

WaveNet

Handbuch

03.06.2026

Inhaltsverzeichnis

1.	Allgemeine Sicherheitshinweise.....	4
2.	Produktspezifische Sicherheitshinweise	6
3.	Bedeutung der Textformatierung.....	8
4.	Weiterführende Dokumentation.....	9
5.	WaveNet-System	10
5.1	Übertragungswege	14
5.2	Artikelnummern	15
5.2.1	RouterNodes	15
5.2.2	LockNodes.....	17
5.2.3	Zubehör.....	19
5.3	Geräte	21
5.3.1	Computer	22
5.3.2	RouterNodes	22
5.3.3	LockNodes.....	22
5.4	Funknetzwerk	23
5.4.1	Segmente	24
5.4.2	Signalqualität.....	25
5.4.3	Herausforderungen in Funknetzwerken.....	27
5.5	Sicherheit und Alarme.....	29
5.5.1	Verschlüsselung (WaveNet)	29
5.5.2	Überwachung der Geräte im Netzwerk.....	30
5.5.3	Alarme	31
5.6	WaveNet und LSM.....	32
5.7	Firmware.....	32
5.7.1	Firmware auslesen	32
5.7.2	Firmware aktualisieren	34
6.	WaveNet-Manager.....	38
6.1	Systemanforderungen.....	38
6.2	Entpacken, Update und Start der Software	38
6.2.1	Entpacken.....	38
6.2.2	Update.....	39
6.2.3	Start.....	40
6.2.4	Passwort.....	42
6.3	Firmware-Informationen	42
6.4	Verwaltung.....	44
6.4.1	Grundlagen.....	44
6.4.2	Autokonfiguration	47

6.4.3	Geräte finden und hinzufügen	52
6.4.4	I/O-Konfiguration und Schutzfunktionen	74
6.4.5	RingCast	103
6.4.6	Gerätespezifische Einstellungen	157
6.5	Fehlerbehebung	161
6.5.1	Signalqualität verbessern	161
6.5.2	Geräteneustart	168
6.5.3	Gerät neu programmieren oder ersetzen.....	172
6.5.4	netcfg.xml löschen	176
6.5.5	Zurücksetzen/Löschen.....	177
6.5.6	Virtual Store überprüfen und beheben.....	188
6.6	Wartung	189
6.6.1	Übersicht	190
6.6.2	Signalqualität prüfen.....	192
6.6.3	Erreichbarkeit testen (WaveNet)	195
6.6.4	Erreichbarkeit testen (LSM).....	198
6.6.5	Geräte-Funktionstest.....	199
6.6.6	IO-Status und LockNode-Reaktionsfähigkeit	200
7.	Batteriemanagement.....	205
7.1	LockNodes.....	205
7.1.1	Batteriewechsel bei integrierten LockNodes.....	211
7.1.2	Batteriewechsel bei externen LockNodes	212
7.2	Schließungen	212
8.	Signalisierung des Betriebszustands	214
8.1	In der LSM.....	225
9.	Technische Daten.....	228
9.1	WaveNet allgemein.....	228
9.2	RouterNodes.....	230
9.3	LockNodes	232
10.	Hilfe und weitere Informationen.....	235

1. Allgemeine Sicherheitshinweise

Signalwort: Mögliche unmittelbare Auswirkungen bei Nichtbeachtung

WARNUNG: Tod oder schwere Verletzung (möglich, aber unwahrscheinlich)

ACHTUNG: Sachschäden oder Fehlfunktionen

HINWEIS: Geringe oder keine



WARNUNG

Versperrter Zugang

Durch fehlerhaft montierte und/oder programmierte Komponenten kann der Zutritt durch eine Tür versperrt bleiben. Für Folgen eines versperrten Zutritts wie Zugang zu verletzten oder gefährdeten Personen, Sachschäden oder anderen Schäden haftet die SimonsVoss Technologies GmbH nicht!

Versperrter Zugang durch Manipulation des Produkts

Wenn Sie das Produkt eigenmächtig verändern, dann können Fehlfunktionen auftreten und der Zugang durch eine Tür versperrt werden.

- Verändern Sie das Produkt nur bei Bedarf und nur in der Dokumentation beschriebenen Art und Weise.

ACHTUNG

Störung des Betriebs durch Funkstörung

Dieses Produkt kann unter Umständen durch elektromagnetische oder magnetische Störungen beeinflusst werden.

- Montieren bzw. platzieren Sie das Produkt nicht unmittelbar neben Geräten, die elektromagnetische oder magnetische Störungen verursachen können (Schaltnetzteile!).

Störung der Kommunikation durch metallische Oberflächen

Dieses Produkt kommuniziert drahtlos. Metallische Oberflächen können die Reichweite des Produkts erheblich reduzieren.

- Montieren bzw. platzieren Sie das Produkt nicht auf oder in der Nähe von metallischen Oberflächen.



HINWEIS

Bestimmungsgemäßer Gebrauch

SimonsVoss-Produkte sind ausschließlich für das Öffnen und Schließen von Türen und vergleichbaren Gegenständen bestimmt.

- Verwenden Sie SimonsVoss-Produkte nicht für andere Zwecke.

Abweichende Zeiten bei G2-Schließungen

Die interne Zeiteinheit der G2-Schließungen hat eine technisch bedingte Toleranz von bis zu ± 15 Minuten pro Jahr.

- Programmieren Sie zeitkritische Schließungen regelmäßig nach.

Qualifikationen erforderlich

Die Installation und Inbetriebnahme setzt Fachkenntnisse voraus.

- Nur geschultes Fachpersonal darf das Produkt installieren und in Betrieb nehmen.

Änderungen bzw. technische Weiterentwicklungen können nicht ausgeschlossen und ohne Ankündigung umgesetzt werden.

Die deutsche Sprachfassung ist die Originalbetriebsanleitung. Andere Sprachen (Abfassung in der Vertragssprache) sind Übersetzungen der Originalbetriebsanleitung.

Lesen Sie alle Anweisungen zur Installation, zum Einbau und zur Inbetriebnahme und befolgen Sie diese. Geben Sie diese Anweisungen und jegliche Anweisungen zur Wartung an den Benutzer weiter.

2. Produktspezifische Sicherheitshinweise



WARNUNG

Personen- oder Sachschäden durch nichtredundantes Sicherheitskonzept

Die Schutzfunktionen Ihres WaveNet-Systems sind nur ein Bestandteil eines Sicherheitskonzepts. Sie sind nicht als einzige Absicherung gegen Gefahren wie Brand, Einbruch oder ähnliches geeignet.

1. Verwenden Sie redundante Systeme zur Absicherung Ihrer individuellen Risiken (Einbruchsmeldeanlagen, Brandmeldeanlagen und ähnliche).
2. Lassen Sie durch einen technischen Risikomanager (Certified Security Manager oder vergleichbar) ein Sicherheitskonzept erstellen und bewerten.
3. Beachten Sie insbesondere relevante Vorschriften zu Flucht- und Rettungswegen.

Beeinträchtigung oder Ausfall von Schutzfunktionen durch geänderte Bedingungen

Die Aktivierung der Schutzfunktionen im RingCast basiert auf kabellosen Verbindungen und Ethernetverbindungen. Insbesondere kabellose Verbindungen können durch sich ändernde Umgebungsbedingungen beeinflusst werden (siehe [Funknetzwerk \[► 23\]](#) und [Herausforderungen in Funknetzwerken \[► 27\]](#)). Damit wird auch die Aktivierung der Schutzfunktionen im RingCast beeinflusst und die Sicherheit von Personen und Sachwerten, die beispielsweise durch die Schutzfunktionen im RingCast zusätzlich abgesichert werden, kann gefährdet sein.

1. Testen Sie die Schutzfunktionen mindestens einmal pro Monat (siehe [RingCast-Funktionstest \[► 151\]](#)).
2. Beachten Sie ggfs. auch weitere Richtlinien bzw. Verordnungen, die für Ihre Schließanlage relevant sind (insbesondere für Flucht- und Rettungswege sowie Brandschutz. Sie stellen die Erfüllung dieser Richtlinien und Verordnungen in Eigenverantwortung sicher.).

Veränderung des Ablaufs von Notfallfunktionen durch Fehlfunktionen

SimonsVoss und "Made in Germany" stehen für höchste Sicherheit und Zuverlässigkeit. In Einzelfällen können Fehlfunktionen Ihrer Geräte dennoch nicht ausgeschlossen werden. Damit wird möglicherweise die Sicherheit von Personen und Sachwerten, die durch die Schutzfunktionen im RingCast zusätzlich abgesichert werden, gefährdet.

1. Testen Sie Ihre Geräte mindestens einmal pro Monat (siehe [Geräte-Funktionstest \[► 199\]](#). Nach anderen Vorschriften bezüglich Ihres Gesamtsystems können auch kürzere Abstände erforderlich sein).
2. Testen Sie die Schutzfunktionen mindestens einmal pro Monat (siehe [RingCast-Funktionstest \[► 151\]](#)).

**HINWEIS****Redundante Absicherung der Netzwerkinfrastruktur**

Zusätzlich zu den SimonsVoss-Sicherheitsmaßnahmen muss auch die Netzwerkinfrastruktur, in der Sie das WaveNet nutzen, aktuellen Sicherheitsstandards entsprechen.

1. Sie erreichen diese Sicherheitsstandards beispielsweise durch: Virtuelle Netzwerke oder aktive Netzwerküberwachung (Liste erhebt keinen Anspruch auf Vollständigkeit).
2. Sprechen Sie mit Ihrem IT-Infrastrukturspezialisten.

Haftungsausschluss für Folgen geänderter Umgebungsbedingungen

Umgebungsbedingungen können sich ändern und trotz regelmäßiger Tests den RingCast und dessen Schutzfunktionen behindern (siehe [Funknetzwerk \[► 23\]](#) und [Herausforderungen in Funknetzwerken \[► 27\]](#)). Weder die SimonsVoss Technologies GmbH noch das Produkt selbst haben Einfluss auf sich ändernde Umgebungsbedingungen. Die Konstanz der Umgebungsbedingungen ist eine Funktionsvoraussetzung. Damit kann es durch den Ausfall von Schutzfunktionen zu Personen- und Sachschäden kommen. Die SimonsVoss Technologies GmbH übernimmt keine Haftung für Personen- und Sachschäden infolge von geänderten Umgebungsbedingungen.

1. Erfassen Sie bei der durchzuführenden Projektierung die aktuellen Umgebungsbedingungen und die aktuelle Signalqualität (siehe [Signalqualität \[► 25\]](#) und [Signalqualität prüfen \[► 192\]](#), vgl. Snapshot).
2. Stellen Sie durch kontinuierliche Überwachung sicher, dass sich die Umgebungsbedingungen nicht unvorhergesehen ändern.
3. Erfassen Sie bei der durchzuführenden Abnahme die aktuellen Umgebungsbedingungen und die aktuelle Signalqualität (finaler Snapshot).

3. Bedeutung der Textformatierung

Diese Dokumentation verwendet Textformatierung und Gestaltungselemente, um das Verständnis zu erleichtern. Die Tabelle erklärt die Bedeutung möglicher Textformatierungen:

Beispiel	Schaltfläche
☒ Beispiel ☐ Beispiel	Checkbox
☒ Beispiel	Option
[Beispiel]	Registerkarte/Tab
"Beispiel"	Name eines angezeigten Fensters
Beispiel	Obere Programmleiste
Beispiel	Eintrag in der ausgeklappten oberen Programmleiste
Beispiel	Kontextmenü-Eintrag
▼ Beispiel	Name eines Dropdown-Menüs
"Beispiel"	Auswahlmöglichkeit in einem Dropdown-Menü
"Beispiel"	Bereich
<i>Beispiel</i>	Feld
<i>Beispiel</i>	Name eines (Windows-)Dienstes
<i>Beispiel</i>	Befehle (z.B. Windows-CMD-Befehle)
Beispiel	Datenbank-Eintrag
[Beispiel]	MobileKey-Typauswahl

4. Weiterführende Dokumentation

Ihr WaveNet verbindet die Verwaltungssoftware (Locking System Management, kurz LSM) und Ihre Schließungen. Dazu finden Sie auf der SimonsVoss-Website (<https://www.simons-voss.com/>) im Downloadbereich weitere Informationen.

- Detaillierte Informationen zur LSM finden Sie im LSM-Handbuch, insbesondere Realisierung gängiger WaveNet basierter Aufgaben in LSM.
- Detaillierte Informationen zu den Schließungen finden Sie in den jeweiligen Handbüchern und Kurzanleitungen.

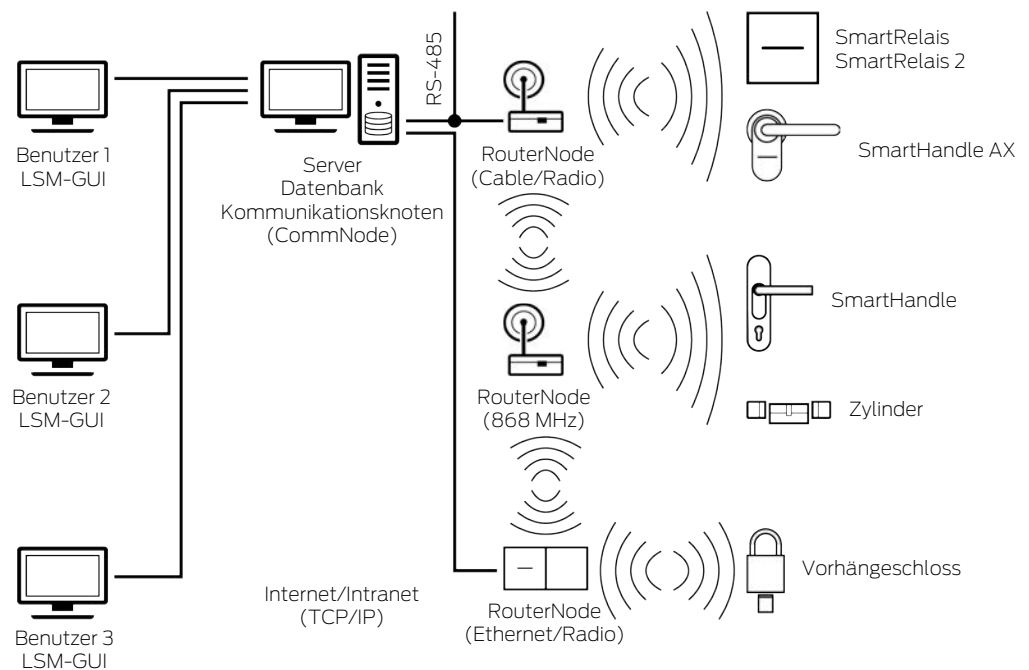
5. WaveNet-System

Sie können SimonsVoss-Schließungen (Schließzylinder, SmartHandles und SmartRelais) auf mehrere Arten vernetzen und so zentral verwalten. Das WaveNet ist die fortschrittlichste und komfortabelste Art, größere Schließanlagen mit vielen Schließungen zu verwalten und zu überwachen.

WaveNet (online)		Virtuelle Vernetzung (virtuell)	Keine Vernetzung (offline)
Funktionsprinzip	Übertragung der Daten mit vernetzten WaveNet-Geräten (siehe <i>Übertragungswege</i> [► 14] und <i>Geräte</i> [► 21]).	Übertragung der Daten mit Identifikationsmedien (außer Programmierdaten).	Übertragung der Daten mit Programmiergeräten.
Ausbreitung	WaveNet-Geräte sind über verschiedene Übertragungsmedien verbunden. Daten aller Art werden mithilfe dieser Übertragungsmedien übermittelt.	Im virtuellen Netzwerk werden bestimmte Daten mithilfe eines Gateways auf die Identifikationsmedien übertragen (Einträge in die Blacklist). Wenn Sie diese Identifikationsmedien an einer virtuell vernetzten Schließung betätigen, dann werden die Daten auf die Schließung übertragen.	Schließungen, die nicht vernetzt sind, können nur mit dem Programmiergerät Daten austauschen. Sie müssen mit dem Programmiergerät zu den Schließungen gehen.
Programmieraufwand	Gering.	Gering.	Aufwand hängt von Größe der Schließanlage ab. ■ Kleine Schließanlage: Geringer Aufwand. ■ Mittlere Schließanlage: Mittlerer Aufwand. ■ Große Schließanlage: Großer Aufwand.

WaveNet (online)		Virtuelle Vernetzung (virtuell)	Keine Vernetzung (offline)
Übertragungsgeschwindigkeit des Datenaustauschs	Unmittelbar. Datenaustausch mit verschiedenen Übertragungsmedien.	Geschwindigkeit zwischen Gateway und Schließungen stark abhängig von Nutzungsdichte der Schließungen. Identifikationsmedien sind Übertragungsmedium - ohne Identifikation keine Datenübertragung.	Langsam.
Zentrale Aktivierung/Deaktivierung von Schließungen	Möglich.	Nicht möglich.	Nicht möglich.
Aktivierung/Deaktivierung zentral nachverfolgbar	Möglich.	Nicht möglich.	Nicht möglich.
Fernöffnung	Möglich.	Nicht möglich.	Nicht möglich.
Fernüberwachung (Door-Monitoring)	Möglich.	Nicht möglich.	Nicht möglich.
Eventmanagement	Möglich.	Nicht möglich.	Nicht möglich.
Zutrittslisten zentral abrufbar	Möglich.	Nicht möglich (außer SREL 3).	Nicht möglich.
Software-/serverunabhängige Schutzfunktionen	Möglich.	Nicht möglich.	Nicht möglich.

WaveNet (online)		Virtuelle Vernetzung (virtuell)	Keine Vernetzung (offline)
Sofortige schließanlagenweite Reaktion auf kritische Situationen (Verfügbarkeit von Schutzfunktionen, siehe <i>I/O-Konfiguration und Schutzfunktionen</i> [► 74] und <i>RingCast</i> [► 103])	Möglich.	Nicht möglich.	Nicht möglich.



WaveNet ist ein eigenes Netzwerk, das Sie in der Gebäudeautomatisierung mit wenigen Kabeln einbauen und einsetzen können. Wenn Sie das WaveNet nachrüsten wollen, dann können Sie auch auf bereits existierende Gebäudenetzwerke wie ein LAN zurückgreifen. Deshalb eignet sich WaveNet nicht nur, wenn Sie Neubauten mit einer Schließanlage ausstatten (beispielsweise bei flexibel genutzten Raumeinheiten). WaveNet eignet sich auch besonders dann, wenn Sie Ihre bestehende 3060-Schließanlage von SimonsVoss in bereits bestehenden Gebäuden online verwalten und steuern wollen.

Alternativ zu einer Vollvernetzung können Sie die Vernetzungsarten frei miteinander kombinieren. Sie können zum Beispiel die Türen der Außenhaut (=Gebäudehülle) und besonders kritische Schließungen (beispielsweise an Serverraum-Türen) mit Ihrem WaveNet und alle weiteren Schließungen virtuell vernetzen.

Sie können in Abhängigkeit Ihrer individuellen Situation aus verschiedenen Geräten und Übertragungsmedien wählen (siehe [Übertragungswege](#) [► 14]). Die Übertragung der Daten im WaveNet ist vom Übertragungsmedium weitgehend unabhängig.

Mit Ihrem WaveNet und den IO-Funktionen (siehe [I/O-Konfiguration und Schutzfunktionen](#) [► 74]) verbessern Sie die Sicherheit bzw. die Vorkehrungen für Gefahrenlagen weit über das Niveau einer mechanischen Schließanlage hinaus.



HINWEIS

WaveNet-Schulung und Planung

WaveNet ist eine umfangreiche Lösung, die sehr gut auf Ihre Anforderungen abgestimmt werden kann. Wenn Sie das Potenzial Ihres WaveNets vollständig ausschöpfen wollen, dann können Sie eine WaveNet-Schulung der SimonsVoss Technologies GmbH besuchen. Sie können Ihr WaveNet-Projekt auch gemeinsam mit einem SimonsVoss-Techniker planen und von dessen langjähriger Erfahrung profitieren.

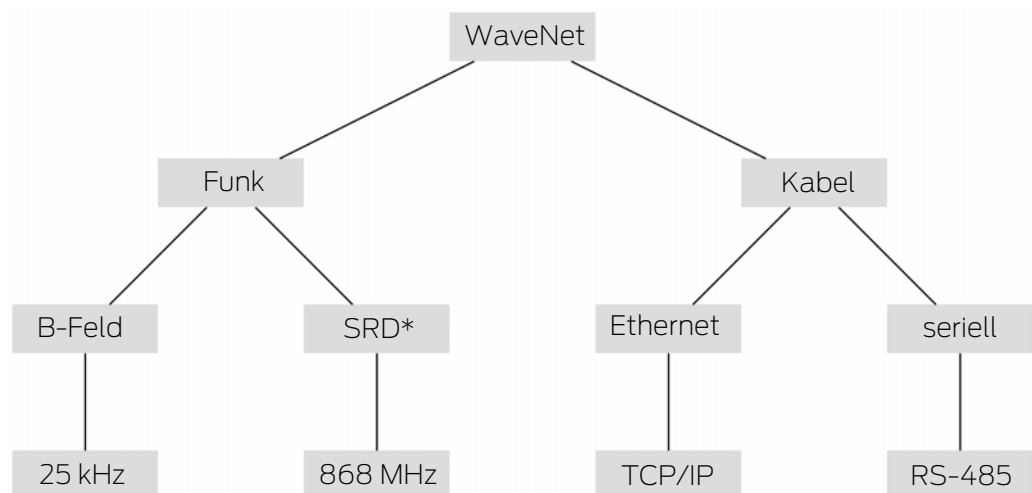
Weitere Informationen zu den Geräten, Schließungen und zur LSM-Software finden Sie in den jeweiligen Handbüchern und Kurzanleitung auf der SimonsVoss-Website (<https://www.simons-voss.com/>) im Downloadbereich unter Dokumente.

