

Secure Remote Maintenance

Anwenderhandbuch

Version: **2.00 (September 2023)**
Bestellnr.: **MASRM-GER**

Originalbetriebsanleitung

Impressum

B&R Industrial Automation GmbH

B&R Straße 1

5142 Eggelsberg

Österreich

Telefon: +43 7748 6586-0

Fax: +43 7748 6586-26

office@br-automation.com

Disclaimer

Alle Angaben entsprechen dem aktuellen Stand zum Zeitpunkt der Erstellung dieses Dokuments. Jederzeitige inhaltliche Änderungen dieses Dokuments ohne Ankündigung bleiben vorbehalten. B&R Industrial Automation GmbH haftet insbesondere für technische oder redaktionelle Fehler in diesem Dokument unbegrenzt nur (i) bei grobem Verschulden oder (ii) für schuldhaft zugefügte Personenschäden. Darüber hinaus ist die Haftung ausgeschlossen, soweit dies gesetzlich zulässig ist. Eine Haftung in den Fällen, in denen das Gesetz zwingend eine unbeschränkte Haftung vorsieht (wie z. B. die Produkthaftung), bleibt unberührt. Die Haftung für mittelbare Schäden, Folgeschäden, Betriebsunterbrechung, entgangenen Gewinn, Verlust von Informationen und Daten ist ausgeschlossen, insbesondere für Schäden, die direkt oder indirekt auf Lieferung, Leistung und Nutzung dieses Materials zurückzuführen sind.

B&R Industrial Automation GmbH weist darauf hin, dass die in diesem Dokument verwendeten Hard- und Softwarebezeichnungen und Markennamen der jeweiligen Firmen dem allgemeinen warenzeichen-, marken- oder patentrechtlichen Schutz unterliegen.

Hard- und Software von Drittanbietern, auf die in diesem Dokument verwiesen wird, unterliegt ausschließlich den jeweiligen Nutzungsbedingungen dieser Drittanbieter. B&R Industrial Automation GmbH übernimmt hierfür keine Haftung. Allfällige Empfehlungen von B&R Industrial Automation GmbH sind nicht Vertragsinhalt, sondern lediglich unverbindliche Hinweise, ohne dass dafür eine Haftung übernommen wird. Beim Einsatz der Hard- und Software von Drittanbietern sind ergänzend die relevanten Anwenderdokumentationen dieser Drittanbieter heranzuziehen und insbesondere die dort enthaltenen Sicherheitshinweise und technischen Spezifikationen zu beachten. Die Kompatibilität der in diesem Dokument dargestellten Produkte von B&R Industrial Automation GmbH mit Hard- und Software von Drittanbietern ist nicht Vertragsinhalt, es sei denn, dies wurde im Einzelfall gesondert vereinbart; insoweit ist die Gewährleistung für eine solche Kompatibilität jedenfalls ausgeschlossen und hat der Kunde die Kompatibilität in eigener Verantwortung vorab zu prüfen.

1 Allgemeines.....	7
1.1 Handbuchhistorie.....	7
1.2 Sicherheitshinweise.....	9
1.2.1 Gestaltung von Hinweisen.....	9
1.2.2 Einleitung.....	9
1.2.3 Bestimmungsgemäße Verwendung.....	9
1.2.4 Schutz vor elektrostatischen Entladungen.....	9
1.2.4.1 Verpackung.....	9
1.2.4.2 Vorschriften für die ESD-gerechte Handhabung.....	10
1.2.5 Transport und Lagerung.....	10
1.2.6 Betrieb.....	10
1.2.6.1 Schutz gegen Berühren elektrischer Teile.....	10
1.2.6.2 Umgebungsbedingungen - Staub, Feuchtigkeit, aggressive Gase.....	11
1.2.6.3 Programme, Viren und schädliche Programme.....	11
1.2.7 Umweltgerechte Entsorgung.....	11
1.2.7.1 Werkstofftrennung.....	11
2 Sichere Fernwartung.....	12
3 Systemübersicht.....	14
3.1 GateManager.....	15
3.1.1 Bestelldaten.....	15
3.1.2 Aktivierung des GateManagers.....	16
3.1.2.1 Auslieferung und Installation der Lizenzen.....	17
3.1.3 Servicegebühr.....	17
3.1.3.1 Bestelldaten.....	17
3.1.4 Zusätzliche Services.....	17
3.1.4.1 LogTunnel– Remote Data Logging.....	17
3.1.4.2 SMS-Lizenz.....	17
3.1.5 Benutzerrechteverwaltung.....	18
3.1.5.1 GateManager Server-Administrator.....	18
3.1.5.2 GateManager Domain-Administrator.....	18
3.1.5.3 LinkManager Benutzer.....	19
3.1.5.4 LinkManager Mobile Benutzer.....	19
3.1.5.5 Domain Beobachter.....	19
3.2 SiteManager.....	20
3.2.1 Modellvergleich.....	20
3.2.2 Bestelldaten.....	21
3.2.2.1 SiteManager Embedded.....	21
3.2.2.2 SiteManager Hardware.....	21
3.2.3 Technische Daten.....	23
3.2.3.1 SiteManager Embedded.....	23
3.2.3.2 SiteManager Hardware (0RMSM13x5).....	23
3.2.4 Zubehör.....	25
3.2.4.1 Feldklemmen.....	25
3.2.4.2 Antennen.....	25
3.2.5 Status-LEDs.....	26
3.2.6 Bedien- und Anschlüsselemente.....	27
3.2.6.1 Reset-Taster.....	27
3.2.6.2 SD-Karten Steckplatz.....	27
3.2.6.3 USB-Schnittstelle.....	27
3.2.6.4 Serielle Schnittstelle.....	27
3.2.6.5 Ethernet-Schnittstellen (DEV1/2/3 und UPLINK1).....	28
3.2.6.6 Spannungsversorgung.....	28
3.2.6.7 I/O-Schnittstellen.....	29
3.2.7 Montage.....	30
3.2.8 Initialkonfiguration durch Steuerung.....	31

3.2.8.1 Ethernet Konfiguration.....	31
3.2.9 SiteManager_1315-1335-1345 - Erstmalige Einrichtung.....	32
3.2.9.1 UPLINK Einstellungen für Internetzugang tätigen.....	32
3.2.9.2 Einstellungen für GateManager-Server-Verbindung.....	33
3.2.9.3 Internetzugang mit integriertem Breitband.....	34
3.2.9.4 Internetzugang mit integriertem WiFi-Modul.....	35
3.2.10 Automation Studio.....	36
3.2.10.1 Funktionsmodell "Standard".....	36
3.2.10.2 Bedienung von Funktionsmodell "Standard".....	40
3.2.11 Verbindung zum GateManager.....	41
3.3 LinkManager.....	42
3.3.1 Bestelldaten.....	42
3.4 Starter Package.....	43
3.4.1 Bestelldaten.....	43
3.5 Netzwerksicherheit.....	44
3.6 Portinformationen.....	45
4 Erste Schritte mit den Systemkomponenten.....	46
5 Umstellung auf neue SiteManager Version.....	49
5.1 Produkte.....	49
5.2 Szenarien.....	49
5.2.1 Entwurf neuer Maschinen.....	49
5.2.1.1 Schritte für die neue Konfiguration.....	49
5.2.2 Modifizierung vorhandener Maschinen.....	49
5.2.2.1 Schritte für die Modifikation der bestehenden Konfiguration.....	49
5.2.3 Wartung von Bestandsanlagen.....	50
5.2.3.1 Schritte für die Modifikation der Bestandsanlage.....	50
6 SIM-Karten-Leitfaden für SiteManager 4G Global – USA und Japan.....	52
6.1 Betroffenes Material.....	52
6.2 Problemstellung und Lösung.....	52
6.2.1 Vereinigte Staaten.....	52
6.2.1.1 Verizon.....	52
6.2.1.2 AT&T.....	52
6.2.1.3 T-Mobile.....	53
6.2.2 Japan.....	53
7 Weiterführende Dokumentation.....	54
8 Anwendungsfälle und Endkunden-Szenarien.....	55
8.1 Anwendungsfälle.....	55
8.1.1 Ferndienst – On-Demand-Zugriff für Programmierung und Fehlerbehebung.....	55
8.1.2 Fernüberwachung - sichere Datenprotokollierung (zwischen 2 SiteManagern).....	56
8.1.3 Fernüberwachung – für sichere Datenprotokollierung.....	56
8.1.4 Direkter Internetzugriff – für Datenprotokollierung und Videoüberwachung.....	57
8.2 Endkunden-Szenarien.....	58
8.2.1 SiteManager und Maschine in einem isolierten Netzwerk.....	59
8.2.2 Maschinennetzwerk isoliert hinter DMZ und SiteManager.....	60
8.2.3 SiteManager isoliert in eigener DMZ.....	60
8.2.4 SiteManager und Maschine in separaten Netzwerken.....	61
8.2.5 Fernwartung - Komplettszenario.....	62
8.3 Verbindungsaufbau mit FTP.....	63
8.3.1 FTP über SiteManager.....	63
8.3.2 Einstellungen am SiteManager.....	65
8.3.3 Erstellen einer Verbindung mit WinSCP.....	66

9 Fehlerbehebung.....	67
9.1 GateManager-Zugang von einem PC aus testen.....	67
9.2 PC kann Verbindung herstellen, SiteManager jedoch nicht.....	68
9.2.1 Grundlegende Fragen.....	68
9.2.2 Web-Proxy issues.....	69
9.2.3 Weitere Möglichkeiten.....	70
10 Normen und Zulassungen.....	71
11 Begriffe und Abkürzungen.....	72
12 Anhang - abgekündigte Module.....	73
12.1 GateManager - ORMGM.4260-TP.....	73
12.1.1 Technische Daten.....	73
12.1.2 Status-LEDs.....	74
12.1.3 Bedien- und Anschlusselemente.....	74
12.1.3.1 Reset-Taster.....	74
12.1.3.2 Ethernet Schnittstellen.....	74
12.1.3.3 USB-Schnittstellen.....	74
12.1.3.4 Spannungsversorgung.....	74
12.2 SiteManager 0RMSM 11x5.....	75
12.2.1 SiteManager 11x5.....	75
12.2.1.1 Technische Daten.....	75
12.2.2 SiteManager 4G - Regionalvarianten.....	76
12.2.2.1 Technische Daten.....	76

1 Allgemeines

Information:

B&R stellt Dokumente so aktuell wie möglich zur Verfügung. Die aktuellen Versionen stehen auf der B&R Homepage www.br-automation.com zum Download bereit.

1.1 Handbuchhistorie

Version	Datum	Kommentar
2.00	September 2023	<ul style="list-style-type: none"> In Abschnitt "SiteManager" neue Modelle 0RMSM1315, 1335.4G und 1345 eingefügt. Technische Daten SiteManager Modelle 0RMSM 11x5 in Anhang verschoben; andere Referenzen entfernt In gesamten Dokument SiteManager Bild gegen neue Version ausgetauscht. Unter "Bedien- und Anschlusselemente" neue Abschnitte "SD-Karten Steckplatz", "USB-Schnittstelle" und "Serielle Schnittstelle" eingefügt. Neuen Abschnitt "Modellvergleich" eingefügt. Neuen Abschnitt "Verbindung zum GateManager" eingefügt. Abschnitt "SiteManager 13x5 - Erstmalige Einrichtung" überarbeitet. Abschnitt "Umstellung auf neue SiteManager Version" überarbeitet. Neuen Abschnitt "Fehlerbehebung" eingefügt. In Abschnitt "Starter Package" Bestellnummern angepasst. Abschnitt "Portinformation" überarbeitet.
1.65	April 2022	<ul style="list-style-type: none"> In Abschnitt "GateManager" Information über maximale E-Mail-Größen eingefügt. In Abschnitt "Bedien- und Anschlusselemente" Zeichnung mit Position des Reset-Tasters hinzugefügt. Bestelldaten für Servicegebühren und Zusätzliche Services eingefügt. Portinformationen für Site- und LinkManager hinzugefügt. Bei "Erste Schritte mit den Systemkomponenten" Information über Downloads hinzugefügt. Neuen Abschnitt "SIMGuideline" eingefügt. In Abschnitt "Anwendungsfälle und Endkunden-Szenarien" "Lösungsmodelle" in "Anwendungsfälle" umbenannt
1.60	August 2021	<ul style="list-style-type: none"> Neuen Abschnitt "Anleitung zur Umstellung auf SiteManager 4G global" aufgenommen. SiteManager 4G Lokalvarianten in Anhang verschoben.
1.56	Mai 2021	<ul style="list-style-type: none"> Impressum verschoben und Disclaimer geändert Neuen SiteManager 0RMSM1135-4G eingefügt. Frequenzbänder in techn. Daten SiteManager aktualisiert.
1.55	April 2021	<ul style="list-style-type: none"> Information zu 0RMGM.4260-TP in Anhang verschoben. Bei SiteManager Information zu Verwendung von Verizon SIM-Karten hinzugefügt In Abschnitt "Erste Schritte mit den Systemkomponenten" Links zu GateManager Doku überarbeitet und Information zu LinkManager 7 geändert Abschnitt Normen und Zulassungen geändert Neuer Abschnitt "Anhang"
1.50	November 2020	<ul style="list-style-type: none"> Abschnitt "Service Agreements" auf "Servicegebühr" umbenannt und Informationen aktualisiert Abschnitt "Zusätzliche Service" aufgenommen Information über Hypervisor in Abschnitt "SiteManager - Allgemeines" aufgenommen Gefahrenhinweis in Abschnitt "Fernwartung" aufgenommen Abschnitt Normen und Zulassungen geändert
1.40	September 2018	<ul style="list-style-type: none"> Abschnitt "Montage": Erweiterung um Mindestabstände im Schaltschrank. Die beiden Abschnitte "Lösungsmodelle" und "Endkunden-Szenarien" zusammengefasst. Neuer Abschnitt "Verbindungsaufbau mit FTP". Redaktionelle Änderungen
1.32	Dezember 2017	<ul style="list-style-type: none"> Neues SiteManager Hardwaremodul 0RMSM1135.4G-JP
1.31	Juni 2017	<ul style="list-style-type: none"> Umbenennung von EasyLogging zu LogTunnel Beschreibung der SiteManager LEDs angepasst Abschnitt "SiteManager": "Bestelldaten" in "Embedded" und "Hardware" unterteilt. Bestelldaten um optionales Zubehör und Lieferumfang erweitert Abschnitt "SiteManager": "Technische Daten" in "Embedded" und "Hardware" unterteilt. Technische Daten von SiteManager Embedded eingefügt Abschnitt "Weiterführende Dokumentation" aktualisiert Redaktionelle Änderungen

Version	Datum	Kommentar
1.30	März 2017	<ul style="list-style-type: none"> • Abschnitt "Sichere Fernwartung" mit neuen Gerätemodellen erweitert. Eigenständige B&R-Lösung im Unterschied zu Secomea hervorgehoben • Abschnitt "Systemübersicht" um minimalen Systemaufbau erweitert • Abschnitt "GateManager": "Allgemeines" erweitert um AWS-Unterstützung sowie GateManager Hosting Service • Abschnitt "Service Agreements": 3 neue Service Levels sowie Option LogTunnel • Abschnitt "SiteManager": "Allgemeines", "Bestelldaten" und "Technische Daten" erweitert. Neue SiteManager Hardwaremodule mit 4G/LTE Unterstützung sowie SiteManager Embedded • Neuer Abschnitt "Zubehör": Antennen für Mobilfunk sowie Wi-Fi • Abschnitt "Automation Studio" um I/O Mapping - Registerübersicht und weitere Registerbeschreibungen ausgebaut • Neuer Abschnitt "Starter Package": Schnellerer Einstieg für Neukunden ohne hohen Installationsaufwand • Abschnitt "Weiterführende Dokumentation" mit neuer Gruppierung Remote Data Logging • Redaktionelle Änderungen
1.20	Oktober 2016	<ul style="list-style-type: none"> • Abschnitt "SiteManager" durch Datenblatt "SiteManager" ersetzt • Kapitelstruktur der inkludierten Datenblätter angepasst • Abschnitt "Reset-Taster" für SiteManager eingefügt • Inhalte des SiteManager Beipackzettels im Datenblatt "SiteManager" eingefügt • Inhalte des GateManager Beipackzettels im Abschnitt "GateManager" eingefügt • Abschnitt "Weiterführende Dokumentation" um LogTunnel erweitert • Beschreibung der Hauptkonfigurationseinträge erweitert (WiFi KEY zwingend, ...) • Parametertabelle der Hauptkonfiguration in den Abschnitt "Funktionsmodell Standard" verschoben • Abschnitt "Normen und Zulassungen" aktualisiert und neu strukturiert • Abschnitt "Begriffe und Abkürzungen" eingefügt • Redaktionelle Änderungen
1.11a	Juni 2016	<ul style="list-style-type: none"> • Abschnitt "Auslieferung und Installation der Lizenzen" eingefügt
1.11		<ul style="list-style-type: none"> • Installation in Inbetriebnahme umbenannt und den Abschnitt "Erste Schritte" erweitert • Weiterführende Dokumentation mit ergänzenden Hinweisen und Erläuterungen zu den aufgelisteten Herstellerdokumenten erweitert • Redaktionelle Änderungen
1.10	März 2016	<ul style="list-style-type: none"> • Kapitelstruktur geändert • Systemübersicht und Geräteübersichten erweitert • Endkunden-Szenarien / Anwendungsfälle eingefügt • Link-Liste der zugehörigen Herstellerdokumente erweitert • Redaktionelle Änderungen
1.00	Februar 2016	Erste Ausgabe

1.2 Sicherheitshinweise

1.2.1 Gestaltung von Hinweisen

Sicherheitshinweise

Enthalten **ausschließlich** Informationen, die vor gefährlichen Funktionen oder Situationen warnen.

Signalwort	Beschreibung
Gefahr!	Bei Missachtung der Sicherheitsvorschriften und -hinweise werden Tod, schwere Verletzungen oder große Sachschäden eintreten.
Warnung!	Bei Missachtung der Sicherheitsvorschriften und -hinweise können Tod, schwere Verletzungen oder große Sachschäden eintreten.
Vorsicht!	Bei Missachtung der Sicherheitsvorschriften und -hinweise können leichte Verletzungen oder Sachschäden eintreten.
Achtung!	Bei Missachtung der Sicherheitsvorschriften und -hinweise können Sachschäden eintreten.

Allgemeine Hinweise

Enthalten **nützliche** Informationen für Anwender und Angaben zur Vermeidung von Fehlfunktionen.

Signalwort	Beschreibung
Information:	Nützliche Informationen, Anwendungstipps und Angaben zur Vermeidung von Fehlfunktionen.

1.2.2 Einleitung

Die Komponenten der B&R Fernwartungslösung Secure Remote Maintenance sind für den gewöhnlichen Einsatz in der Industrie entworfen, entwickelt und hergestellt worden. Sie wurden nicht entworfen, entwickelt und hergestellt für einen Gebrauch, der verhängnisvolle Risiken oder Gefahren birgt, die ohne Sicherstellung außergewöhnlich hoher Sicherheitsmaßnahmen zu Tod, Verletzung, schweren physischen Beeinträchtigungen oder anderweitigem Verlust führen können. Solche Risiken oder Gefahren stellen insbesondere die Verwendung bei der Überwachung von Kernreaktionen in Kernkraftwerken, von Flugleitsystemen, bei der Flugsicherung, bei der Steuerung von Massentransportmitteln, bei medizinischen Lebenserhaltungssystemen und bei der Steuerung von Waffensystemen dar.

Alle Arbeiten wie Installation, Inbetriebnahme und Service dürfen nur durch qualifiziertes Fachpersonal ausgeführt werden. Qualifiziertes Fachpersonal sind Personen, die mit Transport, Aufstellung, Montage, Inbetriebnahme und Betrieb des Produkts vertraut sind und über die ihrer Tätigkeit entsprechenden Qualifikationen verfügen (z. B. IEC 60364). Nationale Unfallverhütungsvorschriften sind zu beachten.

Die Sicherheitshinweise, die Angaben zu den Anschlussbedingungen (Typenschild und Dokumentation) und die in den technischen Daten angegebenen Grenzwerte sind vor der Installation und Inbetriebnahme sorgfältig durchzulesen und unbedingt einzuhalten.

1.2.3 Bestimmungsgemäße Verwendung

Elektronische Geräte sind grundsätzlich nicht ausfallsicher. Bei Ausfall der speicherprogrammierbaren Steuerung, des Bedien- oder Beobachtungsgerätes bzw. einer unterbrechungsfreien Stromversorgung ist der Anwender selbst dafür verantwortlich, dass angeschlossene Geräte, wie z. B. Motoren in einen sicheren Zustand gebracht werden.

Die Baugruppen von B&R sind als "offenes Betriebsmittel" (EN 61131-2) und als "open type equipment" (UL) konzipiert und somit für den Einbau im geschlossenen Schaltschrank bestimmt. Es sind in jedem Fall die einschlägigen nationalen und internationalen Fachnormen und Vorschriften, wie z. B. die Maschinenrichtlinie 2006/42/EG, zu beachten und einzuhalten.

1.2.4 Schutz vor elektrostatischen Entladungen

Elektrische Baugruppen, die durch elektrostatische Entladungen (**ElectroStatic Discharge**) beschädigt werden können, sind entsprechend zu handhaben.

1.2.4.1 Verpackung

- Elektrische Baugruppen mit Gehäuse
... benötigen keine spezielle ESD-Verpackung, sie sind aber korrekt zu handhaben (siehe "Elektrische Baugruppen mit Gehäuse" auf Seite 10).
- Elektrische Baugruppen ohne Gehäuse
... sind durch ESD-taugliche Verpackungen geschützt.

1.2.4.2 Vorschriften für die ESD-gerechte Handhabung

Elektrische Baugruppen mit Gehäuse

- Kontakte von Steckverbindern auf dem Gerät nicht berühren (Bus-Datenkontakte)
- Kontakte von Steckverbindern von angeschlossenen Kabeln nicht berühren
- Kontaktzungen von Leiterplatten nicht berühren

Elektrische Baugruppen ohne Gehäuse

Zusätzlich zu "Elektrische Baugruppen mit Gehäuse" gilt:

- Alle Personen, die elektrische Baugruppen handhaben, sowie Geräte, in die elektrische Baugruppen eingebaut werden, müssen geerdet sein.
- Baugruppen dürfen nur an den Schmalseiten oder an der Frontplatte berührt werden.
- Baugruppen immer auf geeigneten Unterlagen (ESD-Verpackung, leitfähiger Schaumstoff etc.) ablegen.

Information:

Metallische Oberflächen sind als Ablageflächen nicht geeignet.

- Elektrostatische Entladungen auf die Baugruppen (z. B. durch aufgeladene Kunststoffe) sind zu vermeiden.
- Zu Monitoren oder Fernsehgeräten muss ein Mindestabstand von 10 cm eingehalten werden.
- Messgeräte und -vorrichtungen müssen geerdet werden.
- Messspitzen von potenzialfreien Messgeräten sind vor der Messung kurzzeitig an geeigneten geerdeten Oberflächen zu entladen.

Einzelbauteile

- ESD-Schutzmaßnahmen für Einzelbauteile sind bei B&R durchgängig verwirklicht (leitfähige Fußböden, Schuhe, Armbänder etc.).
- Die erhöhten ESD-Schutzmaßnahmen für Einzelbauteile sind für das Handling von B&R Produkten bei unseren Kunden nicht erforderlich.

1.2.5 Transport und Lagerung

Bei Transport und Lagerung müssen die Geräte vor unzulässigen Beanspruchungen (mechanische Belastung, Temperatur, Feuchtigkeit, aggressive Atmosphäre) geschützt werden.

Die Geräte enthalten elektrostatisch gefährdete Bauelemente, die durch unsachgemäße Behandlung beschädigt werden können. Es sind daher beim Ein- bzw. Ausbau der Geräte die erforderlichen Schutzmaßnahmen gegen elektrostatische Entladungen zu treffen (siehe "[Schutz vor elektrostatischen Entladungen](#)" auf Seite 9).

1.2.6 Betrieb

1.2.6.1 Schutz gegen Berühren elektrischer Teile

Gefahr!

Zum Betrieb der speicherprogrammierbaren Steuerungen sowie der Bedien- und Beobachtungsgeräte und der unterbrechungsfreien Stromversorgung ist es notwendig, dass bestimmte Teile unter gefährlichen Spannungen stehen. Werden solche Teile berührt, kann es zu einem lebensgefährlichen elektrischen Schlag kommen. Es besteht die Gefahr von Tod oder schweren gesundheitlichen oder materiellen Schäden.

Vor dem Einschalten der speicherprogrammierbaren Steuerungen, der Bedien- und Beobachtungsgeräte sowie der Unterbrechungsfreien Stromversorgung muss sichergestellt sein, dass das Gehäuse ordnungsgemäß mit Erdpotenzial (PE-Schiene) verbunden ist. Die Erdverbindungen müssen auch angebracht werden, wenn das Bedien- und Beobachtungsgerät sowie die unterbrechungsfreie Stromversorgung nur für Versuchszwecke angeschlossen oder nur kurzzeitig betrieben wird!

Vor dem Einschalten sind spannungsführende Teile sicher abzudecken. Während des Betriebs müssen alle Abdeckungen geschlossen gehalten werden.

1.2.6.2 Umgebungsbedingungen - Staub, Feuchtigkeit, aggressive Gase

Der Einsatz von Bedien- und Beobachtungsgeräten (wie z. B. Industrie PCs, Power Panels, Mobile Panels usw.) und unterbrechungsfreien Stromversorgungen in staubbelasteter Umgebung ist zu vermeiden. Es kann dabei zu Staubablagerungen kommen, die das Gerät in dessen Funktion beeinflussen. Insbesondere bei Systemen mit aktiver Kühlung (Lüfter) kann dadurch u. U. keine ausreichende Kühlung mehr gewährleistet werden.

Treten in der Umgebung aggressive Gase auf, können diese ebenso zu Funktionsstörungen führen. In Verbindung mit hoher Temperatur und Luftfeuchtigkeit setzen aggressive Gase - beispielsweise mit Schwefel-, Stickstoff- und Chlorbestandteilen - chemische Prozesse in Gang, welche sehr schnell elektronische Bauteile beeinträchtigen bzw. schädigen können. Ein Anzeichen für aggressive Gase sind geschwärzte Kupferoberflächen und Kabelenden in vorhandenen Installationen.

Bei Betrieb in Räumen mit funktionsgefährdendem Staub- und Feuchtigkeitsniederschlag sind Bedien- und Beobachtungsgeräte, wie Automation Panel oder Power Panel bei vorschriftsmäßigem Einbau (z. B. Wanddurchbruch) frontseitig gegen das Eindringen von Staub und Feuchtigkeit geschützt. Rückseitig jedoch müssen alle Geräte gegen das Eindringen von Staub und Feuchtigkeit geschützt werden bzw. ist der Staubbefall in geeigneten Zeitabständen zu entfernen.

1.2.6.3 Programme, Viren und schädliche Programme

Jeder Datenaustausch bzw. jede Installation von Software mittels Datenträger (z. B. Diskette, CD-ROM, USB Memory Stick usw.) oder über Netzwerke sowie Internet stellt eine potenzielle Gefährdung für das System dar. Es liegt in der Eigenverantwortung des Anwenders, diese Gefahren abzuwenden und durch entsprechende Maßnahmen wie z. B. Virenschutzprogramme, Firewalls usw. abzusichern sowie nur Software aus vertrauenswürdigen Quellen einzusetzen.

1.2.7 Umweltgerechte Entsorgung

Alle Steuerungskomponenten von B&R sind so konstruiert, dass sie die Umwelt so gering wie möglich belasten.

1.2.7.1 Werkstofftrennung

Damit die Geräte einem umweltgerechten Recycling-Prozess zugeführt werden können, ist es notwendig, die verschiedenen Werkstoffe voneinander zu trennen.

Komponente	Entsorgung
Speicherprogrammierbare Steuerungen Bedien- und Beobachtungsgeräte Unterbrechungsfreie Stromversorgung Batterien und Akkumulatoren Kabel	Elektronik Recycling
Karton/Papier Verpackung	Papier-/Kartonage Recycling
Plastik Verpackungsmaterial	Plastik Recycling

Tabelle 1: Werkstofftrennung

Die Entsorgung muss gemäß den jeweils gültigen gesetzlichen Regelungen erfolgen.

2 Sichere Fernwartung

Secure Remote Maintenance, die sichere Fernwartungslösung von B&R, ermöglicht einfache Diagnose und Wartung von Maschinen und Anlagen aus der Ferne und das im Einklang mit gängigen IT- und Sicherheitsrichtlinien.

Dazu wird eine zertifikatgesicherte und verschlüsselte VPN-Verbindung zwischen dem SiteManager an der Maschine und einem Gateway hergestellt, welches typischerweise im Service-Center des Maschinenbauers steht. Dort können sämtliche Zugriffsberechtigungen für bis zu 10000 Maschinen hinterlegt werden. Der SiteManager verfügt über integrierte digitale Ein- und Ausgänge, so kann z. B. ein Schlüsselschalter angeschlossen werden, um Wartungszugriffe erst nach dessen Betätigung zu ermöglichen. Vor unerwünschten Zugriffen durch Dritte schützt eine integrierte Firewall. Um Sicherheitskonflikte mit werksseitigen Firewalls zu vermeiden, läuft die Kommunikation in das Internet über Firewall-verträgliche, verschlüsselte Web-Protokolle. Es müssen daher keine zusätzlichen Ports geöffnet werden.

Warnung!

Bei einem Zugriff muss das lokale Personal über den Zugriff informiert werden. Der Anwender muss durch geeignete Maßnahmen sicherstellen, dass Fernzugriffe ohne Wissen des lokalen Personals nicht möglich sind.

Maschinen-Pool-Management

Maschinenbauer haben viele Kunden und noch mehr Maschinen im Feld. Um Fernwartung effizient zu gestalten, muss es ein zentrales Maschinen-Pool-Management als untergeordnetes System einer modernen Fernwartungslösung geben. Dieses verwaltet sowohl die Maschinen im Feld als auch die Zugriffsrechte der Servicekräfte auf die einzelnen Maschinen. Ein Maschinen-Pool-Managementsystem ist die wichtigste Funktion eines benutzerfreundlichen und sicheren Fernwartungssystems. Der Zugriff auf das Maschinen-Pool-Management wird über ein Web-Portal im Internet ermöglicht. Dieses Web-Portal ist Bestandteil des GateManagers.

