf Ihren PC.
3. Entpacken Sie die Zip-Datei und kopieren Sie alle Dateien in das Root-Verzeichnis des USB-Sticks. Der USB-Stick sollte mindestens 1GB haben und zuvor im FAT32-Format formatiert sein.
4. Damit das HA1-A1A41-0 auf den USB-Stick automatisch zugreifen kann, öffnen Sie am HA1-A1A41-0 die *"System Settings"*, aktivieren Sie unter *"Dienste"* den Parameter *"Autorun scripts from external storage"* und speichern Sie Ihre Einstellungen.

   ➦ *Kap. 3.3.1 "System Settings" ...Seite 23*
5. Schalten Sie das HA1-A1A41-0 aus.
6. Stecken Sie den USB-Stick.
7. Schalten Sie das HA1-A1A41-0 ein.

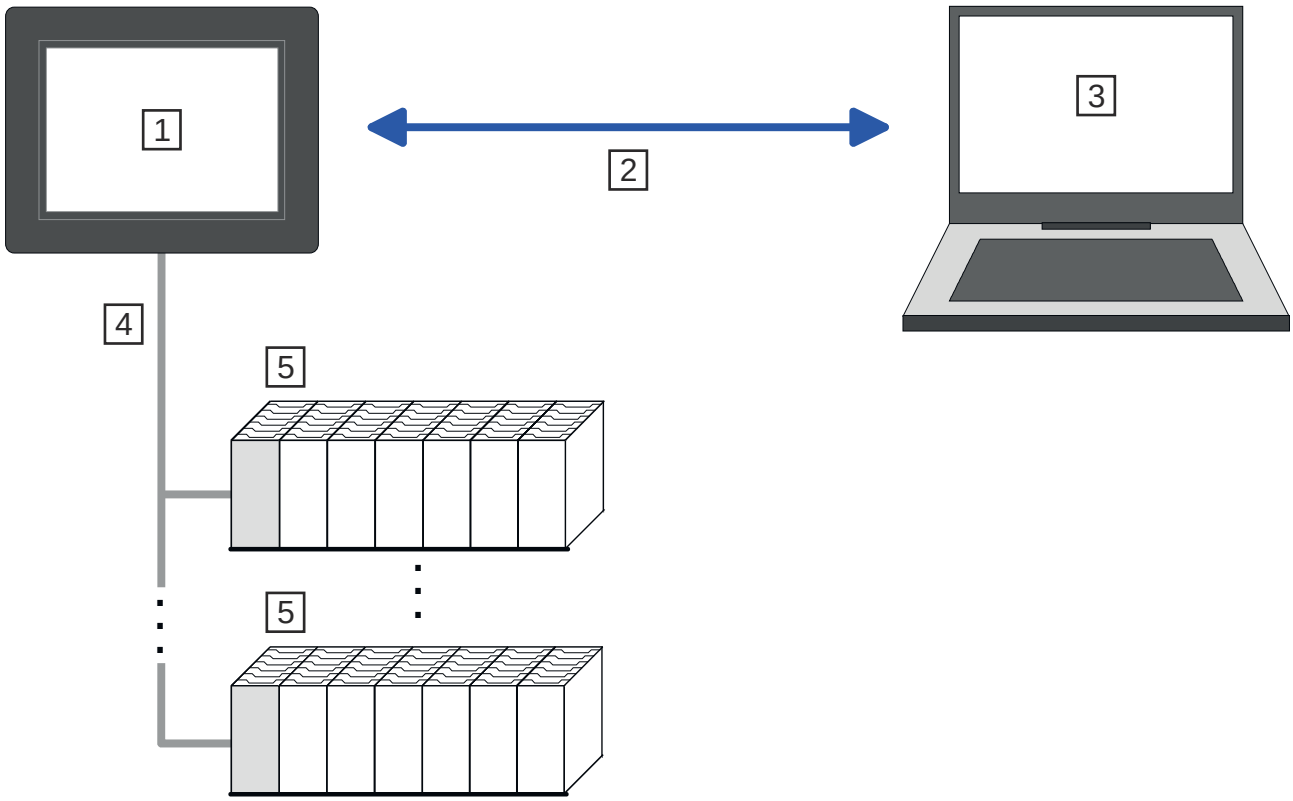
   ➥ Nach dem Bootvorgang wird das Firmware-Paket auf dem USB-Stick erkannt, automatisch das Firmwareupdate gestartet und entsprechend auf dem Display angezeigt.
8. Sobald Sie die Meldung bekommen, dass das Firmwareupdate durchgeführt wurde, schalten Sie das HA1-A1A41-0 aus, entfernen Sie den USB-Stick und schalten Sie das HA1-A1A41-0 wieder ein.
9. Deaktivieren Sie ggf. wieder den Parameter *"Autorun scripts from external storage"*.