5.1 Übertragungswege

Das WaveNet überträgt Daten von den Schließungen zu einer zentralen Verwaltung, darunter:

- Berechtigungen
- Zustandsänderungen
- Schutzfunktionen

Sie können diese Daten über verschiedene Übertragungswege übertragen (Verfügbarkeit von Geräten für bestimmte Übertragungsmedien kann variieren).



*SRD=Short Range Device (Gerät mit kurzer Reichweite)

25 kHz	B-Feld zur Kommunikation zwischen: ■ Transpondern und Schließungen ■ Externen LockNodes und Schließungen
868 MHz	SRD-Feld zur Kommunikation zwischen: ■ RouterNodes und LockNodes ■ RouterNodes und RouterNodes
Ethernet	Ethernetverkabelung zur Kommunikation zwischen: ■ Computer und RouterNodes
RS-485	Busverkabelung für die Anbindung an das Netzwerk: ■ RouterNodes ■ Verkabelte LockNodes

5.2 Artikelnummern

Das WaveNet besteht aus verschiedenen Geräten. Sie können sich Ihr WaveNet nach Ihren Bedürfnissen zusammenstellen.

5.2.1 RouterNodes

Die Artikelnummern der RouterNodes sind aus Bausteinen (die sich je nach Produkteigenschaften ändern) zusammengesetzt.

WNM	.RN2	.E	R	.IO
■ WNM (WaveNet-Manager → Adressierung automatisch) ■ WN (WaveNet → Adressierung fix)	Typ des Nodes: ■ .RN2 (RouterNode 2) ■ .RN (RouterNode) ■ .RP (RepeaterNode) ■ .CN (CentralNode)	Unterstütztes Übertragungsmedium (Eingangssegment: Anschluss an Netzwerk): ■ .E (Ethernet → TCP/IP) ■ .R (Radio → 868 MHz) ■ .C (Cable → RS-485) ■ .W (WLAN → TCP/IP) ■ .U (USB → USB) ■ .S (Serial → RS-232)	Optional unterstütztes zweites Übertragungsmedium (Ausgangssegment: Anschluss an LockNodes): ■ R (Radio → 868 MHz) ■ C (Cable → RS-485)	Optional unterstützte Schutzfunktion: ■ .IO (Schutzrouter)

RouterNode-Portfolio

Die Tabelle zeigt, welche RouterNodes welche Übertragungsmedien unterstützen.

	868 MHz	WLAN	USB	Ethernet	RS-232	RS-485
WNM.RN2.ER.IO	✓			✓		
WNM.RN.R.IO	✓					
WNM.RN.CC.IO						✓
WNM.RN.CR.IO	✓					✓
WNM.RN.EC.IO				✓		✓
WN.RN.R (EOL)	✓					
WN.RN.CR (EOL)	✓					✓
WN.RN.CC (EOL)						✓

	868 MHz	WLAN	USB	Ethernet	RS-232	RS-485
WN.RN.ER (EOL)	✓			✓		
WN.RN.WR (EOL)	✓	✓				
WN.RN.EC (EOL)				✓		✓
WN.CN.UC (EOL)			✓			✓
WN.CN.UR (EOL)	✓		✓			
WN.RP.CC (EOL)						✓
WN.RN.WC (EOL)		✓				✓
WN.CN.SC (EOL)					✓	✓
WN.CN.SR (EOL)	✓				✓	

5.2.2 LockNodes

Die Artikelnummern der LockNodes sind aus Bausteinen (die sich je nach Produkteigenschaften ändern) zusammengesetzt.

WNM	.LN	.I	.(produktspezifisch)
WNM (WaveNetManager → Für alle LockNodes gleich)	.LN (LockNode → Für alle LockNodes gleich)	.I (Inside → LockNode in Schließung integrierbar) .R (Radio → LockNode extern, kommuniziert über 25 kHz mit der Schließung) .C (Cable → LockNode extern, kommuniziert über Kabel mit dem Netzwerk und über 25 kHz mit der Schließung)	Eintragung diverser Kürzel für schließungs- spezifische Eigen- schaften, beispielswei- se: .WP (Wetterfeste Ausführung für wetterfeste Schließungen) .MS (Messingfarbene Ausführung für messingfarbene Schließungen) Diese Auflistung ist nicht abschließend, es sind weitere produkts- pezifische Eigenschaf- ten möglich, die einen speziellen LockNode erfordern. Die Eigen- schaften dieser Spalte können auch mitein- ander kombiniert sein.

LockNode-Portfolio

Die Tabelle zeigt, welche LockNodes welche Übertragungsmedien unterstützen.

	25 kHz	868 MHz	WLAN	USB	Ethernet	RS-232	RS-485
WNM.LN.I		✓					
WNM.LN.I.MP		✓					
WNM.LN.I.S2		✓					
WNM.LN.I.SH		✓					
WNM.LN.I.SREL2.G2		✓					
WNM.LN.I.SREL.G2		✓					
CompactReader- LockNode (nicht nachrüstbar)	✓	✓					

	25 kHz	868 MHz	WLAN	USB	Ethernet	RS-232	RS-485
WNM.LN.R	✓	✓					
WNM.LN.C	✓						✓

5.2.3 Zubehör

Für Ihr WaveNet ist Zubehör erhältlich.

Stromversorgung	Artikelnummer	Bild
Externes Steckernetzteil für RouterNode 2 ■ 12 V_{DC}, 500 mA ■ Hohlstecker Ø5,5/2,5 mm	POWER.SUPPLY.2	
Externes Steckernetzteil für SmartRelais, CentralNode, RouterNode, RepeaterNode und BAMO ■ 12 V_{DC}, 500 mA ■ Verpolungssicherer Steckverbinder (RM 5,08)	WN.POWER.SUPPLY.PPP	
Externes Steckernetzteil für LockNode mit RS-485-Schnittstelle ■ 12 V_{DC}, 500 mA ■ Offene Enden mit Aderendhülsen mm	WN.POWER.SUPPLY.LNC	
Batterieset für WaveNet Lock-Node (10 Stück)	WN.BAT.SET	

Kabel	Artikelnummer	Bild
Sensorkabel zum Anschluss an LockNodes (WN.LN.R/ WN.LN.C) zur Türüberwachung (5m)	WN.LN.SENSOR.CABLE	
Anschlusskabel zur Verbindung des SmartRelais mit einem LockNode (WNM.LN.R/C)	WN.WIRED.BF.G2	
Anschlusskabel für WNM-IO-Router vom Typ RN	WNM.CABLE.IO	

Antenne	Artikelnummer	Bild
Antennenauslagerung für LockNodes: ■ WN(M).LN.R ■ WN(M).LN.C	WN.LN.ANTV	
Externe Zusatzantenne für WNM.RN2.ER.IO (Kabellänge 2,5 m)	ANTENNA.EXT.868	

Halterung	Artikelnummer	Bild
Halterung für RN-Gehäuse (nicht geeignet für Router-Node 2)	WN.RN.BOX	

Ausmessung	Artikelnummer	Bild
Testset zur Ausleuchtung des WaveNet-Funknetzwerks auf 868 MHz: ■ Basisstation ■ Mobilstation Voraussetzung: Zwei Stunden telefonische Einweisung (im Preis enthalten)	WN.TESTER.BAMO.EU	
Basisstation des Testsets	WN.TESTER.BASIS.EU	
Mobilstation des Testsets	WN.TESTER.MOBILE.EU	

5.3 Geräte

Geräte, die im WaveNet als Netzwerkkomponenten eingesetzt werden können, haben grundsätzlich zwei voneinander unabhängige Schnittstellen (erster und zweiter Buchstabe nach Routertyp, siehe [RouterNodes \[▶ 15\]](#) und [LockNodes \[▶ 17\]](#)). Sie können also zwei Netzwerksegmente mit unterschiedlichen Übertragungsmedien miteinander verbinden.

RouterNodes verbinden zwei Netzwerksegmente mit (unterschiedlichen) Übertragungsmedien (siehe [Übertragungswege \[▶ 14\]](#)) miteinander.

LockNodes verbinden eine Schließung mit einem Netzwerksegment. Je nach Ausführung ist der LockNode kabellos (LN.R und LN.C) oder physikalisch (LockNode Inside) mit der Schließung verbunden.

Mit Ausnahme des Computers ist jedem WaveNet-Gerät eine eigene Adresse und eine für alle Geräte einheitliche Netzwerk-ID zugewiesen. Die Zuweisung der Netzwerk-ID macht Ihr WaveNet einzigartig und von anderen ggfs. in Reichweite liegenden unterscheidbar.

5.3.1 Computer

Computer nehmen im WaveNet zwei Rollen ein:

- Server mit LSM-Datenbank
- Client mit LSM-Oberfläche

Wenn der Server und die Clients über ein bestehendes Netzwerk verbunden sind, dann können Sie die WaveNet-Komponenten sowohl vom Server als auch vom Client aus ansprechen. Damit können Sie trotz räumlicher Trennung auch über große Entfernungen Ihr WaveNet aufspannen, das verschiedene Gebäude einschließt. Auf dem Server muss dazu eine spezielle Software für die Kommunikationsknoten installiert sein (CommNode). Die Kommunikationsknoten sind der Anschluss für die WaveNet-Geräte.

Sie können verschiedene Schnittstellen Ihres Computers verwenden:

- Ethernet
- Seriell (RS-485, EOL)
- Seriell (USB, EOL)

5.3.2 RouterNodes

RouterNodes sind das Rückgrat Ihres Netzwerks. Mit RouterNodes können Sie die Daten im WaveNet bis zu den LockNodes übertragen. Die LockNodes übernehmen dann die weitere Kommunikation zur Schließung.

Die neue Generation der RouterNodes (=RN2) ist die Weiterentwicklung der bisherigen Generation der RouterNodes (=RN) und bietet folgende Vorteile:

- Einfache Firmwareupdates (ab 40.1) mit OAM-Tool (siehe *Firmware aktualisieren* [► 34])
- IO-Schnittstellen direkt am Klemmblock
- Erweiterte Auswahl an Kabeln (Verwendung eigener Kabel ist möglich)
- Erweiterte Möglichkeiten zur Stromversorgung

RN2.ER.IO

Dieser RouterNode unterstützt Ethernet und Radio (=868 MHz).

5.3.3 LockNodes

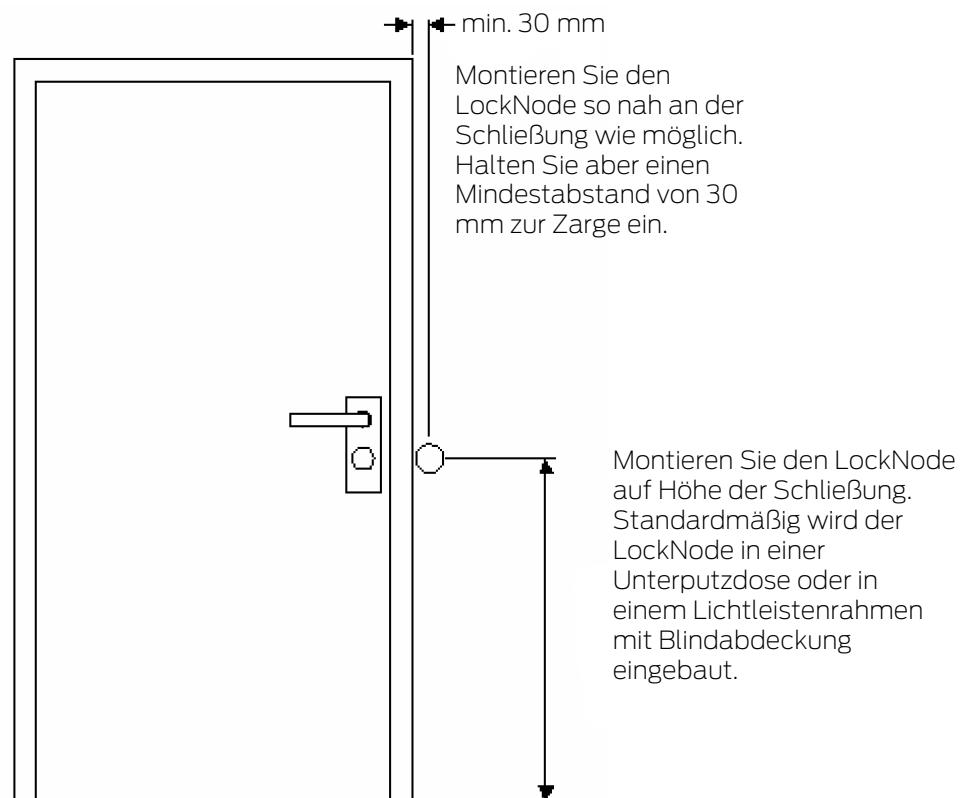
Mit LockNodes schließen Sie Ihre Schließungen an Ihr WaveNet an. Für viele Schließungen erhalten Sie LockNodes als *Inside*-Ausführung (siehe *LockNodes* [► 22]). Diese LockNodes werden im Inneren der vorhandenen

Schließung installiert und sind von außen unsichtbar. Alternativ können Sie externe LockNodes verwenden und in der Nähe der Schließung offen oder versteckt (zum Beispiel in einer Unterputzdose) anbringen.

Montage interner LockNodes ("Inside")

Informationen zur Montage der internen LockNodes finden Sie in den Kurzanleitungen der jeweiligen LockNodes.

Montage externer LockNodes



5.4 Funknetzwerk

Sie können mit dem WaveNet Berechtigungen, Zustandsänderungen, Schutzfunktionen und andere Daten kabellos übertragen.

Die modernen Funktechnologien des WaveNets müssen andere Erwartungen erfüllen als übliche Funknetzwerke.

Seit dem Jahr 2000 ist für diesen Bereich ein spezielles SRD-Band (short range device) im 868-MHz-Bereich verfügbar. Dieses SRD-Band ist in mehrere Subbänder unterteilt (Sie können das Subband wählen, siehe [Funkkanal \[► 46\]](#) und [RouterNode dem WaveNet hinzufügen \[► 57\]](#)).

Für sicherheitstechnische Anwendungen sind eigene Frequenzbereiche reserviert. Zusätzlich senden die WaveNet-Geräte nach dem Prinzip "Listen before talk", das heißt, dass vor der Übertragung geprüft wird, ob auf dem

eingestellten Kanal gerade kommuniziert wird. Wenn gerade kommuniziert wird, dann senden die WaveNet-Geräte erst, wenn die Kommunikation abgeschlossen ist.

Deshalb bietet Ihnen das WaveNet im 868-MHz-Bereich einen sicheren Übertragungsweg.

Das WaveNet wird wie alle Funknetzwerke von Geräte- und Umgebungseigenschaften beeinflusst:

- Sendeleistung
- Antennen (Größe, Ausrichtung)
- (Eigenmächtige) Veränderung der WaveNet-Geräte
- Empfindlichkeit der Empfänger
- Sendefrequenz
- Umwelteinflüsse (Luftfeuchtigkeit, Temperatur, elektromagnetische Störquellen)
- Bauliche Gegebenheiten (Wände, Decken etc. Siehe Tabelle)
- Aufstellungsort (Veränderung der Umgebungsbedingungen, siehe auch *Produktspezifische Sicherheitshinweise* [▶ 6])
- Netzwerkauslastung durch Mitnutzer der Funkfrequenzen
- Zufällige oder bewusste Störungen
 - Unerlaubte Frequenznutzung durch andere Geräte
 - Elektromagnetische Felder (zum Beispiel durch Schaltnetzteile)
 - Störsender (Jammer)

Diese Einflüsse können die Übertragung stören bzw. behindern. Sie erkennen dies an:

- Schlechten RSSI-Werten (Received Signal Strength)
- Langsamer oder fehlgeschlagener Datenübertragung
- Verringerter Reichweite

Das WaveNet wird außerdem beeinflusst durch:

- Spannungsausfall in einem (Teil-)Bereich
- Ausfall eines Übertragungswegs in einem externen Netz (z.B. Ethernetverbindung)

5.4.1 Segmente

Jeder RouterNode kann innerhalb eines Bereichs LockNodes erreichen. Diese Bereiche können sich auch überschneiden – ein LockNode kann sich deshalb in mehreren Bereichen gleichzeitig befinden und könnte von

mehreren RouterNodes gleichzeitig angesprochen werden. Deshalb ordnen Sie im WaveNet-Manager die LockNodes einem Segment zu (siehe *LockNodes dem WaveNet hinzufügen* [► 64]).

Netzwerksegmente sind gekennzeichnet durch:

- Übertragungsmedium (siehe *Übertragungswege* [► 14])
 - Ethernet (TCP/IP)
 - 868 MHz
 - WLAN (TCP/IP)
 - USB
 - RS-485-Kabel
 - RS-232-Kabel
- Eingangsseitige Segmentadresse und ausgangsseitige Segmentadresse
 - GID=Group-ID → Slave- bzw. Masteradresse

Eingangs- und Ausgangssegment

Jeder RouterNode hat ein Eingangssegment und ein Ausgangssegment, jeder LockNode dagegen nur ein Eingangssegment.

Wenn im WaveNet ein RouterNode mit einem LockNode (oder einem anderen RouterNode) kommunizieren soll, dann muss das Eingangssegment des LockNodes (bzw. des anderen RouterNodes) zum Ausgangssegment des RouterNodes passen. Sie können die Segmente unter Berücksichtigung der Netzwerkmaske (siehe *Adressierung* [► 45]) in der WaveNet-Übersicht (siehe *Übersicht* [► 190]) ablesen.

5.4.2 Signalqualität

Ihr WaveNet überträgt Daten kabellos zwischen vernetzten RouterNodes und LockNodes. Damit die Daten übertragen werden können, muss das Funksignal eine gewisse Signalstärke haben, um von Störungen unterschieden und empfangen werden zu können (siehe auch *Herausforderungen in Funknetzwerken* [► 27]).

ACHTUNG**Empfohlene Signalstärke**

Die Signalstärke im WaveNet-Manager sollte zwischen 0 dBm und -70 dBm liegen.

Wenn die Signalstärke nicht ausreicht, dann kann die Verbindung und Kommunikation zwischen den Geräten langsam oder unterbrochen werden und es kommt zudem zu einem höheren Stromverbrauch.

- Wenn die Signalstärke zwischen -75 dBm und -90 dBm liegt, kann es zu eingeschränkter Funktion kommen. Verbessern Sie die Signalqualität (siehe *Signalqualität verbessern* [► 161]).

Einheit der Signalstärke

Der WaveNet-Manager gibt die Signalstärke als RSSI-Wert (Received Signal Strength) in dBm an. Dieser Wert ist:

- Logarithmisch: Eine Verbesserung um 10 dBm bedeutet in der Praxis die doppelte Signalstärke.
- Negativ: Der theoretische Bestwert beträgt 0 dBm und wird nur durch Kabelverbindungen erreicht. Je näher der Wert an 0 dBm ist (je kleiner also der Betrag ist), desto besser ist der Empfang.

Einflüsse auf die Signalstärke

Die Signalstärke wird durch verschiedene Faktoren beeinflusst, vor allem aber durch die Umgebung und die dort verbauten Materialien.

Material	Durchlässigkeit
■ Holz ■ Gips ■ Gipskarton	90%-100%
■ Backstein ■ Pressspan	65%-95%
■ Stahlbeton (Sender auf Metall)	10%-70%
■ Metall ■ Metallgitter ■ Aluverkleidungen	0%-10%

5.4.3 Herausforderungen in Funknetzwerken

Funkwellen breiten sich in alle Richtungen aus. Im Gegensatz zu Kabeln sind sie nicht an ein Übertragungsmedium (Kabel) gebunden. Daraus folgen einige funkspezifische Besonderheiten.