Möglichkeiten

- Diagnose mit dem System-Diagnose-Manager oder in Automation Studio
- Auslesen von Logbucheinträgen und Applikationsdaten
- Änderungen von Maschineneinstellungen und -parametern
- Aktualisieren von Programmen und Firmware über Automation Studio

Starke Partnerschaft mit führendem Technologieanbieter

Die sichere Fernwartungslösung ist ein von Secomea entwickeltes Markenprodukt. Secomea ist ein führender Hersteller industrieller Kommunikationsgeräte mit Schwerpunkt auf Sicherheit und Nutzbarkeit der Produkte.

Die B&R-Versionen der eingesetzten Hardware- und Software-Produkte unterscheiden sich leicht von den Produkten von Secomea:

- Alle B&R-SiteManager sind vollständig in Automation Studio integriert und können daher im Automation Studio-Projekt konfiguriert werden.

Information:

Die SiteManager von Secomea können nicht auf diese Weise konfiguriert werden.

- Des Weiteren werden von den Software-Varianten von GateManager, SiteManager und LinkManager eigene B&R-Versionen eingesetzt.

Information:

Die Software-Versionen von Secomea sind nicht mit den B&R-Versionen kompatibel und dürfen nicht für die B&R-Lösung zur sicheren Fernwartung verwendet werden!

- Bei LinkManager-Verbindung über VNC-Protokoll ist ein dedizierter VNC-Agent zu verwenden (dedizierte Eingabe der Adresse und Portnummer, z. B. 192.168.0.8:5910).

Information:

Bei der Secomea-Lösung wird standardmäßig immer der VNC Port 5900 verwendet.

- Bei B&R werden ausschließlich GateManager Premium Administratorkonten eingesetzt.

3 Systemübersicht

Die B&R Fernwartungslösung Secure Remote Maintenance wurde im Hinblick auf höchste Netzwerksicherheit sowie auf einfache und intuitive Bedienung entwickelt, um einem Servicetechniker Fernzugriff auf eine Maschine zu gewähren. Dazu wird im Servicefall eine sichere Verbindung zwischen Maschine und Techniker aufgebaut werden. Der Techniker braucht lediglich einen Web-Browser und eine Internetverbindung, um sich beim Web-Portal des GateManagers anzumelden. Die Maschine verbindet sich über den SiteManager, ein Fernwartungs-Gateway mit integrierter Firewall, ebenfalls mit dem Web-Portal. Der im Web-Portal integrierte Maschinen-Pool-Manager lässt dann autorisierte Verbindungen zwischen Techniker und Maschine zu – die sichere VPN-Verbindung steht.

Durch VPN-Netzwerke, Firewalls und geeignete Verbindungsaufbau-Strategien ist die Fernwartungsverbindung maximal geschützt. Dieser Schutz erstreckt sich auch auf Man-in-the-Middle- und Denial-of-Service-Angriffe und sorgt so bei der Fernwartungslösung für maximale Sicherheit.

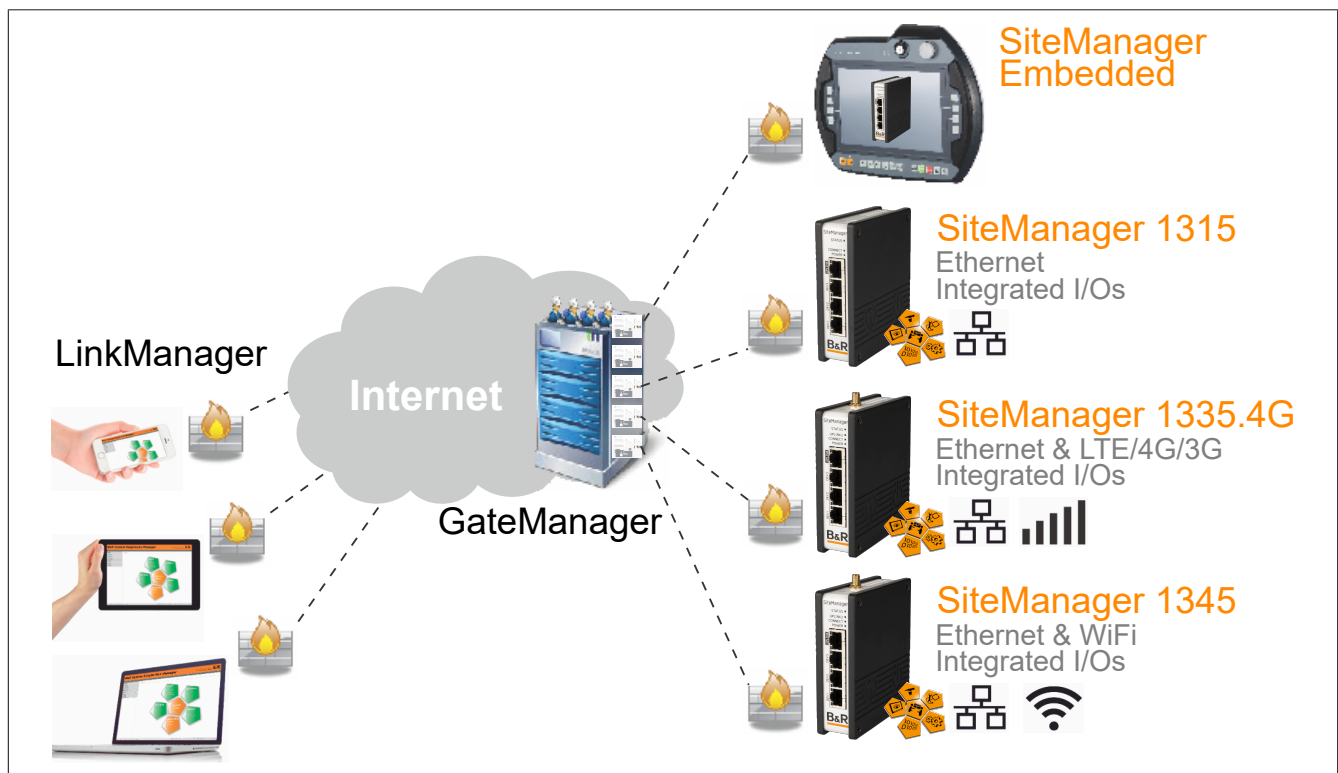
Wo eine Anbindung über LAN oder WLAN nicht möglich oder erwünscht ist, kann die VPN-Verbindung via Mobilfunk aufgebaut werden.

Systemaufbau

Secure Remote Maintenance setzt sich mindestens aus folgenden Komponenten zusammen:

- 1x GateManager (im "Starter Package" enthaltener "B&R Hosting Service" oder 0RMGM.sw)
- 1x LinkManager (0RMLM.WIN) und LinkManager Mobile (0RMLM.MOB) Lizenz
- 1x SiteManager (0RMSM13x5) oder SiteManager Embedded (0RMSME.x)
- Service Agreement

Basierend auf diesem Minimalaufbau werden zum schnellen Einstieg in die Fernwartungslösung verschiedene Starter Packages angeboten (siehe "[Starter Package](#)" auf Seite 43).



3.1 GateManager

Der GateManager ist die zentrale Verbindungsplattform für Techniker und Maschine, wo sich beide zum Verbindungsaufbau einwählen (der GateManager fungiert als sicherer Proxy für SiteManager und LinkManager). Verbindungen werden entsprechend der hinterlegten Autorisierung, sprich den konfigurierten Benutzerkonten und Zugriffsrechten, hergestellt. Die Verwaltung von Benutzerkonten, Autorisierungen und Maschinen ist einfach und intuitiv und erfolgt durch berechnete Personen über ein Web-Portal (Maschinen-Pool-Management).

Der GateManager wird von B&R als Hosting Service und Software-Installer (Linux) angeboten und kann gemäß spezifischen Kundenanforderungen eingerichtet werden. So kann der Maschinenbauer sein eigenes Portal zur Übersicht über seinen Maschinen im Feld einrichten.

Der GateManager ist die einzige Komponente die offene Ports ins Internet besitzt. Das bedeutet, dass der GateManager über einen FQDN (Fully-Qualified Domain Name) verfügen muss und seine Benutzeroberfläche natürlich auch webbasierend ist. In diesen Belangen unterscheidet sich der GateManager nicht von einem normalen Webserver auf dem z. B. die Unternehmens-Webseite gehostet ist. Zugriffe und Verbindungen werden aber nur mit dem richtigen X.509 Zertifikat zugelassen.

Administratoren einer eigenen Instanz (Software-Image) haben die Möglichkeit sogenannte Domains zu erstellen. Domains werden verwendet, um einen GateManager logisch zu unterteilen und zu strukturieren. Jeder Domain können ein oder mehrere Domain-Administratoren zugewiesen werden, die nur den Inhalt der zugewiesenen Domain einsehen und verwalten können.

Information:

GateManager werden mit vorinstallierter LinkManager und LinkManager Mobile Lizenz ausgeliefert.

Softwareinstaller für Linux

Die GateManager Software Variante basiert auf einem Software-Installer für beliebige Linux-Umgebungen. Download der GateManager-Software via <http://www.br-automation.com/gatemanager>.

GateManager Hosting Service

Für einen schnellen Einstieg in die Fernwartungslösung werden verschiedene Starter Packages angeboten (siehe "Starter Package" auf Seite 43), welche den GateManager Hosting Service beinhalten.

Mit dem GateManager Hosting Service kann Secure Remote Maintenance verwendet werden, ohne einen GateManager installieren und betreiben zu müssen. Dadurch entfallen kundenseitig die initialen Aufwände für die Anschaffung der GateManager Variante sowie die Integration in die eigene IT-Landschaft.

E-Mail-Größen

Im Hosting Service von Secomea können E-Mails mit einer maximalen Größe von 10 MByte, inklusive Header, gesendet werden. Das entspricht einer E-Mail-Größe von ca. 7 bis 8 MByte.

3.1.1 Bestelldaten

Bestellnummer	Kurzbeschreibung
	GateManager
0RMGM.SW	Secure Remote Maintenance - GateManager (SoftwareVersion), verwaltet max. 10000 SiteManager, 1x LinkManager und 1x LinkManager Mobile Lizenz inkludiert, Servicegebühr 0RMAS.SERVICE-01 muss separat gezahlt werden

Tabelle 2: 0RMGM.SW - Bestelldaten

Information:

Download der GateManager-Software via <http://www.br-automation.com/gatemanager>.

3.1.2 Aktivierung des GateManagers

Wird ein GateManager ausgeliefert, befindet sich das Gerät im Test-/Demo-Modus. Es sind dabei 1x LinkManager und 1x LinkManager Mobile Lizenz vorinstalliert und es können maximal 3 SiteManager verwaltet und 2 gleichzeitig verwendet werden. Im Demo-Modus sind keine funktionalen Einschränkungen gegeben.

Um den GateManager in vollem Umfang nutzen zu können, muss er aktiviert werden. Für die Aktivierung müssen die "license-id" und der "hostname" des GateManagers an B&R rückgemeldet werden. Basierend auf diesen Informationen wird dann ein Lizenzschlüssel generiert, mit dem der GateManager aktiviert werden kann (eine Lizenz wird nur für den einen bestimmten GateManager erstellt, der durch die "license-id" und den "hostname" identifiziert wird). Die Lizenzen und Benutzer von LinkManager und LinkManager Mobile werden vollständig in GateManager verwaltet.

Information:

Der "hostname" kann in den Einstellungen des GateManager frei definiert werden und muss ein FQDN sein - z. B. "remote.companyname.com". Die Verwendung einer IP-Adresse anstatt des FQDN wird bei der Lizenzgenerierung nicht unterstützt. Des Weiteren muss beachtet werden, dass nach der erfolgreichen Aktivierung der "hostname" nicht mehr geändert werden darf, da dadurch alle installierten Lizenzen ungültig werden.

Zur einfacheren Übertragung der GateManager-Informationen an den Vertreter von B&R enthält der GateManager ein spezielles Formular, das zur Übertragung dieser Informationen verwendet werden kann.

The screenshot shows the 'License Ordering Specification' form in the GateManager interface. The form is divided into three main sections, each highlighted with a red circle and a number:

- Section 1: Your local B&R representative:** This section contains three input fields: 'Company:', 'Contact:', and 'E-mail:'.
- Section 2: Order Reference:** This section contains several input fields and a text area: 'GateManager Model:' (with value 4260), 'Hostname (FQDN):' (with value remote.testcompany.com), 'LicenseID:' (with value 1234567890abCdeFGHijklmn), 'Order number:' (with a text input field), 'Your company:' (with a text input field), 'Your name:' (with value Max Mustermann), 'Your E-mail:' (with value max.mustermann@testcompany.com), and a 'Comment:' text area. A note on the right says 'Your B&R purchase order number related to this license specification'.
- Section 3: Current Agreement of Service and Licenses:** This section shows the current status of the agreement: 'Current Agreement of Service: Trial mode', 'LinkManager Licenses: 1 of 1 installed', 'LinkManager Mobile Licenses: 1 of 1 installed', and 'SiteManagers: 1 of 3 added'.

At the bottom of the form is a 'Submit Information' button.

Das Formular ist folgendermaßen auszufüllen:

1. Die Informationen des B&R-Vertreters angeben. Diese sind z. B. auf dem Lieferschein des GateManagers enthalten. Bitte das Kontakt- und E-Mail-Feld verwenden, um den Namen und die E-Mail-Adresse des Vertriebsmitarbeiters bei B&R oder einer Tochtergesellschaft einzugeben.
2. Die erforderlichen GateManager Informationen werden automatisch eingetragen. Bitte hier die Bestellnummer von dem GateManager Lieferschein sowie den Namen des Unternehmens eingeben. Über das Kommentarfeld können zusätzliche Informationen angegeben werden.
3. Dieser Abschnitt zeigt das aktuell aktive Service Agreement für den GateManager. Dort wird auch angezeigt, wie viele Lizenzen und SiteManager installiert sind oder diesem Service Agreement hinzugefügt werden können.

Mit Betätigen von **<Submit Information>** (Informationen senden), wird das vollständige Formular an B&R und den Vertreter von B&R gesendet.

3.1.2.1 Auslieferung und Installation der Lizenzen

Die übermittelten Daten werden anschließend von B&R mit den vorliegenden Bestelldaten abgeglichen. Nach erfolgreicher Überprüfung wird die Aktivierungslizenz an den zu aktivierenden GateManager automatisch übermittelt und installiert. Da die Lizenzen auf "hostname" und "license-id" des GateManagers gebunden sind, besteht keine Notwendigkeit die Lizenzdateien zu archivieren. Die Auslieferung der Lizenzen erfolgt daher durch die automatische Installation auf dem GateManager.

Sollte der GateManager offline oder aus anderweitigen Gründen nicht erreichbar sein, erfolgt die Auslieferung per E-Mail an die unter Punkt 2 des Formulars angegebene E-Mail-Adresse. In der E-Mail ist ebenfalls eine Installationsanleitung für die Lizenzen enthalten.

Der Auslieferungs- und Installationsvorgang ist für die Aktivierungslizenz und für alle weiteren Lizenzen des GateManagers (LinkManager/LinkManager Mobile Lizenzen, SiteManager Embedded Lizenzen etc.) identisch. Die Auslieferung der Lizenzen erfolgt ausschließlich in digitaler Form.

3.1.3 Servicegebühr

Die Fernwartungslösung unterliegt einem Service Agreement mit entsprechender Servicegebühr. Die Servicegebühr beinhaltet Software-Updates, Security Patches, Maintenance, B&R Support und Hosting Service.

Information:

Die Servicegebühr ist im Voraus zu bezahlen. Die ersten 12 Monate Nutzung der Fernwartungslösung sind kostenlos.

3.1.3.1 Bestelldaten

Bestellnummer	Kurzbeschreibung
ORMAS.SERVICE-01	Secure Remote Maintenance - Servicegebühr pro Jahr - inkludiert Software Updates und Patches sowie Bug Fixes, ersten 12 Monate kostenlos, Abrechnung im Voraus

3.1.4 Zusätzliche Services

3.1.4.1 LogTunnel– Remote Data Logging

LogTunnel ermöglicht die Aufzeichnung von Maschinendaten auf einem zentralen Datenbank-Server (Log-Server) im Rechenzentrum des Maschinenbauers.

3.1.4.1.1 Bestelldaten

Bestellnummer	Kurzbeschreibung
ORMAS.LOG	Secure Remote Maintenance - Aktivierung LogTunnel und Usage Statistics Lizenz

3.1.4.2 SMS-Lizenz

3.1.4.2.1 Bestelldaten

Bestellnummer	Kurzbeschreibung
ORMAS.SMS	Remote Maintenance - SMS Aktivierung SMS Lizenz

3.1.5 Benutzerrechteverwaltung

Alle Benutzerkonten des Fernwartungssystems werden am GateManager angelegt und gewartet. Jedem Benutzerkonto muss eine Benutzerrolle zugeordnet werden, die gewisse Tätigkeiten im Fernwartungssystem erlauben. Diese Benutzerrechteverwaltung dient der Funktionstrennung und stellt eine weitere wichtige Sicherheitsschicht im Fernwartungssystem dar.

Der GateManager protokolliert jede Veränderung der Konfiguration, jede Benutzeranmeldung, jeden Verbindungsaufbau mit einem Benutzerkonto, ausgeführte Aktionen und Events und vieles mehr. Alle diese Ereignisse werden mit Zeitstempel, Beschreibung und ausführendem Benutzer protokolliert.

Die wichtigsten Benutzerrollen sind:

- GateManager Server-Administrator
- GateManager Domain-Administrator
- LinkManager Benutzer
- LinkManager Mobile Benutzer
- Domain Beobachter

Das System kann so konfiguriert werden, dass Zugriffe auf SiteManager und deren Device Agents nur von LinkManager-Benutzern durchgeführt werden. Administratoren können dann innerhalb der GateManager Oberfläche keine Verbindungen zu SiteManagern oder Device Agents aufbauen. Administratoren können dann nur die SiteManager und LinkManager Benutzerkonten, Domains bzw. Sub-Domains zuzuordnen.

3.1.5.1 GateManager Server-Administrator

Diese Benutzerrolle wird für einen Systemadministrator verwendet. Die Aufgabe des Server-Administrators ist es, die initiale Server-Konfiguration zu erstellen und für den weiteren störungsfreien Betrieb zu sorgen. Der Server-Administrator kann Benutzer mit allen verfügbaren Benutzerrollen anlegen, freischalten, deaktivieren, usw.

Der Server-Administrator hat Zugriff auf alle Domains auf dem GateManager. Folgend aufgeführt sind die wichtigsten Tätigkeiten die mit einem Server-Administrator Benutzerkonto durchgeführt werden können:

- Erstellen von weiteren Server-Administrator Benutzerkonten und Benutzerkonten mit anderen Rollen
- Zugriff auf die GateManager Konfiguration (E-mail-Settings, Server-Log, Lizenzverwaltung, Firmware Repository etc.)
- Erstellen von Backups von SiteManager-Einstellungen
- Upgrade von SiteManager-Firmware
- Erstellen von Actions und Alerts
- Erstellen von Domains und Sub-Domains
- Domainübergreifendes Verschieben von Benutzerkonten, SiteManagern und Device Agents.

3.1.5.2 GateManager Domain-Administrator

Diese Benutzerrolle ist der eines Server-Administrators ähnlich. Der Domain-Administrator kann in seiner zugewiesenen Domain Benutzerkonten anlegen und verwalten sowie Sub-Domains erstellen und so seine Domain weiter unterteilen. Der Domain-Administrator hat keine Informationen über mögliche weitere Domains die sich noch auf dem GateManager befinden. Zusätzlich kann der Domain-Administrator SiteManager und Device Agents in Sub-Domains verwalten und dadurch LinkManager Benutzerkonten den Zugriff auf Maschinen gewähren oder verweigern.

Im Folgenden sind Tätigkeiten angeführt die mit einem Domain-Administrator Benutzerkonto durchgeführt werden können. Dies ist nur in der Domain möglich, für die der Domain-Administrator verantwortlich ist:

- Erstellen von Benutzerkonten (keine Server-Administrator Benutzer!)
- Erstellen von Backups von SiteManager-Einstellungen
- Upgrade von SiteManager-Firmware
- Erstellen von Actions und Alerts
- Erstellen von Sub-Domains
- Verschieben von Benutzerkonten, SiteManagern und Device Agents in Sub-Domains.

3.1.5.3 LinkManager Benutzer

Diese Benutzerrolle ist für einen Servicetechniker gedacht, der Zugriff auf Maschinen oder Maschinenteile benötigt. Über vorkonfigurierte Device Agents kann sich der Servicetechniker via PC mit den Device Agents verbinden. Der LinkManager Benutzer ist auf die richtige Konfiguration seiner Zugriffsrechte auf SiteManager und deren Device Agents, durch den Domain-Administrator angewiesen.

3.1.5.4 LinkManager Mobile Benutzer

Der LinkManager Mobile ermöglicht Benutzern den Fernzugriff auf industrielle Anlagen von ihrem iPhone, iPad oder Android Gerät. Die App ist dafür bestimmt, auf grafische Benutzeroberflächen beispielsweise auf SPS-Geräten, HMI-Bedienpults oder Webcams zuzugreifen. Sie stellt auch Verbindungen zu Desktops her, auf denen Linux oder Windows läuft. Mit dem LinkManager Mobile kann man sich einfach mit dem Gerät verbinden, eine VNC starten oder einen MS Remote Desktop Client (RDP) und dann aus der Ferne das Gerät steuern.

3.1.5.5 Domain Beobachter

Diese Benutzerrolle gewährt dem Benutzer Einblick in alle Details einer Domain, inklusive Audit Logs, Lizenzen sowie SiteManager und Device Agents. Diese Rolle dient nur zum Beobachten und Einsehen der Aktivitäten in einer Domain. Der Domain Beobachter kann weder Veränderungen an der Konfiguration vornehmen noch neue Benutzerkonten anlegen.

3.2 SiteManager

Die **SiteManager** 0RMSM1315, 0RMSM1335.4G und 0RMSM1345 ermöglichen die Verbindung von der Maschine oder dem Maschinen-Netzwerk zum GateManager und darüber hinaus in das Internet. Alle SiteManager-Varianten sind mit integrierten Ein- und Ausgängen sowie mit mindestens einer Ethernet-Schnittstelle für den Uplink in das Internet ausgestattet. Die integrierte Firewall regelt alle Zugriffe auf das Maschinennetzwerk. Das bedeutet, dass keine Kommunikation zwischen dem GateManager und dem Maschinennetzwerk möglich ist, solange nicht entsprechende Firewall Regeln erstellt wurden (ab Version 8.2).

Zur einfachen Handhabung können alle SiteManager-Varianten in Automation Studio konfiguriert werden. Der SiteManager muss lediglich einmal installiert werden. Sollte es nötig werden, den SiteManager auszutauschen, werden alle Parameter von der SPS-Steuerung der Maschine auf den neuen SiteManager übertragen. Meldet sich der SiteManager zum ersten Mal auf dem Service Portal an, muss lediglich einmalig die Authentifizierung durchgeführt werden.

SiteManager Embedded

SiteManager Embedded ist die Software-Variante des SiteManager und kann auf x86 Windows und Linux Automation/Panel PCs eingesetzt werden. Der SiteManager Embedded bietet für den LinkManager die gleichen Zugriffsmöglichkeiten auf das Maschinennetzwerk wie die Hardwarevarianten des SiteManager.

Einfach das Installationspaket des SiteManager Embedded runterladen und installieren. Download der SiteManager-Software via <http://www.br-automation.com/sitemanager>.

Die SiteManager Embedded Lizenzen werden dabei auf dem GateManager installiert und den SiteManager Embedded Instanzen zugewiesen.

Der SiteManager Embedded ist in 2 Varianten verfügbar:

- **SiteManager Embedded BASIC:** Die BASIC Variante erlaubt den Zugriff auf den Automation bzw. Panel PC auf dem der SiteManager Embedded installiert ist. Die Verwendung der Hypervisor-Funktionalität ist in dieser Variante jedoch nicht möglich. Der Zugriff auf das Maschinennetzwerk und die darin befindlichen anderen Netzwerkteilnehmer ist nicht möglich.
- **SiteManager Embedded EXTENDED:** Die EXTENDED Variante setzt auf der Funktionalität der BASIC Variante auf und erlaubt zusätzlich den Zugriff auf das Maschinennetz und weiterer Netzwerkteilnehmer sowie die Verwendung der Hypervisor-Funktionalität der Automation- bzw. Panel PCs. Diese Variante bietet den gleichen Funktionsumfang wie die Hardware SiteManager.

SiteManager Hardware

Die Hardwarevarianten des SiteManager unterscheiden sich primär durch die verbauten Uplink-Ports:

- **SiteManager 1315:** 1x Ethernet Uplink Port
- **SiteManager 1335.4G:** 1x LTE/4G/3G Uplink Port und 1x Ethernet Uplink Port
- **SiteManager 1345:** 1x WiFi Uplink Port und 1x Ethernet Uplink Port

3.2.1 Modellvergleich

SiteManager Modellvergleich	0RMSM11xx	0RMSM13xx	SiteManager Embedded BASIC	SiteManager Embedded EXTENDED
Fernzugriff auf IP-Geräte (UDP/TCP)	Ja	Ja	Ja	Ja
Fernzugriff auf USB-/Seriell-/Layer2-Geräte	Ja	Ja	Nein	Nein
Tunnelzugriff auf das GESAMTE Remote-Netzwerk	Ja	Ja	Ja	Ja
Anzahl der einzelnen Geräteagenten	Bis zu 5	Bis zu 10	2	Bis zu 5
Access Gateway für andere IP-Geräte	Ja	Ja	Nein	Ja
Datenerfassungsmodul (DCM)	Ja	Ja	Nein	Ja ¹⁾
Konfigurierbare Weiterleitungs-/Routing-Regeln	Ja	Ja	Nein	Nein
Automatische Erkennung von Ethernet- und USB-Geräten	Ja	Ja	Nein	Nein
LogTunnel-Clients Unterstützung	Ja	Ja	Nein	Ja
LogTunnel Master Push-Unterstützung	Ja	Ja	Nein	Ja
LogTunnel Master Pull-Unterstützung	Ja	Ja	Nein	Ja ¹⁾

1) Nur für Linux verfügbar

3.2.2 Bestelldaten

3.2.2.1 SiteManager Embedded

0RMSME.x

Bestellnummer	Kurzbeschreibung
	SiteManager
0RMSME.B	Secure Remote Maintenance - SiteManager Embedded BASIC Lizenz für Windows/Linux, 2 Device Agents
0RMSME.E	Secure Remote Maintenance - SiteManager Embedded EXTENDED Lizenz für Windows/Linux, 5 Device Agents

Tabelle 3: 0RMSME.B, 0RMSME.E - Bestelldaten

Information:

Download der SiteManager-Software via <http://www.br-automation.com/sitemanager>.

3.2.2.2 SiteManager Hardware

0RMSM1315


Bestellnummer	Kurzbeschreibung	Abbildung
	SiteManager	
0RMSM1315	Secure Remote Maintenance -SiteManager, LAN 1x Ethernet 100Base-T uplink Anschluss, 3x Dev Anschlüsse, 10 Geräteagenten, integrierte Firewall, 2x digitale Eingänge, 2x digitale Ausgänge, 24 VDC	
	Optionales Zubehör	
	Feldklemmen	
0TB6110.2010-01	Zubehör Feldklemme, 10-polig (3,81), Schraubklemme 1,5 mm²	

Tabelle 4: 0RMSM1315 - Bestelldaten

0RMSM1335.4G


Bestellnummer	Kurzbeschreibung	Abbildung
	SiteManager	
0RMSM1335.4G	Secure Remote Maintenance -SiteManager, 1x Ethernet 100BASE-T Uplink Anschluss, 1x GPRS/3G/4G Uplink Anschluss, 3x Dev Anschlüsse, 10 Geräteagenten, integrierte Firewall, 2x digitale Eingänge, 2x digitale Ausgänge, 24 VDC	
	Optionales Zubehör	
	Antennen	
0RMSM.A3G-10	GSM/3G Puck Antenne Frequenzen: 880-960/1710-2170 MHz, SMA Stecker (male), 2,5m Kabel, Schraub- bzw. Loch-Montage, IP67, kompatibel zu 0RMSM1x35	
0RMSM.A3G-20	GSM/3G Mini Antenne Frequenzen: 824-960/1710-2170 MHz, SMA Stecker (male), 3m Kabel, magnetische Befestigung, kompatibel zu 0RMSM1x35	
0RMSM.AMB-10	GSM/3G/LTE Breitband Antenne Frequenzen: 750-1250, 1650-2700MHz, SMA male Stecker, 3m Kabel, Schraub- bzw. Loch-Montage, kompatibel zu 0RMSM1x35, Grundplatte für optimale Verstärkung benötigt, IP67	
	Feldklemmen	
0TB6110.2010-01	Zubehör Feldklemme, 10-polig (3,81), Schraubklemme 1,5 mm²	

Tabelle 5: 0RMSM1335.4G - Bestelldaten

0RMSM1345


Bestellnummer	Kurzbeschreibung	Abbildung
	SiteManager	
0RMSM1345	Secure Remote Maintenance -SiteManager, 1x Ethernet 100Base-T Uplink Anschluss, 1x WiFi uplink Anschluss, 3x Dev Anschlüsse, 10 Geräteagenten, integrierte Firewall, 2x digitale Eingänge, 2x digitale Ausgänge, 24 VDC	
	Optionales Zubehör	
	Antennen	
0RMSM.AWIFI-10	WiFi Puck Antenne, 2,4 & 5 GHz, kompatibel zu 0RMSM1x45, 2m Kabel	
	Feldklemmen	
0TB6110.2010-01	Zubehör Feldklemme, 10-polig (3,81), Schraubklemme 1,5 mm ²	

Tabelle 6: 0RMSM1345 - Bestelldaten

Lieferumfang:

Anzahl	Beschreibung
1	WiFi Antenne, 2,4 GHz, kompatibel zu 0RMSM1345, schwenkbar mit RP-SMA Stecker

3.2.3 Technische Daten

3.2.3.1 SiteManager Embedded

Bestellnummer	0RMSME.B	0RMSME.E
Allgemeines		
Systemvoraussetzungen		
Hardwarevoraussetzungen		
Prozessor	Intel x86 oder kompatible CPU	
Arbeitsspeicher	10 MByte freier RAM	
Festplattenspeicher	5 MByte	
Softwarevoraussetzungen		
Betriebssystem	Windows: 7/8/10, 32/64 Bit, Standard oder Embedded Linux: typische x86 Distributionen, wie Debian, Ubuntu, CentOS, ...	