   ➥ Nach dem Bootvorgang ist das HA1-A1A41-0 mit der neuen Firmware betriebsbereit.

3.7 Anbindung an ein SPS-System

Übersicht

- Zur Einbindung in Ihr SPS-System ist der HMI Designer zu verwenden, welcher auf einem PC zu installieren ist. Hier können Sie Ihr Projekt erstellen, ggf. simulieren und über Ethernet bzw. einen USB-Stick in Ihr smartPanel übertragen. Über die hierbei in Ihrem smartPanel installierte Runtime-Version wird Ihr Projekt auf dem smartPanel ablauffähig.
- Unter Verwendung der entsprechenden Kommunikationstreiber bietet das smartPanel Anschlussmöglichkeiten an Ihre SPS über Ethernet.
- Während des Betriebs kommuniziert das smartPanel mit der entsprechenden Steuerung und reagiert anhand der projektierten Vorgaben auf Programmabläufe in der SPS. Über zuvor projektierte Dialoge können Prozesswerte grafisch dargestellt, geändert und ausgewertet werden.



1 smartPanel mit VNC- / FTP- / Web-Server
2 Ethernet-Verbindung
3 PC mit HMI Designer
4 SPS-Anbindung über Ethernet
5 SPS

3.8 Integrierte Server

Übersicht

Im smartPanel sind folgende Server integriert, welche eine Fernwartung über Ethernet ermöglichen:

- FTP-Server - Default: aktiviert
- VNC-Server - Default: deaktiviert
- Web-Server - nicht deaktivierbar

Bezeichnungen, welche bei Beschreibung der Server zum Einsatz kommen:

- Client
  - Ein *Client* ist eine Anwendung, die in einem Netzwerk den Dienst eines Servers in Anspruch nimmt. Beispielsweise ist ein Web-Browser ein Client, denn er sendet bei jedem Aufruf einer Webseite eine Anfrage an einen Web-Server und erhält dann von diesem eine Antwort.
- Server
  - Ein *Server* ist ein Programm, welches auf die Kontaktaufnahme eines Client-Programms wartet und nach Kontaktaufnahme mit diesem Nachrichten austauscht. Diese Kommunikationsart nennt man Client-Server-Kommunikation.
- Host
  - Ein *Host* ist ein Gerät innerhalb eines Netzwerks, auf dem mindestens ein Server betrieben wird.
- Download
  - Datenübertragung Server >>> Client
- Upload
  - Datenübertragung Server <<< Client

3.8.1 FTP-Server

Das smartPanel hat einen FTP-Server integriert. FTP steht für **F**ile **T**ransfer **P**rotocol und dient zur Übertragung von Dateien über Ethernet zwischen Client und Server. Hierbei können Sie von Ihrem PC auf dem smartPanel Dateien und Verzeichnisse kopieren, löschen oder neu anlegen. Für den Zugriff müssen auf dem smartPanel Benutzerdaten angelegt sein und auf dem PC ist ein entsprechender FTP-Client zu installieren.