Drei maßgebliche Einflüsse entscheiden darüber, ob ein Funksignal erfolgreich übertragen wird:

- Signalstärke
- Signal-Rausch-Verhältnis
- Auslastung der Frequenz

Erklärungen der Einflüsse

Signalstärke	Signal-Rausch-Verhältnis	Auslastung der Frequenz
Die Signalstärke ist die Amplitude der Funkwelle. Je stärker das Signal ist, desto eindeutiger kann der Empfänger die übertragenen Daten empfangen. Die Signalstärke nimmt mit zunehmender Entfernung oder durch ungünstige Übertragungsmedien ab. Je empfindlicher ein Empfänger ist (je besser die Antennen sind), desto weniger Signalstärke braucht er.	Das Signal-Rausch-Verhältnis (SNR=Signal-to-Noise Ratio) gibt an, wie stark das Rauschen im Vergleich zum Nutzsignal ist.. Funkwellen "enden" nicht. Theoretisch ist die Reichweite unbegrenzt, praktisch nimmt nur die Signalstärke ab. Funkwellen dringen also in andere Funknetzwerke ein und ergeben dort kein Nutzsignal mehr, sondern (störendes) Rauschen. Wenn das Rauschen zu stark ist (das Signal-Rausch-Verhältnis also sehr schlecht ist), dann kann der Empfänger das Nutzsignal nicht mehr vom Rauschen unterscheiden.	Die Auslastung der Frequenz ist das Verhältnis aus freier Sendezeit zu belegter Sendezeit. Ein Empfänger kann immer nur ein Funksignal gleichzeitig empfangen. WaveNet-Geräte funktionieren nach dem "Listen-before-talk"-Prinzip. Kein WaveNet-Gerät sendet, wenn es feststellt, dass auf dem verwendeten Frequenzband bereits ein Funksignal übertragen wird. Daraus entstehen Wartezeiten, bis das Frequenzband wieder frei wird. Je länger diese Wartezeiten sind, desto länger dauert es, bis ein Gerät senden kann → Die Übertragungsgeschwindigkeit nimmt ab.

Verständnisbeispiele aus dem Alltag

Signalstärke	Signal-Rausch-Verhältnis	Auslastung der Frequenz
Zwei Menschen sprechen miteinander (Sprache als Signal). Ein Mensch spricht lauter (Signalstärke nimmt zu). Wenn sich zwischen den Menschen eine Wand befindet (ungünstiges Übertragungsmedium), dann wird die Sprache leiser (Signal nimmt ab). Wenn ein Mensch sich nicht zum Sprecher hindreht (Antennen ungünstig ausgerichtet), dann wird die Sprache leiser wahrgenommen (Signal nimmt ab). Gut hörende Menschen (empfindliche Empfänger) können auch leise Gespräche (wenig Signalstärke) verstehen.	Zwei Menschen sprechen miteinander (Sprache als Signal). Neben den Menschen befindet sich eine vielbefahrene Straße, die Geräusche verursacht (Rauschen). Je näher die Menschen an die Straße kommen, desto lauter werden die Geräusche im Verhältnis zur Sprache (Signal-Rausch-Verhältnis nimmt ab). Wenn die Menschen zu nah an der Straße stehen, dann verstehen sie sich nicht mehr. Die Menschen können sich entweder von der Straße entfernen (Rauschen nimmt ab) oder lauter sprechen (Signal nimmt zu), um das Signal-Rausch-Verhältnis zu verbessern. Dabei ist es irrelevant, ob ein Mensch besser hört (Empfindlichkeit höher ist), weil mit der Sprache (Signal) auch die Straße (Rauschen) lauter gehört wird.	Viele Menschen wollen gleichzeitig sprechen (Sprache als Signal). Wenn ein Mensch spricht (Frequenzband ausgelastet), dann kann kein weiterer Mensch sprechen (Wartezeit), sonst wird kein Mensch verstanden. Die Menschen müssen warten, bis sich eine Gesprächspause ergibt ("Listen-before-talk") und können dann sprechen (Funksignalübertragung beginnen). Je mehr Menschen sich in einem Raum befinden, desto länger müssen sie auf eine Gesprächspause warten (Auslastung der Frequenz steigt). Die Menschen können sich entweder räumlich verteilen (um nicht zu hören, wenn andere Menschen gleichzeitig sprechen) oder sich kurz fassen (um die Wartezeiten zu verkürzen), damit mehr Menschen im selben Zeitraum sprechen können (Auslastung der Frequenz verringern).

Mögliche Ursachen für verschlechterte Umgebungsbedingungen im WaveNet

(Liste ohne Anspruch auf Vollständigkeit)

Signalstärke	Signal-Rausch-Verhältnis	Auslastung der Frequenz
❑ Geräte zu weit räumlich entfernt ❑ Absorption durch ungünstige Übertragungsmedien (z.B. Metalloberflächen oder Metalltüren) ❑ Absorption durch ungünstige Umgebungsbedingungen (z.B. Luftfeuchtigkeit, Temperatur) ❑ Ungünstige Ausrichtung der Antennen	❑ Viele Geräte auf dem 868-MHz-Band in der Nähe ❑ Elektromagnetische Störquellen ❑ Elektromagnetische Felder (z.B. durch Schaltnetzteile) ❑ Störsender (Jammer) ❑ Reflektierende Oberflächen	❑ Viele Geräte auf dem 868-MHz-Band in der Nähe ❑ Unerlaubte Frequenznutzung ❑ Störsender (Jammer) ❑ Lange Sendezeiten bzw. große Datenmengen

5.5 Sicherheit und Alarme

Sicherheit hat für SimonsVoss als Hersteller hochwertiger Geräte höchste Priorität.



HINWEIS

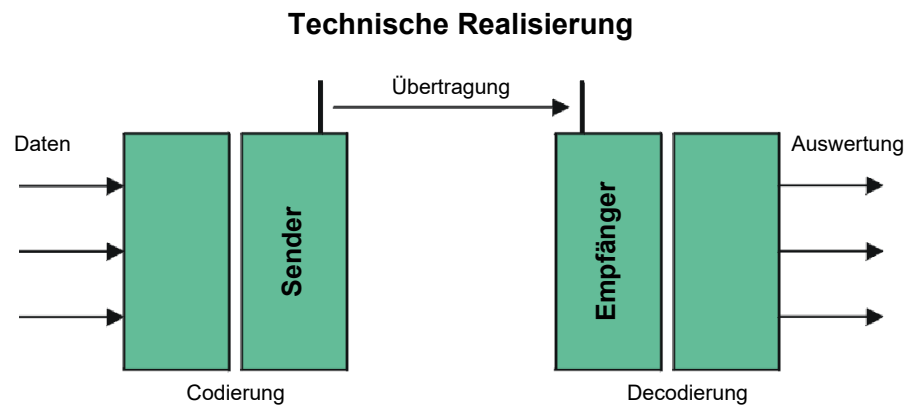
Redundante Absicherung der Netzwerkinfrastruktur

Zusätzlich zu den SimonsVoss-Sicherheitsmaßnahmen muss auch die Netzwerkinfrastruktur, in der Sie das WaveNet nutzen, aktuellen Sicherheitsstandards entsprechen.

1. Sie erreichen diese Sicherheitsstandards beispielsweise durch: Virtuelle Netzwerke oder aktive Netzwerküberwachung (Liste erhebt keinen Anspruch auf Vollständigkeit).
2. Sprechen Sie mit Ihrem IT-Infrastrukturspezialisten.

5.5.1 Verschlüsselung (WaveNet)

Aufwändige Kryptografie schützt die Daten, die in Ihrem WaveNet transportiert werden.



End-to-end-Verschlüsselung

End-to-end bedeutet in diesem Zusammenhang: Zwischen Zentralsoftware und Schließungen. Die Daten werden verschlüsselt und verlassen die Zentralsoftware. Sie werden erst in der Schließung wieder entschlüsselt.

Kommunikation	Verschlüsselung
End-to-end (generell)	3DES (112 bit)
Zutrittslisten (gegen unbefugtes Mitlesen)	Einfach-DES (56 bit)
Broadcast-Signale	AES (128 bit)

Digital signierte Datenpakete

Die 128-Bit-Signierung der Datenpakete schützt gegen Manipulationen auf der Funkstrecke. Wenn die Signatur eines Datenpakets nicht korrekt ist, dann wird das Datenpaket ignoriert.

Schutz gegen Replay-Attacken

Jedes sicherheitsrelevante Datenpaket enthält einen Zähler. Dieser Zähler wird für jedes neue Datenpaket erhöht. Wenn ein Datenpaket mit demselben Zählerstand nochmals ankommt, dann wird das Datenpaket ignoriert. Wenn ein Angreifer also ein Datenpaket mitschneidet und erneut sendet (Replay-Attacke), dann ist der Zähler des Datenpakets derselbe wie der des Originalpakets und die Kopie des Angreifers wird erkannt und ignoriert.

5.5.2 Überwachung der Geräte im Netzwerk

Die Geräte Ihres WaveNets können über weite Teile des Gebäudes verteilt sein. Sie können die Geräte teilweise aus der Ferne überwachen:

Zustände Ihrer Schließungen Wenn Sie DoorMonitoring-Schließungen verwenden, dann wird der aktuelle Zustand Ihrer Schließung über das WaveNet an die LSM übertragen und Ihnen dort angezeigt (Spalte DM). Alternativ zur Anzeige in der LSM können Sie den Zustand Ihrer Schließungen auch mit Smart.Surveil überwachen.

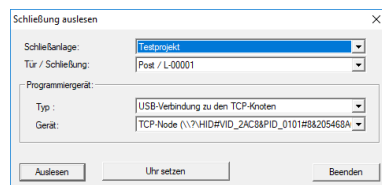
Zusätzliche Informationen finden Sie im LSM-Handbuch und im Smart.Surveil-Handbuch.

Netzwerkverbindungen Ihres WaveNets Der aktuelle Zustand der Verbindungen zwischen der LSM und Ihren WaveNet-Geräten wird Ihnen in der LSM angezeigt (Spalte N).

- Kein Eintrag: Netzwerkverbindung nicht angelegt.
- W (türkis): Letzter Verbindungsversuch erfolgreich.
- W (gelb): Letzter Verbindungsversuch bis zum LockNode erfolgreich, aber nicht bis zur Schließung (Tür geöffnet?).
- W (rot): Letzter Verbindungsversuch fehlgeschlagen.

Zusätzliche Informationen finden Sie in den Kapiteln *WaveNet und LSM* [► 32] und *LockNodes den Schließungen zuweisen* [► 73] sowie in *Fehlerbehebung* [► 161].

Batteriezustände Sie können mit der LSM über Ihr WaveNet auch den Batteriezustand der markierten Schließung auslesen (| Programmierung | - **Markierte Schließung auslesen/Uhr setzen** - Auslesen).



Zusätzliche Informationen finden Sie im LSM-Handbuch.

5.5.3 Alarme

Sie können mit dem WaveNet Zustandsänderungen an die LSM übertragen und so auf diese reagieren. Alarme sind in diesem Zusammenhang Meldungen, auf die Sie reagieren müssen (zum Beispiel Einbruchsversuche).

**WARNUNG****Redundante Absicherung gegen Gefahren**

Das WaveNet-System ist nicht als Ersatz für Überwachungssysteme wie Einbruchs- oder Brandmeldeanlagen geeignet. Nicht erkannte Brände oder Einbrüche können Personen und Sachwerte gefährden.

- Verwenden Sie zusätzlich zum WaveNet ein redundantes Überwachungssystem.

5.6 WaveNet und LSM

Das WaveNet und die LSM sind formal getrennt. Die LSM "denkt" in Schließungen und Kommunikationsknoten, der WaveNet-Manager "denkt" in LockNodes. Sie legen unabhängig voneinander in der LSM Ihre Schließanlage mit Zutrittsberechtigungen und im WaveNet-Manager das WaveNet an.

Das WaveNet "kennt" Ihre Schließungen nicht, sondern nur die daran angeschlossenen LockNodes. Die LockNodes sind mit den Schließungen physikalisch verbunden (Inside-LockNodes) oder in Funkreichweite (externe LockNodes). Die LockNodes "wissen" deshalb, in welcher Schließung sie verbaut sind. Die LSM kann deshalb beide Informationen (Schließung und LockNode) über das WaveNet von den LockNodes auslesen und dann die logische Verbindung zwischen LockNode und Schließung herstellen (siehe *LockNodes den Schließungen zuweisen* [► 73]).

5.7 Firmware

5.7.1 Firmware auslesen

Sie können die Firmwarestände Ihrer Geräte auslesen (Informationen zu Firmwareversionen siehe *Firmware-Informationen* [► 42]).

RouterNodes

Sie können die Firmware der RouterNodes entweder in der Übersicht des OAM-Tools sehen (für RN2, ältere nur als "Digi Device" gelistet) und aktualisieren (siehe *Firmware aktualisieren* [► 34]) oder mit der LSM auslesen (für RN und RN2).

- ✓ LSM geöffnet.
- ✓ RouterNodes mit LSM verbunden (Test siehe *Erreichbarkeit testen (LSM)* [► 198]).

1. Öffnen Sie über | Netzwerk | den Eintrag **WaveNet verwalten**.
 - ➔ Sie sehen eine Liste der WaveNet-relevanten Bestandteile.

2. Aktivieren Sie ggfs. die Checkbox ☒ Alle WaveNet-Knoten anzeigen.
 ↳ Sie sehen eine Liste der WaveNet-relevanten Bestandteile.
3. Markieren Sie den RouterNode, dessen Firmware Sie auslesen wollen.
4. Klicken Sie auf die Schaltfläche **Eigenschaften**.
 ↳ Fenster "Eigenschaften WaveNet-Knoten" öffnet sich.

Eigenschaften WaveNet-Knoten

Name:

Knotentyp:

Interfaces:

Chip-ID:

Adresse:

Firmware Firmware TM

Anschlußgerät:

Beschreibung:

Status

☐ Output ist gesetzt

☒ Input 1

☒ Input 2

☒ Input 3

☐ Batteriezustand ist kritisch

Konfiguration

☐ Weiterleitung der Ereignisse aktivieren

☐ Programmierbedarf

↳ Sie sehen die Firmwareversion in der Zeile **Firmware TM**.

LockNodes

- ✓ LSM geöffnet.
 - ✓ LockNodes mit LSM verbunden (Test siehe *Erreichbarkeit testen (LSM)* [▶ 198]).
1. Öffnen Sie über | Netzwerk | den Eintrag **WaveNet verwalten**.
 ↳ Sie sehen eine Liste der WaveNet-relevanten Bestandteile.
 2. Aktivieren Sie ggfs. die Checkbox ☒ Alle WaveNet-Knoten anzeigen.
 ↳ Sie sehen eine Liste der WaveNet-relevanten Bestandteile.
 3. Markieren Sie den LockNode, dessen Firmware Sie auslesen wollen.

4. Klicken Sie auf die Schaltfläche **Eigenschaften**.

↳ Fenster "Eigenschaften WaveNet-Knoten" öffnet sich.

Eigenschaften WaveNet-Knoten

Name: WNNode_0027

Knotentyp: LockNode

Interfaces: LNI Mifare

Chip-ID: 00017FD4

Adresse: 0x0027

Firmware: 17.6 Firmware TM: 33.6

Anschlußgerät: WN Central Node : DEEPPURPLE : SV_003644

Beschreibung:

Status

- ☐ Output ist gesetzt
- ☐ Input 1
- ☐ Input 2
- ☐ Input 3
- ☐ Batteriezustand ist kritisch

Konfiguration

- ☐ Weiterleitung der Ereignisse aktivieren
- ☐ Programmierbedarf

Übernehmen Beenden Testen Output setzen Output zurücksetzen

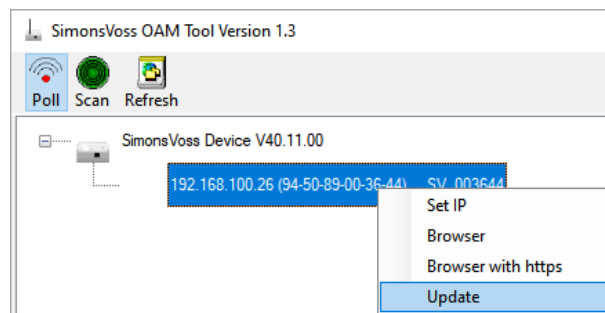
↳ Sie sehen die Firmwareversion in der Zeile **Firmware TM**.

5.7.2 Firmware aktualisieren

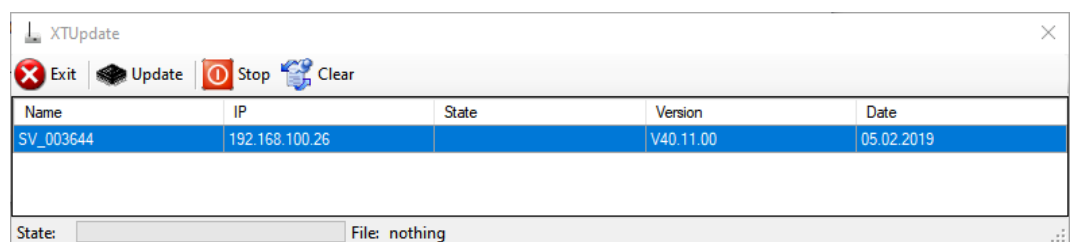
Neuere Firmwareversionen verbessern Ihre Produkte und schalten möglicherweise auch neue Funktionen frei (siehe *Firmware-Informationen* [▶ 42]).

RouterNodes mit Ethernet-Anschluss

Sie können die Firmware mit dem Operations-, Administration- and Maintenance-Tool (OAM-Tool) selbst aktualisieren (nur RN2). Das OAM-Tool ist kostenlos im Downloadbereich auf der SimonsVoss-Website (<https://www.simons-voss.com>) verfügbar. Sie müssen das OAM-Tool nicht installieren.



- ✓ Aktuellste Version des OAM-Tools geöffnet (siehe *IP-Adresse ermitteln und einstellen* [► 53]).
 - ✓ RouterNode aufgelistet (siehe *IP-Adresse ermitteln und einstellen* [► 53]).
 - ✓ Änderung der IP über das OAM-Tool erlaubt (siehe *Browserschnittstelle* [► 157]).
 - ✓ Aktuelle Firmware des RouterNodes 40.1X oder neuer.
 - ✓ RouterNode vom Typ RN2
 - ✓ Firmwaredatei (.REL) verfügbar (Kontaktieren Sie Ihren Fachhändler oder Systempartner).
1. Öffnen Sie mit einem Rechtsklick auf den Eintrag des RouterNodes, den Sie aktualisieren wollen, das Kontextmenü.
 2. Wählen Sie den Eintrag **Update** aus.
 - ↳ Fenster "xtupdate" mit einer RouterNode-Liste öffnet sich.



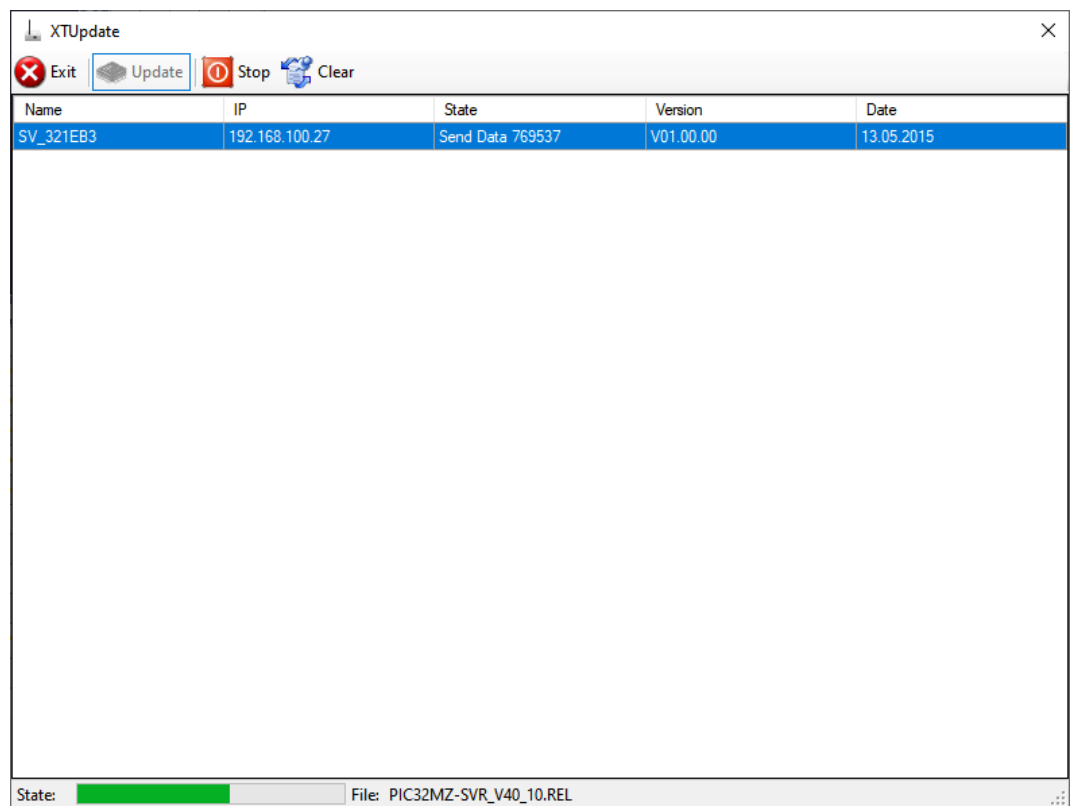
HINWEIS

Update mehrerer RouterNodes

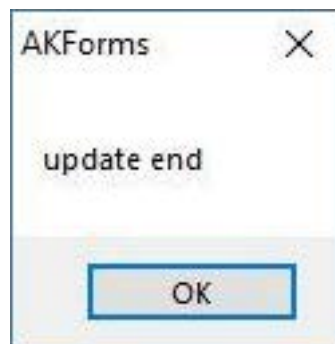
Das OAM-Tool bleibt geöffnet. Sie können der Updateliste im Fenster "xtupdate" weitere Einträge hinzufügen.