3.2.3.2 SiteManager Hardware (0RMSM13x5)

Product ID	0RMSM1315		0RMSM1335.4G	0RMSM1345
Allgemeines				
B&R ID-Code	0x6C5E		0x6C5F	0x6C60
Reset-Taster	Ja			
Status-LED	Versorgungsspannung Status Verbindung LinkManager		Versorgungsspannung Status Verbindung LinkManager drahtlose Verbindung	
Leistungsaufnahme	max. 5 W (ohne USB) max. 8 W (mit USB)			
Funktionalität				
Datenübertragung / Frequenzbereich				
Integriertes Breitbandmodem				
LTE Band	-	Siehe 0RMSM1335.4G Bänder		-
WCDMA/UMTS	-	Siehe 0RMSM1335.4G Bänder		-
GPRS/EDGE	-	B2 (1900) B3 (1800) B5 (850) B8 (900)		-
Integriertes WiFi Modul	-			2,4 GHz 5 GHz
Controller				
Prozessor				
Typ	ARM Cortex A7 MCU			
Taktfrequenz	800 MHz			
Schnittstellen				
RS232	DB9 serielle Schnittstelle mit voller Datenflusssteuerung			
USB				
Anzahl	1			
Typ	USB 2.0			
Schnittstelle IF1				
Typ	Ethernet UPLINK1			
Ausführung	RJ45 geschirmt			
Leitungslänge	max. 100 m zwischen 2 Knoten (Segmentlänge)			
Übertragungsrate	max. 10/100 MBit/s			
Übertragung				
Physik	10BASE-T/100BASE-TX			
Halbduplex	Ja			
Vollduplex	Ja			
Autonegotiation	Ja			
Auto-MDI/MDIX	Ja			
Schnittstelle IF2				
Typ	DEV1			
Ausführung	RJ45 geschirmt			
Übertragungsrate	max. 10/100 MBit/s			
Schnittstelle IF3				
Typ	-	4G/3G/GPRS	-	
Ausführung	-	SMA female	-	
Übertragungsrate	-	Downlink: 50 MBit/s (10 MHz Bandweite) Uplink: 25 MBit/s (10 MHz Bandweite)	-	
Schnittstelle IF4				
Typ	-			WiFi
Ausführung	-			RP-SMA female
Schnittstelle IF5				
Typ	DEV2			
Ausführung	RJ45 geschirmt			
Übertraungsrate	max. 10/100 MBit/s			

Systemübersicht

Product ID	0RMSM1315	0RMSM1335.4G	0RMSM1345
Schnittstelle IF6			
Typ		DEV3	
Ausführung		RJ45 geschirmt	
Übertragungsrate		max. 10/100 MBit/s	
Elektrische Eigenschaften			
Nennspannung		12 bis 24 VDC	
Einsatzbedingungen			
Schutzart nach EN 60529		IP20	
Umgebungsbedingungen			
Temperatur			
Betrieb		-25 bis 60°C	
Lagerung		-40 bis 60°C	
Luftfeuchtigkeit			
Betrieb		5 bis 95%	
Lagerung		5 bis 95%	
Transport		5 bis 95%	
Meereshöhe			
Betrieb		2000 m	
Mechanische Eigenschaften			
Material		Aluminium	
Abmessungen			
Breite		32 mm	
Höhe		107 mm	
Tiefe		97 mm	
Gewicht		0,5 kg	

0RMSM1335.4G Bänder

	LTE-Bänder	WCDMA/UMTS-Bänder
B1 (FDD 2100) IMT	X	X
B2 (FDD 1900) PCS	X	X
B3 (1800 +) DCS	X	
B4 (1700) AWS	X	X
B5 (850) CLR, US Korea etc	X	X
B6 (850) Japan #1		X
B7 (2600) IMT-E	X	
B8 (900) E-GSM	X	X
B12 (700) US	X	
B13 (700c) USMH, LSMH US	X	
B18 (800 or 850?) Japan #4	X	
B19 (800 or 850?) Japan #5	X	X
B20 (800) Digital Dividend	X	
B25 (1900 G Block)	X	
B26 (850+) Extended CLR	X	
B28 (700 APT) APAC	X	
B34 (TDD)	X	
B38 (TDD 2600) IMT-E	X	
B39 (TDD 1900 +) China	X	
B40 (TDD 2300) China	X	
B41 (TDD 2500) BRS/EBS	X	
B66 (TDD)	X	

3.2.4 Zubehör

3.2.4.1 Feldklemmen

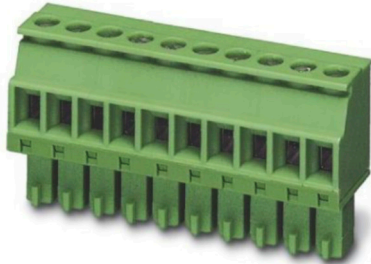
Bestellnummer	Kurzbeschreibung	Abbildung
	Feldklemmen	
0TB6110.2010-01	Zubehör Feldklemme, 10-polig (3,81), Schraubklemme 1,5 mm ²	

Tabelle 7: 0TB6110.2010-01 - Bestelldaten

3.2.4.2 Antennen

Information:

Bei Einbau des SiteManagers im Schaltschrank und Verwendung einer Antenne wird die Montage der Antenne außerhalb des Schaltschranks empfohlen!

Für UL-Konformität ist die Antennenmontage außerhalb des Schaltschranks zwingend!


Bestellnummer	Kurzbeschreibung	Abbildung
	Antennen	
0RMSM.A3G-10	GSM/3G Puck Antenne Frequenzen: 880-960/1710–2170 MHz, SMA Stecker (male), 2,5m Kabel, Schraub- bzw. Loch-Montage, IP67, kompatibel zu 0RMSM1x35	

Tabelle 8: 0RMSM.A3G-10 - Bestelldaten


Bestellnummer	Kurzbeschreibung	Abbildung
	Antennen	
0RMSM.A3G-20	GSM/3G Mini Antenne Frequenzen: 824-960/1710-2170 MHz, SMA Stecker (male), 3m Kabel, magnetische Befestigung, kompatibel zu 0RMSM1x35	

Tabelle 9: 0RMSM.A3G-20 - Bestelldaten


Bestellnummer	Kurzbeschreibung	Abbildung
0RMSM.AMB-10	Antennen	
	GSM/3G/LTE Breitband Antenne Frequenzen: 750-1250, 1650-2700MHz, SMA male Stecker, 3m Kabel, Schraub- bzw. Loch-Montage, kompatibel zu 0RMSM1x35, Grundplatte für optimale Verstärkung benötigt, IP67	

Tabelle 10: 0RMSM.AMB-10 - Bestelldaten


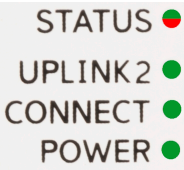
Bestellnummer	Kurzbeschreibung	Abbildung
0RMSM.AWIFI-10	Antennen	
	WiFi Puck Antenne, 2.4 & 5 GHz, kompatibel zu 0RMSM1x45, 2m Kabel	

Tabelle 11: 0RMSM.AWIFI-10 - Bestelldaten

3.2.5 Status-LEDs

Bei allen Varianten sind 3 LEDs zum Anzeigen der Modulversorgung, des Modulstatus und der LinkManager-Verbindung vorhanden. Bei den Varianten 1x35 und 1x45 ist eine weitere LED zur Zustandsanzeige der drahtlosen Verbindung vorhanden:

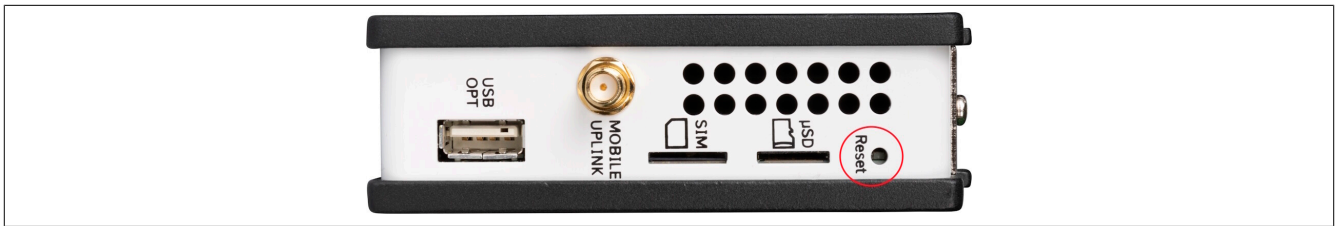
Abbildung	LED	Farbe	Status	Beschreibung
	STATUS	Rot	Dauerblinken	Booten
			2x blinken	GateManager getrennt oder beim Verbindungsaufbau.
			Ein	Mögliche Ursachen: <ul style="list-style-type: none"> • UPLINK ist physisch getrennt. • GateManager-Konfiguration fehlt im SiteManager. • Keine Verbindung zum GateManager-Host, da seine Adresse als DNS-Name konfiguriert ist und kein DNS-Server konfiguriert wurde bzw. nicht erreichbar ist oder nicht funktioniert.
	UPLINK2	Grün	Ein	GateManager verbunden.
		Grün	Aus	1x35: Keine SIM-Karte erkannt.
				1x45: Mögliche Ursachen: <ul style="list-style-type: none"> • Keine WiFi-SSID konfiguriert. • SSID konfiguriert, aber kein WiFi KEY konfiguriert. • SSID und WiFi KEY konfiguriert, aber kein Zugangspunkt gefunden, der mit der SSID übereinstimmt.
			3x blinken	1x35: Falscher oder fehlender SIM-PIN-Code.
			2x blinken	1x35: SIM-PIN-Code OK, aber keine Verbindung (Fehlerbehebung in der SiteManager-Benutzeroberfläche).
				1x45: WiFi SSID gefunden, aber noch nicht verbunden. Möglicher Fehler mit WiFi KEY.
			Ein + 1x blinken	1x35: Erfolgreich verbunden. Langsame Verbindung (GPRS).
			Ein	1x35: Erfolgreich verbunden. Schnelle Verbindung.
				1x45: WiFi erfolgreich verbunden.
	CONNECT	Grün	Lange Pause + 2x blinken	Das Remote Management ist über Input 1 oder die SiteManager-Benutzeroberfläche deaktiviert.
			Ein	LinkManager verbunden.
	POWER	Grün	Ein	Mit Strom versorgt.

Information:

Es ist zu beachten, dass es einige Zeit dauern kann, bis die Status-LED einen neuen Zustand wiedergibt. Beispielsweise kann es, je nach Einstellung des Keep-Alive Intervalls am GateManager, bis zu 4 Minuten dauern bis die Trennung eines GateManagers angezeigt wird.

3.2.6 Bedien- und Anschlusselemente

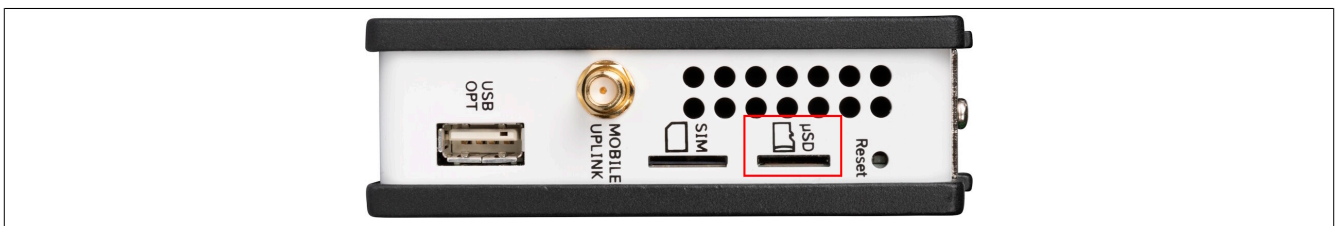
3.2.6.1 Reset-Taster



Der SiteManager verfügt auf der Oberseite über einen Reset-Taster, mit dem auch die Werkseinstellungen wiederhergestellt werden können.

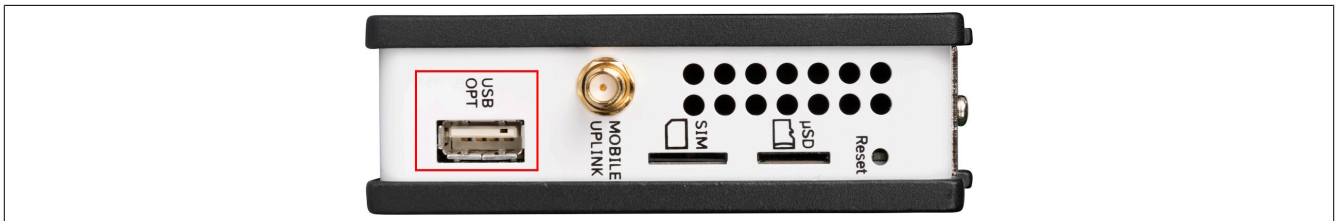
- Wird der Reset-Taster betätigt, so wird der SiteManager neu gestartet.
- Wird der Reset-Taster länger als 5 Sekunden betätigt, so wird der SiteManager nicht nur neu gestartet, sondern auch noch auf die Werkseinstellungen zurückgesetzt.

3.2.6.2 SD-Karten Steckplatz



Der SiteManager verfügt auf der Oberseite über einen Micro-SD-Steckplatz. Es ist dadurch möglich, den internen Speicher des SiteManagers mittels SD-Speicherkarte zu erweitern. Diese Speichererweiterung ist jedoch nur für das DCM (Data Collection Module) nutzbar.

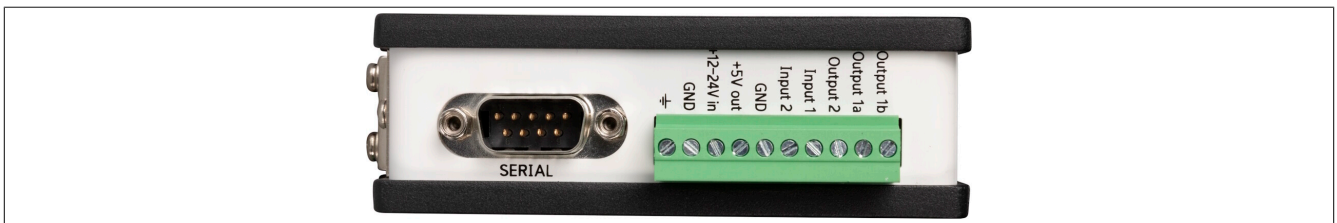
3.2.6.3 USB-Schnittstelle



Der SiteManager verfügt auf der Oberseite über eine USB-Schnittstelle. Diese kann z. B. für folgende Möglichkeiten benutzt werden:

- Für Initial Setup (siehe ["Verwendung eines USB-Speichersticks" auf Seite 33](#))
- Verwendung als Speichermedium (max. 2 GB)
- Verwendung für USB WiFi Adapter (siehe [WiFi USB Adapter with SMA Initial Contact](#))

3.2.6.4 Serielle Schnittstelle



Der SiteManager verfügt auf der Unterseite über eine serielle Schnittstelle. Die serielle Schnittstelle bietet die Möglichkeit sich mit Geräten zu verbinden, die noch über keine Ethernet-Schnittstelle verfügen (z. B. alte Steuerungen in Bestandsanlagen).

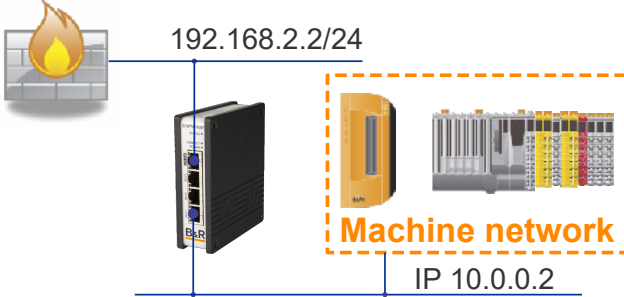
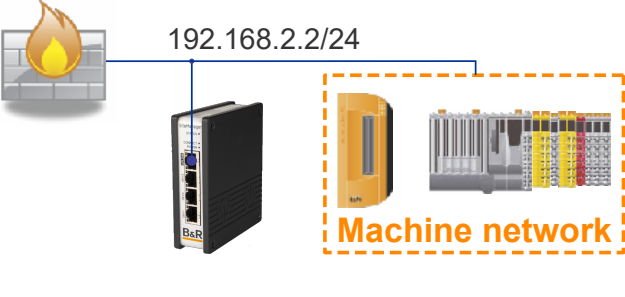
3.2.6.5 Ethernet-Schnittstellen (DEV1/2/3 und UPLINK1)

Der SiteManager verfügt auf der Frontseite über Ethernet-Schnittstellen. Es ist ein Standard-Ethernet-Patchkabel (gerade oder gekreuzt) zu verwenden, um die UPLINK1-Schnittstelle mit einem Switch in einem Netzwerk zu verbinden, der über Internetzugang verfügt.

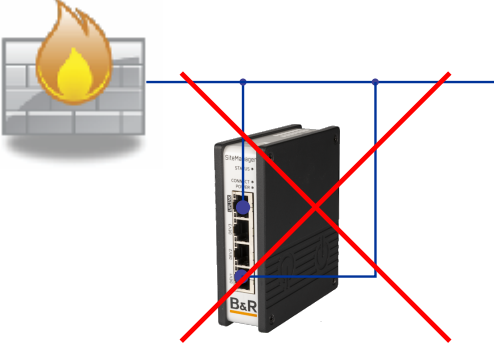
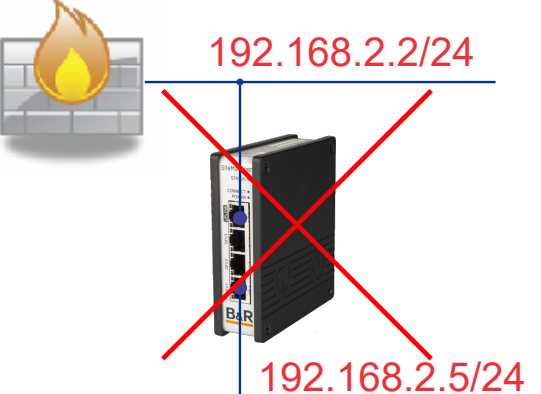
Defaulteinstellungen

DEV1 bis DEV3 sind als Switch konfiguriert, wobei die Einstellungen der DEV1-Schnittstelle für DEV2 und DEV3 übernommen werden. DEV2 und DEV3 können auch separiert werden, dazu müssen die Einstellungen direkt am SiteManager über die Benutzeroberfläche vorgenommen werden. Dies erfordert jedoch zusätzliches Expertenwissen im Gebiet Netzwerktechnik. Eine Verwendung dieses Features ist daher nur in Ausnahmefällen zu empfehlen.

Siehe folgende mögliche Verkabelungen und Konfigurationen:

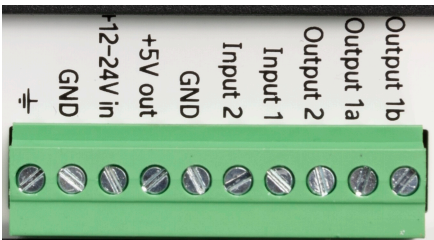
	
<p>Die DEVx-Schnittstelle kann an ein existierendes Netz, dass getrennt vom UPLINK1-Netzwerk ist, angeschlossen werden, oder es kann ein separates Gerätenetzwerk isoliert vom UPLINK1-Netzwerk erstellt werden.</p>	<p>Es kann aber auch nur die UPLINK1-Schnittstelle verbunden werden und nur Geräte auf der Uplink-Seite zugänglich gemacht werden.</p>

Im Folgenden sind einige verbotene Verkabelungs- und Konfigurationsszenarien angeführt.

	
<p>DEVx- und UPLINK1-Schnittstelle nicht mit demselben physischen Netzwerk verbinden.</p>	<p>Die DEVx-Adresse nicht im gleichen logischen Netzwerk zuweisen wie UPLINK1.</p>

3.2.6.6 Spannungsversorgung

Der SiteManager verfügt auf der Unterseite über Anschlüsse. Die Spannungsversorgung darf nur an den Anschlüssen **GND** und **+12 bis 24 V** in angelegt werden!

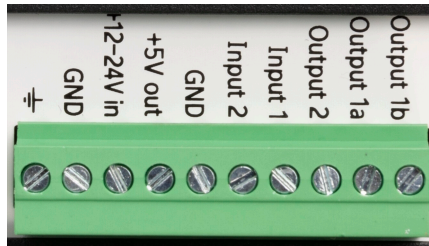
	
--	--

Information:

Es wird empfohlen, die Erdung zu verbinden, um Störgeräusche zu reduzieren.

3.2.6.7 I/O-Schnittstellen

Der SiteManager verfügt auf der Unterseite über Anschlüsse.



Digitaleingänge (Input 1, Input 2):

Die Digitaleingänge sind bei 2,34 V oder höher im Zustand "AUS" (inaktiv) und bei 0,16 V oder darunter im Zustand "EIN". Das Verhalten für Eingangsspannungen zwischen 0,16 V und 2,34 V ist undefiniert. Es gibt einen internen 10 k Ω Pullup-Widerstand auf 3,3 V, so dass ein nicht verbundener Eingang im "AUS" -Zustand ist.

Input 1 ist standardmäßig vorgesehen den GateManager-Zugriff umzuschalten. Durch Anschließen eines einfachen Ein-/Aus-Schalters lässt sich somit steuern, wann Fernwartung erlaubt werden soll.

Der konfigurierbare **Input 2** kann für benutzerdefinierte E-Mail / SMS-Alarmauslösung eingesetzt werden.

Relaisausgang (Output 1a und Output 1b):

Output 1 ist ein "Dual-Pin"-Anschluss, bei dem beide Pins im Zustand "AUS" isoliert sind und bei Zustand "EIN" kurzgeschlossen werden. Der maximale Sinkstrom beträgt 0,5 A. Die maximale Spannung beträgt 24 V.

Der Ausgang ist standardmäßig so konfiguriert, dass er aktiv ist, wenn ein LinkManager verbunden ist und kann verwendet werden, um eine Lampe einzuschalten, die die Benutzer darüber informiert, dass das Gerät bedient wird.

Digitalausgang (Output 2)

Output 2 ist ein "Einzel-Pin"-Anschluss, der im Zustand "EIN" auf GND gezogen wird und im Zustand "AUS" hochohmig ist. Der Anschluss ist von der Art "Open Drain", das bedeutet es wird (wie bei einem Schalter) keine Spannung am Anschluss selbst ausgegeben, sondern muss entweder von einer externen Quelle (max. 24 V) oder von Anschluss **+5 V out** versorgt werden. Im Zustand "AUS" (inaktiv) beträgt die Impedanz min. 24 M Ω . Im Zustand "EIN" ist die Impedanz max. 0,5 Ω . Der maximale Sinkstrom beträgt 0,2 A.

3.2.6.7.1 Beschaltung der Eingänge/Ausgänge

Für eine generelle Beschreibung wie die Eingänge und Ausgänge des SiteManagers betrieben werden können, siehe [SiteManager xx29, xx39 and xx49 - Working with I/O Ports](#), beziehungsweise die auf dem SiteManager installierte Onlinehilfe (über den Menüeintrag **HELP**).

Achtung!

Um einen fehlerlosen Betrieb sicherzustellen wird eine Relaisbeschaltung der Eingänge und Ausgänge dringend empfohlen. Für die einzelnen I/Os gilt:

- Output 1: potenzialfrei
- Output 2: B&R Eingangsmodul (Sink) (z. B. X20DI2372)
- Input 1: B&R Relaismodule (z. B. X20DO4649)
- Input 2: B&R Relaismodule (z. B. X20DO4649)

Achtung!

Keine Spannungen (z. B. 24 V) direkt an einen SiteManager Output-Anschluss anlegen. Der Ausgang kann dadurch dauerhaft beschädigt werden.

Information:

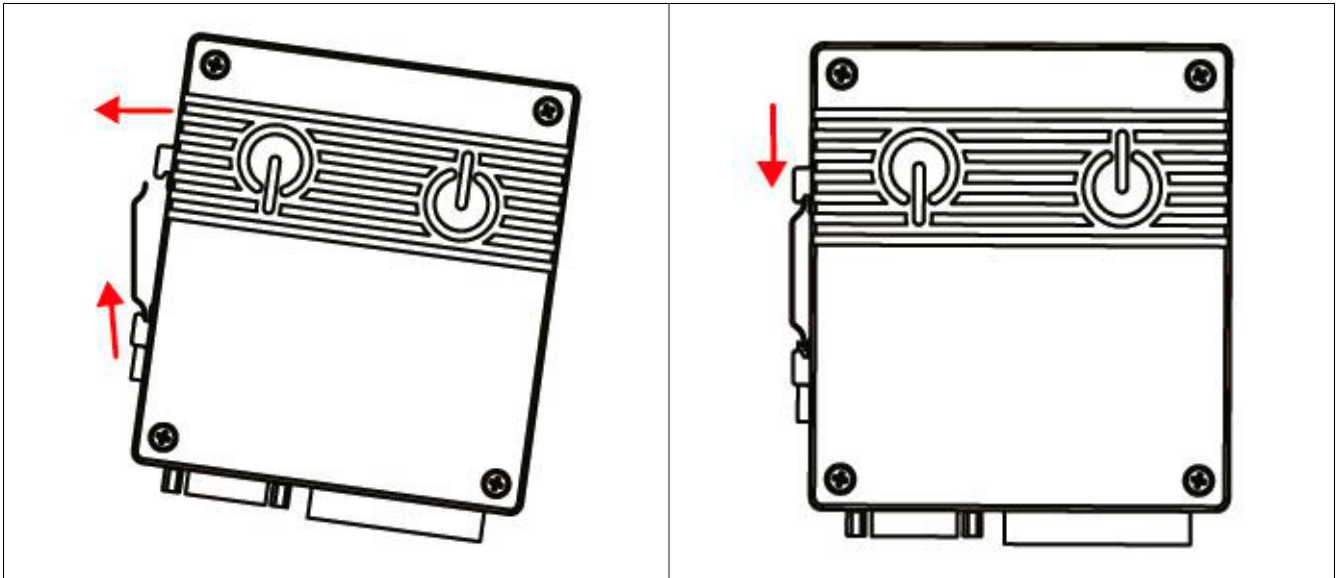
Der SiteManager verfügt zusätzlich zur Versorgung noch über einen GND und einen permanenten 5 V Ausgang. Es wird empfohlen diese für die Anschaltung der Eingänge und Ausgänge des SiteManager zu verwenden.

3.2.7 Montage

Zur Befestigung eines SiteManager ist eine Hutschiene erforderlich, die der Norm EN 60715 (TH35-7.5) entsprechen muss.

Für eine optimale Kühlung und Luftzirkulation muss oberhalb der Module ein mindestens 35 mm hoher freier Raum sein. Links und rechts ist ein Freiraum von 10 mm einzuhalten. Unterhalb der Module ist für die Kabelführung der Ein- und Ausgänge und der Versorgung ein Raum von 35 mm vorzusehen.

Hutschiene-Montage



- | | | | |
|----------|--|----------|---|
| 1 | Den SiteManager von unten nach oben drücken, um Druck auf die Federverriegelung auszuüben, und in derselben Bewegung den SiteManager nach innen und über die Oberseite der Hutschiene drücken. | 2 | Den SiteManager loslassen und sicher stellen, dass er fest sitzt. |
|----------|--|----------|---|

Information:

Bei Einbau des SiteManagers im Schaltschrank und Verwendung einer Antenne wird die Montage der Antenne außerhalb des Schaltschranks empfohlen!

Bedingungen für UL-konforme Montage

Für eine UL-konforme Montage, müssen folgende Punkte beachtet werden:

- Der SiteManager muss von einer SELV/PELV Quelle versorgt werden. Des Weiteren ist eine Sicherung nach UL CCN JDYX2/8 max. 3A zu verwenden.
- Eine Antenne ist außerhalb des Schaltschranks zu montieren. Für die Verdrahtung sind geeignete Kabeldurchführungen zu verwenden.

Information:

Um den UL-Sicherheitszertifizierungen für dieses Produkt zu entsprechen, muss der SiteManager an einem Standort mit eingeschränktem Zugang (Restricted Access Location) montiert werden.

3.2.8 Initialkonfiguration durch Steuerung

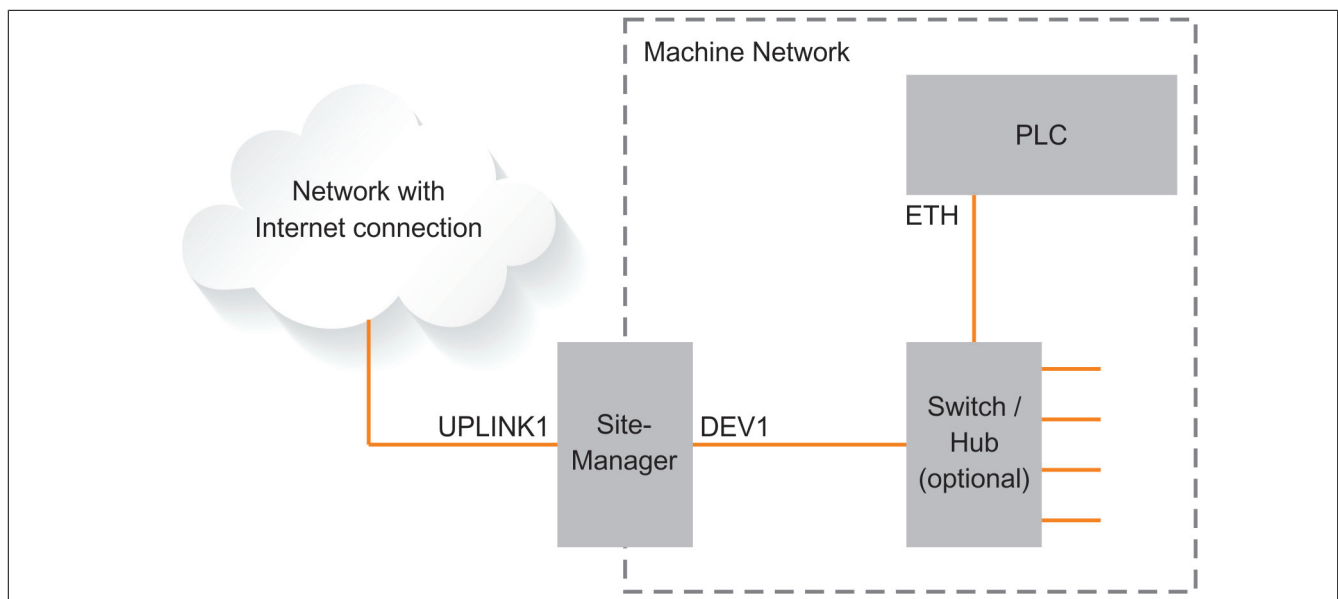
Im nicht konfigurierten Zustand (Werkseinstellungen) wird der SiteManager von der Steuerung konfiguriert. Dazu muss der SiteManager im Automation Studio Projekt an der gewünschten Ethernet-Schnittstelle der Steuerung eingefügt werden. Im Austauschfall können dadurch die wichtigsten Einstellungen wiederhergestellt werden, so dass der SiteManager die Fernwartungsverbindung aufbauen kann.