Bei deaktivierter Benutzerverwaltung/Sicherheit erfolgt der Zugriff über folgende Zugangsdaten:

- Server: IP-Adresse des smartPanel
- Benutzername: admin
- Passwort: admin
- Port: 21

Näheres hierzu finden im Handbuch zum HMI Designer.

Bitte beachten Sie, dass der FTP-Server nur eine Verbindung unterstützt. Stellen Sie, sofern verfügbar, an Ihrem FTP-Client die Anzahl der maximalen Verbindungen auf 1 ein.

3.8.2 VNC-Server

Das smartPanel hat einen VNC-Server integriert. VNC steht für **V**irtual **N**etwork **C**ontrol und bietet die vollständige Kontrolle des smartPanel über das angebundene Ethernet mit einem PC. Hierbei werden Mausaktionen und Tastatureingaben an das smartPanel gesendet, die Bildschirminhalte an den PC übertragen und in einem Fenster dargestellt. Für den Zugriff muss auf dem smartPanel der VNC-Server aktiviert sein und auf dem PC ist ein entsprechender VNC-Viewer zu installieren.

Da mit dem VNC-Server alle Sicherheitseinstellungen umgangen werden können, sollten Sie diesen ausschließlich für Tests und die Inbetriebnahme verwenden! Aus Sicherheitsgründen ist dieser im Auslieferungszustand deaktiviert.

Bitte beachten Sie auch, dass Yaskawa für die VNC-Funktionalität keinen Support anbieten kann. Nähere Informationen hierzu finden beim Hersteller des VNC-Viewer, welcher auch als Open Source zur Verfügung steht.

Aufbau einer VNC-Verbindung

1. Starten Sie Ihr smartPanel und rufen Sie die ➦ *Kap. 3.3.1 "System Settings" ...Seite 23* auf.
2. Aktivieren Sie unter *"Dienste"* den Dienst *"VNC Service"* und Speichern Sie die Einstellung.
   ➥ Der VNC-Server auf dem smartPanel wird gestartet.
3. Installieren Sie auf Ihrem PC einen VNC-Viewer wie z.B. den TightVNC Viewer und starten Sie diesen.
4. Geben Sie unter *"Remote Host"* die IP-Adresse Ihres smartPanel an und klicken Sie auf [Connect].
   ➥ Eine Verbindung zum smartPanel wird aufgebaut und der Bildschirminhalt in einem Fenster dargestellt. Mausaktionen und Tastatureingaben werden an das smartPanel gesendet.
5. Nach der Inbetriebnahme sollten Sie immer den VNC-Server über die *"System Settings"* wieder deaktivieren.

3.8.3 Web-Server

Das smartPanel hat einen Web-Server integriert, der je nach Zugang die Verwaltung des smartPanel bzw. von Web-Seiten im smartPanel erlaubt. Der administrative Zugriff auf den Web-Server erfolgt über Ethernet vom PC unter Angabe der IP-Adresse des smartPanel.

Der Zugriff auf die Webseite ist über Zugangsdaten geschützt, welche Sie bei der Inbetriebnahme bzw in den System Settings vergeben können.

➦ *Kap. 3.2 "Inbetriebnahme" ...Seite 21*

➦ *Kap. 3.3.1 "System Settings" ...Seite 23*

Näheres hierzu finden im Handbuch zum HMI Designer.

Bitte beachten Sie, das der integrierte Web-Server nicht deaktiviert werden kann. Über "Dienste" der ➦ Kap. 3.3.1 "System Settings" ...Seite 23 können Sie unter "Web Server" weitere Einstellungen vornehmen.