1. Markieren Sie einen weiteren RouterNode im OAM-Tool.
2. Wählen Sie den Eintrag **Update** aus.
 - ↳ RouterNode ist der Updateliste im Fenster "xtupdate" hinzugefügt.
3. Wiederholen Sie die Schritte so lange, bis alle RouterNodes, die sie aktualisieren möchten, in der Updateliste sind.
 - ↳ RouterNodes sind der Updateliste im Fenster "xtupdate" hinzugefügt.

3. Stellen Sie sicher, dass die RouterNodes, die Sie aktualisieren wollen, markiert sind.
4. Klicken Sie auf die Schaltfläche **Update**.
 - ↳ Explorersfenster öffnet sich.
5. Navigieren Sie zum Speicherort der Firmwaredatei.
6. Markieren Sie die Firmwaredatei.
7. Klicken Sie auf die Schaltfläche **Öffnen**.
 - ↳ Explorersfenster schließt sich.
 - ↳ Firmware der RouterNodes wird aktualisiert.



- ↳ Fenster "AKForms" öffnet sich.



8. Klicken Sie auf die Schaltfläche **OK**.
 - ↳ Fenster "AKForms" schließt sich.

9. Klicken Sie auf die Schaltfläche `Exit`.
 - ↳ Fenster "xtupdate" schließt sich.
 - ↳ Firmware der RouterNodes ist aktualisiert.

6. WaveNet-Manager

6.1 Systemanforderungen

Allgemein

- Lokale Administratorenrechte
- Kommunikation: TCP/IP
- LAN-Verbindung (Empfehlung: 100 MBit oder besser)
- Hilfefunktion: PDF-Reader, beispielsweise Adobe Reader

Zusätzlich gelten folgende Vorassetzungen für die Einbindung von Ethernet-Routern mit Hostnamen:

- Kommunikation: TCP/IP mit aktiviertem NetBIOS
- Windows-Domäne mit Namensauflösung

Sprechen Sie mit Ihrer IT-Abteilung.

Client

Anforderungen analog zur LSM.

- Monitor: 19" und 1024x768 (oder besser)
- Rechner: 2,66 GHz und 2 GB RAM (oder besser)
- Betriebssystem mit statischer IP und Namensauflösung für LSM
- Windows-Betriebssystem (7, 8/8.1 oder 10 Professional)
- LSM: .NET-Framework 2.0 (oder höher)
- USB-Schnittstelle bzw. LAN-Anschluss

6.2 Entpacken, Update und Start der Software

6.2.1 Entpacken

Sofern Sie mit mehreren LSM-Datenbanken arbeiten: Verwenden Sie für jede LSM-Datenbank einen eigenen WaveNet-Manager-Ordner (zum Beispiel Unterordner). Damit vermeiden Sie unterschiedlich konfigurierte Stränge.

LSM Basic Online

Entpacken Sie den WaveNet-Manager in ein geeignetes Verzeichnis.

SimonsVoss empfiehlt, den Ausgabeordner des WaveNet-Managers im selben Verzeichnis anzulegen. Wählen Sie deshalb ein Verzeichnis mit freiem Schreibzugriff aus, z.B.:

C:\WaveNet-Manager.

LSM Business/Professional

Entpacken Sie den WaveNet-Manager in ein geeignetes Verzeichnis (in der Regel ein Ordner auf einem Netzlaufwerk). SimonsVoss empfiehlt, den Ausgabeordner des WaveNet-Managers im selben Verzeichnis anzulegen.

Beachten Sie folgende Empfehlungen für das Verzeichnis:

- Das Verzeichnis liegt auf dem Server der LSM Business. Server und Client können unterschiedliche Portfreigaben haben. Der WaveNet-Manager sollte deshalb immer vom Server aus gestartet werden. Andernfalls können clientseitige Portfreigaben fehlen und im späteren Betrieb Kommunikationsprobleme auftreten.
- Sämtliche Clients bzw. Benutzer, die mit dem WaveNet-Manager arbeiten sollen, haben das *Lesen/Ausführen*-Recht für den freigegebenen Ordner. Erteilen Sie den Clients bzw. Benutzern dieses Recht, wenn nicht vorhanden.
- Wenn Sie mit mehreren LSM-Datenbanken arbeiten: Erstellen Sie für jede Datenbank ein eigenes Unterverzeichnis, das einen eigenen Ausgabeordner enthält. Entpacken Sie den WaveNet-Manager in jedes Unterverzeichnis. Rufen Sie den aus den jeweiligen LSM-Datenbanken den WaveNet-Manager im entsprechenden Unterverzeichnis auf und wählen Sie den Ausgabeordner des entsprechenden Unterverzeichnisses.

6.2.2 Update

Sofern der WaveNet Manager bereits installiert wurde, müssen für ein Update lediglich folgende Dateien im WaveNet-Installationsordner ersetzt werden:

- boost_threadmon.dll
- WaveNetManager.exe
- WNIPDiscoveryLib.dll

Die neueste Version des WaveNet Managers finden Sie auf der Homepage:

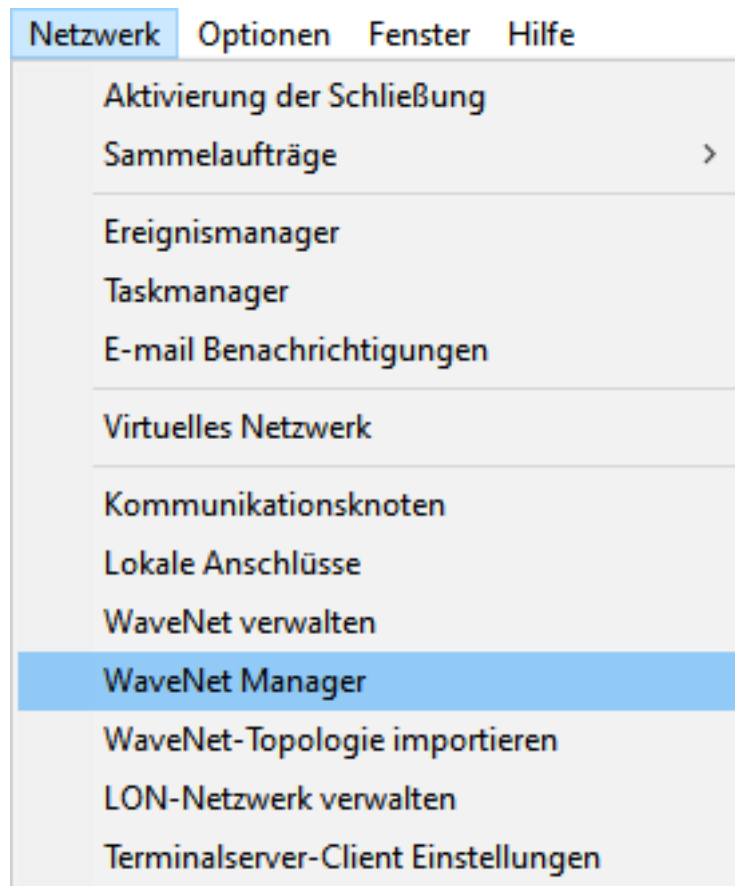
<https://www.simons-voss.com/de/service/software-downloads.html>

6.2.3 Start

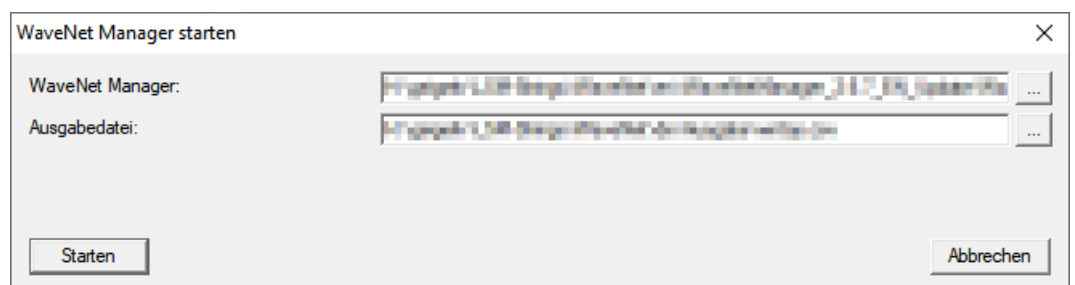
6.2.3.1 Best Practice: Aus der LSM-Software

✓ LSM mit Administratorrechten gestartet.

1. Öffnen Sie den WaveNet Manager über | Netzwerk | - WaveNet-Manager.



2. Überprüfen Sie die Dateipfade.



**HINWEIS****Fehler beim Abspeichern durch fehlende Schreibrechte**

Auf geschützte Speicherorte (wie C:\Program Files) kann der WaveNet-Manager nicht schreiben. Die Ausgabe wird dann in den Virtual Store umgeleitet (siehe *Virtual Store überprüfen und beheben* [▶ 188]).

- Wählen Sie für die Ausgabe einen Speicherort aus, für den alle Schreibrechte haben.

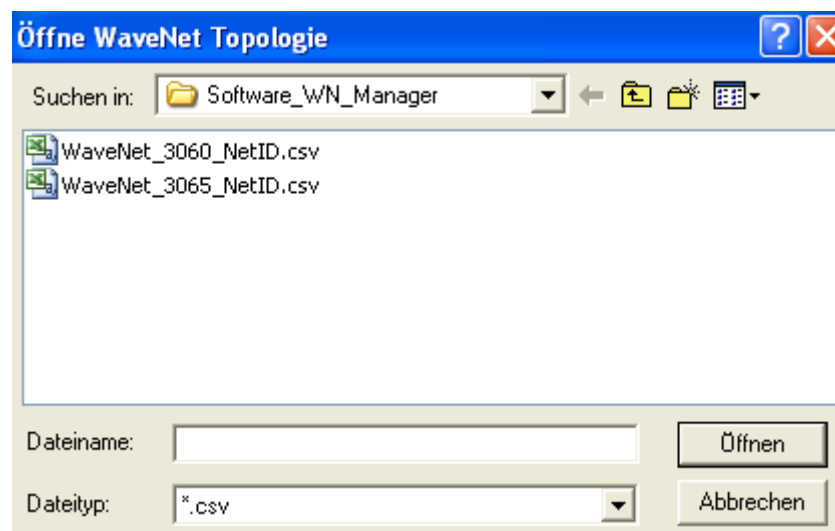
3. Klicken Sie auf die Schaltfläche **Start**.

→ WaveNet-Manager öffnet sich.

6.2.3.2 Manuell

Starten Sie den WaveNet-Manager nur dann manuell, wenn Sie das zu konfigurierende WaveNet nicht direkt an die LSM anbinden und zum Beispiel nur die I/O-Funktion verwenden wollen.

1. Führen Sie die Datei „WaveNetManager.exe“ im Installationsverzeichnis aus.
2. Wählen Sie Ihre Topologie aus oder legen Sie über **Abbrechen** ein neues Netzwerk an.



→ WaveNet-Manager öffnet sich.

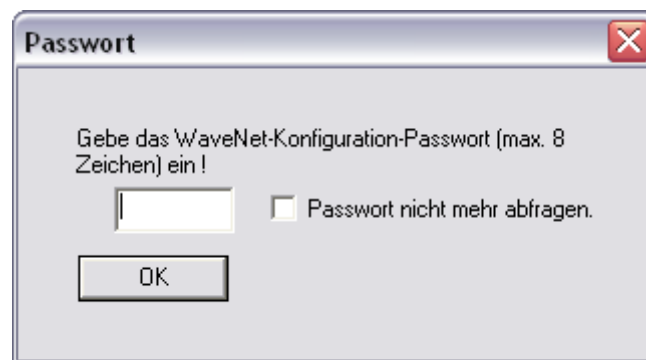
Falls mehr als eine WaveNet-Topologie vorhanden ist, erscheint eine Dialogbox. In der Dialogbox wählen Sie das Netzwerk aus, das Sie bearbeiten wollen. Wenn Sie keine Topologie auswählen (**Abbrechen**), dann startet der WaveNet-Manager und ein neues Netzwerk kann angelegt werden.

Wenn Sie bisher den WaveNet-Manager über die LSM gestartet haben und jetzt lokal starten, dann kann die LSM dem WaveNet-Manager nicht mitteilen, wie das bisherige WaveNet aussieht. Sie erstellen in diesem Fall ein neues WaveNet.

6.2.4 Passwort

Das Passwort muss 1-8 Zeichen lang sein. Sie können Ihr Passwort ansonsten frei wählen. Dieses Passwort wird in alle WaveNet-Komponenten programmiert. Ein nachträgliches Ändern des Passwortes ist nicht möglich!

Das Passwort verhindert ein versehentliches Umprogrammieren Ihrer bereits bestehenden oder fremder Netze. Verwenden Sie unbedingt nur ein Passwort pro WaveNet-Datenbank.



ACHTUNG

Passwortvergabe beim ersten Start

Sie können das Passwort nur beim ersten Start des WaveNet-Managers vergeben. Wenn Sie beim ersten Start kein Passwort vergeben, dann können Sie nachträglich kein Passwort mehr vergeben. Das Passwort ist dann leer.

- Vergeben Sie beim ersten Start des WaveNet-Managers ein Passwort.

6.3 Firmware-Informationen

Die Verfügbarkeit einzelner Funktionen ist firmwareabhängig. Sie können die Firmware selbst auslesen (siehe [Firmware auslesen \[32 \]](#)) und möglicherweise selbst aktualisieren (siehe [Firmware aktualisieren \[34 \]](#)).

RouterNodes

Folgende Funktionen sind erst ab bestimmten Firmwareständen verfügbar:

< 30.9	≥ 30.9	≥ 30.10	≥ 30.11	≥ 40.5	≥ 40.6	≥ 40.8	≥ 40.10
Schutzfunktionen (IO) siehe <i>I/O-Konfiguration und Schutzfunktionen</i> [► 74]							
✗	✓	✓	✓	✓	✓	✓	✓
RingCast siehe <i>RingCast</i> [► 103]							
✗	✗	✓	✓	✓	✓	✓	✓
Verzögerungen siehe <i>I/O-Konfiguration und Schutzfunktionen</i> [► 74]							
✗	✗	✓	✓	✓	✓	✓	✓
Inputquittung (Ausgang setzen), kurz → Intervall, nicht statisch siehe <i>I/O-Konfiguration und Schutzfunktionen</i> [► 74]							
✗	✗	✓	✓	✓	✓	✓	✓
Fast Wake-Up siehe <i>Maximale Übertragungsdauer im RingCast</i> [► 138]							
✗	✗	✗	✓	✓	✓	✓	✓
Inputquittung (Ausgang setzen) statisch → statisch, kein Intervall siehe <i>I/O-Konfiguration und Schutzfunktionen</i> [► 74]							
✗	✗	✗	✗	✓	✓	✓	✓
Datenpaketversand über Ethernet siehe <i>RingCast</i> [► 103]							
✗	✗	✗	✗	✓	✓	✓	✓
Wiederholung bei fehlgeschlagenem Broadcast siehe <i>Maximale Übertragungsdauer im RingCast</i> [► 138]							
✗	✗	✗	✗	✗	✓	✓	✓
LockNodes für Auslösen eines Inputereignisses einzeln auswählbar siehe <i>I/O-Konfiguration und Schutzfunktionen</i> [► 74]							
✗	✗	✗	✗	✗	✗	✓	✓
Zentraler Output-Router siehe <i>Zentraler Output-Router</i> [► 145]							
✗	✗	✗	✗	✗	✗	✗	✓

LockNodes

Folgende Funktionen sind erst ab bestimmten Firmwareständen verfügbar:

<30.8.16.0	≥ 30.8.16.0	≥ 30.8.16.2	≥ 30.8.16.3	≥ 33.3.16
Schutzfunktionen (IO) siehe <i>I/O-Konfiguration und Schutzfunktionen</i> [► 74]				
✗	✓	✓	✓	✓
Quittung nach Broadcast senden siehe <i>RingCast</i> [► 103]				
✗	✗	✗	✓	✓
Fast Wake-Up siehe <i>Maximale Übertragungsdauer im RingCast</i> [► 138]				
✗	✗	✓	✓	✓
LockNodes für Auslösen eines Inputereignisses einzeln auswählbar siehe <i>I/O-Konfiguration und Schutzfunktionen</i> [► 74]				
✗	✗	✗	✗	✓

6.4 Verwaltung

6.4.1 Grundlagen

Netzwerk Optionen

Netzwerkparameter für RN_ER - SV_003644.

Netzwerk ID: 4FDA

Funkfrequenz: 1

Netzwerkmaske: WaveNet_11_5

Möchten Sie diesen Knoten hinzufügen ?

Ja

Nein

6.4.1.1 Adressierung

Sie legen die Adressierung bei der erstmaligen Einrichtung fest (wenn Sie also Ihren ersten RouterNode hinzufügen). Falls Sie diese Einstellungen später verändern wollen, müssen Sie alle WaveNet-Geräte zurücksetzen (siehe [Zurücksetzen/Löschen \[► 177\]](#)).

Netzwerk-ID

Das WaveNet verwendet eine Netzwerk-ID. Die Netzwerk-ID muss Folgendes erfüllen:

- Länge: Vier Zeichen
- Zulässige Zeichen: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F
- Unzulässige Kombinationen: 0000, 0001, DDDD, FFFF

Die Netzwerk-ID macht in Kombination mit einem Passwort Ihr WaveNet einzigartig und verhindert das versehentliche Umprogrammieren von Netzwerken.

Adresse im Netzwerk/Netzwerkmaske

Geräte im WaveNet haben eine Netzwerkadresse (16-bit). Das WaveNet verwendet eine Netzwerkmaske für die Adresse im Netzwerk. Die Netzwerkmaske legt die Aufteilung der Bits zwischen GROUP-ID (RouterNode) und der MEMBER-ID (LockNode) und somit der maximalen Anzahl von RouterNodes und der maximalen Anzahl von LockNodes und RouterNodes fest.

Eine 11_5-Netzwerkmaske sieht 11 Bit ($2^{11}=2048$ Adressen, davon können 1790 genutzt werden. Einige Adressen sind für die Adressierung von seriell erreichbaren RouterNodes, also "RouterNodes hinter RouterNodes" und Ansprache des gesamten Netzwerks bzw. für Broadcasts reserviert) für die RouterNodes und 5 Bit ($2^5=32$ Adressen, davon können 25 genutzt werden) für die LockNodes vor.

Sie können zwischen folgenden Netzwerkmasken wählen:

Netzwerkmaske	Anzahl RouterNodes	Anzahl LockNodes
8_8	Max. 249	Max. 249 pro Router-Node
11_5	Max. 1790	Max. 25 pro RouterNode
12_4	Max. 3200	Max. 9 pro RouterNode

Wenn Sie keine andere Auswahl treffen, dann ist die Netzwerkmaske mit 11_5 voreingestellt. Dieser Wert hat sich erfahrungsgemäß als universell anwendbar herausgestellt.

Adresse in GROUP-ID und MEMBER-ID umrechnen

Sie können die angezeigte Adresse in das Binärsystem umrechnen, um aus der angezeigten Adresse die GROUP-ID und MEMBER-ID abzulesen.

Beispiel:

Angezeigte Adresse	0xA23F			
Aufteilung hexadezimal	A	2	3	F
Aufteilung dezimal	10	2	3	15
Aufteilung binär	1010	0010	0011	1111
Gesamt binär	1010001000111111			
Verteilung nach 8_8	8 GROUP-ID: 10100010 (=A2), 8 MEMBER-ID: 00111111 (=3F)			
Verteilung nach 11_5	11 GROUP-ID: 10100010001, 5 MEMBER-ID: 11111			
Verteilung nach 12_4	12 GROUP-ID: 101000100011 (=A23), 4 MEMBER-ID: 1111 (=F)			

Sie können im Falle von 8_8 und 12_4 Netzwerkmasken die GROUP-ID und MEMBER-ID im Hexadezimalsystem auch direkt aus der angezeigten Adresse ablesen.

6.4.1.2 Funkkanal

Wählen Sie bei der Ersteinrichtung einen Funkkanal für Ihr WaveNet aus. Jeder Funkkanal verwendet einen anderen Frequenzbereich. Nachdem Sie den Funkkanal ausgewählt haben, verwenden alle WaveNet-Geräte denselben Funkkanal. Die zur Verfügung stehenden Funkkanäle unterscheiden sich bei Geräten für den US-amerikanischen Markt von Geräten für den europäischen Markt. Weitere Informationen zum Aufbau des Funknetzwerks siehe *Funknetzwerk* [► 23]).

Sie können den Funkkanal nur bei der Ersteinrichtung einstellen. Um den Funkkanal später zu ändern müssen Sie das WaveNet zurücksetzen (siehe *Zurücksetzen/Löschen* [► 177]).



HINWEIS

Genehmigungspflicht oder Anmeldungspflicht

Der Betrieb von Funkgeräten kann in manchen Gebieten genehmigungspflichtig oder anmeldungspflichtig sein.

1. Bitte erkundigen Sie sich nach den gesetzlichen Bestimmungen in Ihrem Gebiet.
2. Verwenden Sie für neue Projekte im europäischen Raum den Kanal 1 oder 2.