Die Initialkonfiguration durch die Steuerung ist auch nötig, damit das Register "ModuleOK" der I/O Zuordnung seine Funktion aufnehmen kann.

Damit der SiteManager von der Steuerung automatisch konfiguriert werden kann, muss die DEV1-Schnittstelle an eine Ethernet-Schnittstelle der Steuerung angeschlossen werden. Dabei darf sich kein geroutetes Netzwerk dazwischen befinden. Es ist nur ein Ethernet Switch oder ein Hub möglich.

An einer Schnittstelle der Steuerung und im gesamten Layer 2 Netzwerk darf eine SiteManager-ModuleID nur einmal verwendet werden. Um mehrere SiteManager zu verwenden, müssen diese unterschiedliche ModuleIDs besitzen.

Netzwerkdiagramm



3.2.8.1 Ethernet Konfiguration

Schnittstelle der Steuerung

Die Netzwerkschnittstelle der Steuerung muss mit einer privaten IPv4-Adresse konfiguriert werden.

- 10.x.x.x
- 172.16.x.x
- 192.168.x.x

Wird eine ungültige IP-Adresse verwendet, so kann die automatische Konfiguration aus Sicherheitsgründen vom SiteManager nicht durchgeführt werden.

DEVx-Schnittstelle des SiteManagers

Die DEVx-Schnittstelle muss sich im selben Subnetz wie die Schnittstelle der Steuerung befinden, andernfalls müssen statische Routen gesetzt werden.

3.2.9 SiteManager_1315-1335-1345 - Erstmalige Einrichtung

3.2.9.1 UPLINK Einstellungen für Internetzugang tätigen

Der SiteManager muss über eine UPLINK-Schnittstelle auf das Internet zugreifen können, um auf einen GateManager-Server zuzugreifen. Standardmäßig empfängt es seine IP-Adresse per DHCP, und es müssen nur die Uplink-Einstellungen manuell konfiguriert werden, wenn eine feste IP an der Ethernet-Schnittstelle (UPLINK1) verwendet wird oder ein USB-Breitbandmodem als UPLINK2 eingesetzt werden soll.

Es stehen folgenden 5 Methoden zur Verfügung:

3.2.9.1.1 Verwendung von Automation Studio

- a) Für Einzelheiten siehe "Secure Remote Maintenance" in ["Automation Studio" auf Seite 36](#).

3.2.9.1.2 Verwendung des Appliance Launcher

- a) [Appliance Launcher](#) von der B&R-Webseite herunterladen und installieren.
- b) Die DEV1- oder UPLINK1-Schnittstelle des SiteManagers mit dem lokalen Netzwerk verbinden und einschalten. Der SiteManager muss sich auf demselben Subnetz wie der PC befinden. Alternativ kann der SiteManager mit einem Ethernet-Kabel direkt an den PC angeschlossen werden.
- c) SiteManager einschalten und ca. 1 Minute warten, damit er betriebsbereit wird.
- d) Nach dem Start des Appliance Launchers sollte der SiteManager auf dem ersten Bildschirm aufgelistet sein. Wenn er nicht sofort erscheint, die Schaltfläche Suchen ein paar Mal drücken. (Es ist zu beachten, dass der Appliance Launcher den SiteManager nur anzeigt, wenn der PC eine echte private IP-Adresse hat (10.x.x.x, 172.16-31.x.x, 192.168.x.x oder 169.254.x.x))
- e) Dem Assistenten folgen und die UPLINK1-Adresse einstellen, wenn eine feste IP-Adresse verwenden werden soll, oder zum Menü UPLINK2 gehen, um den SSID/WiFi-Schlüssel für ein integriertes oder optionales USB-WiFi-Modul einzustellen oder einen PIN-Code für ein integriertes oder optionales Breitbandmodem festzulegen.
- f) Für weitere Informationen zu den GateManager-Einstellungen siehe ["Einstellungen für GateManager-Server-Verbindung" auf Seite 33](#).

3.2.9.1.3 Verwenden der Standard IP-Adresse (10.0.0.1)

- a) Die DEV1-Schnittstelle des SiteManagers über ein Standard-Ethernet-Kabel mit der Ethernet-Schnittstelle des PCs verbinden.
- b) Den Ethernet-Adapter des PCs auf 10.0.0.2, Subnetzmaske 255.255.255.0 konfigurieren.
- c) SiteManager einschalten und ca. 1 Minute warten, damit er betriebsbereit wird.
- d) Folgendes in den Webbrowser eingeben: `https://10.0.0.1`
- e) Sich mit dem Benutzer **admin** und der MAC-Adresse des SiteManagers als Passwort anmelden (auf dem Etikett aufgedruckt).
- f) Das Menü **System > UPLINK1** aufrufen, um die UPLINK1-Adresse einzustellen, wenn eine feste IP-Adresse verwenden werden soll, oder das Menü **UPLINK2** aufrufen, um den SSID/WiFi-Schlüssel für ein integriertes oder optionales USB-WiFi-Modul oder einen PIN-Code für ein integriertes oder optionales Breitbandmodem einzustellen.
- g) Für weitere Informationen zu den GateManager-Einstellungen siehe ["Einstellungen für GateManager-Server-Verbindung" auf Seite 33](#).

3.2.9.1.4 Verwenden eines DHCP-Servers

- a) Die UPLINK-Schnittstelle des SiteManagers mit dem lokalen Netzwerk verbinden und einschalten.
- b) Nach ca. 1 Minute sollte der SiteManager eine IP-Adresse vom DHCP-Server erhalten haben.
- c) Die Lease-Liste des DHCP-Servers überprüfen, um die IP-Adresse zu erfahren.
- d) Die IP-Adresse in Ihrem Webbrowser mit vorhergehendem `https://` eingeben (z. B. `https://192.168.41.13`).
- e) Sich mit dem Benutzer **admin** und der MAC-Adresse des SiteManagers als Passwort anmelden (auf dem Etikett aufgedruckt).
- f) Das Menü **System > UPLINK1** aufrufen, um die UPLINK1-Adresse einzustellen, wenn eine feste IP-Adresse verwendet werden soll, oder das Menü **UPLINK2** aufrufen, um den SSID/WiFi-Schlüssel für ein integriertes oder optionales USB-WiFi-Modul oder einen PIN-Code für ein integriertes oder optionales Breitbandmodem einzustellen.
- g) Für weitere Informationen zu den GateManager-Einstellungen siehe "[Einstellungen für GateManager-Server-Verbindung](#)" auf Seite 33.

3.2.9.1.5 Verwendung eines USB-Speichersticks

- a) Mit dem Admin-Konto in das GateManager Portal einloggen und die Domäne, mit der sich der SiteManager verbinden soll, suchen.
- b) Auf das Symbol "USB-Konfiguration" klicken und den **UPLINK1**- oder **UPLINK2**-Port einstellen. Wenn der SiteManager mit einem lokalen Intranet mit einem DHCP-Server verbunden ist, muss nichts konfiguriert werden.
- c) Auf "Erstellen" klicken, um die Konfigurationsdatei lokal auf dem PC zu speichern.
- d) Die Konfigurationsdatei auf einen mit fat32 formatierten USB-Speicherstick kopieren.
- e) Den SiteManager einschalten und warten, bis der SiteManager bereit ist (Status blinkt nicht mehr)
- f) Den Speicherstick einstecken und warten, bis der SiteManager automatisch neu gebootet hat. Wenn der SiteManager Zugriff auf den GateManager hat, sollte die Status-LED grün leuchten.
- g) Den Speicherstick entfernen. Es ist keine weitere Konfiguration erforderlich.

3.2.9.2 Einstellungen für GateManager-Server-Verbindung

- 1) In der SiteManager Web-Benutzeroberfläche in das Menü **GateManager > General** gehen (wenn der Appliance Launcher verwendet wird, dem Assistenten zur GateManager Parameterseite folgen).
- 2) Die **IP-Adresse** des **GateManager**-Servers eingeben, mit dem sich der SiteManager verbinden soll, und ein **Domain Token** für die Domain, in der der SiteManager erscheinen soll. Diese Informationen soll vom Administrator zur Verfügung gestellt werden oder von der Stelle, von der der SiteManager erhalten wurde. Diese Informationen sind auch im unteren Abschnitt der vom GateManager gesendeten Konto-E-Mails aufgeführt.
- 3) Die Status-LED leuchtet konstant grün, was bedeutet, dass der SiteManager mit dem GateManager verbunden ist.
- 4) Sobald der SiteManager mit dem GateManager verbunden ist, kann das GateManager Admin- oder Link-Manager Client-Konto verwendet werden, um Fernzugriff auf die SiteManager Web-Benutzeroberfläche zu erhalten, um zusätzliche Konfigurationen durchzuführen (DEV-Schnittstellen, Agenten etc.)
- 5) Detaillierte Anleitungen, neue Firmware usw. können von <http://www.br-automation.com/sitemanager> heruntergeladen werden.

3.2.9.3 Internetzugang mit integriertem Breitband

Information:

Dieser Abschnitt ist nur für die Variante 1x35 gültig.

Die Breitbandmodemverbindung wird als UPLINK2 bezeichnet. Der SiteManager versucht standardmäßig immer, die Ethernet-Verbindung (UPLINK1) zu verwenden. UPLINK2 wird nur dann verwendet, wenn die Internetverbindung auf UPLINK1 verloren geht. Sobald eine Verbindung zu UPLINK2 hergestellt ist, erfolgt eine Umschaltung nach UPLINK1 erst beim nächsten Neustart oder wenn die Internetverbindung auf UPLINK2 verloren geht.

Wenn das Modem einen SIM-PIN-Code verwendet, sollte der PIN-Code in das Menü **System > UPLINK2** des SiteManagers eingegeben werden. Der SiteManager erkennt automatisch den APN (Access Point Name) aus einer internen Tabelle. Diese kann aber auch manuell über das Menü **UPLINK2** eingegeben werden.

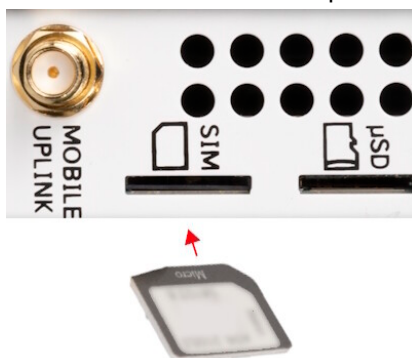
Wenn die verwendete SIM-Karte keinen PIN-Code hat, ist im SiteManager keine weitere Konfiguration von UPLINK2 nötig. (Der PIN-Code kann von einer SIM-Karte entfernt werden, indem diese in ein Standard-Mobiltelefon eingesetzt und die "SIM-Karte entfernen"-Funktion des Telefons benutzt wird).

Um den Datenverkehr zu reduzieren, lässt sich UPLINK2 so konfigurieren, dass die Mobilfunk-Verbindung bei Nichtverwendung in den Ruhemodus wechselt. Die Verbindung wird wiederhergestellt, wenn eine SMS an die Telefonnummer auf der SIM-Karte gesendet wird.

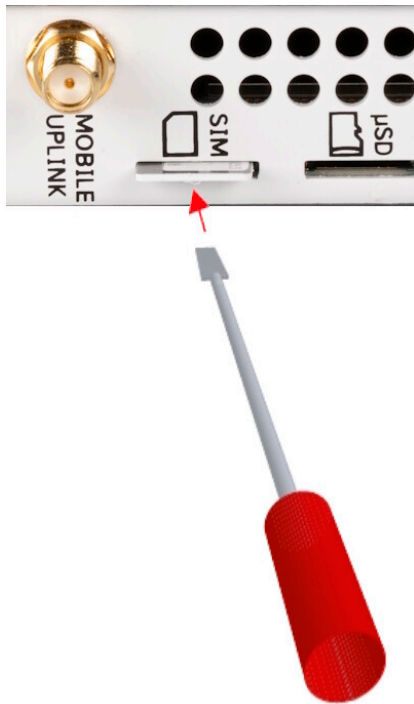
SIM-Karte einsetzen

Es wird eine Micro-SIM-Karte 3DD (12 x 15 mm) benötigt. Die SIM-Karte wie folgt einsetzen:

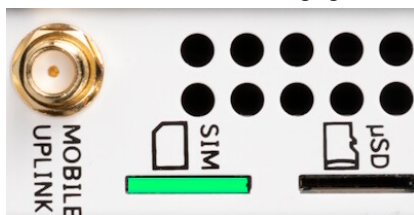
- Die SIM-Karte in den Steckplatz schieben.



- Ein schmales Objekt verwenden, wie z. B. einen Schraubendreher, um die SIM-Karte weiter in den Steckplatz (ca. 2 mm) zu drücken, bis das Klicken der Federverriegelung zu hören ist.



- Die SIM-Karte ist ordnungsgemäß eingelegt, wenn sie eben mit dem SiteManager-Gehäuse abschließt.



3.2.9.4 Internetzugang mit integriertem WiFi-Modul

Information:

Dieser Abschnitt ist nur für die Variante 1x45 gültig.

Der SiteManager kann über das integrierte WiFi-Modul eine Verbindung zu einem WiFi-Zugangspunkt herstellen. Die Verbindung wird als **UPLINK2** bezeichnet.

Beim Aktivieren des WiFi-Clients wird der SiteManager standardmäßig versuchen sich mit "sitemanager" als SSID und der MAC-Adresse des SiteManagers als WiFi KEY zu verbinden.

SSID und WiFi KEY können im Menü **System > UPLINK2** konfiguriert werden.

3.2.10 Automation Studio

Information:

Die verschiedenen Varianten des SiteManager verfügen in "Automation Studio" über eindeutige fixe Gerätekennungen. Pro CPU-Modul darf daher nur ein SiteManager je SiteManager-Variante konfiguriert werden.

Information:

Zur Anbindung und Konfiguration von Modulen aus dem B&R-Produktbereich "Sicherheitstechnik" über die B&R Fernwartungslösung Secure Remote Maintenance sind standardmäßig die beiden Ports 50000 und 51000 freigegeben. Über diese Ports können Daten von Automation Studio an Safety-Module gesendet (z. B. Konfiguration) und von diesen Empfangen werden (z. B. Statusinformation).

In Automation Studio ist es möglich die Portnummer eines Safety-Moduls frei zu vergeben. Wird eine Portnummer gesetzt, die nicht standardmäßig im SiteManager von Secure Remote Maintenance freigegeben ist (50000 oder 51000), so müssen diese Ports im SiteManager auch freigegeben werden. Dazu muss über die SiteManager-Benutzeroberfläche ein neuer B&R-Agent (unter Agents) angelegt werden, der eine Port-Erweiterung mit der im Safety-Modul gesetzten Portnummer enthalten muss.

3.2.10.1 Funktionsmodell "Standard"

I/O-Zuordnung Registerübersicht

Register	Name	Beschreibung	Datentyp	Lesen		Schreiben	
				Zyklisch	Azyklisch	Zyklisch	Azyklisch
0	ModuleOK	Modul Status (1 = Modul gesteckt)	BOOL	•			
4	SerialNumber	Seriennummer	UDINT	•			
10	ModuleID	Modulkennung	UINT	•			
16	ConfigurationMismatch	Parameter der Hauptkonfiguration geändert	BOOL	•			
0	RefreshCnt01	Abfragezähler	UINT	•			
4	RemoteManagement01	Aktueller Wert von Remote Management	USINT	•			
5	ConnectionStatus01	Aktueller Verbindungsstatus	USINT	•			
8	StatusUPLINK1	Status der UPLINK1-Schnittstelle	USINT	•			
9	StatusUPLINK2	Status der UPLINK2-Schnittstelle	USINT	•			
10	StatusUPLINK3	Status der UPLINK3-Schnittstelle	USINT	•			
11	StatusUPLINK4	Status der UPLINK4-Schnittstelle	USINT	•			
12	StatusDEV1	Status der DEV1-Schnittstelle	USINT	•			
13	StatusDEV2	Status der DEV2-Schnittstelle	USINT	•			
14	StatusDEV3	Status der DEV3-Schnittstelle	USINT	•			
15	StatusDEV4	Status der DEV4-Schnittstelle	USINT	•			
16	RemoteManagementControlFlags01	Statusbits der Remote Management Steuerung	USINT	•			
0	RemoteManagementControl01	Steuern des Fernzugriffes (überschreibt Remote-Management01)	USINT			•	
1	RemoteManagementControlEnable01	Remote Management Steuerung einschalten	BOOL			•	

Automation Studio Hauptkonfiguration

Die Hauptkonfiguration umfasst alle Einstellungen, die für den Verbindungsaufbau vom SiteManager zum Gate-Manager notwendig sind. Die Übertragung auf den SiteManager ist initial einmal möglich (siehe "[Initialkonfiguration durch Steuerung](#)" auf Seite 31). Durch Drücken des Reset-Tasters für mehr als 5 Sekunden wird ein erneutes Übertragen der SiteManager Konfiguration ausgelöst.

Folgende Tabelle zeigt die Parameter der über Automation Studio zugänglichen Hauptkonfiguration:

Parameter	Beschreibung
DEV1-Schnittstelle ¹⁾	
IP-Adresse	IP-Adresse der DEV1-Schnittstelle am SiteManager
Netzmaske	Subnetzmaske des DEV1-Netzwerks am SiteManager
UPLINK1-Schnittstelle	
Modus	Modus UPLINK1-Schnittstelle: DHCP oder Static (aktiviert die folgenden 4 Einträge)
IP-Adresse	IP-Adresse der UPLINK1-Schnittstelle am SiteManager (Modus = Static)
Netzmaske	Subnetzmaske des DEV1-Netzwerks am SiteManager (Modus = Static)
Standard Gateway	Default Gateway (Modus = Static)
DNS-Server	DNS-Server Adresse, wenn Hostname für GateManager oder Proxy verwendet wird (Modus = Static)
UPLINK2-Schnittstelle (nur bei Gerätevarianten 1x35 und 1x45)	
Integriertes Modem (1x35) WiFi Modul (1x45)	UPLINK2-Schnittstelle aus- oder einschalten (aktiviert je nach Variante 2 der folgenden Einträge)
APN (1x35)	Access Point Name (UPLINK2 = Mobilfunk)
SIM PIN-Code (1x35)	SIM PIN-Code (UPLINK2 = Mobilfunk)
SSID (1x45)	WLAN-Netzwerk Name (UPLINK2 = WiFi)
WiFi KEY (1x45)	WiFi KEY (UPLINK2 = WiFi) Aus Sicherheitsgründen sind WLAN-Netzwerke mit einem Passwort zu versehen. Es muss ein ASCII-String mit einer Zeichenlänge von mindestens 8 bis maximal 63 Zeichen eingegeben werden.
GateManager Einstellungen	
Remote Management ²⁾	<p>GateManager Zugriff. Steuert Verbindungsaufbau zwischen SiteManager und GateManager. Die folgenden Optionen können dabei gewählt werden (siehe auch "RemoteManagement01" auf Seite 38):</p> <ul style="list-style-type: none"> • Disabled: Keine Verbindung zum GateManager. Unterbinden aller Fernüberwachung und -management Möglichkeiten (ähnlich dem Ausschalten dieses SiteManager). • Heartbeat only: Verbindung mit dem GateManager herstellen, aber nur um regelmäßige Statusinformationen zu liefern und optional eine Verbindung mit dem SiteManager selbst bereitstellen (wenn die "Go To Appliance" Einstellungen es erlauben). • Enabled: Verbindung mit dem GateManager herstellen, sowie Remote-Zugriff auf den SiteManager (wenn die "Go To Appliance" Einstellungen es erlauben) und angeschlossenen Geräten • Heartbeat and relays only: Verbindung mit dem GateManager mit statischen Gerät und aktivierten Server-Relais herstellen, aber nur um regelmäßige Statusinformationen zu liefern und optional eine Verbindung mit dem SiteManager selbst bereitstellen (wenn die Go To Appliance Einstellungen es erlauben).
Go To Appliance ²⁾	<p>Anzeige der Verbindungsoptionen für den Zugriff auf die Benutzeroberfläche des SiteManagers Diese Option gibt an, ob und wie ein GateManager Administrator oder LinkManager Benutzer die "Go To Appliance" Funktion verwenden kann um sich auf die Benutzeroberfläche des SiteManager zu verbinden (dies kann nicht über Appliance Launcher eingestellt werden):</p> <ul style="list-style-type: none"> • Disabled: Der Zugang zu "Go To Appliance" ist gesperrt. • Manual Login: Bei Verwendung von "Go To Appliance", müssen die normale Login-Daten (Benutzer und Kennwort) des SiteManager angegeben werden, um sich am SiteManager anmelden. • Automatic Login: Bei Verwendung von "Go To Appliance" im GateManager Portal oder in der LinkManager Konsolen-Domain-Ansicht, kann das von GateManager erzeugte dynamische Passwort verwendet werden. Wenn die GateManager-Konsole für die automatische Anmeldung konfiguriert ist, werden die Login-Daten automatisch dem SiteManager dargelegt. Wenn die GateManager-Konsole für die manuelle Anmeldung konfiguriert ist, wird der Login-Dialog angezeigt. • Manual, not LinkManager: Wie manueller Login, aber "Go To Appliance" von LinkManager Konsolen-Domain-Ansicht ist nicht möglich. • Automatic, not LinkManager: Wie automatischer Login, aber "Go To Appliance" von LinkManager Konsolen-Domain-Ansicht ist nicht möglich.
Appliance Name	<p>Name des Geräts am GateManager Server mit maximal 127 Zeichen. Dieser wird vom GateManager Administrator verwendet, um den jeweiligen SiteManager zu identifizieren. Der Wert dieses Feldes entspricht dem %N Feldcode aus den Gerätenamen-Format-Spezifikationen. Mit dem Standard-Gerätenamen-Format wird auch, falls dieses Feld leer ist, der Device Name verwendet, oder falls dieser auch leer ist, die SiteManager-Seriennummer verwendet.</p>
Domain Token	<p>Domain am GateManager Server mit maximal 127 Zeichen (inkl. Punkte und Leerzeichen) Der Domain Token wird nur für das Herstellen der ersten Verbindung verwendet. Wenn ein Multiple-Domain Account verwendet wird und ein vollständiger Domain-Token benötigt 48 oder mehr Zeichen, so ist eine höhere Token-Ebene (z. B. TOPLEVEL.INTERNATIONAL.AUSTRIA.EGELSBERG) zu verwenden.</p>
GateManager Adresse	<p>Adresse des GateManager Servers (IP-Adresse oder DNS-Hostname) Wenn es für den Zugriff auf den gleichen GateManager Server eine alternative IP-Adresse gibt, so sind hier beide Adressen durch ein Leerzeichen getrennt anzugeben. Wird der Appliance Launcher verwendet, um den GateManager zu konfigurieren, so ist die Schaltfläche DNS zu betätigen, damit anschließend die beiden IP-Adressen durch ein Leerzeichen getrennt eingegeben werden können.</p>
Proxy Einstellungen	
Proxy	Proxy-Einstellungen aus oder einschalten (aktiviert die folgenden 3 Einträge)
Web-proxy Adresse	<p>Proxy Adresse für GateManager Verbindung (IP-Adresse oder Hostname) Es ist die IP-Adresse (und optional durch Doppelpunkt getrennt die Portnummer) des Web-Proxy, über die der SiteManager zum GateManager Verbindung herstellen soll. Alternativ kann hier auch ein Web-Proxy Auto-Discovery (WPAD) URL angegeben werden, von dem der SiteManager die tatsächliche Web-Proxy-Adresse erhalten kann, z. B. http://172.16.1.1:8080/wpad.dat.</p>
Web-proxy Benutzer	Proxy Benutzername
Web-proxy Passwort	Proxy Passwort

1) Die Einstellungen der DEV1 Schnittstelle werden für DEV2 und DEV3 übernommen. Für weitere Details siehe "[Defaulteinstellungen](#)" auf Seite 28

2) Diese Automation Studio Projekt Parameter werden nicht überprüft und können nachträglich mittels Web-Benutzeroberfläche am SiteManager geändert werden.

3.2.10.1.1 ModuleOK

Statusbit, ob das Modul physikalisch vorhanden und konfiguriert ist. Erkennung erfolgt über den Feldbusanschluss.

Datentyp	Werte	Information
BOOL	0	Module nicht einsatzbereit
	1	Modul vorhanden und konfiguriert

3.2.10.1.2 ModuleID

Aus diesem Register kann die Modul-Hardware-ID zur Bestimmung des Gerätetyps ausgelesen werden. Diese kann auch als "B&R ID-Code" den jeweiligen technischen Daten entnommen werden. Des Weiteren ist auf jedem Modul eine Seriennummer aufgedruckt; die Modul-Hardware-ID entspricht den ersten 4 Stellen dieser Seriennummer.

Datentyp	Werte
UINT	0 bis 65535

3.2.10.1.3 SerialNumber

Aus diesem Register kann die eindeutige Seriennummer des Moduls ausgelesen werden. Diese 7-stellige SerialNumber ist in dezimaler Form auf dem Modul-Gehäuse aufgedruckt.

Datentyp	Werte
UDINT	0 bis 4.294.967.295

Information:

Modul-Seriennummer

Die vollständige Modul-Seriennummer setzt sich aus der 4-stelligen ModuleID und der anschließenden 7-stelligen SerialNumber zusammen.

Beispiel:

- ModuleID = 0xE908
- SerialNumber = 0x0001234
- Seriennummer am Modul aufgedruckt = 0xE9080001234

3.2.10.1.4 ConfigurationMismatch

Mithilfe dieses Datenpunktes kann festgestellt werden, ob ein Parameter der Hauptkonfiguration geändert wurde.

Eine Auflistung aller überprüften Parameter bietet die Tabelle der in Automation Studio zugänglichen Hauptkonfiguration, siehe ["Automation Studio Hauptkonfiguration" auf Seite 36](#).

Datentyp	Wert	Information
BOOL	0	Konfiguration vom Automation Studio Projekt ist ident mit der Konfiguration am SiteManager.
	1	Mindestens ein Parameter der Hauptkonfiguration am Gerät wurde geändert, bzw. die Konfiguration des Automation Studio Projekts passt nicht mit der Konfiguration am Gerät zusammen.

3.2.10.1.5 RefreshCnt01

Der Abfragezähler wird nach jedem Auslesevorgang der Statusinformationen um 1 erhöht.

Datentyp	Werte
UINT	0 bis 65535

3.2.10.1.6 RemoteManagement01

Aktueller Wert der "Remote Management" Einstellung. Diese definiert den Verbindungsaufbau vom SiteManager zum GateManager.

Datentyp	Wert	Name	Information
USINT	0	Disabled	Fernwartungszugang ausgeschaltet
	1	Heartbeat only	Verbindungsprüfung zum GateManager
	2	Enabled	Fernwartungszugang eingeschaltet
	3	Heartbeat and relays only	Verbindungsprüfung und Relays aktiviert
	4 bis 255	-	Reserviert

3.2.10.1.7 ConnectionStatus01

Status der derzeitigen GateManager Verbindung:

Datentyp	Wert	Information
USINT	0	NC
	1	GateManager Verbindung OK (Heartbeat OK)
	2	Fernwartungsverbindung aktiv (Einwahl mit LinkManager)
	3 bis 255	Reserviert

3.2.10.1.8 StatusUPLINK1 bis 4

Status der jeweiligen UPLINK-Schnittstelle. Die tatsächliche Anzahl der UPLINK-Schnittstellen ist anhängig von der Gerätevariante:

Datentyp	Wert	Information
USINT	0	DOWN
	1	UP, Default Interface
	2	UP, Secondary Interface
	3 bis 254	Reserviert
	255	Nicht installiert

3.2.10.1.9 StatusDEV1 bis 4

Status der jeweiligen DEV-Schnittstelle:

Datentyp	Wert	Information
USINT	0	DOWN
	1	10 Mbps HDX
	2	10 Mbps FDX
	3	100 Mbps HDX
	4	100 Mbps FDX
	5	Reserviert
	6	1000 Mbps FDX
	7 bis 254	Reserviert
	255	Nicht installiert

3.2.10.1.10 RemoteManagementControl01

Steuert den Verbindungsaufbau vom SiteManager zum GateManager. Mit diesem Datenpunkt kann der Wert der "Remote Management"-Einstellung überschrieben werden.

Datentyp	Wert	Name	Information
USINT	0	Disabled	Fernwartungszugang ausgeschaltet
	1	Heartbeat only	Verbindungsprüfung zum GateManager
	2	Enabled	Fernwartungszugang eingeschaltet
	3	Heartbeat and relays only	Verbindungsprüfung und Relays aktiviert
	4 bis 255	-	Reserviert

3.2.10.1.11 RemoteManagementControlEnable01

Remote Management Steuerung einschalten.

Zuvor muss der gewünschte Wert im Datenpunkt [RemoteManagementControl01](#) eingestellt werden.

Datentyp	Wert	Information
BOOL	0	RemoteManagementControl ausschalten.
	1	RemoteManagementControl einschalten.

Nachdem RemoteManagementControlEnable01 wieder auf FALSE gesetzt wurde, nimmt die "Remote Management"-Einstellung wieder den ursprünglichen konfigurierten Wert an.

3.2.10.1.12 RemoteManagementControlFlags01

Statusbits der Remote Management Steuerung:

Datentyp	Bit	Name	Information
USINT	0	RemoteManagementControlAck01	Acknowledge von RemoteManagementControlEnable01
	1	RemoteManagementControlStatus01	Status der Remote Management Steuerung (0 = OK)
	2 bis 7	-	Reserviert

RemoteManagementControlAck01

Das Bit dient zur Überprüfung, ob die mit [RemoteManagementControlEnable01](#) gesetzte Aktion abgeschlossen wurde. Übernimmt RemoteManagementControlAck01 den Wert von [RemoteManagementControlEnable01](#), ist die Übertragung ausgeführt worden. Danach kann in RemoteManagementControlStatus01 abgelesen werden, ob der Vorgang erfolgreich war.