4 Industrielle Sicherheit und Aufbaurichtlinien

4.1 Industrielle Sicherheit in der Informationstechnologie

Aktuellste Version

Dieses Kapitel finden Sie auch als Leitfaden *"Industrielle IT-Sicherheit"* im *"Download Center"* unter www.yaskawa.eu.com

Gefahren

Datensicherheit und Zugriffsschutz wird auch im industriellen Umfeld immer wichtiger. Die fortschreitende Vernetzung ganzer Industrieanlagen mit den Unternehmensebenen und die Funktionen zur Fernwartung führen zu höheren Anforderungen zum Schutz der Industrieanlagen. Gefährdungen können entstehen durch:

- Innere Manipulation wie technische Fehler, Bedien- und Programmfehler und vorsätzliche Programm- bzw. Datenmanipulation.
- Äußere Manipulation wie Software-Viren, -Würmer und Trojaner.
- Menschliche Unachtsamkeit wie z.B. Passwort-Phishing.

Schutzmaßnahmen

Die wichtigsten Schutzmaßnahmen vor Manipulation und Verlust der Datensicherheit im industriellen Umfeld sind:

- Verschlüsselung des Datenverkehrs mittels Zertifikaten.
- Filterung und Kontrolle des Datenverkehrs durch VPN - "Virtual Private Networks".
- Identifizierung der Teilnehmer durch "Authentifizierung" über sicheren Kanal.
- Segmentierung in geschützte Automatisierungszellen, so dass nur Geräte in der gleichen Gruppe Daten austauschen können.
- Deaktivierung überflüssiger Hard- und Software.

Weiterführende Informationen

Nähere Informationen zu den Maßnahmen finden Sie auf den folgenden Webseiten:

- Bundesamt für Informationstechnik ➦ *www.bsi.bund.de*
- Cybersecurity & Infrastructure Security Agency ➦ *us-cert.cisa.gov*
- VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik ➦ *www.vdi.de*

4.1.1 Absicherung von Hardware und Applikationen

Maßnahmen

- Integrieren Sie keine Komponenten bzw. Systeme in öffentliche Netzwerke.
  - Setzen Sie bei Einsatz in öffentlichen Netzwerken VPN "Virtual Private Networks" ein. Hiermit können Sie den Datenverkehr entsprechend kontrollieren und filtern.
- Halten Sie Ihre Systeme immer auf dem neuesten Stand.
  - Verwenden Sie immer den neuesten Firmwarestand für alle Geräte.
  - Führen Sie regelmäßige Updates Ihrer Bedien-Software durch.
- Schützen Sie Ihre Systeme durch eine Firewall.
  - Die Firewall schützt Ihre Infrastruktur nach innen und nach außen.
  - Hiermit können Sie Ihr Netzwerk segmentieren und ganze Bereiche isolieren.
- Sichern Sie den Zugriff auf Ihre Anlagen über Benutzerkonten ab.
  - Verwenden Sie nach Möglichkeit ein zentrales Benutzerverwaltungssystem.
  - Legen Sie für jeden Benutzer, für den eine Autorisierung unbedingt erforderlich ist, ein Benutzerkonto an.
  - Halten Sie die Benutzerkonten immer aktuell und deaktivieren Sie nicht verwendete Benutzerkonten.
- Schützen Sie den Zugriff auf Ihre Anlagen durch sichere Passwörter.
  - Ändern Sie das Passwort einer Standard-Anmeldung nach dem ersten Start.
  - Verwenden Sie sichere Passwörter bestehend aus Groß-/Kleinschreibung, Zahlen und Sonderzeichen. Der Einsatz eines Passwort-Generators bzw. -Managers wird empfohlen.
  - Ändern Sie die Passwörter gemäß den für Ihre Anwendung geltenden Regeln und Vorgaben.
- Deaktivieren Sie inaktive Kommunikations-Ports bzw. Protokolle.
  - Es sollten immer nur die Kommunikations-Ports aktiviert sein, über die auch kommuniziert wird.
  - Es sollten immer nur die Kommunikations-Protokolle aktiviert sein, über die auch kommuniziert wird.
- Berücksichtigen Sie bei der Anlagenplanung und Absicherung mögliche Verteidigungsstrategien.
  - Die alleinige Isolation von Komponenten ist nicht ausreichend für einen umfassenden Schutz. Hier ist ein Gesamt-Konzept zu entwerfen, welches auch Verteidigungsmaßnahmen im Falle eines Cyper-Angriffs vorsieht.
  - Führen Sie in regelmäßigen Abständen Bedrohungsanalysen durch. Unter anderem erfolgt hier eine Gegenüberstellung zwischen den getroffenen zu den erforderlichen Schutzmaßnahmen.
- Beschränken Sie den Einsatz von externen Datenträgern.
  - Über externe Datenträger wie USB-Speichersticks oder SD-Speicherkarten kann Schadsoftware unter Umgehung einer Firewall direkt in eine Anlage gelangen.
  - Externe Datenträger bzw. deren Steckplätze müssen z.B. unter Verwendung eines abschließbaren Schaltschranks vor unbefugtem physischem Zugriff geschützt werden.
  - Stellen Sie sicher, dass nur befugte Personen Zugriff haben.
  - Stellen Sie bei der Entsorgung von Datenträgern sicher, dass diese sicher zerstört werden.
- Verwenden Sie sichere Zugriffspfade wie HTTPS bzw. VPN für den Remote-Zugriff auf Ihre Anlage.
- Aktivieren Sie die sicherheitsrelevante Ereignisprotokollierung gemäß der gültigen Sicherheitsrichtlinie und den gesetzlichen Anforderungen zum Datenschutz.