Kanalnummer	Frequenzbereich	Empfohlene geographische Einsatzregion
0 (nur für Suche nach Komponenten)	868,1 MHz (Standardvariante)	Europa
	920,1 MHz (australische Variante)	Australien
1	868,3 MHz für (Standardvariante)	Europa
	920,3 MHz (australische Variante)	Australien
2	868,5 MHz (Standardvariante)	Europa
	920,5 MHz (australische Variante)	Australien
9	869,9 MHz	Europa
	921,9 MHz	Australien

6.4.2 Autokonfiguration

Wenn Ihre Geräte die automatische Konfiguration unterstützen, dann können Sie das Netzwerk auch automatisch konfigurieren. Sie müssen die Geräte dann nicht mehr manuell hinzufügen (Manuelles Hinzufügen siehe *Geräte finden und hinzufügen* [► 52]).

Die vollständige Autokonfiguration kann je nach Umfang Ihres WaveNets längere Zeit in Anspruch nehmen. Sie können deshalb die automatische Konfiguration auch auf Zweige Ihres WaveNets beschränken (RouterNodes manuell markieren oder direkt auswählen). Dabei werden nicht alle Verbindungen geprüft und es ist möglich, dass den LockNodes nicht der am besten erreichbare RouterNode zugewiesen wird. Verwenden Sie die beschränkte Autokonfiguration nur, wenn Sie sich ganz sicher sind.

Optimierte Autokonfiguration

Wenn Sie die Checkbox optimiert aktivieren, dann wird sowohl nach neuen als auch nach bereits konfigurierten Geräten gesucht.

Sollte der WaveNet-Manager dabei feststellen, dass bereits konfigurierte Knoten von anderen Segmenten (von anderen RouterNodes) wesentlich besser erreichbar sind, dann verschiebt der WaveNet-Manager diese Knoten in die Segmente mit der besseren Erreichbarkeit.

Sie können die Knoten nachträglich auch manuell verschieben (siehe *LockNodes einem anderen RouterNode zuweisen* [▶ 161]).

1. Der WaveNet-Manager sucht nach erreichbaren RouterNodes.
2. Der WaveNet-Manager sucht an jedem erreichten RouterNode nach erreichbaren LockNodes (sechs Suchläufe).

Nach erfolgter Autokonfiguration zeigt der WaveNet-Manager Ihnen alle erreichten Geräte mit Hex-Adresse und Chip-ID an.



HINWEIS

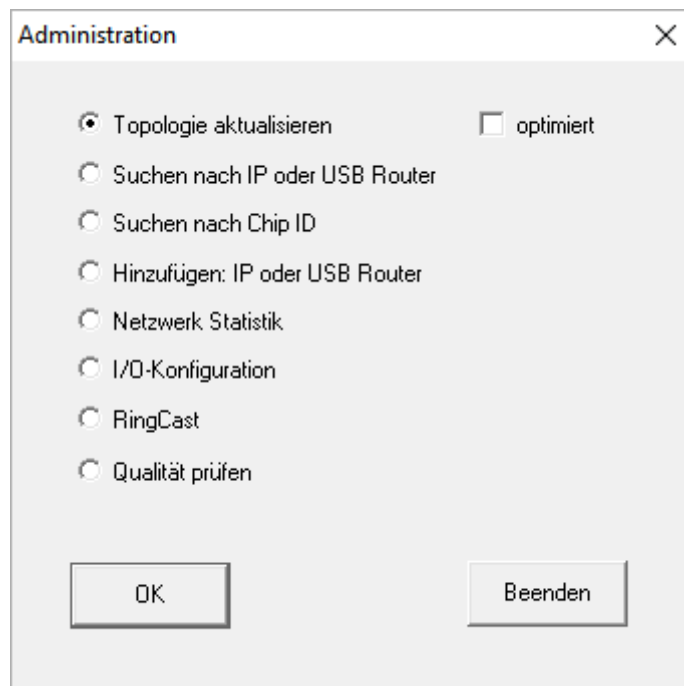
Zeitliche Einschätzung

Je nach Größe Ihres WaveNets kann die automatische Konfiguration einige Minuten dauern.

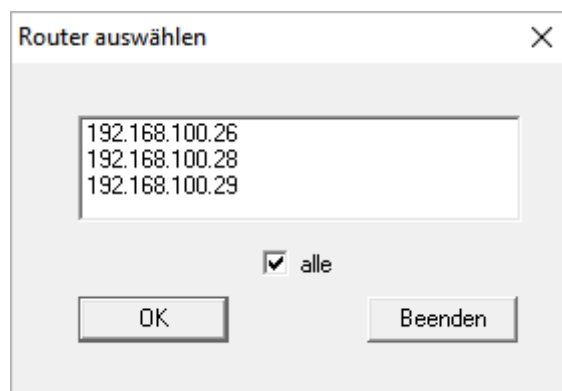
- Rechnen Sie mit etwa zwei Minuten pro Router.

6.4.2.1 Vollständig oder beschränkt (RouterNodes aus Liste auswählen)

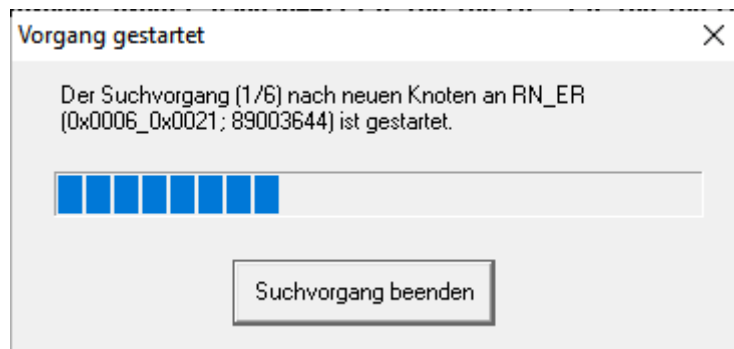
- ✓ WaveNet-Manager über LSM geöffnet (siehe *Best Practice: Aus der LSM-Software* [▶ 40]).
 - ✓ RouterNodes/LockNodes in Reichweite.
1. Klicken Sie mit der rechten Maustaste auf den Eintrag WaveNet_XX_X.
 - ➞ Fenster "Administration" öffnet sich.



2. Wählen Sie die Option ☒ Topologie aktualisieren aus.
3. Klicken Sie auf die Schaltfläche **OK**.
 - ↳ Fenster "Administration" schließt sich.
 - ↳ Fenster "Router auswählen" öffnet sich.



4. Markieren Sie alle RouterNodes, mit denen Sie suchen wollen oder markieren Sie die Checkbox ☒ alle, um Ihr ganzes WaveNet automatisch zu konfigurieren.
5. Klicken Sie auf die Schaltfläche **OK**.
 - ↳ Fenster "Router auswählen" schließt sich.
 - ↳ Fenster "Vorgang gestartet" öffnet sich vorübergehend.



↳ Erreichte Geräte (RouterNodes, LockNodes) sind aufgelistet.

6. Klicken Sie auf die Schaltfläche **Speichern**.

↳ Erreichte Geräte (RouterNodes, LockNodes) sind hinzugefügt. LockNodes wurden den RouterNodes aus Ihrer Auswahl zugeordnet, die am besten erreichbar sind.

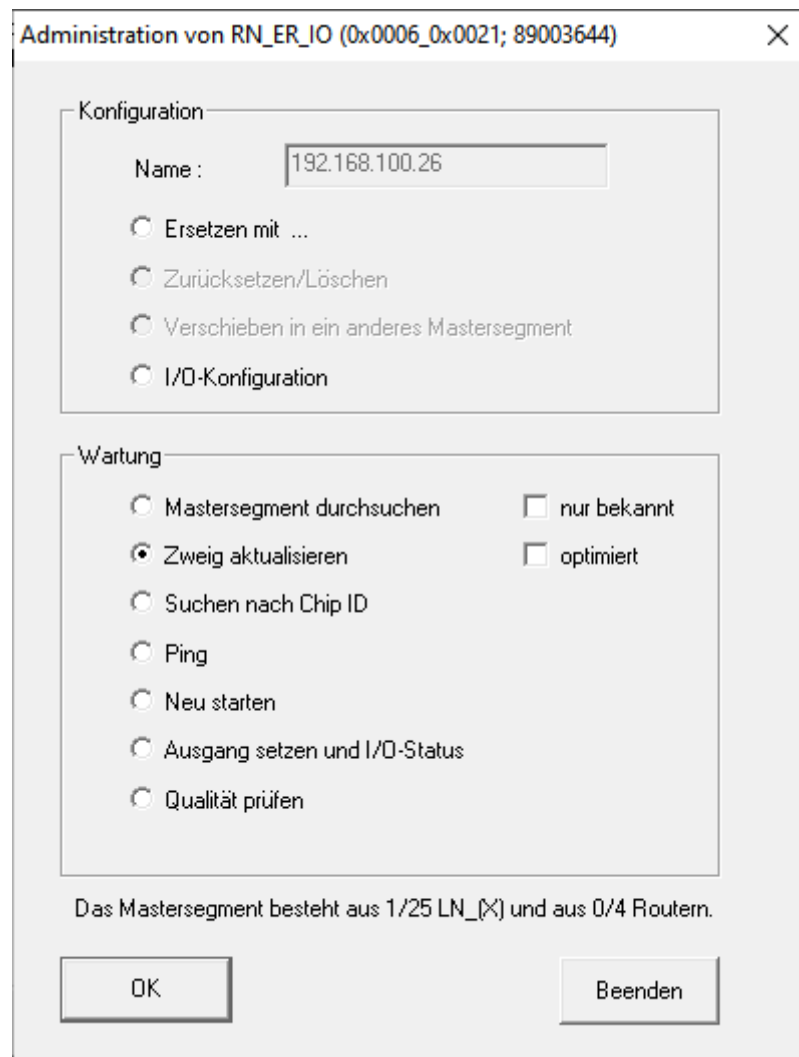
6.4.2.2 Beschränkt (RouterNode direkt auswählen)

✓ WaveNet-Manager über LSM geöffnet (siehe *Best Practice: Aus der LSM-Software [► 40]*).

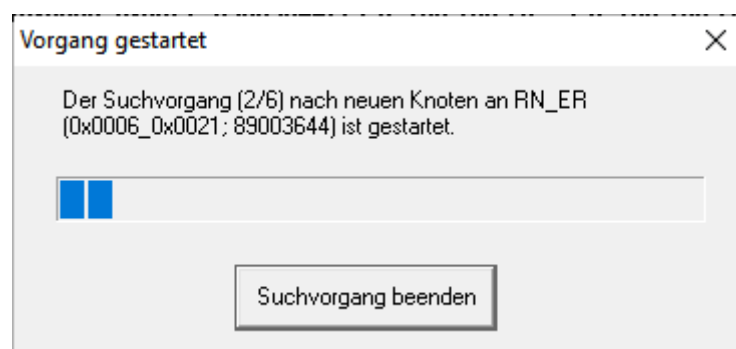
✓ RouterNodes/LockNodes in Reichweite.

1. Klicken Sie mit der rechten Maustaste auf den Eintrag des RouterNodes, ab dem Sie automatisch suchen und konfigurieren wollen.

↳ Fenster "Administration" öffnet sich.



2. Wählen Sie im Bereich "Wartung" die Option ☒ Zweig aktualisieren.
3. Klicken Sie auf die Schaltfläche **OK**.
 - ↳ Fenster "Administration" schließt sich.
 - ↳ Fenster "Vorgang gestartet" öffnet sich vorübergehend.



- ↳ Erreichte Geräte (RouterNodes, LockNodes) sind aufgelistet.
4. Klicken Sie auf die Schaltfläche **Speichern**.
 - ↳ Erreichte Geräte (RouterNodes, LockNodes) sind hinzugefügt.

Suche mit individuellem RouterNode

6.4.3 Geräte finden und hinzufügen

Sie weisen während der Einrichtung Ihres WaveNets Ihre RouterNodes optional einem Kommunikationsknoten zu. Stellen Sie in diesem Fall vor dem Erstellen Ihres WaveNets sicher, dass in Ihrer Schließanlage mindestens ein freier Kommunikationsknoten verfügbar ist. Legen Sie ggfs. einen an und übertragen Sie die Änderungen (siehe LSM-Handbuch).

Im Standalone-Betrieb (zum Beispiel bei einer LSM Basic) müssen Sie keinen Kommunikationsknoten anlegen bzw. verwenden. Stattdessen hängen Sie das WaveNet über lokale Anschlüsse ein. Beachten Sie, dass das Schließen der LSM-Software die Verbindung zum WaveNet unterbricht.

6.4.3.1 RouterNode anschließen

Sie haben zwei Optionen, um Ihren Ethernet-RouterNode an Ihrem Computer anzuschließen:

Option 1: Direktanschluss mit CAT.5-Patchkabel

- ✓ Computer nicht an einem Netzwerk angeschlossen.
- ✓ Computer mit zugewiesener statischer IP-Adresse.
- Verbinden Sie den Ethernet-Anschluss des RouterNodes mit dem Ethernet-Anschluss des Computers.

Sie können die IP-Adresse für den späteren Standort festlegen (siehe *IP-Adresse ermitteln und einstellen* [► 53]) oder den RouterNode dauerhaft direkt am Ethernetanschluss Ihres Computers betreiben.

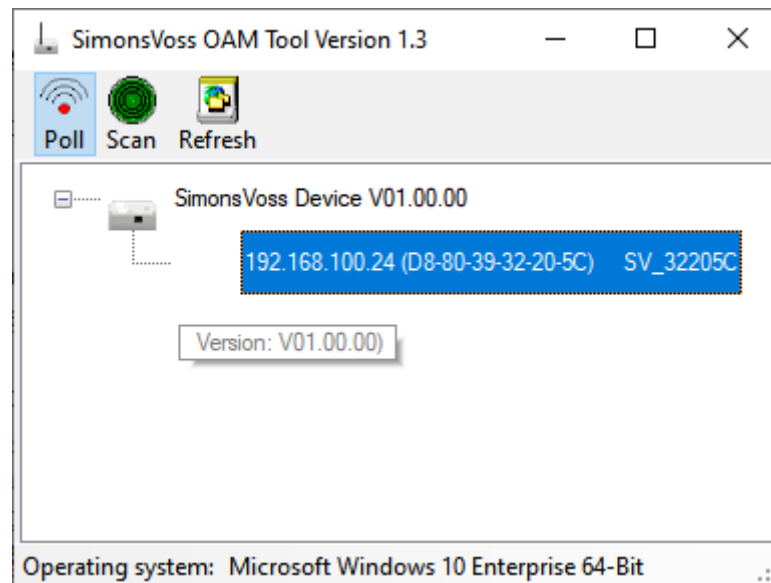
Option 2: Anschluss an das lokale Netzwerk

- ✓ RouterNode und Computer im selben Netzwerk (Subnet).
- ✓ DHCP-Server vorhanden.
- 1. Verbinden Sie den Ethernet-Anschluss des RouterNodes mit einem freien Netzwerkanschluss des Netzwerks.
- 2. Verbinden Sie den Ethernet-Anschluss Ihres Computers mit einem freien Netzwerkanschluss des Netzwerks.

Sie können die IP-Adresse für den späteren Standort festlegen (siehe *IP-Adresse ermitteln und einstellen* [► 53]) oder den RouterNode dauerhaft im selben Netzwerk wie Ihren Computer betreiben.

6.4.3.2 IP-Adresse ermitteln und einstellen

Mit dem Operations-, Administrations- und Maintenance-Tool (OAM-Tool) können Sie die IP-Adresse sowohl auslesen als auch einstellen. Das OAM-Tool ist kostenlos im Downloadbereich auf der SimonsVoss-Website (<https://www.simons-voss.com>) verfügbar. Sie müssen das OAM-Tool nicht installieren.



ACHTUNG

Unbefugtes Ändern der IP-Adresse

Das OAM-Tool ist frei zugänglich. Das OAM-Tool kann von Unbefugten missbraucht werden, um die IP-Adresse Ihrer RouterNodes/SmartBridges/GatewayNodes zu ändern.

- Sperren Sie das Ändern der IP-Adresse im OAM-Tool über die Browserschnittstelle (siehe *Browserschnittstelle* [▶ 157]).



HINWEIS

Unbefugter Zugriff mit Standard-Zugangsdaten

1. Ändern Sie das frei einsehbare Webserver-Standardpasswort. Unbefugte können zwar keinen Zutritt erlangen, aber die Konfiguration ändern. In diesem Fall erreichen Sie das Gerät nicht mehr und müssen es zurücksetzen.
2. Verwenden Sie keine Leerzeichen am Anfang oder am Ende (werden von manchen Browsern nicht übertragen).

IP ermitteln

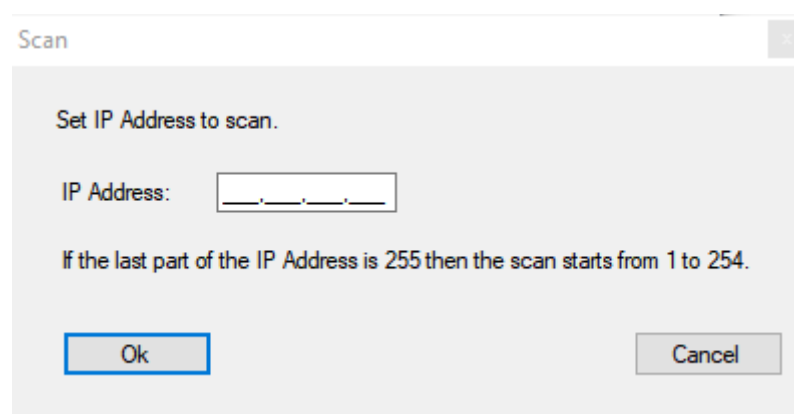
**HINWEIS****Fehler bei gleichzeitiger Verbindung mit mehreren Netzwerken**

Das OAM-Tool durchsucht das Netzwerk nach SimonsVoss-Netzwerkgeräten. Computer können mit mehreren Netzwerken verbunden sein (z.B. Kabel und WiFi). In so einem Fall ist für das OAM-Tool nicht eindeutig, welches Netzwerk durchsucht werden soll und es werden möglicherweise nicht alle SimonsVoss-Netzwerkgeräte gefunden.

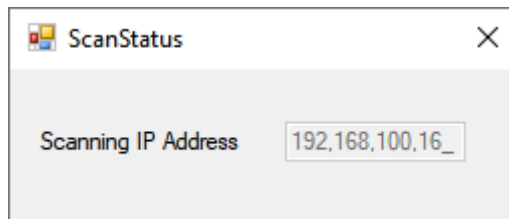
1. Trennen Sie nicht benötigte Netzwerkverbindungen.
2. Verbinden Sie den Computer ausschließlich mit dem Netzwerk, in dem die Netzwerkgeräte enthalten sind.

Der Ablauf ist für RouterNodes beschrieben. Verfahren Sie für SmartIntego-GatewayNodes und MobileKey-SmartBridges ebenso.

- ✓ OAM-Tool verfügbar und entpackt.
 - ✓ RouterNode am Netzwerk angeschlossen.
 - ✓ Subnetz bekannt.
1. Doppelklicken Sie auf die ausführbare Datei, um das OAM-Tool zu starten.
 - ↳ OAM-Tool öffnet sich.
 2. Klicken Sie auf die Schaltfläche **Scan**.
 - ↳ Fenster "Scan" öffnet sich.



3. Geben Sie eine bekannte IP-Adresse eines Geräts im (WaveNet)-Netzwerk ein (Andere oder neue Geräte werden ebenfalls gefunden. Wenn Sie keine IP-Adresse kennen, dann verwenden Sie folgende IP-Adresse: 192.168.100.255 - je nach Subnetz möglicherweise abweichend).
4. Klicken Sie auf die Schaltfläche **OK**.
 - ↳ Fenster "Scan" schließt sich.
 - ↳ OAM-Tool scannt den Adressbereich.



↳ OAM-Tool zeigt gefundene Geräte in der Liste an.

Sie haben die Wahl: DHCP-Server oder statische IP. Die nachfolgend beschriebenen Einstellungen können Sie auch in der Browserschnittstelle vornehmen (siehe *Browserschnittstelle* [▶ 157]).

Der Ablauf ist für RouterNodes beschrieben. Verfahren Sie für SmartIntego-GatewayNodes und MobileKey-SmartBridges ebenso.

IP einstellen für DHCP-Betrieb (Standard)

Wenn Sie einen DHCP-Server verwenden, dann wird die IP-Adresse durch einen DHCP-Server festgelegt.

- ✓ OAM-Tool verfügbar und entpackt.
 - ✓ RouterNode am Netzwerk angeschlossen.
1. Doppelklicken Sie auf die ausführbare Datei, um das OAM-Tool zu starten.
 - ↳ OAM-Tool öffnet sich.
 2. Klicken Sie auf die Schaltfläche **Refresh**.
 - ↳ IP-Adresse des RouterNodes aktualisiert.
 3. Öffnen Sie mit einem Rechtsklick auf den Eintrag der IP-Adresse des RouterNodes das Kontextmenü.