RemoteManagementControlStatus01

Das Bit ist gesetzt, wenn beim Aktivieren oder Deaktivieren der Remote Management Steuerung ein Fehler aufgetreten ist. Dies kann durch folgende Aktionen verursacht werden:

- Ungültiger Wert im Datenpunkt RemoteManagementControl01
- Netzwerkverbindung ist abgerissen

3.2.10.2 Bedienung von Funktionsmodell "Standard"

Mit dem Konfigurationsparameter "Remote Management" kann der Verbindungszustand, den der SiteManager von sich aus erlauben soll, eingestellt werden. Dieser Wert kann auch zur Laufzeit gesteuert werden.

Dazu muss zunächst der gewünschte Wert im Datenpunkt RemoteManagementControl01 eingestellt werden. Danach wird die Remote Management Steuerung durch das Setzen von RemoteManagementControlEnable01 auf TRUE aktiviert. Nachdem RemoteManagementControlAck01 auf TRUE gewechselt hat, kann mittels RemoteManagementControlStatus01 überprüft werden, ob der Vorgang erfolgreich war.

Durch Rücksetzen von RemoteManagementControlEnable01 auf FALSE nimmt "Remote Management" wieder den ursprünglichen Wert vom Konfigurationsparameter an.

3.2.11 Verbindung zum GateManager

Standardmäßig versucht ein SiteManager automatisch eine Reihe von verschiedenen Methoden und Protokollen, um sich mit einer GateManager-Adresse zu verbinden. Die bevorzugte Verbindungsmethode kann in der SiteManager-Konfiguration festgelegt werden.

Information:

Dem SiteManager muss der Zugang zum GateManager durch die Firewall des Endkunden ermöglicht werden. Der SiteManager unterstützt Proxy Server, die es ermöglichen diesen Zugang noch genauer zu regeln.

- **ACM/PXP (Port 11444 TCP):** Dies ist ein dedizierter Port für die Verbindung mit dem GateManager-Server. Die Verwendung eines dedizierten Ports wird normalerweise bevorzugt, da es den GateManager-bezogenen Verkehr von anderem ausgehenden Verkehr im Netzwerk trennt, so dass der GateManager-Verkehr im lokalen Netzwerk und in der Internetverbindung leichter verfolgt werden kann. Aber die Verwendung eines dedizierten Ports bedeutet auch, dass dieser Port wahrscheinlich in der Firmen-Firewall geöffnet werden muss, was gegen die Unternehmensrichtlinien verstoßen kann.
- **HTTPS/TLS (Anschluss 443 TCP):** Dies stellt eine Verbindung zu GateManager über das TLS-Protokoll an Port 443 her. Dies sollte durch Firewalls funktionieren, die ausgehende HTTPS-Verbindungen erlauben.
- **TLS über HTTP (Anschluss 80 TCP):** Die Verbindung zu GateManager wird über den Standard-HTTP-Port 80 hergestellt, aber sofort in eine sichere TLS-Verbindung umgewandelt. Dies kann durch eine Firewall funktionieren, die nur ausgehende HTTP-Verbindungen zulässt.
- **TLS über Web-Proxy:** Dies stellt eine Verbindung über einen spezifizierten Web-Proxy her und fordert den Web-Proxy auf, sich mit GateManager über Port 443 TCP zu verbinden. Sobald die Verbindung hergestellt ist, wird das normale TLS-Protokoll verwendet.
- **HTTP über Web-Proxy:** Die Verbindung wird über einen spezifizierten Web-Proxy hergestellt, wobei der Web-Proxy aufgefordert wird, sich mit GateManager über Port 80 TCP zu verbinden. Sobald die Verbindung hergestellt ist, wird sie auf eine sichere TLS-Verbindung umgestellt.

Zusätzliche ausgehende Verbindungen

Zusätzlich sucht der SiteManager nach 193.242.155.50-59 Port 80 und fragt, ob die GateManager-Adresse bekannt ist. Dies ist eine eingebaute Funktion des SiteManagers als Service für den Endbenutzer. Wenn z. B. ein Kunde seinen eigenen GateManager mit der öffentlichen IP xx.xx.xx.xx hat, aber sie auf xx.xx.yy.yy ändern muss. B&R kann in diesem Fall das "NATting" im GateManager-Ermittlungsdienst erstellen, das besagt, dass SiteManager, die sich mit xx.xx.xx.xx verbinden, sich mit xx.xx.yy.yy verbinden sollen.

Erstmalige Verbindung zum GateManager

Wenn der SiteManager zum ersten Mal eine Verbindung zu einem GateManager herstellt, fordert der SiteManager das "Appliance TLS X.509 Certificate" vom GateManager an. Dies ist ein eindeutiges selbstsigniertes Zertifikat. Der SiteManager initiiert einen TLS-Handshake mit dem GateManager. Nach einem erfolgreichen ersten Handshake wird der SiteManager mit dem eindeutigen "Appliance TLS X.509 Certificate" des GateManagers verbunden. Da der SiteManager nun an das eindeutige Zertifikat des GateManagers gebunden ist, ist er gegen MITM/redirect-Angriffe sicher.

3.3 LinkManager

Der LinkManager ist eine einfach zu installierende Windows-Anwendung, die auf dem PC des Servicetechnikers ausgeführt wird. Der LinkManager verbindet sich über eine 2-Faktor-Authentifizierung mit dem GateManager und ermöglicht zusammen mit den SiteManagern sicheren Zugriff auf Ferngeräte. Sobald die Verbindung hergestellt wurde, wird das Ferngerät dem Techniker vor Ort so angezeigt, als ob der Windows-PC direkt mit dem Gerät verbunden wäre. Außerdem können per FTP, Web, RDP, VNC oder Automation Studio Verbindungen mit dem Ferngerät hergestellt werden.

Des Weiteren steht mit der Variante LinkManager Mobile eine browserbasierte und reduzierte Version des LinkManagers zur Verfügung. Um LinkManager Mobile auszuführen, muss keine Software installiert werden. LinkManager Mobile läuft auf jedem Betriebssystem (Windows, iOS, Android, Mac und viele mehr). Unterstützt wird eine Verbindung per Internet-, RDP- und VNC-Protokoll.

Information:

Es sind max. 10 parallele LinkManager-Verbindungen über einen SiteManager möglich.

Information:

Bei Verbindung über VNC-Protokoll ist ein dedizierter VNC Agent zu verwenden (dedizierte Adresse und Portnummer, z. B. 192.168.0.8:5910).

3.3.1 Bestelldaten

Bestellnummer	Kurzbeschreibung
0RMLM.MOB	Secure Remote Maintenance - LinkManager Mobile Lizenz, einzelne Lizenz, kann nicht geteilt werden, Betriebssystem unabhängig
0RMLM.WIN	Secure Remote Maintenance - LinkManager Lizenz, geteilte Lizenz (floating license), Win XP/7/8/10/11 ¹⁾

Tabelle 12: 0RMLM.MOB, 0RMLM.WIN - Bestelldaten

1) Windows 11 Unterstützung ab Version ≥ 9.7.x

Information:

Download der LinkManager-Software via <http://www.br-automation.com/linkmanager>.

3.4 Starter Package

Ein Starter Package dient zum schnellen Einstieg in die Fernwartungslösung. Es enthält dabei folgende Komponenten:

- **GateManager:** 1x GateManager mit Hosting Agreement
- **SiteManager:** 1x SiteManager Modell freier Wahl oder 1x SiteManager Embedded Variante
- **LinkManager:** 1x LinkManager Lizenz und 1x LinkManager Mobile Lizenz
- **Service Agreement**

Kern eines Starter Package ist der Zugang zu einem von B&R zur Verfügung gestellten und administrierten GateManager (GateManager Hosting Service). Hierin können dann die eigenen SiteManager und LinkManager verwaltet werden.

Ein Starter Package kann nach Bedarf erweitert werden, z. B. durch Umstieg auf andere Service Levels oder Erwerb weiterer LinkManager Lizenzen und SiteManager. Der Umstieg vom GateManager Hosting Service auf einen eigenen GateManager (Hardware oder Software-Variante) ist ebenfalls jederzeit möglich.

3.4.1 Bestelldaten

Bestellnummer	Kurzbeschreibung
	SiteManager
0RMGMZSP.1315	GateManager Hosting Service – Starter Package, enthält 1x jeweiligen SiteManager, 1x LinkManager und 1x LinkManager Mobile Lizenz, Servicegebühr 0RMAS.SERVICE-01 muss separat gezahlt werden.
0RMGMZSP.1335	
0RMGMZSP.1335.4G	
0RMGMZSP.1345	
0RMGMZSP.SME.B	GateManager Hosting Service – Starter Package, enthält 1x SiteManager Embedded BASIC Lizenz, 1x LinkManager und 1x LinkManager Mobile Lizenz, Servicegebühr 0RMAS.SERVICE-01 muss separat gezahlt werden
0RMGMZSP.SME.E	GateManager Hosting Service – Starter Package, enthält 1x SiteManager Embedded EXTENDED Lizenz, 1x LinkManager und 1x LinkManager Mobile Lizenz, Servicegebühr 0RMAS.SERVICE-01 muss separat gezahlt werden

3.5 Netzwerksicherheit

Die Kommunikation zwischen den Komponenten der Fernwartungslösung basiert auf SSL-VPN mit AES-Verschlüsselung. Der LinkManager kommuniziert dabei mit dem SiteManager ausschließlich über den GateManager. LinkManager und SiteManager melden sich über eine 2 Faktor Authentifizierung beim GateManager an.

Die 2 Faktor Authentifizierung basiert auf einem X.509 Zertifikat. Jeder GateManager ist in der Lage, eindeutige TLS-Zertifikate zu erzeugen auf die sich ein SiteManager bindet. Diese Bindung wird einmalig hergestellt und kann nur vom GateManager oder vom SiteManager aufgehoben werden, was eine man-in-the-middle Attacke unmöglich macht. Alternativ kann beim LinkManager auch eine Authentifizierung über SMS verwendet werden.

Der SiteManager kann dahingehend konfiguriert werden, dass er in einem zyklischen Intervall (Standardeinstellung 10 min.) Informationen an den GateManager übermittelt (keep-alive Signal). Zusätzlich kann der Fernzugriff auch physikalisch vom Maschinenbetreiber gesteuert werden. Dies ist durch Unterbrechen der Spannungsversorgung möglich oder durch einen Schalter an dem digitalen Eingang, der die Verbindung zum GateManager unterbricht oder zulässt.

Ein wichtiger Faktor in der Netzwerksicherheit ist die integrierte Firewall im SiteManager. Die Firewall wird mit sogenannten "Device Agents", die Firewall-Regeln entsprechen, konfiguriert. Mit einem Device Agent kann definiert werden, mit welchem Protokoll und über welche Ports Zugriff auf einen Netzwerkteilnehmer erlaubt wird. Der Device Agent lässt dann den Zugriff nur auf diesen einen Netzwerkteilnehmer zu. Zusätzlich können die Device Agents auch LinkManager Benutzern zugewiesen werden. Dies ermöglicht auch auf der Benutzerebene eine genaue Zugriffskontrolle.

Die Fernwartungslösung erfüllt alle Sicherheitsstandards die durch das "National Institute of Standards and Technology" (www.nist.gov) für Verschlüsselung und Schlüsselübertragung vorgegeben wurden.

Information:

Um das Maximum an IT-Sicherheit zu erreichen, wird dringend empfohlen, immer die aktuellen GateManager, SiteManager und LinkManager Softwareversionen zu verwenden.

3.6 Portinformationen

Site- und LinkManager

Diese verbinden sich mit der öffentlichen IP-Adresse des GateManager Servers über TCP-Port 11444 (Secomea ACM /TLS), 443 (Standard HTTPS/TLS) oder 80 (Standard TLS über HTTP). Bei Verwendung eines Internet-Firewall / NAT-Router muss dieser so konfiguriert werden, dass alle eingehenden Verbindungen über eine feste, öffentliche IP-Adresse, Port 11444 (bzw. 443 oder 80), zur privaten IP-Adresse des GateManager-Servers weitergeleitet werden.

GateManager Administrator-Webportal

Dieser verbindet sich mit dem GateManager Server über TCP-Port 443.

Information:

Wenn sich das Webportal hinter einem NAT-Router befindet, darf dieser eingehende Verbindungen NICHT maskieren. Der GateManager muss immer die IP-Adresse der Originalquelle ermitteln können.

Über das Administrator-Webportal kann der Administrator auf die Web-Schnittstelle der SiteManager, LinkManager und webfähigen Geräten, die mit dem SiteManager verbunden sind, zugreifen. Diese Funktion verwendet den TCP-Portbereich 55000 bis 59999. Um diese Funktion von außerhalb benutzen zu können, muss der NAT-Router so konfiguriert sein, dass eingehende Verbindungen an die entsprechenden Ports des GateManager-Servers weitergeleitet werden.

Ports für LinkManager Mobile

Damit LinkManager Mobile funktioniert, müssen folgende ausgehende Ports geöffnet sein:

Port	Protokoll	Beschreibung
80	TCP	HTTP
443	TCP	HTTPS

Um eine externe Anwendung mit LinkManager Mobile benutzen zu können, müssen folgende ausgehende Ports geöffnet sein.

Port	Protokoll	Beschreibung
22	TCP	SSH
3389	TCP	RDP
5800	TCP	JVNC
5900	TCP	VNC

Installation des GateManagers

Bei der Installation des GateManagers werden zusätzliche Ports und Dienste verwendet. Diese sind im "GateManager 8250 Setup Guide" beschrieben und haben keine Auswirkungen auf, z. B. die Benutzer des gehosteten Dienstes.

4 Erste Schritte mit den Systemkomponenten

Die folgenden Schritte leiten durch die wichtigsten zur Verfügung gestellten weiterführenden Dokumentationen und Anwendertipps (siehe "[Weiterführende Dokumentation](#)" auf Seite 54) um GateManager, SiteManager und LinkManager für die erste Verwendung einzurichten.

GateManager

Information:

Die Schritte in diesem Abschnitt sind notwendig, wenn der GateManager nicht von B&R gehostet wird.

Für den Fall, dass der gehostete Service in Anspruch genommen wird, muss nur ein Zugang bei B&R beantragen werden, um eine E-Mail mit der GateManager Adresse und den Zugangsdaten für eine Aktivierung (Zertifikat und Passwort) zu erhalten.

1. Wird als GateManager Server die Software-Installer verwenden, dann sind die Instruktionen aus den folgenden Dokumenten zu befolgen, um die Software zu installieren:
 - [GateManager 8250 Setup Guide - Red Hat Enterprise Linux](#)
 - [GateManager 8250 Setup Guide - Debian](#)
 - [Setup Guide Postfix SMTP Relay](#)
 - [GateManager Commands](#)

Achtung!

Manche Dokumente enthalten Links bzw. Anweisungen für Software-Downloads von der Secomea-Webseite. Diese dürfen nicht verwendet werden, sondern der Download MUSS IMMER von der B&R-Webseite erfolgen.

Information:

Ein GateManager der mit den genannten Dokumenten aufgesetzt wurde, ist nun mit allen Funktionen betriebsbereit, aber vorerst nur im Test-/Demo-Modus (max. 3 SiteManager verwaltbar). Um den GateManager in vollem Umfang zu nutzen, muss er entsprechend aktiviert werden. Siehe dazu "[Aktivierung des GateManagers](#)" auf Seite 16.

2. Die Instruktionen aus dem Dokument [Getting Started GateManager PREMIUM Domain Administration](#) anwenden, um den GateManager Softwareseitig zu konfigurieren und Domains zu erstellen und zu verwalten (siehe auch "[Domains und ihren Inhalt verwalten](#)" auf Seite 47).

SiteManager

1. Die Instruktionen aus dem Beipackzettel ([SiteManager_1315-1335-1345_Initial-Setup](#) bzw. aus Abschnitt "[SiteManager_1315-1335-1345 - Erstmalige Einrichtung](#)" auf Seite 32 befolgen, um den SiteManager zu konfigurieren und die Einstellungen zu tätigen, die für die Internetanbindung sowie die Verbindung zum GateManager Server nötig sind.
Für den Appliance Launcher steht auch noch folgende Downloadmöglichkeit zur Verfügung:
[Appliance Launcher](#)
2. Wird der SiteManager mittels Automation Studio konfiguriert, siehe die dort enthaltene Automation Help zum SiteManager, bzw. auch Abschnitt "[Automation Studio](#)" auf Seite 36.

Domains und ihren Inhalt verwalten

Information:

Der GateManager ist jene Stelle, wo die LinkManager Benutzer und die SiteManager verwaltet werden.

Innerhalb der Domains lassen sich in weiterer Folge auch die Benutzer und Lizenzen verwalten.

Es müssen für GateManager Administratoren und LinkManager Benutzer separate Accounts angelegt werden.

Es können Device Agents auf einem Gerät angelegt werden. Ein Device Agent kann entweder eine SPS sein, oder ein Regelsatz. Device Agents ermöglichen somit den Zugriff auf Netzwerkteilnehmer im Gerätenetzwerk des SiteManager.

Im GateManager lässt sich mit der Schaltfläche "SiteManager GUI" die Web-Schnittstelle des gewählten SiteManagers öffnen. In der Sektion **GateManager ► Agents** können die Agents passend zu den eigenen Geräten erstellt werden.

LinkManager Mobile Benutzer

Der LinkManager Mobile ermöglicht Benutzern den Fernzugriff auf industrielle Anlagen von ihrem iPhone, iPad oder Android Gerät. Die App ist dafür bestimmt, auf grafische Benutzeroberflächen beispielsweise auf SPS-Geräten, HMI-Bedienpults oder Webcams zuzugreifen. Sie stellt auch Verbindungen zu Desktops her, auf denen Linux oder Windows läuft. Mit dem LinkManager Mobile kann man sich einfach mit dem Gerät verbinden, eine VNC starten oder einen MS Remote Desktop Client (RDP) und dann aus der Ferne das Gerät steuern.

LinkManager 7

Information:

Dieses Produkt wird nicht mehr gewartet, ebenso stehen keine neuen Security Updates mehr zur Verfügung.

Daher soll ein Versionswechsel auf LinkManager durchgeführt werden.

LinkManager 8 und höher

Information:

Damit der LinkManager verwendet werden kann, muss vom GateManager Administrator eine E-Mail mit den Zugangsdaten (LinkManager Benutzer-Zertifikat und das zugehörige Account Passwort) zugesandt werden.

1. Falls noch nicht erfolgt, den LinkManager installieren. Für den LinkManager steht auch folgende Downloadmöglichkeit zur Verfügung: <http://www.br-automation.com/linkmanager>

GateManager

Select a GateManager Service:

GateManager Portal

LinkManager

LinkManager Mobile

Remote Maintenance
LinkManager

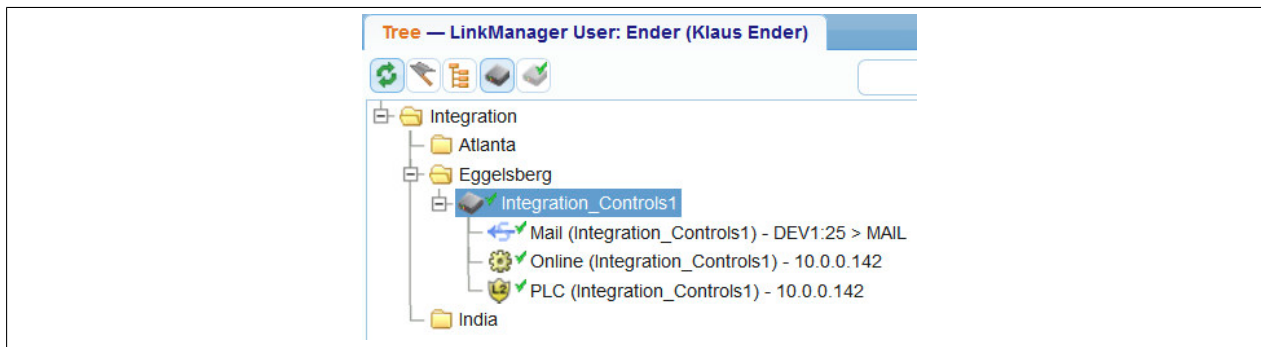
GateManager Login

☐ Certificate:

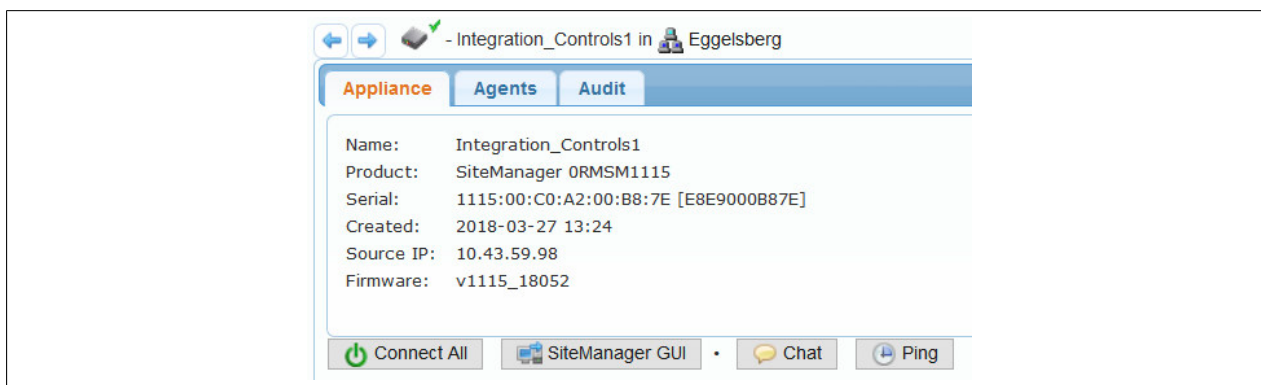
☒ User name:

Password:

2. Ein Browserfenster öffnen und zum GateManager (IP-Adresse oder Hostname) navigieren. Anschließend den Eintrag "LinkManager" selektieren. Es öffnet sich ein Browserfenster, in dem das LinkManager Benutzer-Zertifikat oder Benutzername und das Account Passwort für den LinkManager eingetragen wird.



3. Nach dem Einloggen wird die gegenwärtige Domain angezeigt.



4. Es lässt sich mit dem LinkManager nun auf die einzelnen Agents zugreifen.
5. Weitere Informationen zum LinkManager 8 finden sich [hier](#).

5 Umstellung auf neue SiteManager Version

In dieser Anleitung werden verschiedene Szenarien für den Umstellungsprozess von einer abgekündigten SiteManager Varianten (z. B. 1135 3G/4G Regionalvarianten oder 11xx Versionen) auf die SiteManager 13xx vorgestellt. Andere Vorgehensweisen, wie z. B. Projektupdate über USB-Stick, können ebenfalls funktionieren, wurden aber nicht getestet.

5.1 Produkte

Bestellnummer	Kurzbeschreibung
0RMSM1315	Secure Remote Maintenance -SiteManager, LAN 1x Ethernet 100Base-T uplink Anschluss, 3x Dev Anschlüsse 10 Geräteagenten, integrierte Firewall, 2x digitale Eingänge, 2x digitale Ausgänge, 24 VDC
0RMSM1335.4G	Secure Remote Maintenance -SiteManager, 1x Ethernet 100BASE-T Uplink Anschluss, 1x GPRS/3G/4G Uplink Anschluss, 3x Dev Anschlüsse 10 Geräteagenten, integrierte Firewall, 2x digitale Eingänge, 2x digitale Ausgänge, 24 VDC
0RMSM1345	Secure Remote Maintenance -SiteManager, 1x Ethernet 100Base- T Uplink Anschluss, 1x WiFi uplink Anschluss, 3x Dev Anschlüsse 10 Geräteagenten, integrierte Firewall, 2x digitale Eingänge, 2x digitale Ausgänge, 24 VDC

5.2 Szenarien

Bei allen Szenarien wird davon ausgegangen, dass der Maschinenbauer aus Gründen der automatischen Konfiguration bzw. der I/O-Zuordnung die nahtlose Integration des SiteManagers in Automation Studio nutzen möchte. Falls die automatische Konfiguration und die I/O-Zuordnung nicht verwendet wird, ist der Abschnitt "[SiteManager_1315-1335-1345 - Erstmalige Einrichtung](#)" auf Seite 32 zu beachten.

5.2.1 Entwurf neuer Maschinen

Ein Maschinenbauer möchte eine neue Maschine, in der ein SiteManager verwendet wird, konstruieren und in Betrieb nehmen.

5.2.1.1 Schritte für die neue Konfiguration

- Die neue Version des SiteManager muss in "Physical View - System Designer" von Automation Studio konfiguriert werden.
- Die Konfiguration der Geräteagenten kann manuell über die SiteManager-Benutzeroberfläche oder automatisch über GateManager "Actions" erfolgen.

5.2.2 Modifizierung vorhandener Maschinen

Ein Maschinenbauer möchte in einem bereits bestehenden Maschinenentwurf die neue Version des SiteManagers verwenden.

5.2.2.1 Schritte für die Modifikation der bestehenden Konfiguration

- Das aktuelle Automation Studio Projekt öffnen und in "Physical View - System Designer" von Automation Studio den aktuell konfigurierten SiteManager durch den neuen SiteManager ersetzen. Dies ermöglicht eine automatische SiteManager-Konfiguration beim Hochfahren der Maschine durch die SPS. Die Konfiguration des SiteManagers muss nicht geändert werden.
- Die Konfiguration der Geräteagenten kann manuell über die SiteManager-Benutzeroberfläche oder automatisch über GateManager "Actions" erfolgen.

5.2.3 Wartung von Bestandsanlagen

Ein Maschinenbauer möchte in einer bereits bestehenden Anlage eine abgekündigte Variante des SiteManagers, durch einen aktuellen SiteManager ersetzen. In diesem Szenario ist der SiteManager defekt, der Status des SiteManagers ist down und er ist daher offline.

Information:

Bei allen SiteManager-Varianten ist der "Überwachungsmodus" dauerhaft deaktiviert, d. h. ein Gerätetausch stört den Maschinenbetrieb nicht.

Der GateManager (B&R GateManager Hosted Service oder GateManager Software) bietet eine automatische Funktion, um einen SiteManager zu ersetzen und dessen Konfiguration wiederherzustellen. Der GateManager speichert dabei automatisch die Konfiguration des SiteManagers (Netzwerkconfiguration, konfigurierte Agenten und Funktionen wie DCM, Nutzungshistorie und Audit-Logs).

5.2.3.1 Schritte für die Modifikation der Bestandsanlage

5.2.3.1.1 Vorkonfiguration

- Der SiteManager sollte vom Maschinenbauer vor der Auslieferung an den Endbenutzer mit der GateManager-Adresse, dem Appliance-Namen und dem Domain-Token vorkonfiguriert werden.
- Abhängig davon, wer die SIM-Karte bereitstellt, erfolgt die Konfiguration der Breitband-Netzwerkverbindung schon beim Maschinenbauer oder erst beim Endkunden.
- Um den Prozess der Vorkonfiguration mehrerer SiteManager zu automatisieren, kann der Maschinenbauer eine Dummy-SPS-Applikation mit der korrekten Konfiguration schreiben und diese somit über Automation Studio / Runtime vorkonfigurieren.
- Wenn der SiteManager ohne Vorkonfiguration ausgeliefert wurde, muss die Konfiguration durch den Servicetechniker beim Endbenutzer erfolgen. Diese umfassen alle oben genannten Konfigurationen und die Breitband-Netzwerkverbindung für die Fernverbindung zum GateManager.

Für weitere Informationen siehe Abschnitt "[SiteManager_1315-1335-1345 - Erstmalige Einrichtung](#)" auf Seite 32.

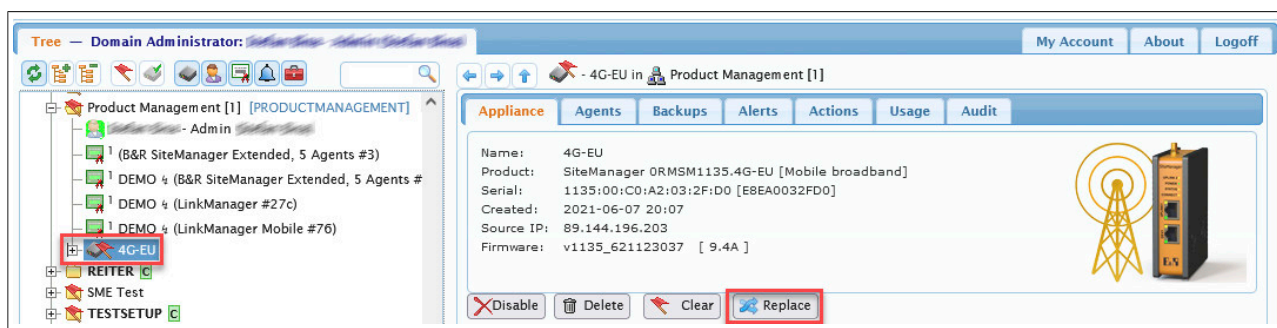
5.2.3.1.2 Austausch des Geräts

In diesem Schritt wird die komplette SiteManager-Konfiguration (Netzwerkconfiguration, konfigurierte Agenten und Funktionen wie DCM) sowie die Nutzungshistorie und Audit-Protokolle auf den "neuen" SiteManager repliziert.

- GateManager-Benutzeroberfläche öffnen. In der Übersicht des "alten" SiteManagers auf "Ersetzen" klicken und den Anweisungen des GateManagers für den Vorgang folgen.
- Nach erfolgreichem Austausch dauert es ca. 2 bis 5 Minuten, bis die richtigen Agenten wieder im GateManager-Benutzeroberfläche sichtbar sind. Nun können die veralteten Agenten gelöscht werden.

Information:

Die Schaltfläche "Ersetzen" (siehe Abbildung) erscheint nur in der GateManager-Benutzeroberfläche, wenn der SiteManager offline ist (nach einem Timeout von 9 min).



5.2.3.1.3 I/O-Zuordnung

In diesem Schritt wird erklärt, wie das Automation Studio-Projekt aktualisiert werden kann, um die I/O-Zuordnung wieder zu nutzen. Wenn die I/O-Zuordnung nicht benutzt wird, kann dieser Schritt übersprungen werden.