4.1.2 Absicherung von PC-basierter Software

Maßnahmen

Da PC-basierte Software zur Programmierung, Konfiguration und Überwachung verwendet wird, können hiermit auch ganze Anlagen oder einzelne Komponenten manipuliert werden. Hier ist besondere Vorsicht geboten!

- Verwenden Sie Benutzerkonten auf Ihren PC-Systemen.
  - Verwenden Sie nach Möglichkeit ein zentrales Benutzerverwaltungssystem.
  - Legen Sie für jeden Benutzer, für den eine Autorisierung unbedingt erforderlich ist, ein Benutzerkonto an.
  - Halten Sie die Benutzerkonten immer aktuell und deaktivieren Sie nicht verwendete Benutzerkonten.
- Schützen Sie Ihre PC-Systeme durch sichere Passwörter.
  - Ändern Sie das Passwort einer Standard-Anmeldung nach dem ersten Start.
  - Verwenden Sie sichere Passwörter bestehend aus Groß-/Kleinschreibung, Zahlen und Sonderzeichen. Der Einsatz eines Passwort-Generators bzw. -Managers wird empfohlen.
  - Ändern Sie die Passwörter gemäß den für Ihre Anwendung geltenden Regeln und Vorgaben.
- Aktivieren Sie die sicherheitsrelevante Ereignisprotokollierung gemäß der gültigen Sicherheitsrichtlinie und den gesetzlichen Anforderungen zum Datenschutz.
- Schützen Sie Ihre PC-Systeme durch Sicherheitssoftware.
  - Installieren Sie auf Ihren PC-Systemen Virenscanner zur Identifikation von Viren, Trojanern und anderer Malware.
  - Installieren Sie Software, die Phishing-Attacken erkennen und aktiv verhindern kann.
- Halten Sie Ihre Software immer auf dem neuesten Stand.
  - Führen Sie regelmäßige Updates Ihres Betriebssystems durch.
  - Führen Sie regelmäßige Updates Ihrer Software durch.
- Führen Sie regelmäßige Datensicherungen durch und lagern Sie die Datenträger an einem sicheren Ort.
- Führen Sie regelmäßige Neustarts Ihrer PC-Systeme durch. Starten Sie nur von Datenträgern, welche gegen Manipulation geschützt sind.
- Setzen Sie Verschlüsselungssysteme auf Ihren Datenträgern ein.
- Führen Sie regelmäßig Sicherheitsbewertungen durch, um das Manipulationsrisiko zu verringern.
- Verwenden Sie nur Daten und Software aus zugelassenen Quellen.
- Deinstallieren Sie Software, welche nicht verwendet wird.
- Deaktivieren Sie nicht verwendete Dienste.
- Aktivieren Sie an Ihrem PC-System eine passwortgeschützte Bildschirmsperre.
- Sperren Sie Ihre PC-Systeme immer, sobald Sie den PC-Arbeitsplatz verlassen.
- Klicken Sie auf keine Links, welche von unbekannten Quellen stammen. Fragen Sie ggf. nach, z.B. bei E-Mails.
- Verwenden Sie sichere Zugriffspfade wie HTTPS bzw. VPN für den Remote-Zugriff auf Ihr PC-System.