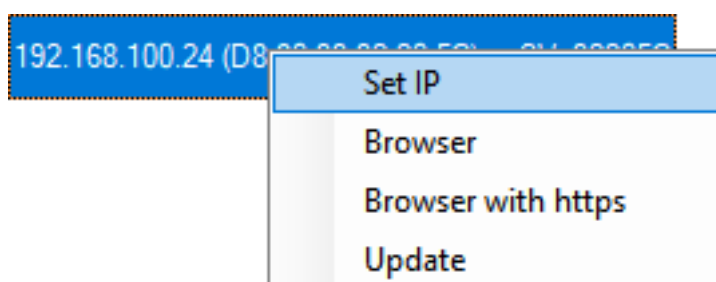
HINWEIS

MAC vergleichen

Wenn Sie den falschen RouterNode auswählen, dann könnten Sie dieselbe IP-Adresse mehrfach vergeben.

- Vergleichen Sie die MAC-Adresse des Eintrags mit dem Etikett auf Ihrem RouterNode.

4. Klicken Sie auf den Eintrag **Set IP**.



- ↳ Fenster "Network configuration" öffnet sich.
- 5. Stellen Sie sicher, dass die Checkbox ☒ Enable DHCP aktiviert ist.
- 6. Falls keine Adressreservierung am DHCP-Server für diesen RouterNode vorgesehen ist, notieren Sie sich den *Host name* (Bsp. SV_32205C). Sie brauchen ihn später bei der Konfiguration im WaveNet-Manager (siehe WaveNet-Handbuch - *RouterNode dem WaveNet hinzufügen* [▶ 57]).
- 7. Klicken Sie auf die Schaltfläche **OK**.
 - ↳ Fenster "Network configuration" schließt sich.
 - ↳ RouterNode startet neu.
- 8. Schließen Sie das Hinweisfenster über den Neustart.
- 9. Schließen Sie das OAM-Tool.
 - ↳ DHCP-Betrieb ist eingestellt.

IP einstellen für Betrieb mit statischer IP-Adresse

Wenn Sie keinen DHCP-Server verwenden, dann ist die IP-Adresse in der Werkseinstellung. Sie müssen die IP-Adresse in diesem Fall ändern, da sonst mehrere RouterNodes die gleiche IP (nämlich die Werks-IP) haben und nicht kommunizieren können.

- ✓ OAM-Tool verfügbar und entpackt.
- ✓ RouterNode am Netzwerk angeschlossen.
- 1. Doppelklicken Sie auf die ausführbare Datei, um das OAM-Tool zu starten.
 - ↳ OAM-Tool öffnet sich.
- 2. Klicken Sie auf die Schaltfläche **Refresh**.
 - ↳ IP-Adresse des RouterNode aktualisiert.
- 3. Öffnen Sie mit einem Rechtsklick auf den Eintrag der IP-Adresse des RouterNodes das Kontextmenü.



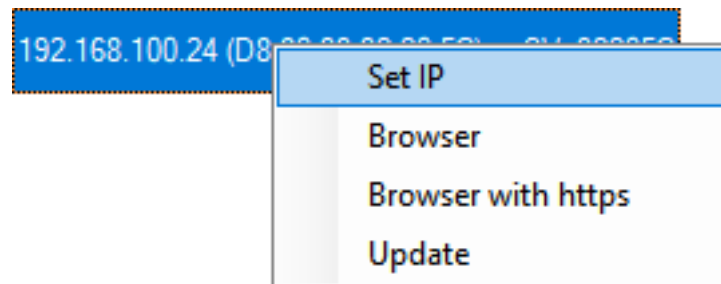
HINWEIS

MAC vergleichen

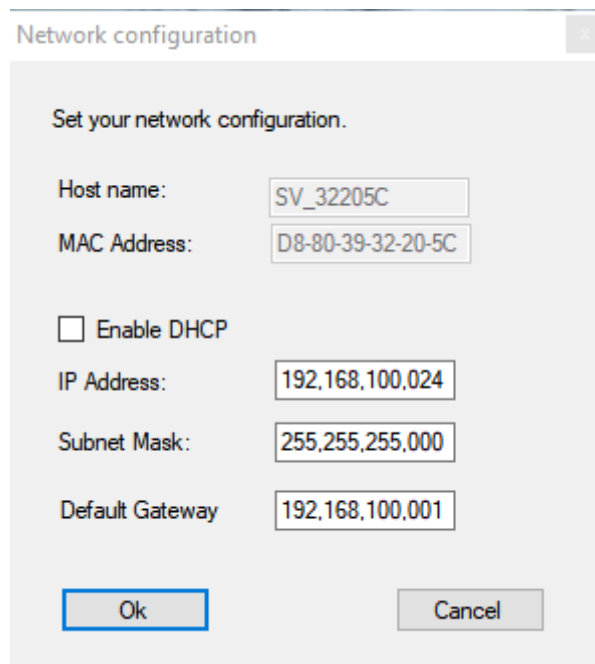
Wenn Sie den falschen RouterNode auswählen, dann könnten Sie dieselbe IP-Adresse mehrfach vergeben.

- Vergleichen Sie die MAC-Adresse des Eintrags mit dem Etikett auf Ihrem RouterNode.

4. Klicken Sie auf den Eintrag **Set IP**.



- ↳ Fenster "Network configuration" öffnet sich.



5. Deaktivieren Sie die Checkbox ☐ Enable DHCP.
6. Tragen Sie ggfs. eine neue IP-Adresse ein.
7. Klicken Sie auf die Schaltfläche **OK**.
- ↳ Fenster "Network configuration" schließt sich.
- ↳ RouterNode startet neu.
8. Schließen Sie das Hinweisfenster über den Neustart.
9. Schließen Sie das OAM-Tool.
- ↳ IP-Adresse ist eingestellt.

6.4.3.3 RouterNode dem WaveNet hinzufügen

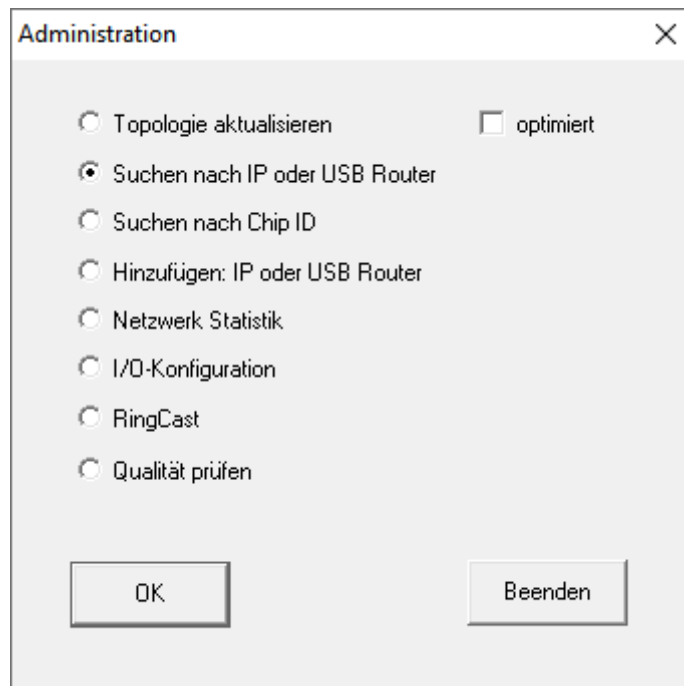
Wenn Sie RouterNodes in Ihrem WaveNet verwenden wollen, dann müssen Sie die RouterNodes zuerst im WaveNet-Manager in Ihre WaveNet-Topologie importieren.

Option	Anwendungssituation
☒ Suchen nach IP oder USB Router	Verwenden Sie diese Option, wenn Sie viele RouterNodes mit Ethernet-Schnittstelle an dasselbe Netzwerk angeschlossen haben. Diese müssen sich im selben Subnetz befinden, andernfalls verwenden Sie ☒ Hinzufügen: IP oder USB Router. Mit dieser Option müssen Sie nicht jede IP ermitteln und anschließend manuell eintragen.
☒ Suchen nach Chip ID	Verwenden Sie diese Option, um RouterNodes ohne Ethernet-Schnittstelle hinzuzufügen (siehe Übertragungswege [► 14]). Router ohne Ethernet-Schnittstelle haben keine IP-Adresse und können deshalb nur über die Chip-ID gefunden und hinzugefügt werden.
☒ Hinzufügen: IP oder USB Router	Verwenden Sie diese Option, wenn Sie gezielt einen RouterNode mit Ethernet-Schnittstelle Ihrem Netzwerk hinzufügen möchten. Die IP-Adresse (statisch / reserviert) oder der Hostname (DHCP) muss Ihnen bekannt sein. Diese können sich auch in einem anderen Subnet befinden.

Suchen nach IP oder USB Router

- ✓ RouterNode am Netzwerk angeschlossen.
 - ✓ WaveNet-Manager über LSM geöffnet (siehe [Best Practice: Aus der LSM-Software \[► 40\]](#)).
1. Klicken Sie mit der rechten Maustaste auf den Eintrag WaveNet_XX_X.
 - ↳ Fenster "Administration" öffnet sich.

2. Wählen Sie die Option ☒ Suchen nach IP oder USB Router aus.



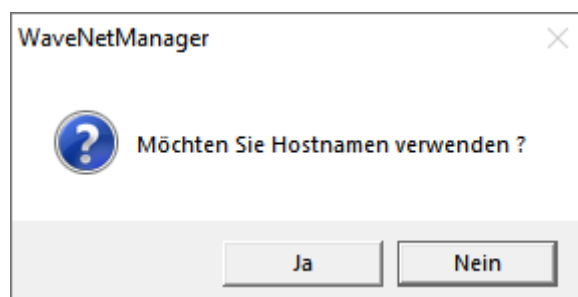
3. Klicken Sie auf die Schaltfläche **OK**.

→ Fenster "Administration" schließt sich.

→ Fenster "Vorgang gestartet" öffnet sich vorübergehend.

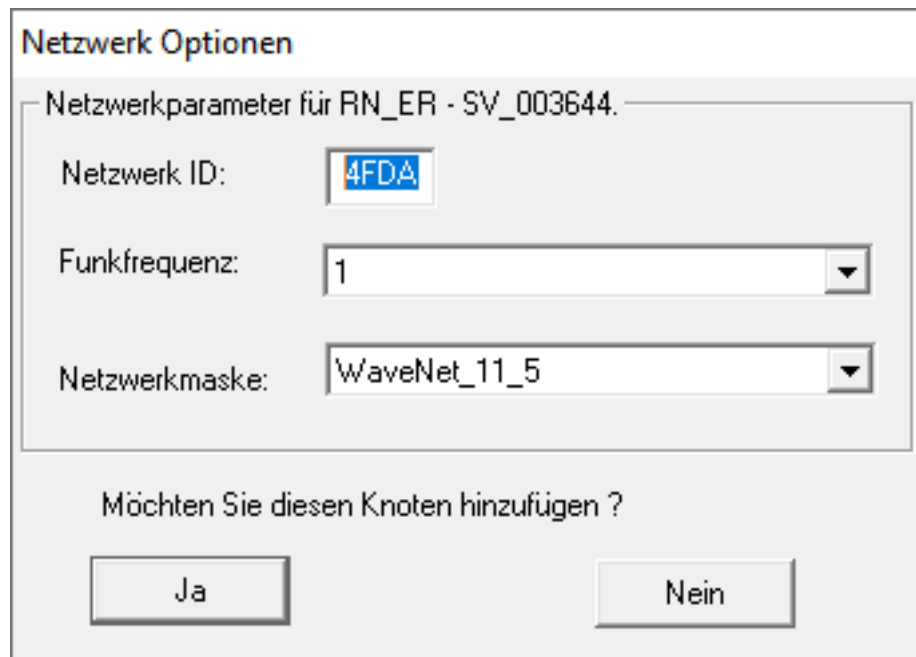


→ Fenster "WaveNet-Manager" öffnet sich.



4. Ist der Router per DHCP eingebunden und Sie verfügen über eine funktionierende Namensauflösung im Netzwerk, bestätigen Sie mit der Schaltfläche **Ja** um den Hostnamen zu verwenden. Haben Sie den Router per statischer IP-Adresse eingebunden, klicken Sie auf die Schaltfläche **Nein**.

- ➔ Fenster "WaveNet-Manager" schließt sich.
- ➔ Fenster "Netzwerk Optionen" öffnet sich.



HINWEIS

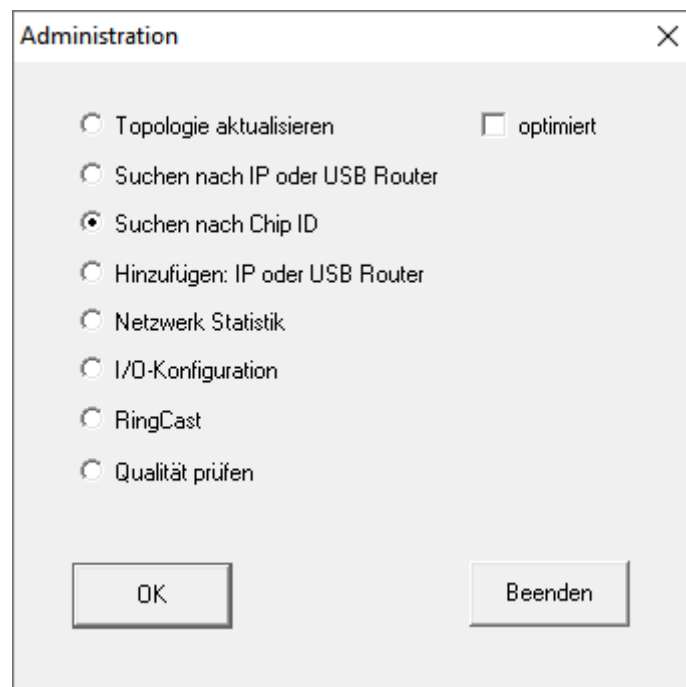
Netzwerkparameter einstellen

Wenn Sie ein neues WaveNet einrichten und Ihren ersten RouterNode hinzufügen, dann können Sie hier Netzwerkoptionen einstellen (siehe *Adressierung* [► 45] und *Funkkanal* [► 46]). Nach der Einrichtung Ihres WaveNets können Sie diese Einstellungen nicht mehr verändern, ohne Ihre WaveNet-Geräte zurückzusetzen.

5. Klicken Sie auf die Schaltfläche **Ja**.
- ➔ Fenster "Netzwerk Optionen" schließt sich.
6. Klicken Sie auf die Schaltfläche **Save**.
- ➔ RouterNode ist hinzugefügt und wird aufgelistet. Alle weiteren unkonfigurierten RouterNodes werden automatisch hinzugefügt.

Suchen nach Chip ID

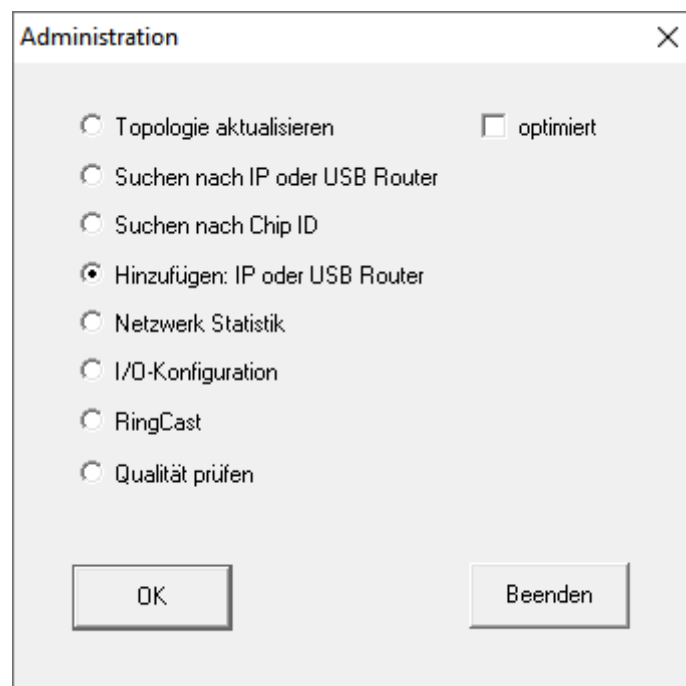
- ✓ RouterNode am Netzwerk angeschlossen.
 - ✓ Chip-ID des noch zu konfigurierenden RouterNodes bekannt.
 - ✓ WaveNet-Manager geöffnet.
1. Klicken Sie mit der rechten Maustaste auf den Eintrag WaveNet_XX_X.
 - ↳ Fenster "Administration" öffnet sich.
 2. Wählen Sie die Option ☒ Suchen nach Chip ID aus.



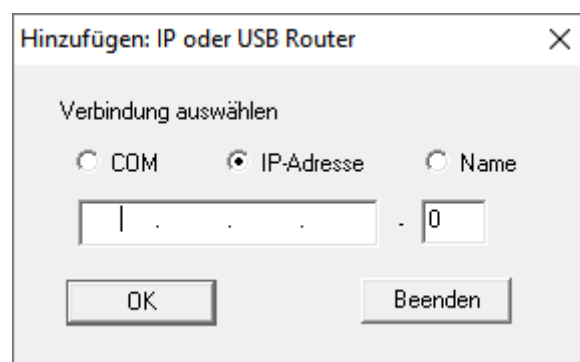
3. Klicken Sie auf die Schaltfläche **OK**.
 - ↳ Fenster "Administration" schließt sich.
 - ↳ Fenster "Suche Knoten" öffnet sich.
4. Geben Sie die Chip-ID ein.
5. Klicken Sie auf die Schaltfläche **Starten**.
 - ↳ Fenster "Suche Knoten" schließt sich.
 - ↳ Fenster "Vorgang gestartet" öffnet sich vorübergehend.
6. Fügen Sie den RouterNode hinzu.
 - ↳ RouterNode ist aufgelistet.
7. Klicken Sie auf die Schaltfläche **Save**.
 - ↳ RouterNode ist hinzugefügt.

Hinzufügen: IP oder USB Router

- ✓ RouterNode am Netzwerk angeschlossen.
 - ✓ IP des RouterNodes bekannt (siehe *IP-Adresse ermitteln und einstellen* [▶ 53]).
 - ✓ WaveNet-Manager geöffnet.
1. Klicken Sie mit der rechten Maustaste auf den Eintrag WaveNet_XX_X.
↳ Fenster "Administration" öffnet sich.
 2. Wählen Sie die Option ☒ Hinzufügen: IP oder USB Router aus.



3. Klicken Sie auf die Schaltfläche **OK**.
↳ Fenster "Administration" schließt sich.
↳ Fenster "Hinzufügen: IP oder USB Router" öffnet sich.



4. Wählen Sie die Option ☒ IP-Adresse aus.
5. Geben Sie die IP-Adresse Ihres RouterNodes ein.

**HINWEIS****IP-Bereich**

Sie können einen Bereich von IP-Adressen angeben. Wenn Sie zum Beispiel 192.168.100.XX bis 192.168.100.YY nutzen, dann geben Sie die erste IP-Adresse Ihres Bereichs (192.169.100.XX) ein und die Endung der letzten IP-Adresse (YY). Der WaveNet-Manager fügt dann alle RouterNodes hinzu, die er in diesem Bereich findet.

6. Klicken Sie auf die Schaltfläche **OK**.

- ↳ Fenster "Hinzufügen: IP oder USB Router" schließt sich.
- ↳ Fenster "Netzwerk Optionen" öffnet sich.

Netzwerk Optionen

Netzwerkparameter für RN_ER - SV_003644.

Netzwerk ID: 4FDA

Funkfrequenz: 1

Netzwerkmaske: WaveNet_11_5

Möchten Sie diesen Knoten hinzufügen ?

Ja Nein

**HINWEIS****Netzwerkparameter einstellen**

Wenn Sie ein neues WaveNet einrichten und Ihren ersten RouterNode hinzufügen, dann können Sie hier Netzwerkoptionen einstellen (siehe *Adressierung* [► 45] und *Funkkanal* [► 46]). Nach der Einrichtung Ihres WaveNets können Sie diese Einstellungen nicht mehr verändern, ohne Ihre WaveNet-Geräte zurückzusetzen.

7. Klicken Sie auf die Schaltfläche **Ja**.

- ↳ Fenster "Netzwerk Optionen" schließt sich.

8. Klicken Sie auf die Schaltfläche **Save**.

- ↳ RouterNode ist hinzugefügt und wird aufgelistet.