- Den aktuell konfigurierten SiteManager durch die neue Version des SiteManagers in "Physical View - System Designer" von Automation Studio ersetzen.
- Eine LinkManager-Verbindung herstellen und das Projekt aktualisieren.
- Wenn das "ModuleOK"-Flag noch False ist, ist es notwendig, den SiteManager zurückzusetzen und ihn von der SPS neu programmieren zu lassen, damit die SPS das neue Gerät akzeptiert. Das Rücksetzen erfolgt durch einen 5-Sekunden-Druck auf die Reset-Taste. Vor dem drücken der Reset-Taste ist sicherzustellen, dass die SiteManager-Netzwerkconfiguration im Automation Studio Projekt gültig ist. Während dieses Vorgangs wird der SiteManager 2mal automatisch neu gestartet.
- Nach dem erfolgreichen Hochfahren des SiteManagers zur GateManager-Benutzeroberfläche gehen, um das letzte SiteManager-Backup wiederherzustellen. Eine Aktualisierung der GateManager-Benutzeroberfläche kann erforderlich sein, um die richtigen Appliances/Agenten zu sehen, die im SiteManager konfiguriert sind.
- Um das korrekte Verhalten zu überprüfen, eine Verbindung zur SPS über den LinkManager herstellen und prüfen, ob das Flag "ModuleOK" True ist.

Erst nach erfolgreichem Abschluss dieser Schritte sind Funktionalitäten wie "Uplink Status" oder der Eingang "Remote Management Control 1" wieder zugänglich.

6 SIM-Karten-Leitfaden für SiteManager 4G Global – USA und Japan

Dieses Dokument enthält Richtlinien für den Erwerb und die Verwendung von SIM-Karten sowie Empfehlungen für das Modell SiteManager 4G Global mit Schwerpunkt auf den Regionen USA und Japan.

Information:

Haftungsausschluss

Die in diesem Dokument enthaltenen Informationen wurden von unserem Lieferanten Secomea gesammelt und bestätigt. B&R garantiert nicht, dass SIM-Karten der empfohlenen Netzbetreiber funktionieren oder immer unterstützt werden, da B&R keinen Einfluss auf die Netzbetreiber und deren Aktivitäten hat.

Dieser Leitfaden ist lediglich eine Empfehlung für Kunden und Partner, um den Einsatz des SiteManager 4G Global in den Regionen USA und Japan zu erleichtern.

6.1 Betroffenes Material

Die Richtlinien beziehen sich auf das folgende B&R-Material:

Bestellnummer	Kurzbeschreibung
0RMSM1335.4G	Secure Remote Maintenance -SiteManager, 1x Ethernet 100BASE-T Uplink Anschluss, 1x GPRS/3G/4G Uplink Anschluss, 3x Dev Anschlüsse 10 Geräteagenten, integrierte Firewall, 2x digitale Eingänge, 2x digitale Ausgänge, 24 VDC

Der SiteManager 4G Global verwendet das Modem SIMCom SIM7600G-H, also ein anderes Modem als die bisher verwendeten Modems für die regionalspezifischen SiteManager (4G EU/US/JP/CN).

6.2 Problemstellung und Lösung

6.2.1 Vereinigte Staaten

In den USA verwenden Kunden und Partner von B&R in der Regel den folgenden SIM-Kartenanbieter: AT&T. Dies bedeutet jedoch nicht, dass andere SIM-Karten-Anbieter nicht mit dem SiteManager 4G Global funktionieren. AT&T wird lediglich aufgrund seiner Netzabdeckung und Kundenzahl erwähnt. Verizon ist einer der größten Anbieter in den USA, wird aktuell aber nicht von B&R unterstützt.

6.2.1.1 Verizon

Der SiteManager 4G Global ist noch nicht für das Netz von Verizon zertifiziert, da die IMEI noch nicht in deren System registriert ist. Daher unterstützen wir noch keine SIM-Karten von Verizon.

6.2.1.2 AT&T

Eine bekannte Einschränkung von AT&T ist, dass SIM-Karten, die einige Abonnements verwenden, keinen Zugang zum 4G-Netz von AT&T über den SiteManager 4G Global erhalten. Der Grund dafür ist, dass der SiteManager 4G Global nicht im IMEI-System von AT&T gelistet ist und eine Typgenehmigung von AT&T benötigt. Daher können SIM-Karten nicht von AT&T für die Verwendung des SiteManager 4G Global aktiviert werden. Obwohl das Modem selbst von AT&T zertifiziert ist, gibt es immer noch Probleme mit AT&T bei der Verbindung mit einigen Abonnements, die die Verwendung von AT&T-zertifizierten IoT-Geräten erfordern. Es gibt jedoch immer noch viele Secomea-Kunden in den USA, die AT&T-SIM-Karten auf dem folgenden Online-Marktplatz bestellt haben und diese erfolgreich verwenden, um den SiteManager 4G Global mit dem 4G-Netz zu verbinden: <https://marketplace.att.com/products/att-iot-dataplans-lte-north-america>. Dies ist daher der von B&R empfohlene Kanal für den Kauf von AT&T-SIM-Karten.

Derzeit gibt es keine Informationen darüber, wann diese Einschränkung behoben wird.

6.2.1.3 T-Mobile

Auf Grund geänderter Verbindungsanforderungen kann der SiteManager mit T-Mobile derzeit nicht oder nur mit großen Schwierigkeiten verwendet werden.

Ursache

Nachdem T-Mobile sein 3G-Netz geschlossen hat, hat das Unternehmen die Art und Weise geändert, wie sich Kunden mit dem 4G-Mobilfunknetz verbinden können. Es wird erwartet, dass alle Geräte VoLTE-kompatibel sind. (VoIP über LTE) . Die B&R SiteManager sind jedoch nicht VoLTE-kompatibel.

6.2.2 Japan

Um SiteManager 4G Global in Japan zu nutzen, müssen Kunden einen MVNO (Mobile Virtual Network Operator) wählen, da das integrierte 4G-Global-Modem SIM7600G-H nicht mit MNOs (Mobile Network Operators) verwendet werden kann. Der Grund dafür ist, dass SIMCom noch kein MNO-Verbindungszertifikat für das Modem SIM7600G-H erhalten hat. Daher unterbrechen MNOs in Japan die Verbindung für nicht zertifizierte Modems wie das SIM7600G-H, wovon der SiteManager 4G Global betroffen ist. Beispiele für MNOs sind NTT Docomo, au, Softbank und Rakuten. Wir raten davon ab, diese Anbieter zu nutzen. Wir empfehlen stattdessen die Nutzung von MVNOs.

In Japan gibt es Hunderte von MVNOs, die wir nicht alle überprüfen können. Wir haben jedoch gute Erfahrungen mit den folgenden MVNOs im Hinblick auf den Einsatz des SiteManager 4G Global:

IIJ mio	
mineo	
OCN	
BIGLOBE	
Y!mobile	

7 Weiterführende Dokumentation

Anwenderhandbücher und Datenblätter sind für alle B&R SiteManager Varianten sowie zugehörige GateManager- und TrustGate Produkte verfügbar. Die Links zu den PDF-Handbüchern sind auf der Homepage von B&R unter www.br-automation.com/de/produkte/software/fernwartung/ bei den allgemeinen Informationen zu den Produkten zu finden.

Information:

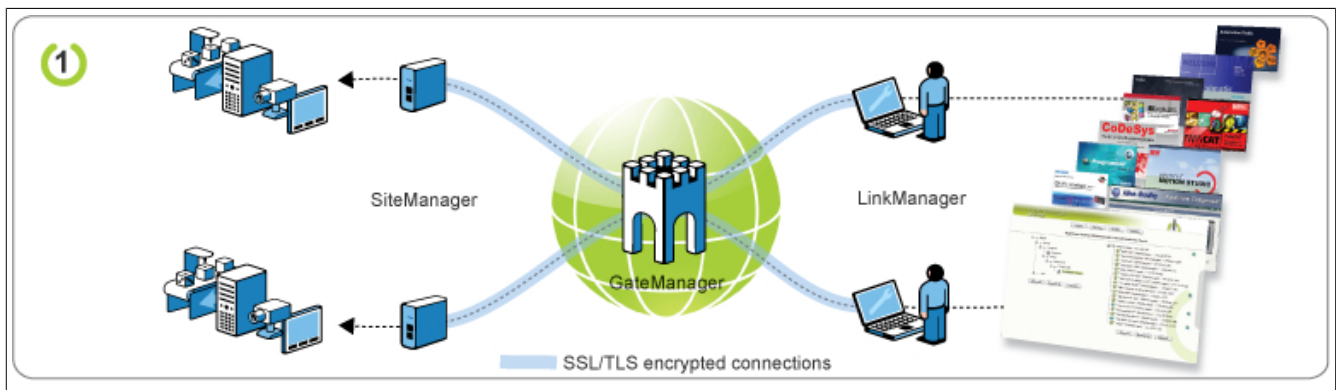
Die Dokumente auf der B&R Homepage beziehen sich auf Secomea Produktmodelle und können unter Umständen auf Funktionen wie z. B. eine serielle oder eine USB-Schnittstelle verweisen, die nicht bei allen B&R SiteManager Modellen verfügbar sind.

8 Anwendungsfälle und Endkunden-Szenarien

In diesem Kapitel werden verschiedene Anwendungsfälle und Endkunden-Szenarien behandelt.

8.1 Anwendungsfälle

8.1.1 Ferndienst – On-Demand-Zugriff für Programmierung und Fehlerbehebung

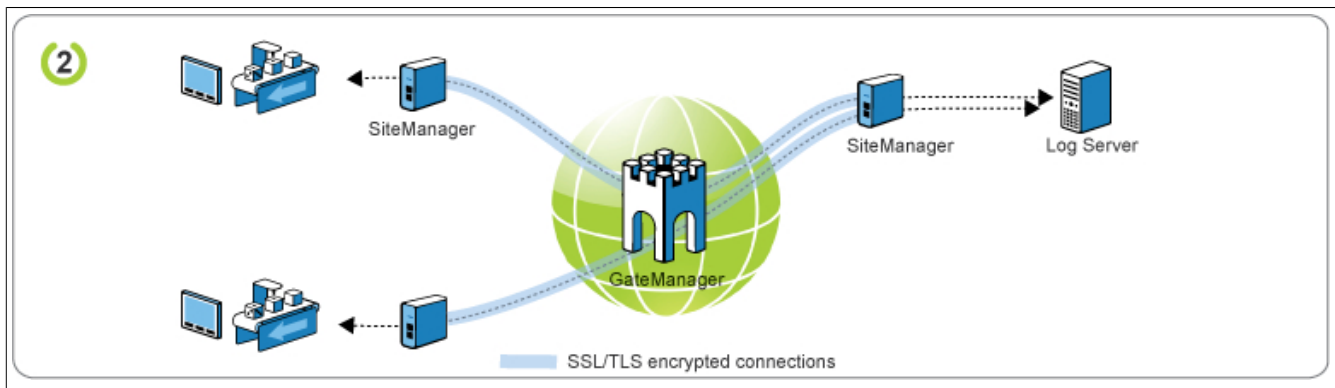


Hierbei handelt es sich um die primäre Funktion der Industrielösung von B&R. Der Zweck ist, dass mehrere Techniker Programmierzugriff auf Geräte an mehreren Standorten bekommen.

Wer worauf zugreifen kann, wird zentral über das LinkManager Konto auf dem GateManager gesteuert, auf dem auch der gesamte Zugriff protokolliert wird.

Es werden keine festen oder öffentlichen IP-Adressen benötigt und alle Verbindungen von SiteManagern und LinkManagern verwenden standardmäßige webbasierte SSL-/TLS-Protokolle. Dadurch ist die Lösung äußerst Firewall-freundlich.

8.1.2 Fernüberwachung - sichere Datenprotokollierung (zwischen 2 SiteManagern)



Mit dieser Funktion können statische Verbindungen zwischen Geräten hinter SiteManagern an unterschiedlichen Standorten hergestellt werden. Dies ist eine einfache Methode, um beispielsweise einem Protokollserver zu ermöglichen, Daten von Geräten zu erfassen, und wird gewöhnlich für Versorgungsinstallationen verwendet.

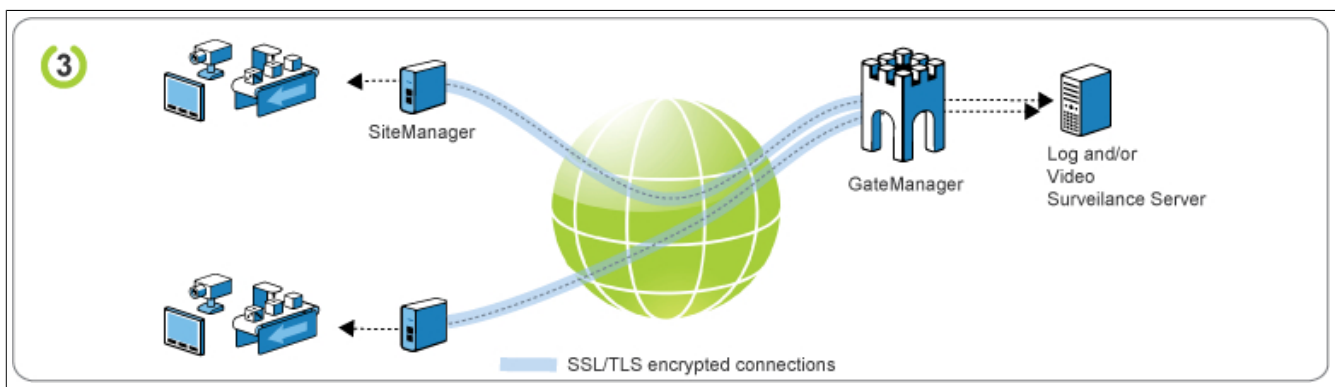
Das Setup kann entweder einem Geräte-Relais oder einem Server-Relais zugrunde gelegt werden, je nachdem, ob die Geräte Protokoll Daten an den Server senden sollen oder der Server Daten vom Gerät abrufen soll. Das Setup basiert auf virtuellen IP-Adressen, das bedeutet, dass keine Subnetzkonflikte auftreten. Tatsächlich könnten alle Geräte dieselbe IP-Adresse haben.

Genau wie die obige Lösung basiert dieses Setup nur auf webbasierten SSL-/TLS-Verbindungen und ist daher äußerst Firewall-freundlich.

Information:

Für die Durchführung von Video-Streaming oder Full-Tunneling siehe die Lösungen aus den folgenden Abschnitten: ["Fernüberwachung – für sichere Datenprotokollierung" auf Seite 56](#) und ["Direkter Internetzugriff – für Datenprotokollierung und Videoüberwachung" auf Seite 57](#)

8.1.3 Fernüberwachung – für sichere Datenprotokollierung

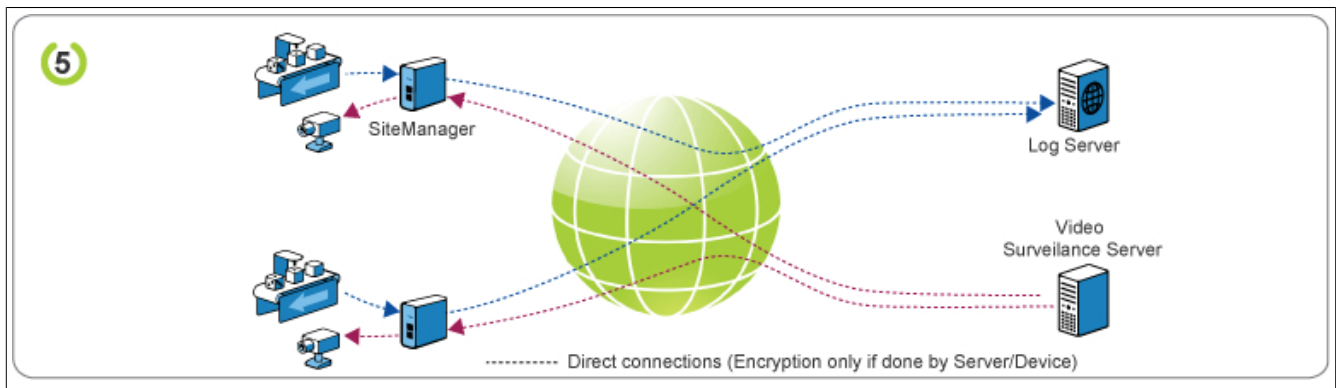


Dieses Setup verwendet die gleichen Relaisprinzipien wie Lösung 2, allerdings wird hier der GateManager Server am gleichen Standort wie der Server installiert.

Der Vorteil ist, dass nun die Relaisverbindungen für Daten mit hohen Anforderungen an die Bandbreite (z. B. Videos) verwendet werden können. Ähnlich wie ein VPN-Konzentrator muss von einer öffentlichen IP-Adresse auf den GateManager Server zugegriffen werden können. Allerdings kann der Server in eine demilitarisierte Zone (DMZ) oder hinter eine Firewall gelegt werden, die die Verbindung per NAT zum GateManager umwandelt.

Wie oben basiert das Setup auf virtuellen IP-Adressen, weshalb keine Subnetzkonflikte auftreten und alle Geräte dieselbe IP-Adresse haben könnten. Außerdem basiert die Lösung ausschließlich auf webbasierten SSL-/TLS-Verbindungen und ist daher äußerst Firewall-freundlich.

8.1.4 Direkter Internetzugriff – für Datenprotokollierung und Videoüberwachung



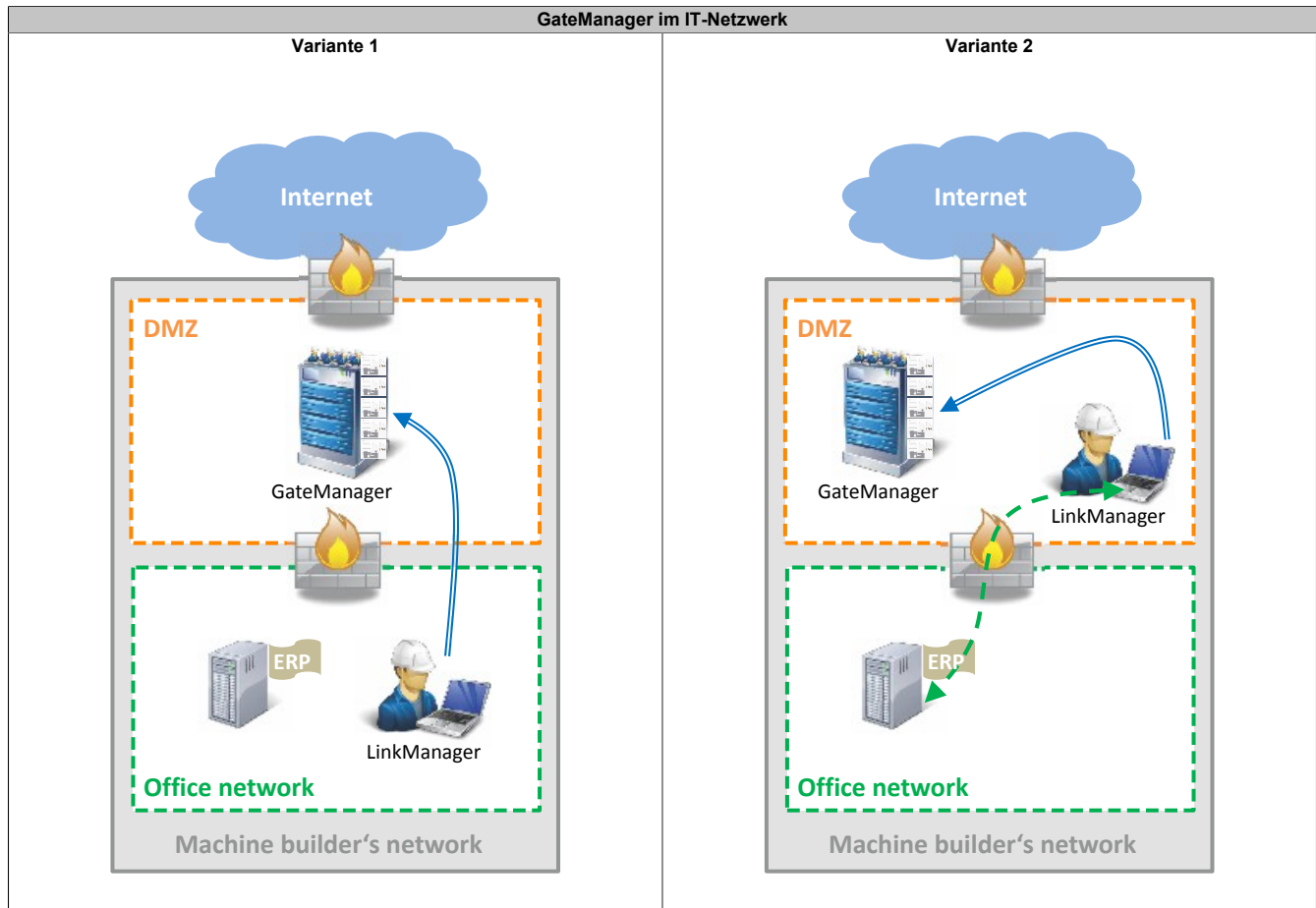
Diese Funktion wird durch den SiteManager Forwarding Agent aktiviert. Damit kann ein Gerät den SiteManager als Internet-Gateway verwenden, um Protokolldaten an einen Web-Dienst zu senden.

Alternativ kann es z. B. von einem Videoüberwachungssystem verwendet werden, das mit der IP-Adresse des SiteManagers verbunden ist. Dieser wiederum leitet die Verbindungsanfrage an einen festgelegten Port auf dem Gerät weiter. (Dazu muss dem SiteManager eine öffentliche IP-Adresse zugewiesen werden und es wird gewöhnlich für per Mobilfunk verbundene SiteManager mit einem Internetvertrag mit fester IP-Adresse verwendet.)

8.2 Endkunden-Szenarien

Der Betreiber des Fernwartungssystems ist in der Regel der Maschinenbauer, der seine Endkunden betreut und der den GateManager in der eigenen IT-Abteilung betreibt. Das bedeutet, dass jede ausgelieferte Anlage/Maschine Zugriff auf den GateManager hat, um sicher und einfach Fernwartung durchführen zu können.

Aus Gründen der IT-Sicherheit ist es empfehlenswert, den GateManager in einer DMZ (eigene Netzwerkzone) zu installieren. Der LinkManager Benutzer kann sich dann durch die Firewall hindurch mit dem GateManager in der DMZ verbinden. Alternativ kann aber auch der LinkManager Benutzer Teil der GateManager-DMZ sein und hat somit von seinem PC aus über den verschlüsselten VPN-Tunnel direkt Zugriff auf den GateManager. Somit befindet sich der PC des Servicetechnikers in dem Subnetz des GateManagers. Die unverschlüsselte Kommunikation von dem selbigen PC in das Office Netzwerk wird von der Firewall der DMZ überprüft.

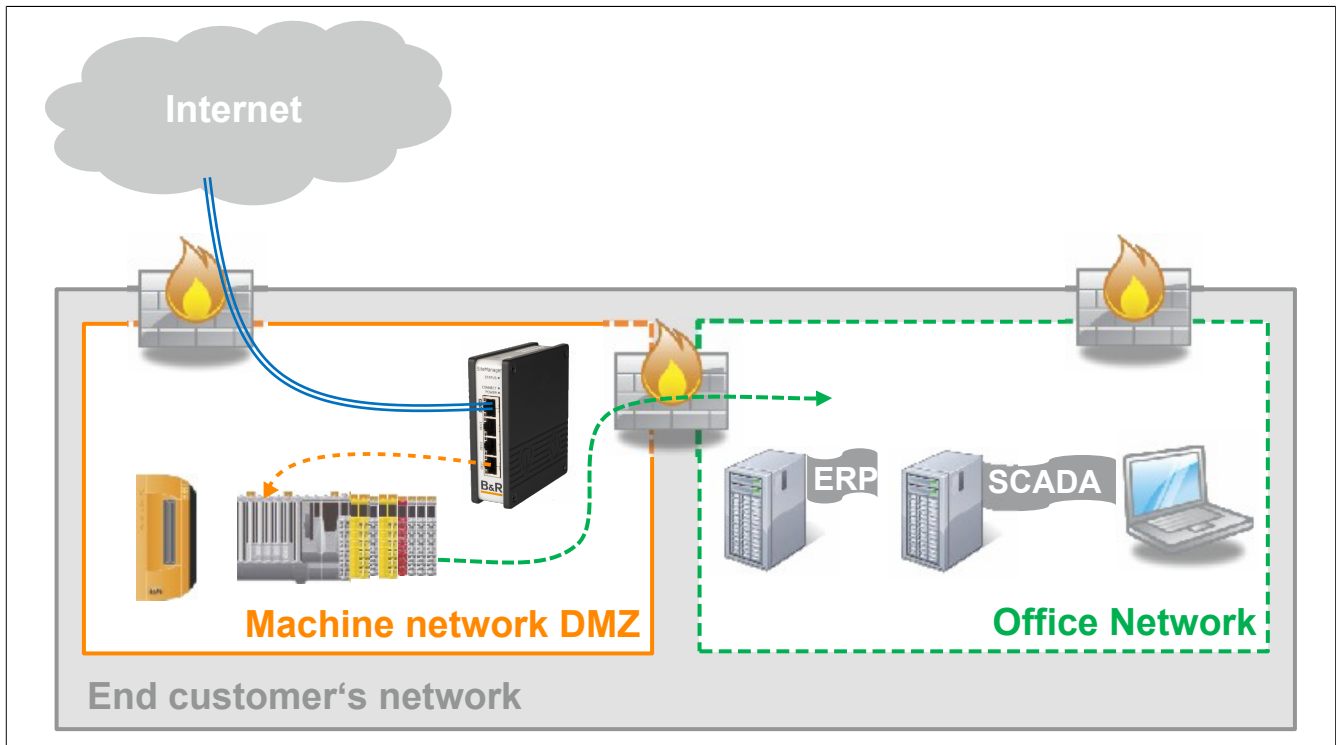


Generell ist festzuhalten, dass der Maschinenbauer in der Regel die Device Agents für die SiteManager definiert und die SiteManager im Maschinennetzwerk des Endkunden integriert. Meist sind beim Endkunden ein Maschinennetzwerk und ein Büronetzwerk vorhanden. Oft müssen dabei Geräte aus dem Maschinennetzwerk auf das Büronetzwerk zugreifen, um Rezept- oder Auftragsdaten abrufen zu können. Welches der folgenden Szenarien realisiert werden kann, hängt sehr stark von der vorhandenen IT-Infrastruktur des Endkunden ab. Folgend sind einige Szenarien skizziert, die eine Möglichkeit der Integration des SiteManagers in ein Fabriks- oder Maschinennetz darstellen.

8.2.1 SiteManager und Maschine in einem isolierten Netzwerk

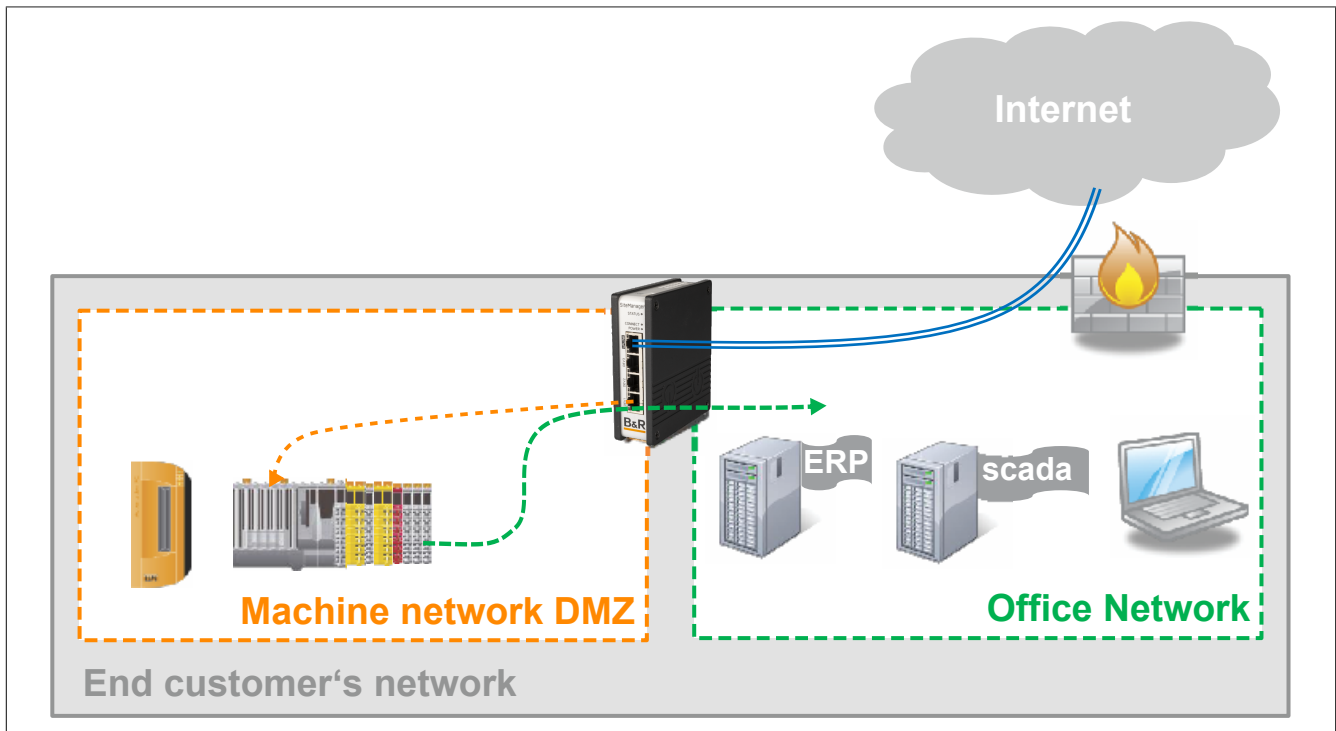
Maschinennetzwerk und Büronetzwerk sind durch eine Firewall voneinander getrennt. Es erhalten nur ausgewählte Maschinen Zugriff auf das Büronetzwerk. Der Datenverkehr des Maschinennetzwerks sowie des SiteManager aus und in das Internet erfolgen über eine Firewall.

Zur Kommunikation durch die Firewall des SiteManagers sind vom Maschinenbauer entsprechende Device Agents zu definieren. Die Kommunikation vom Fernwartungszugriff ist ausschließlich über die Device Agents möglich. Um dem SiteManager Zugriff auf den GateManager zu gewähren, könnte ein eigener Web-Proxy des Endkunden verwendet werden.