4.2 Aufbaurichtlinien

Allgemeines

Die Aufbaurichtlinien enthalten Informationen über den störsicheren Aufbau eines SPS-Systems. Es werden die Wege beschrieben, wie Störungen in Ihre Steuerung gelangen können, wie die elektromagnetische Verträglichkeit (EMV) sicher gestellt werden kann und wie bei der Schirmung vorzugehen ist.

Was bedeutet EMV?

Unter Elektromagnetischer Verträglichkeit (EMV) versteht man die Fähigkeit eines elektrischen Gerätes, in einer vorgegebenen elektromagnetischen Umgebung fehlerfrei zu funktionieren, ohne vom Umfeld beeinflusst zu werden bzw. das Umfeld in unzulässiger Weise zu beeinflussen.

Die Komponenten sind für den Einsatz in Industrieumgebungen entwickelt und erfüllen hohe Anforderungen an die EMV. Trotzdem sollten Sie vor der Installation der Komponenten eine EMV-Planung durchführen und mögliche Störquellen in die Betrachtung einbeziehen.

Mögliche Störeinwirkungen

Elektromagnetische Störungen können sich auf unterschiedlichen Pfaden in Ihre Steuerung einkoppeln:

- Elektromagnetische Felder (HF-Einkopplung)
- Magnetische Felder mit energietechnischer Frequenz
- Bus-System
- Stromversorgung
- Schutzleiter

Je nach Ausbreitungsmedium (leitungsgebunden oder -ungebunden) und Entfernung zur Störquelle gelangen Störungen über unterschiedliche Kopplungsmechanismen in Ihre Steuerung.

Man unterscheidet:

- galvanische Kopplung
- kapazitive Kopplung
- induktive Kopplung
- Strahlungskopplung

Grundregeln zur Sicherstellung der EMV

Häufig genügt zur Sicherstellung der EMV das Einhalten einiger elementarer Regeln. Beachten Sie beim Aufbau der Steuerung deshalb die folgenden Grundregeln.

- Achten Sie bei der Montage Ihrer Komponenten auf eine gut ausgeführte flächenhafte Massung der inaktiven Metallteile.
  - Stellen Sie eine zentrale Verbindung zwischen der Masse und dem Erde/Schutzleitersystem her.
  - Verbinden Sie alle inaktiven Metallteile großflächig und impedanzarm.
  - Verwenden Sie nach Möglichkeit keine Aluminiumteile. Aluminium oxidiert leicht und ist für die Massung deshalb weniger gut geeignet.
- Achten Sie bei der Verdrahtung auf eine ordnungsgemäße Leitungsführung.
  - Teilen Sie die Verkabelung in Leitungsgruppen ein. (Starkstrom, Stromversorgungs-, Signal- und Datenleitungen).
  - Verlegen Sie Starkstromleitungen und Signal- bzw. Datenleitungen immer in getrennten Kanälen oder Bündeln.
  - Führen Sie Signal- und Datenleitungen möglichst eng an Masseflächen (z.B. Tragholme, Metallschienen, Schrankbleche).
- Achten Sie auf die einwandfreie Befestigung der Leitungsschirme.
  - Datenleitungen sind geschirmt zu verlegen.
  - Analogleitungen sind geschirmt zu verlegen. Bei der Übertragung von Signalen mit kleinen Amplituden kann das einseitige Auflegen des Schirms vorteilhaft sein.
  - Leitungen für Frequenzumrichter, Servo- und Schrittmotore sind geschirmt zu verlegen.
  - Legen Sie die Leitungsschirme direkt nach dem Schrankeintritt großflächig auf eine Schirm-/Schutzleiterschiene auf, und befestigen Sie die Schirme mit Kabelschellen.