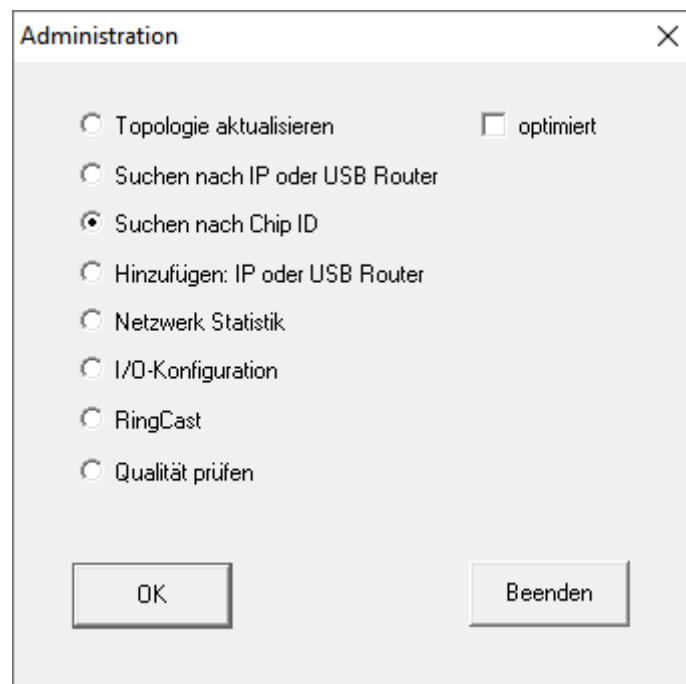
6.4.3.4 LockNodes dem WaveNet hinzufügen

Wenn Sie LockNodes in Ihrem WaveNet verwenden wollen, dann müssen Sie die LockNodes zuerst im WaveNet-Manager hinzufügen. LockNodes haben keine IP-Adresse und können deshalb nur über die Chip-ID gefunden werden. Sie finden die Chip-ID auf dem LockNode selbst, auf dem mitgelieferten Aufkleber oder auf dessen Verpackung.

Sie können den LockNode später manuell einem anderen RouterNode zuordnen (siehe *LockNodes einem anderen RouterNode zuweisen [▶ 161]*).

Einzelnen LockNode: Suchen nach Chip ID

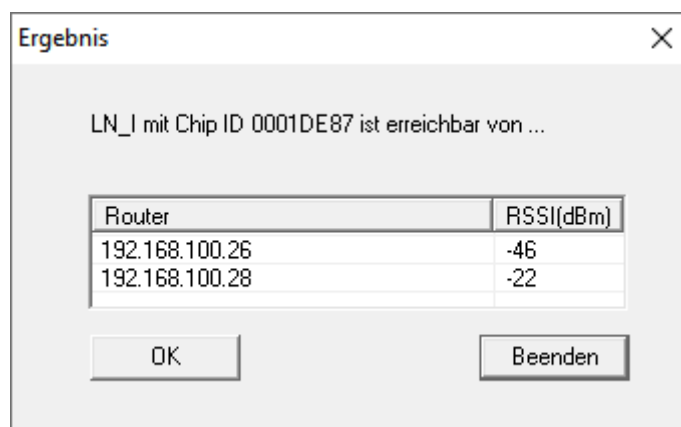
- ✓ RouterNode am Netzwerk angeschlossen.
 - ✓ WaveNet-Manager über LSM geöffnet (siehe *Best Practice: Aus der LSM-Software [▶ 40]*).
 - ✓ LockNode eingebaut bzw. mit Strom versorgt.
 - ✓ LockNode in Reichweite des WaveNets.
 - ✓ Chip-ID des LockNodes bekannt.
1. Klicken Sie mit der rechten Maustaste auf den Eintrag WaveNet_XX_X.
 - ↳ Fenster "Administration" öffnet sich.
 2. Wählen Sie die Option ☒ Suchen nach Chip ID.



3. Klicken Sie auf die Schaltfläche **OK**.
 - ↳ Fenster "Administration" schließt sich.
 - ↳ Fenster "Suche Knoten" öffnet sich.



4. Geben Sie die Chip-ID ein.
5. Klicken Sie auf die Schaltfläche **Starten**.
 - ↳ Fenster "Suche Knoten" schließt sich.
 - ↳ WaveNet-Manager sucht nach erreichbaren Chip-IDs.
 - ↳ Fenster "Ergebnis" öffnet sich. Sie sehen eine Liste der RouterNodes, die den LockNode erreichen.



Router	RSSI(dBm)
192.168.100.26	-46
192.168.100.28	-22

6. Wählen Sie den RouterNode aus, mit dem Sie den LockNode anfunken wollen.



HINWEIS

Signalstärke beachten

Die Signalstärke im WaveNet-Manager sollte zwischen 0 dBm und -70 dBm liegen.

Wenn die Signalstärke nicht ausreicht, dann kann die Verbindung und Kommunikation zwischen den Geräten langsam oder unterbrochen werden und es kommt zudem zu einem höheren Stromverbrauch.

1. Wählen Sie den RouterNode mit der besten Signalstärke aus.
2. Wenn kein RouterNode eine ausreichende Signalstärke hat, dann positionieren Sie einen RouterNode näher am LockNode (siehe *Signalqualität verbessern* [▶ 161]).

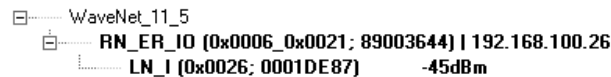
7. Klicken Sie auf die Schaltfläche **OK**.
 - ↳ Fenster "Ergebnis" schließt sich.

↳ Fenster "Vorgang gestartet" öffnet sich vorübergehend.

8. Klicken Sie auf die Schaltfläche **Save**.

↳ LockNode ist importiert und mit dem ausgewählten RouterNode verknüpft.

LockNodes werden in der WaveNet-Topologie unterhalb des RouterNodes angezeigt, zu dem sie zugeordnet sind.

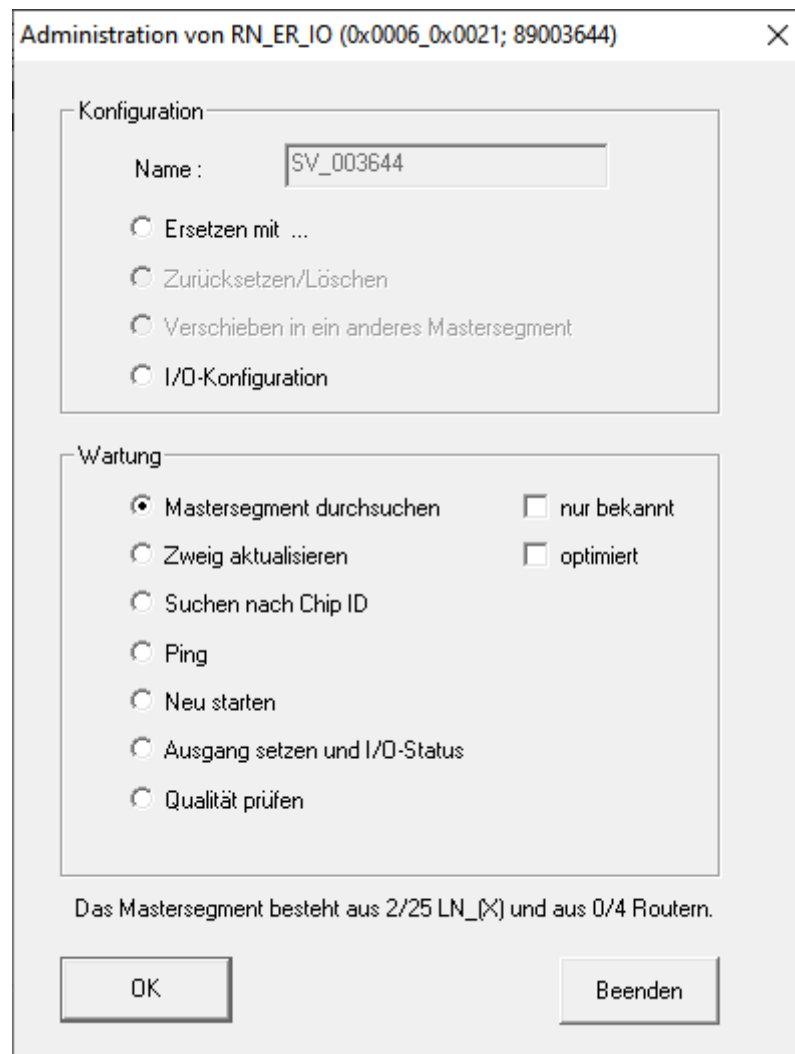


```
WaveNet_11_5
├── RN_ER_IO (0x0006_0x0021; 89003644) | 192.168.100.26
│   └── LN_I (0x0026; 0001DE87) -45dBm
```

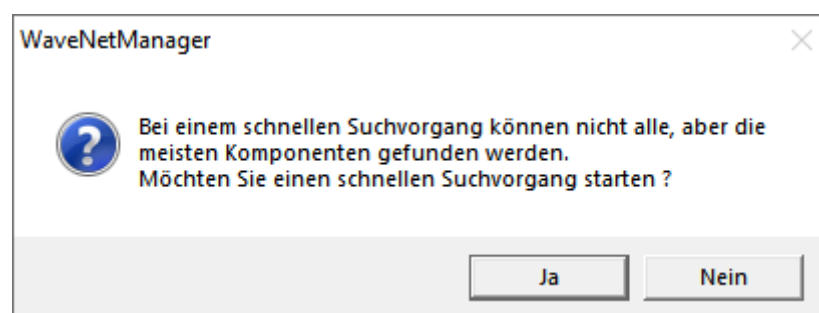
Mehrere LockNodes: Suchen durch RouterNode

Alternativ können Sie auch mit einem RouterNode nach erreichbaren LockNodes suchen und anschließend aus einer Liste von LockNodes die LockNodes auswählen, die Sie diesem RouterNode zuweisen wollen.

- ✓ WaveNet-Manager über LSM geöffnet (siehe *Best Practice: Aus der LSM-Software* [► 40]).
 - ✓ RouterNodes und LockNodes an Stromversorgung angeschlossen.
 - ✓ RouterNodes mit WaveNet verbunden (Test siehe *Erreichbarkeit testen (WaveNet)* [► 195]).
1. Klicken Sie mit der rechten Maustaste auf den RouterNode, mit dem Sie nach neuen LockNodes suchen wollen.
 - ↳ Fenster "Administration" öffnet sich.



2. Wählen Sie im Bereich "Wartung" die Option ☒ Mastersegment durchsuchen.
3. Stellen Sie sicher, dass die ☐ bekannt deaktiviert ist.
4. Klicken Sie auf die Schaltfläche **OK**.
 - ➔ Fenster "Administration" schließt sich.
 - ➔ Fenster "WaveNetManager" öffnet sich.



5. Klicken Sie auf die Schaltfläche **Ja** (Schneller Suchvorgang) oder **Nein** (Normaler Suchvorgang).

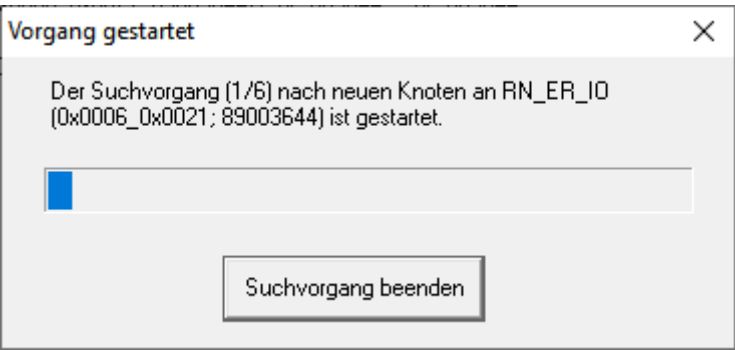


HINWEIS

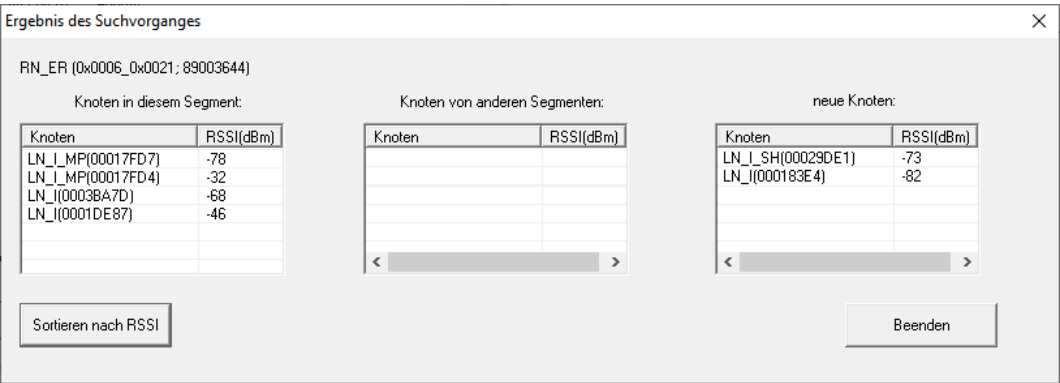
Schneller Suchvorgang

Wenn Sie einen schnellen Suchvorgang durchführen, dann sendet der RouterNode nur einen einzigen Broadcast. Wenn Sie einen normalen Suchvorgang durchführen, dann sendet der RouterNode insgesamt sechs Broadcasts. Der schnelle Suchvorgang ist schneller abgeschlossen, dafür ist der normale Suchvorgang gründlicher und findet auch LockNodes, die bei einem schnellen Suchvorgang nicht erreicht wurden.

- ➞ Fenster "WaveNetManager" schließt sich.
- ➞ Fenster "Vorgang gestartet" öffnet sich vorübergehend.



- ➞ Fenster "Ergebnis des Suchvorganges" öffnet sich.



Sie sehen eine Übersichtstabelle der LockNodes, die der RouterNode während der Suche gefunden hat. Diese Tabelle hat drei Spalten:

Knoten in diesem Segment	Knoten von anderen Segmen-ten	Neue Knoten
Diese LockNodes befinden sich in der WaveNet-Topologie und sind dem RouterNode bereits zugeordnet.	Diese LockNodes befinden sich in der WaveNet-Topologie, sind aber einem anderen RouterNode zugeordnet.	Diese RouterNodes sind un-konfiguriert und befinden sich in keiner Topologie.

Jede Spalte enthält zwei Unterspalten:

Knoten	RSSI
Name des LockNodes	Signalstärke der Verbindung des LockNodes zum suchenden Router-Node

Einheit der Signalstärke

Der WaveNet-Manager gibt die Signalstärke als RSSI-Wert (Received Signal Strength) in dBm an. Dieser Wert ist:

- Logarithmisch: Eine Verbesserung um 10 dBm bedeutet in der Praxis die doppelte Signalstärke.
 - Negativ: Der theoretische Bestwert beträgt 0 dBm und wird nur durch Kabelverbindungen erreicht. Je näher der Wert an 0 dBm ist (je kleiner also der Betrag ist), desto besser ist der Empfang.
1. Markieren Sie die LockNodes der rechten Spalte (Neue Knoten), die Sie dem RouterNode zuweisen wollen.
 2. Verschieben Sie die LockNodes mithilfe von Drag-and-Drop in die linke Spalte (Knoten in diesem Segment), um sie dem aktuellen RouterNode (mit dem Sie gesucht haben) zuzuweisen.
- ➞ LockNodes werden dem aktuellen RouterNode zugewiesen.



HINWEIS

Dauer der Zuweisung

Wenn Sie LockNodes neu zuweisen, dann kommuniziert der WaveNet-Manager mit den LockNodes, um die Konfiguration zu übertragen und den LockNode zu prüfen. Diese Prüfung dauert einige Sekunden.

3. Bestätigen Sie ggfs. die IO-Konfiguration des LockNodes mit einem Klick auf die Schaltfläche **OK** (Sie können die IO-Konfiguration jederzeit ändern, siehe *IO-Konfiguration und Schutzfunktionen* [► 74]).
- ➞ LockNode ist importiert und mit dem ausgewählten RouterNode verknüpft.

LockNodes werden in der WaveNet-Topologie unterhalb des RouterNodes angezeigt, zu dem sie zugeordnet sind.

```

WaveNet_11_5
├── RN_ER_IO (0x0006_0x0021; 89003644) | 192.168.100.26
│   └── LN_I (0x0026; 0001DE87) -45dBm

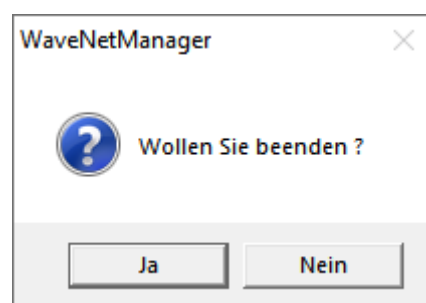
```

6.4.3.5 LSM-Import

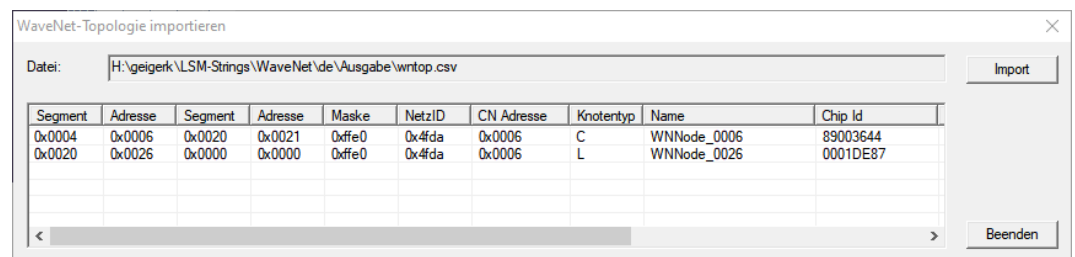
Sie müssen die erstellte WaveNet-Topologie in die LSM importieren, damit Sie die WaveNet-Topologie dort verwenden können.

- ✓ WaveNet-Manager über LSM geöffnet (siehe *Best Practice: Aus der LSM-Software* [► 40]).
- ✓ Freier Kommunikationsknoten in der LSM verfügbar (bzw. lokaler Anschluss beim Betrieb ohne Kommunikationsknoten).
- ✓ WaveNet-Topologie angelegt und gespeichert (siehe *RouterNode dem WaveNet hinzufügen* [► 57] und *LockNodes dem WaveNet hinzufügen* [► 64]).

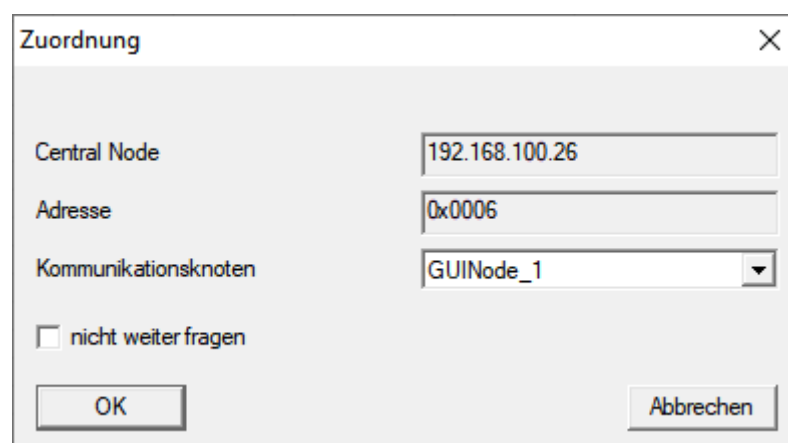
1. Klicken Sie auf die Schaltfläche **Beenden**.
 ↳ Fenster "WaveNetManager" öffnet sich.



2. Klicken Sie auf die Schaltfläche **Ja**.
 ↳ Fenster "WaveNetManager" schließt sich.
 ↳ Fenster "WaveNet-Topologie importieren" öffnet sich. Sie sehen eine Liste der zu importierenden Geräte.



3. Klicken Sie auf die Schaltfläche **Import**.
 ↳ Fenster "Zuordnung" öffnet sich.



4. Wählen Sie im Dropdown-Menü ▼ **Kommunikationsknoten** den Kommunikationsknoten in der LSM aus, den Sie für den RouterNode verwenden wollen (zur Erstellung siehe *Geräte finden und hinzufügen* [► 52] oder LSM-Handbuch).
5. Klicken Sie auf die Schaltfläche **OK**.
 - ↳ Fenster "Zuordnung" schließt sich.
 - ↳ Fenster "Ergebnis" öffnet sich.

Ergebnis

Net-Ids
In der Datenbank: In der WaveNet-Topologie Datei:

Central Nodes

Adresse	Name	Zustand
0x0006	192.168.100.26	bereits vorhanden

Fehler: Vorhanden: Werden eingefügt: **Alles auswählen**

Segmente

Adresse	Zustand
0x0020	wird eingefügt

Fehler: Vorhanden: Werden eingefügt: **Alles auswählen**

Knoten

Segm...	Adresse	Segm...	Adresse	Maske	NetzID	CN A...	Kno...	Name	Zustand
0x0020	0x0026	0x0000	0x0000	0xffe0	0x4fda	0x0006	L	WNNNode_0026	kann eingefügt werden

Fehler: Vorhanden: Werden eingefügt:

OK **Abbrechen**

6. Klicken Sie auf die Schaltfläche **OK**.
 - ↳ Fenster "Ergebnis" schließt sich.
 - ↳ Fenster "LockSysMgr" öffnet sich.