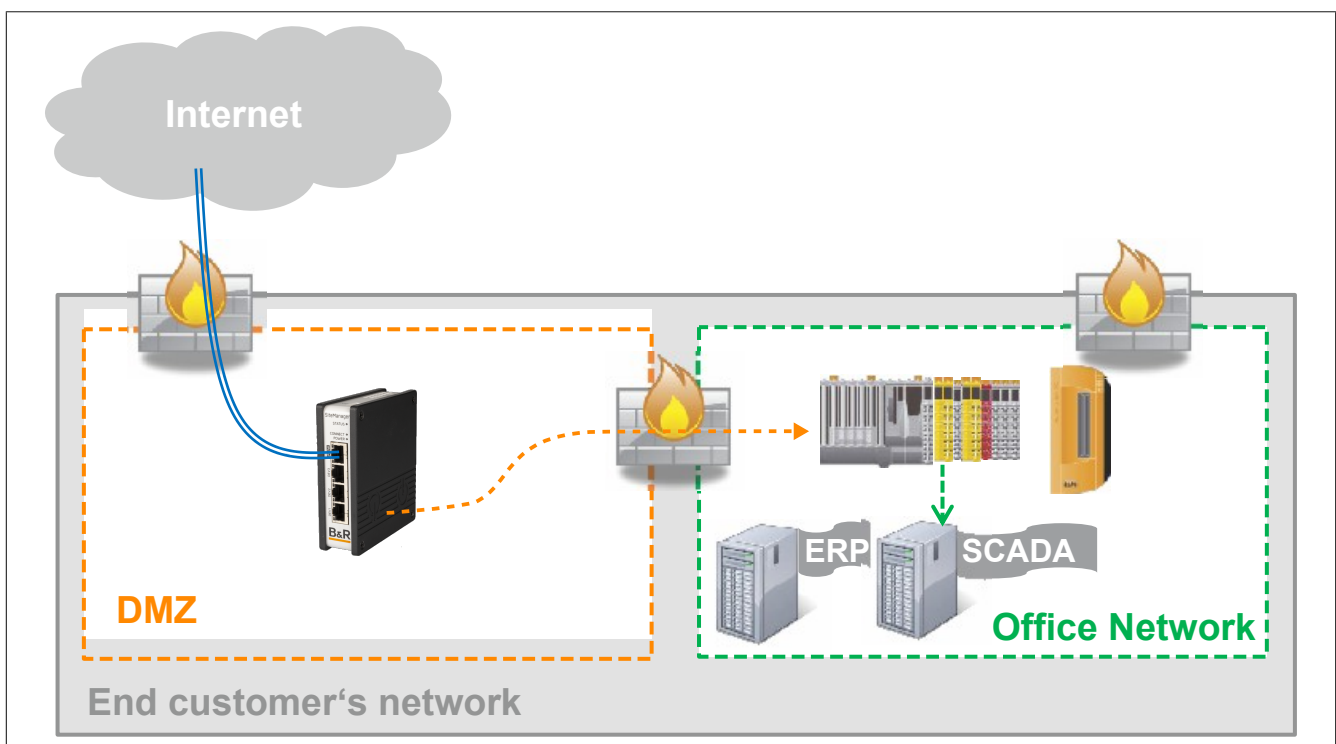
8.2.2 Maschinennetzwerk isoliert hinter DMZ und SiteManager

Maschinennetzwerk und Büronetzwerk sind durch den SiteManager voneinander getrennt. Durch die Device Agents ist es einem LinkManager Benutzer möglich, auf die Geräte im Maschinennetzwerk zuzugreifen, jedoch nicht auf das Büronetzwerk. Es erhalten nur ausgewählte Maschinen Zugriff auf das Büronetzwerk. Dies kann durch statische Routen oder Port-Weiterleitung am SiteManager erreicht werden.



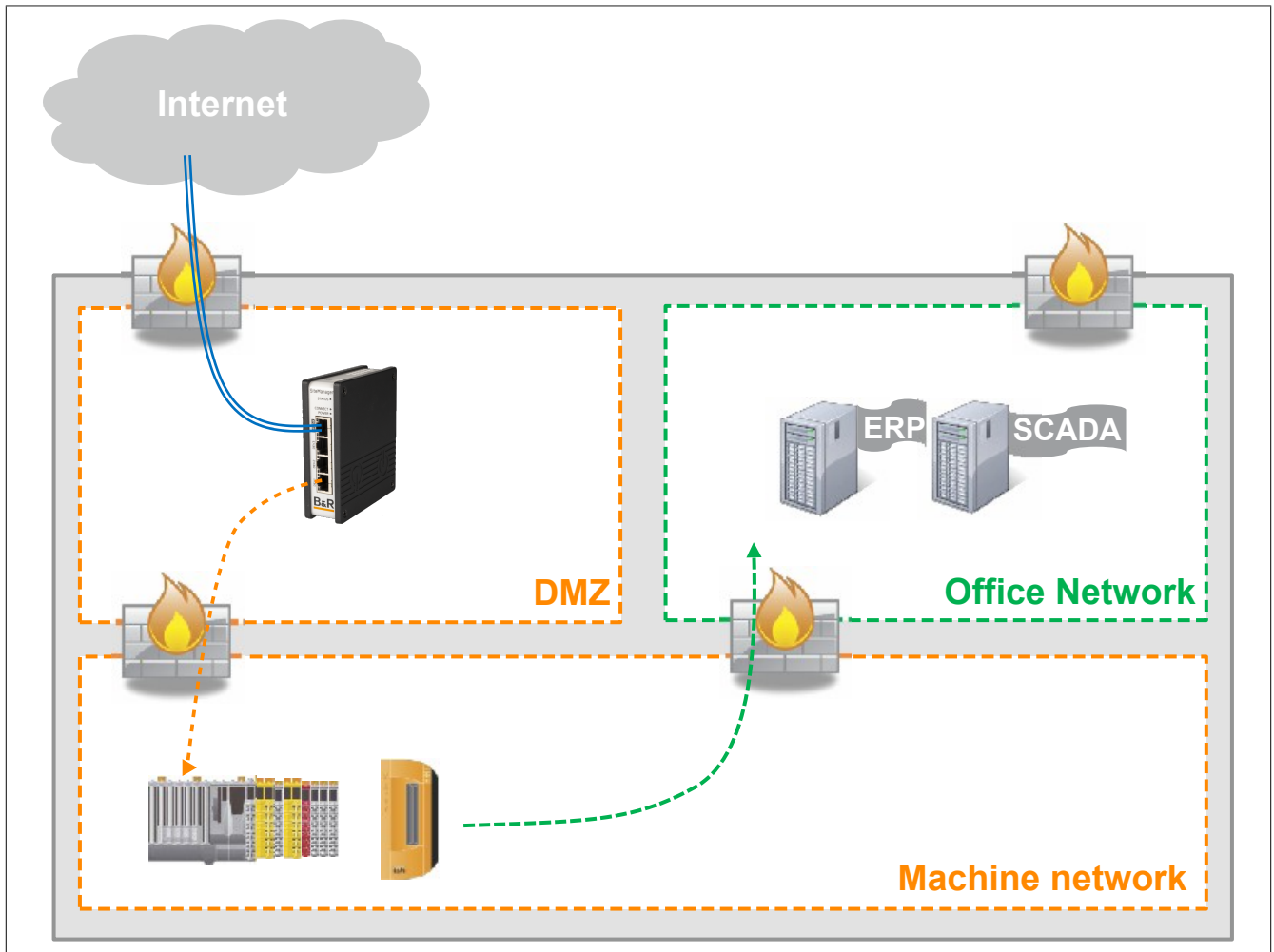
8.2.3 SiteManager isoliert in eigener DMZ

In diesem Szenario sind das Büro- und das Maschinennetzwerk nicht voneinander getrennt. Der SiteManager ist in einer eigenen DMZ integriert. Jeglicher Datenverkehr vom SiteManager zu den Maschinen muss eine Firewall passieren. Da der Endpunkt der VPN-Verbindung in der DMZ liegt, kann nun eine Application Firewall, die sich zwischen DMZ und Büronetz befindet, den Datenverkehr einsehen und auf Schadsoftware überprüfen. Zusätzlich kann diese Firewall noch den Zugriff auf das Büronetzwerk einschränken, so dass durch eventuelle Konfigurationsfehler in den Device Agents kein ungewollter Zugriff möglich ist.



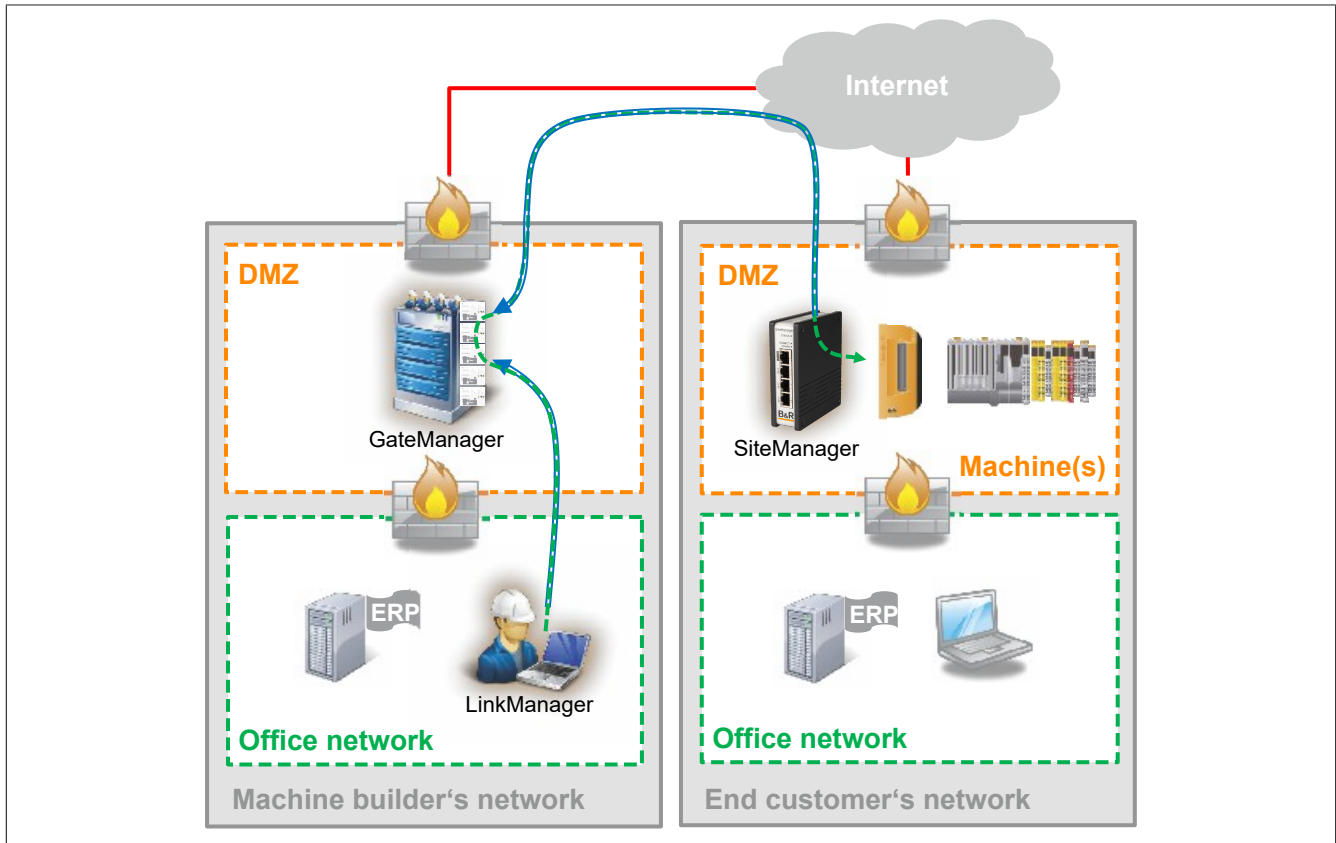
8.2.4 SiteManager und Maschine in separaten Netzwerken

In diesem Szenario sind das Büro- und Maschinennetz voneinander getrennt und der SiteManager befindet sich in einer eigenen DMZ. Auch hier liegt der Endpunkt der VPN-Verbindung in einer DMZ und der Datenstrom vom SiteManager in das Maschinennetz kann von der Application Firewall überprüft werden. Da das Büronetzwerk nicht im Maschinennetzwerk integriert ist, kann der SiteManager auch nicht auf Geräte im Büronetzwerk (z. B. ERP-System) zugreifen. Dieses Szenario bietet die meiste Sicherheit von den hier aufgelisteten Anwendungsfällen.



8.2.5 Fernwartung - Komplettszenario

Die Abbildung verdeutlicht ein mögliches Realisierung-Szenario. Auf der Seite des Maschinenbauers ist der GateManager in einer eigenen DMZ installiert. Service Techniker verbinden sich via LinkManager aus dem Büronetzwerk in die DMZ. Die Firewall zwischen Büronetzwerk und DMZ regelt wer auf die DMZ zugreifen darf. Auf der Seite des Endkunden und der Maschine ist eine ähnliche Struktur gewählt. Hierbei sind der SiteManager und das Maschinennetzwerk durch eine eigene DMZ vom Büronetzwerk des Endkunden getrennt. Die Firewall zwischen den Netzwerken wird verwendet, um den Zugriff zu kontrollieren.



8.3 Verbindungsaufbau mit FTP

Einleitung

Für die Verbindung mit dem FTP-Server wird nur der passive Modus verwendet. Durch Verwendung einer Firewall und NAT können im aktiven Modus Fehler auftreten. Da der SiteManager über eine Firewall verfügt, müssen die für FTP notwendigen Ports zuerst freigegeben werden. Beispielsweise erfolgt die Kommunikation mit dem FTP-Server über Port 21. Die Datenübertragung erfolgt zufällig über einen Port zwischen 49152 bis 65535. Dieser Bereich ist deshalb ebenfalls freizugeben.

8.3.1 FTP über SiteManager

Setup des Beispiels

Verwendete Steuerung und Software

- X20CP3685
- Automation Runtime I4.33

Konfiguration FTP-Client

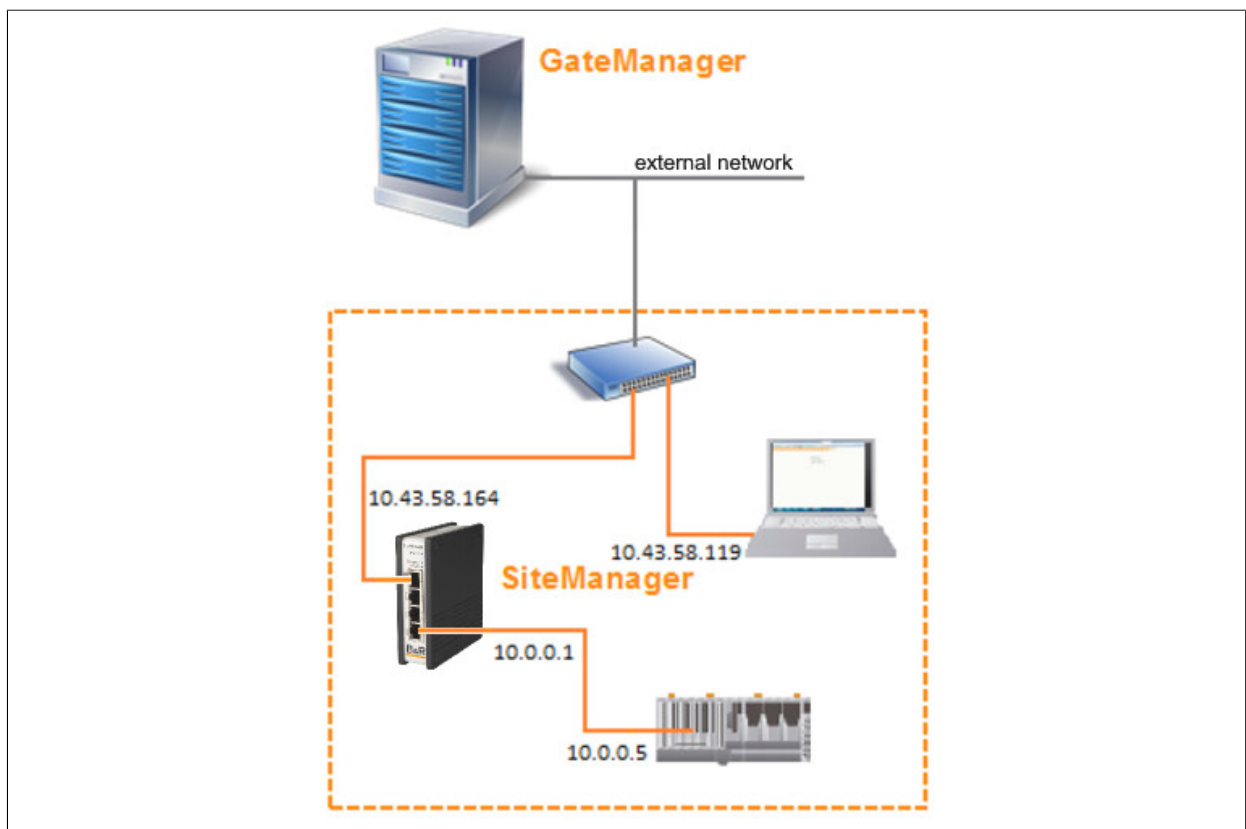
- IP-Adresse: 10.43.58.119
Subnetzmaske: 255.255.255.0

Konfiguration SiteManager

- Externe IP-Adresse (UPLINK): 10.43.58.164
Subnetzmaske: 255.255.255.0
- Interne IP-Adresse (DEV): 10.0.0.1
Subnetzmaske: 255.255.255.0

Konfiguration FTP-Server

- IP-Adresse (ETH): 10.0.0.5
Subnetzmaske: 255.255.255.0



Forwarding Agent

Der Forwarding Agent wird als Gerätetyp **Custom (Advanced)** erstellt.

Der Forwarding Agent kann auf 2 Arten genutzt werden:

- 1) Zugriff eines Geräts auf eine andere Schnittstelle erlauben
- 2) über die UPLINK-Schnittstelle eine Verbindung zu einem Gerät erlauben

Dieser Agent bietet eine schnelle Möglichkeit über die UPLINK-IP-Adresse auf ein Gerät auf der Geräteseite zuzugreifen und umgekehrt. So entspricht die Funktion des SiteManagers der eines Routers. Dabei sind nur die Ports, die im Forwarding Agent angegeben werden, zugänglich. Es können gleichzeitig mehrere Forwarding Agents aktiv sein, wovon jeder bis zu 10 Regeln beinhalten kann.

Sind die Forwarding- und Routing-Agents korrekt konfiguriert, sind sie, unabhängig von GeräteManager oder Internetverbindung, immer eingeschaltet. Sie müssen dann auch nicht über eine LinkManager-Verbindung aktiviert werden. Die Forwarding- und Routing-Agents werden nicht im Gate- oder LinkManager angezeigt.

Regelformat

Jede Forwarding-Regel muss aus einer Kombination von folgenden Elementen erstellt werden:

```
[#|?][[IN_IFACE*][LOCAL_IP]:][PROTOCOL:][SOURCE_IP/MASK:]
[NAT_PORT]>][OUT_IFACE*:]TARGET[/MASK]:TARGET_PORT]
```

Information:

Leerzeichen sind in der Regel nicht erlaubt.

Parameter

- ⇒ #
Ein "#" am Beginn der Regel gibt an, dass diese deaktiviert ist.
- ⇒ ?
Eine mit "?" eingeleitete Regel ist optional. Von dieser Regel verursachte Fehler werden nicht als schwerwiegend behandelt.
- ⇒ IN_IFACE / LOCAL_IP
Hiermit wird die eingehende Schnittstelle beziehungsweise optional die lokale IP-Adresse oder das Alias, für die Verbindung angegeben.
- ⇒ PROTOCOL
Spezifiziert das Netzwerkprotokoll aus TCP, UDP oder ANY. Der Standardwert für dieses Element ist TCP. Wird ANY in einer Regel mit NAT_PORT oder TARGET_PORT verwendet, entspricht dies "TCP als auch UDP", ansonsten entspricht es "irgendein IP-Protokoll".
- ⇒ SOURCE_IP
Gibt entweder eine Quelladresse oder einen Subnetzfilter in der Regel an.
- ⇒ NAT_PORT
Gibt den Zielport bzw. Portbereich für die Portweiterleitung an, auf die IN_IFACE gerichtet ist. Portweiterleitung bedeutet, dass der an einen bestimmten Port bzw. Portbereich einer SiteManager-Schnittstelle adressierte Verkehr übersetzt und an ein bestimmtes externes Ziel weitergeleitet wird.

Information:

Wenn eine Portweiterleitungsregel für TCP-Port 443 hinzugefügt wird, deaktiviert dies den Zugriff auf die SiteManager-WEB-Benutzeroberfläche von der eingehenden Schnittstelle der Regel. Auf die WEB-Benutzeroberfläche kann jederzeit von einer anderen Schnittstelle, über den Appliance Launcher oder über den RemoteManager oder GateManager (falls dieser ferngesteuert wird) zugegriffen werden.

- ⇒ >> oder >
Bei ">" wird keine Quellübersetzung angewendet.
Bei ">>" wird die Quell-NAT-Übersetzung für den von dieser Regel weitergeleiteten Verkehr angewendet, wodurch der SiteManager Quelle des weitergeleiteten Verkehrs ist.
- ⇒ OUT_IFACE:
Hiermit wird die ausgehende Schnittstelle für die Verbindung angegeben.
- ⇒ TARGET
Gibt die zugelassene IP-Adresse oder das Subnetz für die Verbindung zum externen Bereich ausgehend vom SiteManagers an.

⇒ TARGET_PORT

Wenn NAT_PORT gesetzt ist, gibt TARGET_PORT den Zielport bzw. den Zielportbereich für den weitergeleiteten Verkehr an. Ist TARGET_PORT nicht gesetzt, entspricht der Zielport dem NAT_PORT.

Information:

Wenn in NAT_PORT ein Portbereich angegeben ist, hier keinen Portbereich angeben. Andernfalls gibt der TARGET_PORT-Teil die zulässige Zielportnummer (n) auf dem Zielsystem an.

Optionale Parameter

- +TUP

Wenn diese Option gesetzt ist, wendet der Forwarding-Agent Quell-NAT an alle Verbindungen an, die über eine UPLINK-Schnittstelle (von einem Gerät auf einer DEV-Schnittstelle) ausgegeben werden, unabhängig von den Einstellungen ">" bzw. ">>" in den Weiterleitungsregeln. Dies bedeutet, dass das Zielsystem die SiteManager UPLINK IP-Adresse als Quelladresse und nicht als die ursprüngliche Geräte-IP-Adresse sehen wird. Diese Option wird meist bei der Erstellung von Outbound-Weiterleitungsregeln (von DEV bis UPLINK) aktiviert. Ist dieser Parameter deaktiviert, ist wahrscheinlich das statische Routen auf dem Zielsystem zu konfigurieren, das auf die UPLINK IP-Adresse zeigt, damit das Zielsystem das Gateway zurück zum Gerät ermittelt.

- +TDEV

Wenn diese Option gesetzt ist, wendet der Forwarding-Agent Quell-NAT an alle Verbindungen an, die über eine DEV-Schnittstelle (von einem System auf einer UPLINK-Schnittstelle) ausgegeben werden, unabhängig von den Einstellungen ">" bzw. ">>" in den Weiterleitungsregeln. Dies bedeutet, dass das Zielgerät die SiteManager DEV-IP-Adresse als Quelladresse anstelle der IP-Adresse des ursprünglichen Systems sieht. Diese Option werden in der Regel bei der Erstellung eingehender Weiterleitungsregeln (von UPLINK nach DEV) aktiviert.

8.3.2 Einstellungen am SiteManager

Erstellen der benötigten Agents

In der Menüleiste wird GateManager und anschließend Agents geöffnet. Hier können neue Agents erstellt, bearbeitet, deaktiviert, aktiviert und gelöscht werden. Für dieses Setup müssen 2 Agents erstellt und konfiguriert werden.

Agent Nr. 1 Konfiguration

- Device Name: bspw. Forwarding Agent 1
- Device: CUSTOM (Advanced)
- Type: Forwarding
- Forwarding Rule: UPLINK*:TCP:21>>DEV1:10.0.0.5

Forwarding Agent 1	CUSTOM (Advanced) ▼	Forwarding ▼	UPLINK*:TCP:21>>DEV1:10.0.0.5
--------------------	---------------------	--------------	-------------------------------

Diese Regel leitet automatisch alle TCP-Pakete die von der UPLINK-Schnittstelle über Port 21 an den SiteManager (10.43.58.164) geschickt werden, zu dem FTP-Server (10.0.0.5) weiter.

Agent Nr. 2 Konfiguration

- Device Name: bspw. Forwarding Agent 2
- Device: CUSTOM (Advanced)
- Type: Forwarding
- Forwarding Rule: UPLINK*:TCP:49152-65535>>DEV1:10.0.0.5

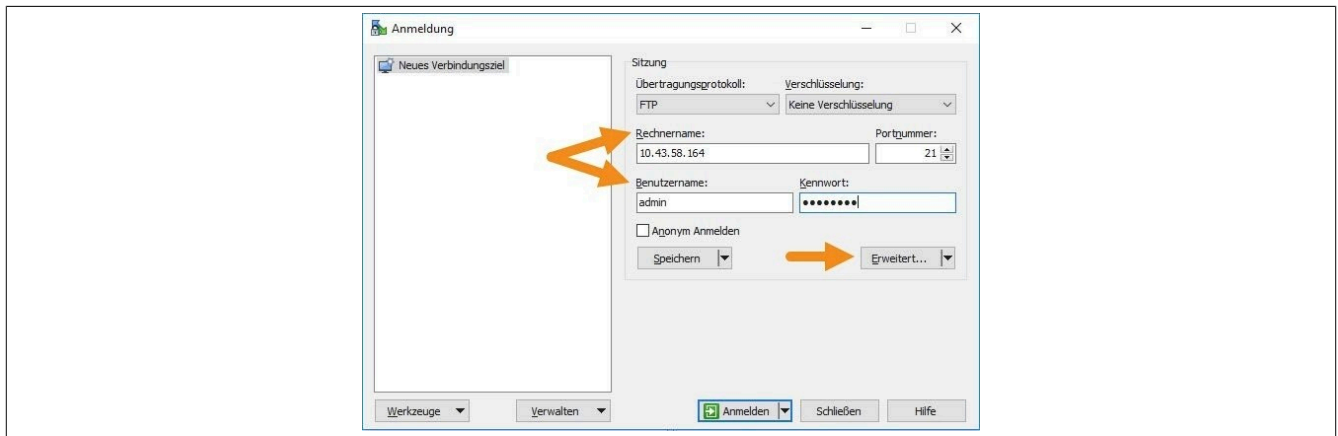
Forwarding Agent 2	CUSTOM (Advanced) ▼	Forwarding ▼	UPLINK*:TCP:49152-65535>>DEV1:10.0.0.5
--------------------	---------------------	--------------	--

Diese Regel entspricht der ersten, jedoch werden nur TCP-Pakete weitergeleitet, die über die Ports des Bereichs von 49152 bis 65535 an den SiteManager (10.43.58.164) gesendet werden.

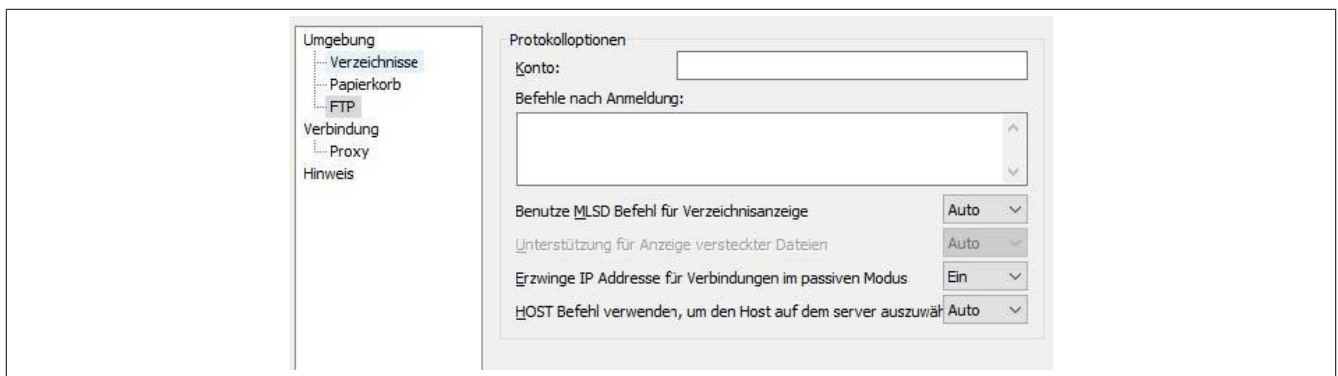
8.3.3 Erstellen einer Verbindung mit WinSCP

Dieses Beispiel bezieht sich auf die Version 5.9.6, Build 7601 des WinSCP.

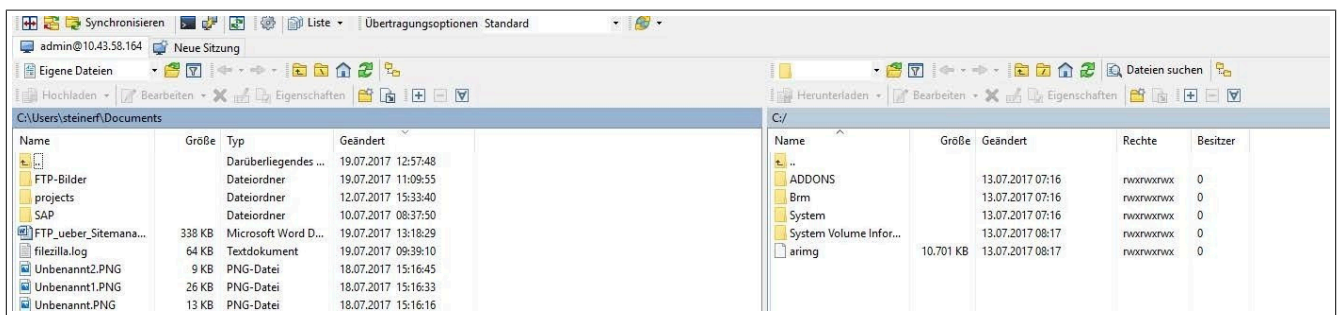
Nach dem Start des Clients öffnet sich ein Anmeldefenster, in dem die IP-Adresse des SiteManagers und die Anmeldedaten des FTP-Servers eingetragen werden.