  - Achten Sie darauf, dass die Schirm-/Schutzleiterschiene impedanzarm mit dem Schrank verbunden ist.
  - Verwenden Sie für geschirmte Datenleitungen metallische oder metallisierte Steckergehäuse.
- Setzen Sie in besonderen Anwendungsfällen spezielle EMV-Maßnahmen ein.
  - Erwägen Sie bei Induktivitäten den Einsatz von Löschgliedern.
  - Beachten Sie, dass bei Einsatz von Leuchtstofflampen sich diese negativ auf Signalleitungen auswirken können.
- Schaffen Sie ein einheitliches Bezugspotenzial und erden Sie nach Möglichkeit alle elektrischen Betriebsmittel.
  - Achten Sie auf den gezielten Einsatz der Erdungsmaßnahmen. Das Erden der Steuerung dient als Schutz- und Funktionsmaßnahme.
  - Verbinden Sie Anlagenteile und Schränke mit Ihrer SPS sternförmig mit dem Erde/Schutzleitersystem. Sie vermeiden so die Bildung von Erdschleifen.
  - Verlegen Sie bei Potenzialdifferenzen zwischen Anlagenteilen und Schränken ausreichend dimensionierte Potenzialausgleichsleitungen.

Schirmung von Leitungen

Elektrische, magnetische oder elektromagnetische Störfelder werden durch eine Schirmung geschwächt; man spricht hier von einer Dämpfung. Über die mit dem Gehäuse leitend verbundene Schirmschiene werden Störströme auf Kabelschirme zur Erde hin abgeleitet. Hierbei ist darauf zu achten, dass die Verbindung zum Schutzleiter impedanzarm ist, da sonst die Störströme selbst zur Störquelle werden.

Bei der Schirmung von Leitungen ist folgendes zu beachten:

- Verwenden Sie möglichst nur Leitungen mit Schirmgeflecht.
- Die Deckungsdichte des Schirmes sollte mehr als 80% betragen.
- In der Regel sollten Sie die Schirme von Leitungen immer beidseitig auflegen. Nur durch den beidseitigen Anschluss der Schirme erreichen Sie eine gute Störunterdrückung im höheren Frequenzbereich. Nur im Ausnahmefall kann der Schirm auch einseitig aufgelegt werden. Dann erreichen Sie jedoch nur eine Dämpfung der niedrigen Frequenzen. Eine einseitige Schirmanbindung kann günstiger sein, wenn:
  - die Verlegung einer Potenzialausgleichsleitung nicht durchgeführt werden kann.
  - Analogsignale (einige mV bzw. µA) übertragen werden.
  - Folienschirme (statische Schirme) verwendet werden.
- Benutzen Sie bei Datenleitungen für serielle Kopplungen immer metallische oder metallisierte Stecker. Befestigen Sie den Schirm der Datenleitung am Steckergehäuse. Schirm nicht auf den PIN 1 der Steckerleiste auflegen!
- Bei stationärem Betrieb ist es empfehlenswert, das geschirmte Kabel unterbrechungsfrei abzuisolieren und auf die Schirm-/Schutzleiterschiene aufzulegen.
- Benutzen Sie zur Befestigung der Schirmgeflechte Kabelschellen aus Metall. Die Schellen müssen den Schirm großflächig umschließen und guten Kontakt ausüben.
- Legen Sie den Schirm direkt nach Eintritt der Leitung in den Schrank auf eine Schirmschiene auf.

VORSICHT

Bitte bei der Montage beachten!

Bei Potenzialdifferenzen zwischen den Erdungspunkten kann über den beidseitig angeschlossenen Schirm ein Ausgleichsstrom fließen.

Abhilfe: Potenzialausgleichsleitung.