Über die Schaltfläche "Erweitert" öffnet sich ein neues Fenster, in dessen Menübaum "Umgebung" das Untermenü "FTP" selektiert werden kann. Hier werden die Einstellungen gemäß der folgenden Abbildung konfiguriert.



Anschließend müssen die Eingaben bestätigt, die vorgenommenen Einstellungen gespeichert und ein Name für die Verbindung vergeben werden. Nachdem ein gegebenenfalls vorhandenes Passwort für den Benutzer bestätigt wurde, wird die Verbindung zum FTP-Server hergestellt.



9 Fehlerbehebung

Fehlerbehebung beim Zugriff von SiteManager auf GateManager über ein Firmen-Intranet

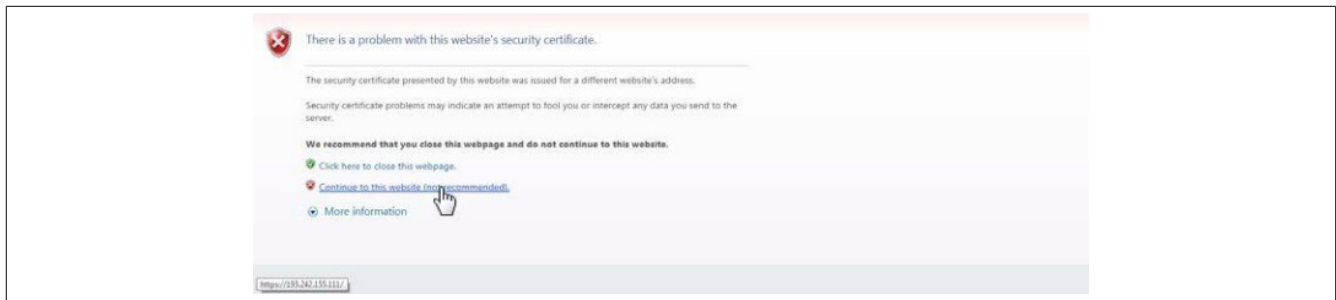
Mit den folgenden Abschnitten kann vom PC aus überprüft werden, ob ein SiteManager durch die Unternehmens-Firewall auf den GateManager zugreifen kann.

9.1 GateManager-Zugang von einem PC aus testen

Der SiteManager versucht, auf das Internet zuzugreifen, indem er nacheinander die folgenden Verbindungsmethoden von seinem Uplink-Port aus ausprobiert:

- 1) Port 11444 (Überprüfung: <https://gm01.br-automation.com:11444>)
- 2) Port 443 mit HTTPS/TLS (Überprüfung: <https://gm01.br-automation.com>)
- 3) Port 80 mit TLS über HTTP (Überprüfung: <https://gm01.br-automation.com:80>)
- 4) TLS über Web-Proxy

Werden die oben genannten Verifizierungslinks angeklickt oder in einen Webbrowser eingegeben, sollte mindestens einer der Links dieses Ergebnis liefern:



Nach Auswahl von "Weiter zu dieser Website" sollte diese Ansicht erscheinen:



Wenn keiner der Links zu den oben genannten Ansichten führt, kann dies an folgenden Ursachen liegen:

1. Eine Firewall blockiert den TLS-Zugang und lässt nur einfachen Text/html zu (d. h. <http://...> wird unterstützt, <https://...> nicht). Möglicherweise müssen spezielle Regeln in der Firewall für den PC eingerichtet werden. Dies kann durch die Genehmigung der IP-Adresse, der MAC-Adresse, des DNS-Namens des PCs oder des PCs selbst auf einem lokalen MS Directory Services-Server gelöst werden.
2. Für den Internetzugang ist ein Web-Proxy erforderlich, der auf dem PC, von dem aus versucht wird, eine Verbindung herzustellen, nicht konfiguriert ist. Normalerweise wird dieser vom DHCP-Server bereitgestellt, muss aber möglicherweise auch manuell konfiguriert werden (im MS Internet Explorer wird dies unter: Extras → Internetoptionen → Verbindungen → LAN-Einstellungen → Proxyserver).

Wenn alle oben genannten Punkte überprüft wurden und immer noch nicht der LinkManager Mobile Anmeldebildschirm auf dem PC zu sehen ist, ist auch eine Verbindung durch den SiteManager nicht möglich. In diesem Fall muss man sich an den IT-Administrator wenden.

9.2 PC kann Verbindung herstellen, SiteManager jedoch nicht

9.2.1 Grundlegende Fragen

- **Ethernet-Kabel ist nicht richtig angeschlossen**

Fehlerhaft angeschlossene Kabel sind eine häufige Fehlerursache. Überprüfen, ob das Netzwerk, über das der SiteManager Internetzugang erhalten soll, mit dem SiteManager Uplink-Port verbunden ist, und prüfen, ob der Ethernet-Port verbunden ist (die grün-gelben LEDs am Ethernet-Anschluss selbst leuchten).

- **Probleme bei der Konfiguration der Uplink1 IP-Adresse**

Sicherstellen, dass der SiteManager eine IP-Adresse hat, die zu dem Netzwerk passt, über das er Zugang zum Internet erhalten soll.

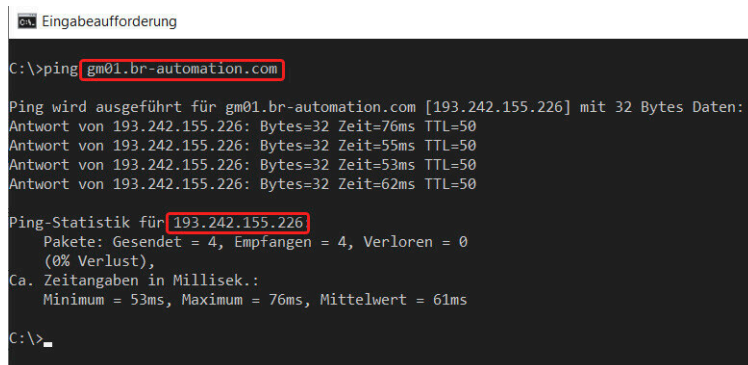
Wenn die Uplink1 IP-Adresse per DHCP zugewiesen wird, überprüfen, ob tatsächlich eine Adresse zugewiesen wurde. Den PC an das DEV-Netzwerk anschließen und den Secomea Appliance Launcher verwenden, um nach dem SiteManager zu suchen und die zugewiesene Uplink-IP-Adresse zu überprüfen. Alternativ kann auch die Lease-Tabelle des DHCP-Servers überprüft werden. Ebenso versuchen, diese IP-Adresse von einem PC im selben Netzwerk anzupingen.

Wenn die Uplink1 IP-Adresse statisch konfiguriert ist, überprüfen, ob diese mit dem Subnetz des Netzwerks übereinstimmt, mit dem sie verbunden ist. Auch prüfen, ob die Subnetzmaske mit der Subnetzklasse übereinstimmt und ob als Standard-Gateway der Router definiert ist, der den Internetzugang bereitstellt. Versuchen, die IP-Adresse von einem PC im selben Netzwerk aus anzupingen. Ein guter Test ist der Zugriff auf die SiteManager Web-Benutzeroberfläche von der Uplink1- oder DEV-Seite aus (in den Webbrowser vor der IP-Adresse "https://" eingeben. Standard-Login/Passwort ist "admin/admin"), und die Ping-Funktion im SiteManager-Menü Status → ping/trace verwenden, um das Internet-Gateway anzupingen).

- **DNS-Problem**

Wenn in der SiteManager-Konfiguration den DNS-Namen des GateManager-Servers verwendet wird, z. B. "gm01.br-automation.com", wird dieser möglicherweise nicht korrekt in die IP-Adresse aufgelöst, und sollte in die IP-Adresse geändert werden (Menü GateManager → Allgemein)

Eingabeaufforderung öffnen und den DNS-Namen des GateManagers anpingen, so dass die IP-Adresse (193.242.155.112) aufgelöst wird:



```

Eingabeaufforderung
C:\>ping gm01.br-automation.com

Ping wird ausgeführt für gm01.br-automation.com [193.242.155.226] mit 32 Bytes Daten:
Antwort von 193.242.155.226: Bytes=32 Zeit=76ms TTL=50
Antwort von 193.242.155.226: Bytes=32 Zeit=55ms TTL=50
Antwort von 193.242.155.226: Bytes=32 Zeit=53ms TTL=50
Antwort von 193.242.155.226: Bytes=32 Zeit=62ms TTL=50

Ping-Statistik für 193.242.155.226:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0
    (0% Verlust),
    Ca. Zeitangaben in Millisek.:
        Minimum = 53ms, Maximum = 76ms, Mittelwert = 61ms

C:\>
  
```

Der SiteManager unterstützt die Verwendung eines DNS-Namens als GateManager-Server-Ziel, aber es wird empfohlen, die IP-Adresse zu verwenden, um nicht von einem DNS-Server im Netzwerk abhängig zu sein.

9.2.2 Web-Proxy issues

Ein Web-Proxy wird oft verwendet, um den Internetzugang zu validieren. Der SiteManager ist so konzipiert, dass er über einen Web-Proxy auf das Internet und den GateManager zugreifen kann.

Wenn der SiteManager seine Uplink-IP-Adresse über DHCP erhält, betrachtet er das Standard-Gateway automatisch als Web-Proxy einschließlich Web-Proxy Auto-Discovery (WPAD). Er extrahiert also automatisch die Informationen aus der vom DHCP-Server verteilten PAC-Datei.

Es gibt jedoch 2 Szenarien, die eine manuelle Konfiguration des Web-Proxys im SiteManager Konfigurationsmenü erfordern:

- 1) Wenn der SiteManager seine IP-Adresse zwar über DHCP erhält, der Web-Proxy jedoch die Eingabe eines Passworts erfordert.
- 2) Wenn der SiteManager seine Uplink-IP-Adresse nicht über DHCP erhält (sondern statisch konfiguriert ist), kann der SiteManager die Web-Proxy-Einstellungen nicht automatisch erkennen.

Diese Einstellungen müssen daher manuell in der SiteManager-Benutzeroberfläche unter GateManager → Allgemein eingegeben werden.

Detaillierte Informationen zur Konfiguration der Web-Proxy-Einstellungen sind in der Online-Hilfe des SiteManagers zu finden.

Dabei ist zum Beispiel zu beachten, dass der URL-Pfad zur WPAD-Datei im Feld Web-Proxy-Adresse manuell festgelegt werden kann, was nützlich ist, wenn keine Web-Proxy-Informationen von einem DHCP-Server erhalten wurde.

Wenn ein NTLM-basierter Web-Proxy verwendet wird, kann auch das Konto im Feld Web-Proxy-Konto im Format "DOMAIN\USER" eingegeben werden.

Information:

Es kann vorkommen, dass der LinkManager Zugriff auf den GateManager erhält, obwohl das NTLM-Konto im LinkManager nicht konfiguriert ist. Dies kann darauf zurückzuführen sein, dass der PC selbst bereits vom Proxy zugelassen wurde.

9.2.3 Weitere Möglichkeiten

Wenn der SiteManager korrekt konfiguriert ist, noch Folgendes im Netzwerk überprüfen.

Diese Dinge müssen in der Regel von der lokalen IT-Administration überprüft werden und erfordern definitiv eine Person aus der IT-Abteilung, um Änderungen vorzunehmen:

- 1) Muss die Firewall eine Ausnahme für die Quell-IP eines unbekannten Geräts in die Firewall eingeben, um auf das Internet zugreifen zu können?
Wenn ja, die IP-Adresse des SiteManager Uplink1 Ports eingeben.
- 2) Erfordert die Firewall eine Ausnahme für die MAC-Adresse eines Geräts, die in die Firewall eingegeben werden muss, um auf das Internet zugreifen zu können?
Wenn ja, die MAC-Adresse des Uplink1-Ports des SiteManagers eingeben. Es ist zu beachten, dass die Uplink1-MAC-Adresse in der Regel um eins höher ist als die DEV1-MAC-Adresse, die auch die SiteManager-Seriennummer ist. Wenn der Appliance Launcher also z. B. 00:05:B6:00:97:6C an der DEV-Schnittstelle erkennt, lautet die Uplink-MAC-Adresse 00:05:B6:00:97:6D. Die MAC-Adresse überprüfen, indem die DHCP-Lease-Tabelle des Netzwerks überprüft wird, oder Uplink1 anpingen und den ARP-Cache überprüfen.
- 3) Erfordert die Firewall oder der Proxy, dass der DNS eines Geräts als vertrauenswürdig eingestuft wird (z. B. durch Reverse-Lookup geprüft)?
Da es sich bei SiteManager nicht um einen Windows-PC handelt, muss möglicherweise eine besondere Ausnahme gemacht werden.
- 4) Muss eine Ausnahme für die Ziel-IP, auf die ein Gerät zuzugreifen versucht, in die Firewall eingetragen werden?
IP-Adresse des GateManager-Servers eingeben.
- 5) Verlangt die Firewall die Verwendung von DNS-Namen, die lokal aufgelöst werden?
In diesem Fall muss der DNS-Name des GateManagers beim DNS-Server eingetragen werden (z. B. "gm02.secomea.com", und mit seiner IP-Adresse 193.242.155.112 angegeben werden). Anschließend muss sichergestellt werden, dass der SiteManager mit der IP-Adresse des DNS-Servers konfiguriert wird. Diese wird in der Regel automatisch über DHCP verteilt, muss aber für die Schnittstelle Uplink1 manuell eingegeben werden, wenn diese mit einer festen IP-Adresse konfiguriert ist.
- 6) Wenn die Firewall so konfiguriert ist, dass sie KEINEN "rekey" bei einer TLS-Sitzung toleriert, kann der SiteManager abgewiesen werden, falls die Firewall das Erstellen der ursprünglichen Sitzung nicht mitbekommen hat. Dies ist darauf zurückzuführen, dass der SiteManager beim Verbindungsaufbau zu einem GateManager 4x Server ein Re-Keying verwendet und die Firewall daher keine zwischengespeicherte Sitzungs-ID verwenden kann.
Dafür kann auch die Protokollmeldungen der Firewall überprüft werden (falls aktiviert). Auf einer Fortinet-Firewall würde die Meldung z. B. lauten: "Die SSL-Sitzung wurde blockiert, weil die Sitzungs-ID unbekannt war".
In diesem Fall muss in der Firewall eine Ausnahme hinzugefügt werden, damit SiteManager diese Prüfung umgehen kann.

Information:

Dies ist kein Problem für GateManager 5, sondern NUR für SiteManager, die sich mit GateManager 4x Servern verbinden.

10 Normen und Zulassungen

SiteManager



Konformitätserklärung

[Homepage](#) > [Downloads](#) > [Industrial IoT](#) > [Remote Maintenance](#) > [SiteManager](#)

11 Begriffe und Abkürzungen

Abkürzung	Begriff	Bedeutung
DMZ	Demilitarized Zone	Ein Computernetz mit sicherheitstechnisch kontrollierten Zugriffsmöglichkeiten auf die daran angeschlossenen Server.
ERP	Enterprise-Resource-Planning	Bezeichnet meistens die eingesetzte Software für die Einsatzplanung der in einem Unternehmen vorhandenen Ressourcen aller Art (z. B. SAP)
FQDN	Fully-Qualified Domain Name	Ein vollständig angegebener Rechnername, der als vollqualifizierter Name einer Domain (z. B. remote.companyname.com) dargestellt wird. Der FQHN bezeichnet einen bestimmten Rechner eindeutig.
SCADA	Supervisory Control and Data Acquisition	Überwachen und Steuern technischer Prozesse mittels eines Computer-Systems.

12 Anhang - abgekündigte Module

Information:

Die in diesem Abschnitt erwähnten Produkte dienen nur zu Referenzzwecken bei bereits bestehender Verwendung.

12.1 GateManager - 0RMGM.4260-TP

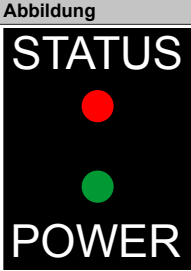
Der GateManager 0RMGM.4260-TP ist nicht mehr von B&R verfügbar.

12.1.1 Technische Daten

Bestellnummer	0RMGM.4260-TP
Allgemeines	
B&R ID-Code	0xE8EB
Funktionalität	
Anzahl der unterstützten SiteManager	bis zu 2000
Netzanschluss	
Netzeingangsspannung	100 bis 240 V
Frequenz	50 bis 60 Hz
Anschlussleistung	36 W
Controller	
Prozessor	
Typ	Dual Core Intel Atom™ C2358
Taktfrequenz	1,7 GHz
Flash	32 GByte
DRAM	2 GByte
Schnittstellen	
Schnittstelle IF1	
Typ	CONSOLE
Ausführung	1x RJ45 geschirmt
Leitungslänge	max. 100 m zwischen 2 Knoten (Segmentlänge)
Übertragungsrate	max. 10/100/1000 MBit/s
Schnittstelle IF2	
Typ	USB 2.0
Schnittstelle IF3	
Typ	USB 2.0
Schnittstelle IF4	
Typ	LAN
Ausführung	1x RJ45 geschirmt
Übertragungsrate	max. 10/100/1000 MBit/s
Schnittstelle IF5	
Typ	WAN
Ausführung	1x RJ45 geschirmt
Übertragungsrate	max. 10/100/1000 MBit/s
Schnittstelle IF6	
Typ	AUX1
Ausführung	1x RJ45 geschirmt
Übertragungsrate	max. 10/100/1000 MBit/s
Schnittstelle IF7	
Typ	AUX2
Ausführung	1x RJ45 geschirmt
Übertragungsrate	max. 10/100/1000 MBit/s
Umgebungsbedingungen	
Temperatur	
Betrieb	0 bis 40°C
Mechanische Eigenschaften	
Abmessungen	
Breite	177 mm
Höhe	44 mm
Tiefe	145,5 mm
Gewicht	1,2 kg

Tabelle 13: 0RMGM.4260-TP - Technische Daten

12.1.2 Status-LEDs

Abbildung	LED	Farbe	Status	Beschreibung
	STATUS	Rot	Schnell blinkend (0,5 s EIN, 0,5 s AUS) Langsam blinkend (2 s EIN, 2 s AUS)	Booten Überprüfung des Dateisystems. Die Überprüfung des Dateisystems erfolgt bei jedem 20. Booten (oder alle 180 Tage). Die Überprüfung kann bis zu 5 Minuten dauern.
	POWER	Grün	Ein	Achtung! Mögliche Beschädigung des Gerätes! Während der Überprüfung des Dateisystems das Modul nicht von der Spannungsversorgung trennen! Mit Strom versorgt.

12.1.3 Bedien- und Anschlusselemente

12.1.3.1 Reset-Taster

Die Reset-Taste hat derzeit keine Wirkung, ist aber für zukünftige Verwendung reserviert.

12.1.3.2 Ethernet Schnittstellen

Schnittstellen sind 10/100/1000 MBit/s - fähig. Standard CAT5-Kabel oder höher verwenden, um eine Verbindung zu einem geschalteten Netzwerk herzustellen. Die Schnittstellen erkennen Auskreuzungen automatisch, so dass, bei Direktanbindung an einen PC (z. B. für Konfiguration), das beiliegende ausgekreuzte Kabel oder ein Standard-Kabel verwendet werden können.

Die WAN-Schnittstelle wird für den normalen Betrieb verwendet. Die LAN-Schnittstelle wird nur für Debugging und spezielle Konfigurationen verwendet.

Die beiden Schnittstellen AUX1 und AUX2 haben derzeit keine Wirkung, sind aber für zukünftige Verwendung reserviert.

12.1.3.3 USB-Schnittstellen

USB-Schnittstellen werden für Sichern und Wiederherstellung und/oder den Anschluss eines optionalen externen USB-Modems verwendet, das für SMS-Benachrichtigungen und/oder Login-Authentifizierung verwendet wird.

Information:

SMS-Unterstützung kann durch die Konfiguration eines externen SMS-Gateway erhalten werden.

Siehe dazu [Configuring SMS Gateways on GateManager](#).

Die Schnittstellen unterstützen ein USB 2.0 kompatibles Flash-Laufwerk, das mit FAT 32 formatiert ist. Empfohlene Größe ist 4 GB oder mehr.

12.1.3.4 Spannungsversorgung

Das mitgelieferte Netzteil an einer 100 - 240 V und 50 - 60 Hz Steckdose verwenden.

12.2 SiteManager 0RMSM 11x5

12.2.1 SiteManager 11x5

Funktionell und bedienungsmäßig sind diese Produkte mit den Modellen 13x5 identisch.

12.2.1.1 Technische Daten

Bestellnummer	0RMSM1115	0RMSM1135	0RMSM1135.4G	0RMSM1145
Allgemeines				
B&R ID-Code	0xE8E9	0xE8EA	0x29BE	0xE908
Reset-Taster	Ja			
Status-LED	Versorgungsspannung Status Verbindung LinkManager	Versorgungsspannung Status Verbindung LinkManager drahtlose Verbindung		
Leistungsaufnahme	max. 3 W	max. 5 W		max. 3 W
Funktionalität				
Datenübertragung / Frequenzbereich				
Integriertes Breitbandmodem				
LTE-Band	-		Siehe 0RMSM1335. 4G Bänder	-
WCDMA/UMTS	-		Siehe 0RMSM1335. 4G Bänder	-
WCDMA	-	850 MHz 1900 MHz 2100 MHz	-	
GPRS/EDGE	-	850 MHz 900 MHz 1800 MHz 1900 MHz	B2 (1900) B3 (1800) B5 (850) B8 (900)	-
Integriertes WiFi Modul	-			2400 MHz für Client mode
Controller				
Prozessor				
Typ	ARM Cortex A5			
Taktfrequenz	563 MHz			
Schnittstellen				
Schnittstelle IF1				
Typ	Ethernet UPLINK1			
Ausführung	RJ45 geschirmt			
Leitungslänge	max. 100 m zwischen 2 Knoten (Segmentlänge)			
Übertragungsrate	max. 10/100 MBit/s			
Übertragung				
Physik	10BASE-T/100BASE-TX			
Halbduplex	Ja			
Vollduplex	Ja			
Autonegotiation	Ja			
Auto-MDI/MDIX	Ja			
Schnittstelle IF2				
Typ	DEV1			
Ausführung	RJ45 geschirmt			
Übertragungsrate	max. 10/100 MBit/s			
Schnittstelle IF3				
Typ	-	3G/GPRS	4G/3G/GPRS	-
Ausführung	-	SMA female		-
Übertragungsrate	-		Downlink: 50 MBit/ s (10 MHz Bandweite) Uplink: 25 MBit/s (10 MHz Bandweite)	-
Schnittstelle IF4				
Typ	-			WiFi
Ausführung	-			RP-SMA female
Elektrische Eigenschaften				
Nennspannung	12 bis 24 VDC			
Schutzart nach EN 60529	IP20			
Umgebungsbedingungen				
Temperatur				
Betrieb	-25 bis 60 °C	-25 bis 45°C	-25 bis 60 °C	-25 bis 60°C
Luftfeuchtigkeit				
Betrieb	5 bis 95%			
Lagerung	5 bis 95%			
Transport	5 bis 95%			
Mechanische Eigenschaften				
Material	Aluminium			

Bestellnummer	0RMSM1115	0RMSM1135	0RMSM1135.4G	0RMSM1145
Abmessungen				
Breite			32 mm	
Höhe			107 mm	
Tiefe			97 mm	
Gewicht			0,5 kg	

0RMSM1135.4G Bänder

	LTE-Bänder	WCDMA/UMTS-Bänder
B1 (FDD 2100) IMT	X	X
B2 (FDD 1900) PCS	X	X
B3 (1800 +) DCS	X	
B4 (1700) AWS	X	X
B5 (850) CLR, US Korea etc	X	X
B6 (850) Japan #1		X
B7 (2600) IMT-E	X	
B8 (900) E-GSM	X	X
B12 (700) US	X	
B13 (700c) USMH, LSMH US	X	
B18 (800 or 850?) Japan #4	X	
B19 (800 or 850?) Japan #5	X	X
B20 (800) Digital Dividend	X	
B25 (1900 G Block)	X	
B26 (850+) Extended CLR	X	
B28 (700 APT) APAC	X	
B34 (TDD)	X	
B38 (TDD 2600) IMT-E	X	
B39 (TDD 1900 +) China	X	
B40 (TDD 2300) China	X	
B41 (TDD 2500) BRS/EBS	X	
B66 (TDD)	X	

12.2.2 SiteManager 4G - Regionalvarianten

Der SiteManager 4G - Regionalvarianten sind nicht mehr von B&R verfügbar.

12.2.2.1 Technische Daten

Information:

Die Variante SiteManager 1135.4G-xx ist jeweils in einer Ausprägung für die Regionen USA, EMEA, Japan und China verfügbar. Jede Ausprägung unterstützt dedizierte Frequenzen/Bänder sowie Mobilfunkanbieter (Der SiteManager 0RMSM1135.4G-US funktioniert jedoch nicht mit einer Verizon SIM-Karte). Alle SiteManager 1135.4G-xx unterstützen auch 3G, sollte in einer Region 4G noch nicht verfügbar sein.

Bestellnummer	0RMSM1135.4G-CN	0RMSM1135.4G-EU	0RMSM1135.4G-JP	0RMSM1135.4G-US
Allgemeines				
B&R ID-Code	0xEE28	0xEE27	0xF241	0xEE26
Reset-Taster	Ja			
Status-LED	Versorgungsspannung Status Verbindung LinkManager drahtlose Verbindung			
Leistungsaufnahme	max. 5 W			

Tabelle 14: 0RMSM1135.4G-CN, 0RMSM1135.4G-EU, 0RMSM1135.4G-JP, 0RMSM1135.4G-US - Technische Daten

Bestellnummer	0RMSM1135.4G-CN		0RMSM1135.4G-EU	0RMSM1135.4G-JP	0RMSM1135.4G-US
Funktionalität					
Datenübertragung / Frequenzbereich					
Integriertes Breitbandmodem					
LTE Band	B1 (FDD 2100) IMT B3 (1800 +) DCS B5 (850) CLR, US Korea etc. B7 (2600) IMT-E B8 (900) E-GSM B38 (TDD 2600) IMT-E B39 (TDD 1900 +) China B40 (TDD 2300) China B41 (TDD 2500) BRS/EBS	B1 (FDD 2100) IMT B3 (1800 +) DCS B7 (2600) IMT-E B8 (900) E-GSM B20 (800) Digital Dividend B38 (TDD 2600) IMT-E B40 (TDD 2300) China	B1 (FDD 2100) IMT B3 (1800 +) DCS B8 (900) E-GSM B18 (800 or 850?) Japan #4 B19 (800 or 850?) Japan #5	B2 (FDD 1900) PCS B4 (1700) AWS B5 (850) CLR, US Korea etc. B17 (700bc) USMH, LSMH US	
WCDMA/UMTS	B1 (FDD 2100) IMT B8 (900) E-GSM	B1 (2100) IMT B8 (900) E-GSM	B1 (2100) IMT B6 (850) Japan #1 B8 (900) E-GSM	B2 (1900) PCS B5 (850) CLR	
GPRS/EDGE	B3 (1800) B8 (900)	B3 (1800) B8 (900)			-
Controller					
Prozessor					
Typ		ARM Cortex A5			
Taktfrequenz		563 MHz			
Schnittstellen					
Schnittstelle IF1					
Typ		Ethernet UPLINK1			
Ausführung		RJ45 geschirmt			
Leitungslänge		max. 100 m zwischen 2 Knoten (Segmentlänge)			
Übertragungsrate		max. 10/100 MBit/s			
Übertragung					
Physik		10BASE-T/100BASE-TX			
Halbduplex		Ja			
Vollduplex		Ja			
Autonegotiation		Ja			
Auto-MDI/MDIX		Ja			
Schnittstelle IF2					
Typ		DEV1			
Ausführung		RJ45 geschirmt			
Übertragungsrate		max. 10/100 MBit/s			
Schnittstelle IF3					
Typ		4G/3G/GPRS			
Ausführung		SMA female			
Übertragungsrate		Downlink: 50 MBit/s (10 MHz Bandweite) Uplink: 25 MBit/s (10 MHz Bandweite)			
Elektrische Eigenschaften					
Nennspannung		12 bis 24 VDC			
Einsatzbedingungen					
Schutzart nach EN 60529		IP20			
Umgebungsbedingungen					
Temperatur					
Betrieb		-25 bis 45°C			
Luftfeuchtigkeit					
Betrieb		5 bis 95%			
Lagerung		5 bis 95%			
Transport		5 bis 95%			
Mechanische Eigenschaften					
Material		Aluminium			
Abmessungen					
Breite		32 mm			
Höhe		107 mm			
Tiefe		97 mm			
Gewicht		0,5 kg			

Tabelle 14: 0RMSM1135.4G-CN, 0RMSM1135.4G-EU, 0RMSM1135.4G-JP, 0RMSM1135.4G-US - Technische Daten

LTE-Bänder

	0RMSM1135.4G-CN	0RMSM1135.4G-EU	0RMSM1135.4G-JP	0RMSM1135.4G-US
B1 (FDD 2100) IMT	X	X	X	
B2 (FDD 1900) PCS				X
B3 (1800 +) DCS	X	X	X	
B4 (1700) AWS				X
B5 (850) CLR, US Korea etc	X			X
B7 (2600) IMT-E	X	X		
B8 (900) E-GSM	X	X	X	
B17 (700bc) USMH, LSMH US				x
B18 (800 or 850?) Japan #4			X	
B19 (800 or 850?) Japan #5			X	
B20 (800) Digital Dividend		X		
B38 (TDD 2600) IMT-E	X	X		
B39 (TDD 1900 +) China	X			
B40 (TDD 2300) China	X	X		
B41 (TDD 2500) BRS/EBS	X		X	

WCDMA/UMTS-Bänder

Band	0RMSM1135.4G-CN	0RMSM1135.4G-EU	0RMSM1135.4G-JP	0RMSM1135.4G-US
B1 (FDD 2100) IMT	X	X	X	
B2 (FDD 1900) PCS				X
B5 (850) CLR, US Korea etc.				X
B6 (850) Japan #1			X	
B8 (900) E-GSM	X	X	X	