LockSysMgr

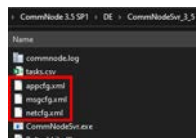
 **Die WaveNet-Topologie wurde erfolgreich importiert.**

OK

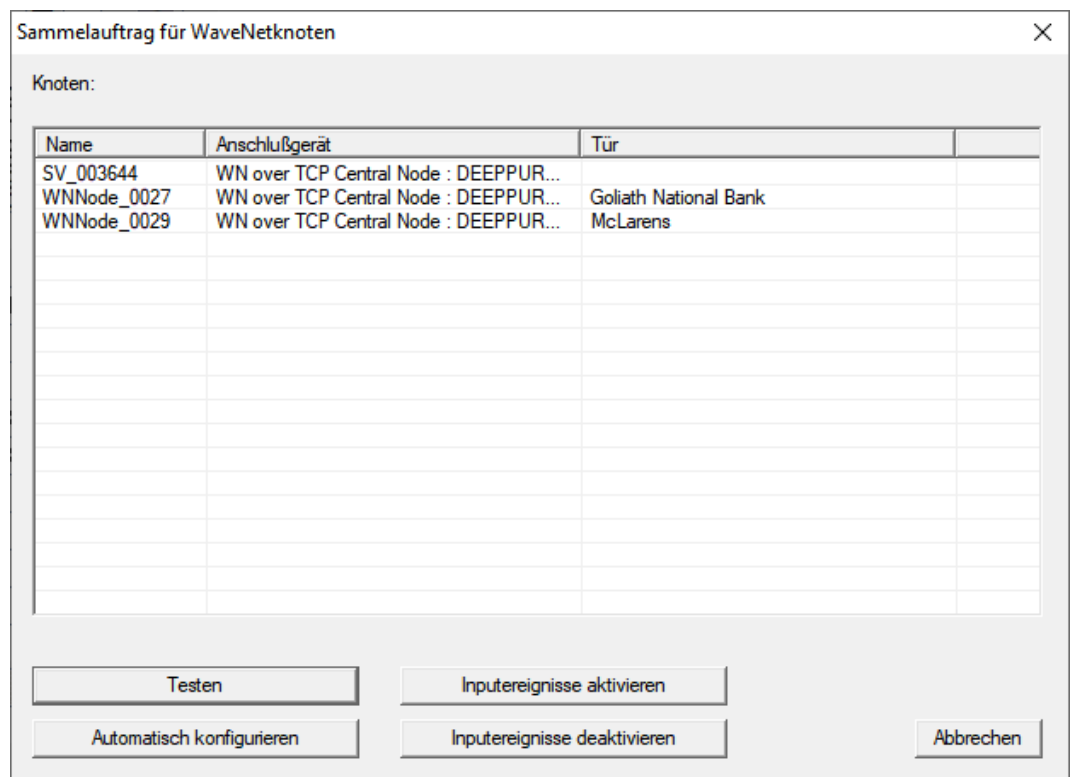
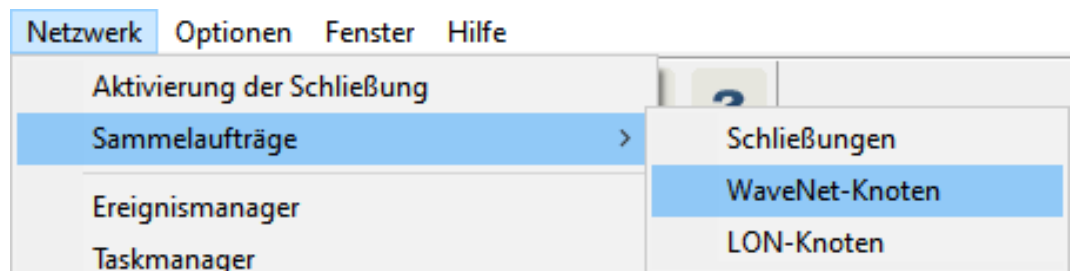
7. Klicken Sie auf die Schaltfläche **OK**.
 - ↳ Fenster "LockSysMgr" schließt sich.

An Kommunikati-
onsknoten übertra-
gen

- ↳ WaveNet-Manager schließt sich.
- ↳ WaveNet-Topologie ist importiert und RouterNode wird beim Kommunikationsknoten in der Liste der Anschlüsse aufgelistet.
- ✓ LSM geöffnet.
- 1. Wählen Sie über | Netzwerk | den Eintrag **Kommunikationsknoten** aus.
- 2. Wählen Sie mit den Schaltflächen ◀ oder ▶ den Kommunikationsknoten aus, den Sie eben verwendet haben.
- 3. Klicken Sie auf die Schaltfläche **Konfig-Dateien**.
 - ↳ Fenster "Ordner suchen" öffnet sich.
- 4. Stellen Sie sicher, dass das Installationsverzeichnis des CommNode-Servers ausgewählt ist.
- 5. Klicken Sie auf die Schaltfläche **OK**.
 - ↳ Fenster "Ordner suchen" schließt sich.
- 6. Klicken Sie auf die Schaltfläche **Nein**, um nicht in einen knotenspezifischen Ordner zu speichern.
 - ↳ XML-Konfigurationsdateien sind gespeichert.



- 7. Klicken Sie auf die Schaltfläche **Übertragen**.
 - ↳ Fenster "LockSysMgr" öffnet sich.
- 8. Klicken Sie auf die Schaltfläche **OK**.
 - ↳ Fenster "LockSysMgr" schließt sich.
- ↳ Daten sind an Kommunikationsknoten übertragen.



The screenshot shows a window titled 'WaveNet Manager' with a light gray background. It is divided into several sections:

- Erfolgreich:** A text box containing two lines of text: 'WNNode_0027 Goliath National Bank / 00DRXXM LID=129 SID=92' and 'WNNode_0029 McLaren / 00ESSNC LID=131 SID=9215'.
- Fehler:** An empty text box.
- In Bearbeitung:** An empty text box.
- Buttons:** At the bottom, there are four buttons: 'Beenden', 'Abbrechen', 'Erfolgsliste', and 'Fehlerliste'. Above the 'Erfolgsliste' and 'Fehlerliste' buttons is a 'Drucken' label.
- Checkbox:** A checkbox labeled 'Die gescheiterten Protokolle automatisch wiederholen, bis der Prozess angehalten wird.' is located to the right of the 'In Bearbeitung' box.
- Footer:** A button labeled 'Gescheiterte Protokolle wiederholen' is located at the bottom right.

Sie können Ihre Schließungen mit LockNodes nach der erfolgreichen Zuweisung über Ihr WaveNet ansprechen.

6.4.4 I/O-Konfiguration und Schutzfunktionen

Mit den Schutzfunktionen können Sie Schließungen über Funk (868 MHz) deaktivieren, aktivieren oder auch aus der Ferne öffnen. Sie legen dazu mit der IO-Konfiguration im WaveNet-Manager fest:

- Wann ein Ereignis ausgelöst wird (durch ein Identifikationsmedium oder einen Eingang, siehe *Eingang (Relaiskontakt)* [▶ 95]) und
- wie auf dieses Ereignis reagiert wird (Auslösen einer Schutzfunktion)

Schutzfunktionen sind grundsätzlich unabhängig von der LSM oder deren Diensten. Wenn Sie Schutzfunktionen verwenden, dann erhöhen Sie mit Ihrem WaveNet - im Zusammenspiel mit in öffentlichen Gebäuden ohnehin erforderlichen Sicherheitsmaßnahmen - das Sicherheitsniveau.



WARNUNG

Personen- oder Sachschäden durch nichtredundantes Sicherheitskonzept

Die Schutzfunktionen Ihres WaveNet-Systems sind nur ein Bestandteil eines Sicherheitskonzepts. Sie sind nicht als einzige Absicherung gegen Gefahren wie Brand, Einbruch oder ähnliches geeignet.

1. Verwenden Sie redundante Systeme zur Absicherung Ihrer individuellen Risiken (Einbruchsmeldeanlagen, Brandmeldeanlagen und ähnliche).
2. Lassen Sie durch einen technischen Risikomanager (Certified Security Manager oder vergleichbar) ein Sicherheitskonzept erstellen und bewerten.
3. Beachten Sie insbesondere relevante Vorschriften zu Flucht- und Rettungswegen.



HINWEIS

Proprietäres WaveNet ohne rechtliche Vorgaben

Das WaveNet ist eine SimonsVoss-Eigenentwicklung, um mit den angebotenen Schutzfunktionen zusätzlich zu vorhandenen Sicherheitskonzepten die Sicherheit Ihres Gebäudes weiter zu erhöhen. Aktuell gibt es zu diesen Schutzfunktionen keine bekannten rechtlichen Vorgaben.

Sie können die Eingänge und Ausgänge Ihres RouterNodes nach Ihren Bedürfnissen einstellen:

Ausgänge	Eingänge (digital)	Eingang (analog)
Reagieren Sie auf Identifikationsmedien oder quittieren Sie abgeschlossene Reaktionen, die von den digitalen Eingängen ausgelöst wurden. Schalten Sie die Ausgänge in Abhängigkeit von erkannten Identifikationsmedien (siehe <i>RouterNode: Digitaler Ausgang</i> [► 81]).	Reagieren Sie auf Zustandsänderungen an den digitalen Eingängen. Lösen Sie eine Reaktion an den verbundenen Schließungen aus (siehe <i>RouterNode: Digitaler Eingang</i> [► 84]).	Reagieren Sie auf Zustandsänderungen am analogen Eingang. Lösen Sie ein Ereignis in der LSM aus (siehe <i>RouterNode: Analoger Eingang</i> [► 90]).

Die Option  Ausgang setzen und I/O-Status zeigt Ihnen den aktuellen Zustand und das Ergebnis der letzten Reaktionen an (siehe *IO-Status und LockNode-Reaktionsfähigkeit* [► 200]).

Einzelner RouterNode

1. Klicken Sie mit der rechten Maustaste auf den Eintrag des RouterNodes, dessen I/O-Konfiguration Sie ändern wollen.
↳ Fenster "Administration" öffnet sich.

The screenshot shows a dialog box titled "Administration von RN_ER_IO (0x0006_0x0021; 89003644)". It has a close button (X) in the top right corner. The dialog is divided into two main sections: "Konfiguration" and "Wartung".

Konfiguration:

- Name: 192.168.100.26
- ☐ Ersetzen mit ...
- ☐ Zurücksetzen/Löschen
- ☐ Verschieben in ein anderes Mastersegment
- ☒ I/O-Konfiguration

Wartung:

- ☐ Mastersegment durchsuchen ☐ nur bekannt
- ☐ Zweig aktualisieren ☐ optimiert
- ☐ Suchen nach Chip ID
- ☐ Ping
- ☐ Neu starten
- ☐ Ausgang setzen und I/O-Status
- ☐ Qualität prüfen

Das Mastersegment besteht aus 2/25 LN_(X) und aus 0/4 Routern.

Buttons: OK, Beenden

2. Wählen Sie im Bereich "Konfiguration" die Option ☒ I/O-Konfiguration.
3. Klicken Sie auf die Schaltfläche **OK**.
↳ Fenster "Administration" schließt sich.
↳ Fenster "I/O Konfiguration" öffnet sich.

I/O Konfiguration für RN_ER_IO (0x0006_0x0021; 89003644)

Konfiguration digitaler Ausgang

I/O Anwendung :

1	2	3
Ausgang : Ausgang	Ausgang : Ausgang	Ausgang : Ausgang
LN auswählen		Ereignisse an Managementsystem übermitteln : keine

Konfiguration digitaler Eingang

1	2	3
Eingang : Eingang	Eingang : Eingang	Eingang : Eingang
Verzögerung [s] : 0	Verzögerung [s] : 0	Verzögerung [s] : 0
Ereignisse an Managementsystem übermitteln : ☐ Ja	Ereignisse an Managementsystem übermitteln : ☐ Ja	Ereignisse an Managementsystem übermitteln : ☐ Ja
LN auswählen : für alle Eingänge für Eingang 1 für Eingang 2 für Eingang 3		
Protokollgeneration :		Passwort unsichtbar
G1 Schließanlagenpasswort :		
G2 Schließanlagenpasswort :		

Konfiguration analoger Eingang

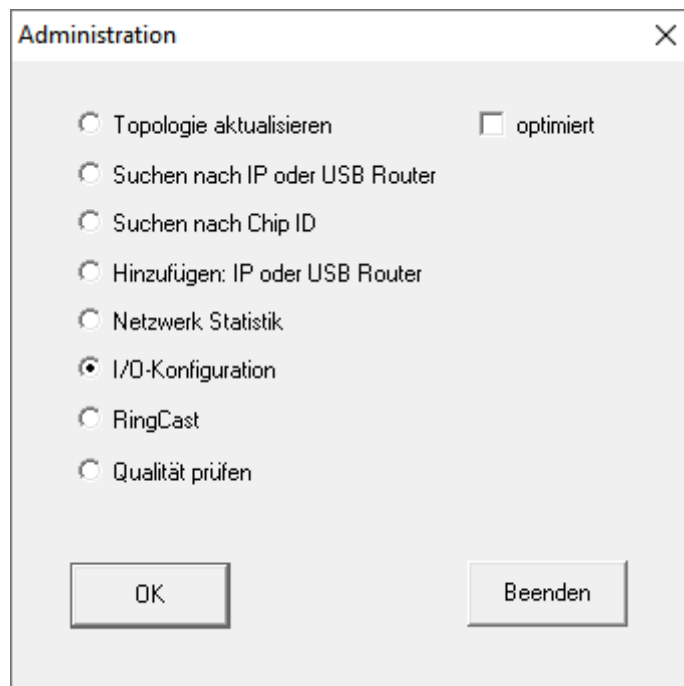
Eventverarbeitung :

Schwellwert [mV] : Unterschreitung : Überschreitung :

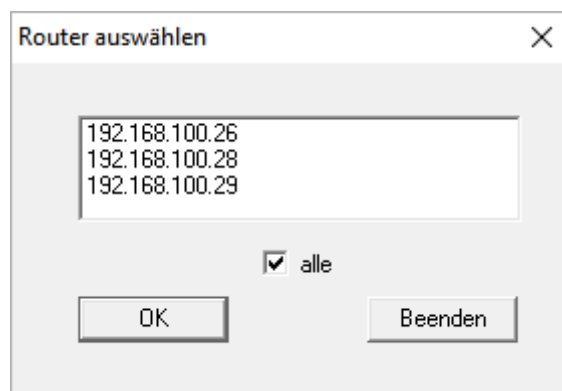
Abtastintervall [s] :

Mehrere RouterNodes

1. Klicken Sie mit der rechten Maustaste auf den Eintrag WaveNet_XX_X.
→ Fenster "Administration" öffnet sich.



2. Wählen Sie die ☒ I/O-Konfiguration.
3. Klicken Sie auf die Schaltfläche **OK**.
 - ↳ Fenster "Administration" schließt sich.
 - ↳ Fenster "Router auswählen" öffnet sich.



4. Markieren Sie entweder alle gewünschten RouterNodes oder aktivieren Sie die Checkbox ☒ alle.
5. Klicken Sie auf die Schaltfläche **OK**.
 - ↳ Fenster "Router auswählen" schließt sich.
 - ↳ Fenster "I/O Konfiguration" öffnet sich.

I/O Konfiguration für RN_ER_IO (0x0006_0x0021; 89003644)

Konfiguration digitaler Ausgang

I/O Anwendung :

1	2	3
Ausgang : Ausgang	Ausgang : Ausgang	Ausgang : Ausgang
LN auswählen		Ereignisse an Managementsystem übermitteln : keine

Konfiguration digitaler Eingang

1	2	3
Eingang : Eingang	Eingang : Eingang	Eingang : Eingang
Verzögerung [s] : 0	Verzögerung [s] : 0	Verzögerung [s] : 0
Ereignisse an Managementsystem übermitteln : ☐ Ja	Ereignisse an Managementsystem übermitteln : ☐ Ja	Ereignisse an Managementsystem übermitteln : ☐ Ja
LN auswählen : für alle Eingänge für Eingang 1 für Eingang 2 für Eingang 3		
Protokollgeneration :		Passwort unsichtbar
G1 Schließanlagenpasswort :		
G2 Schließanlagenpasswort :		

Konfiguration analoger Eingang

Eventverarbeitung :

Schwellwert [mV] : Unterschreitung : Überschreitung :

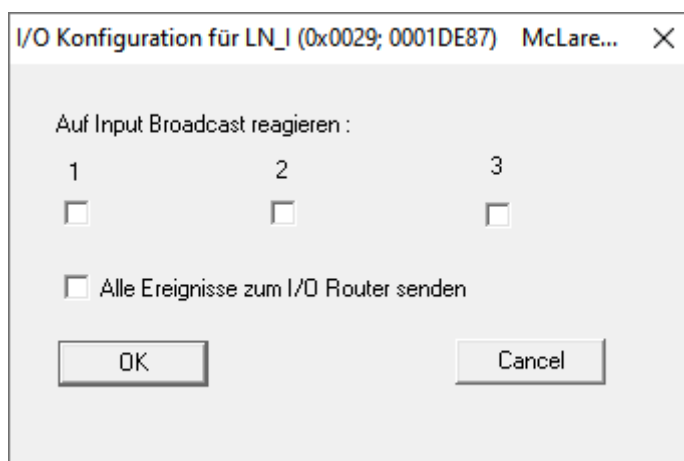
Abtastintervall [s] :

Einzelner LockNode

1. Klicken Sie mit der rechten Maustaste auf den Eintrag des LockNodes, dessen I/O-Konfiguration Sie verändern wollen.
↳ Fenster "Administration" öffnet sich.



2. Wählen Sie die ☒ I/O-Konfiguration.
3. Klicken Sie auf die Schaltfläche **OK**.
 - ↳ Fenster "Administration" schließt sich.
 - ↳ Fenster "I/O Konfiguration" öffnet sich.



6.4.4.1 Beschreibung der Optionen

RouterNode: Digitaler Ausgang

Konfiguration digitaler Ausgang

I/O Anwendung : Standard

1

2

3

Ausgang : Ausgang Ausgang Ausgang

LN auswählen

Ereignisse an Management-system übermitteln : keine

Sie können in der Dropdown-Liste ▼ I/O-Anwendung folgende Einträge auswählen:

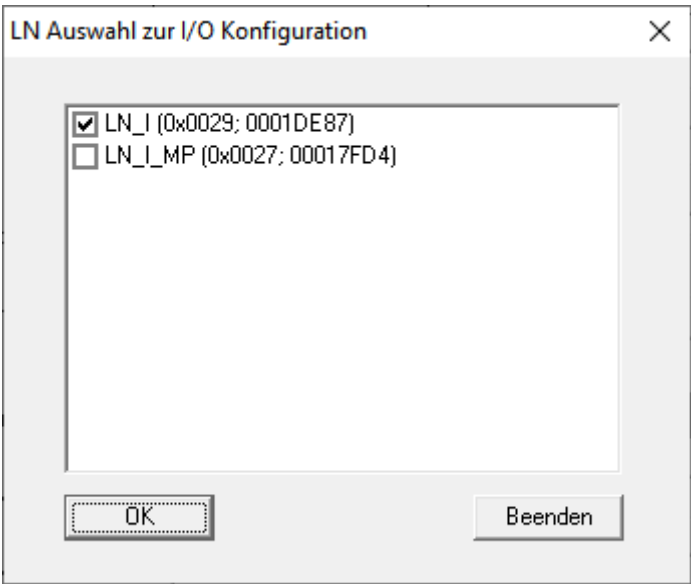
"Standard"	Standardeintrag.
------------	------------------

Sie können in der Dropdown-Liste ▼ Ausgang einstellen, wann der Ausgang im RouterNode schaltet:

"Ausgang"	Standardeintrag. Der RouterNode schaltet den Ausgang nicht. Sie können den Ausgang manuell schalten (siehe <i>IO-Status und LockNode-Reaktionsfähigkeit [► 200]</i>).
"berechtigt"	Der Ausgang schaltet bei einem berechtigten Identifikationsmedium an einer oder mehreren frei wählbaren Schließungen mit einem dem RouterNode zugeordneten LockNode für ca. eine Sekunde. Das Identifikationsmedium muss in der Schließanlage vorhanden sein.
"unberechtigter Versuch"	Der Ausgang schaltet bei einem unberechtigten Identifikationsmedium an einer oder mehreren frei wählbaren Schließungen mit einem dem RouterNode zugeordneten LockNode für ca. eine Sekunde. Das Identifikationsmedium muss in der Schließanlage vorhanden sein.
"alle LN Ereignisse"	Der Ausgang schaltet bei einem beliebigen Identifikationsmedium an einer oder mehreren frei wählbaren Schließungen mit einem dem RouterNode zugeordneten LockNode für ca. eine Sekunde. Das Identifikationsmedium muss in der Schließanlage vorhanden sein.

"Input Quittung kurz" (an allen LockNodes)	Der Ausgang schaltet, wenn die Reaktion (siehe <i>RouterNode: Digitaler Eingang [► 84]</i>) auf ein Signal am entsprechenden Eingang an allen LockNodes durchgeführt wurde (=Inputereignis) für ca. eine Sekunde.	
"Input Quittung statisch" (an allen LockNodes)	Der Ausgang schaltet, wenn die Reaktion (siehe <i>RouterNode: Digitaler Eingang [► 84]</i>) auf ein Signal am entsprechenden Eingang an allen LockNodes durchgeführt wurde. Solange das Inputereignis nach Abschluss der Reaktion anliegt, bleibt der Ausgang geschaltet.	
Ausgang 1	O1	Relaisausgang, besteht aus O1.NC, O1.NO und O1.COM ■ NC=Normally connected, ist im Ruhezustand mit COM verbunden. ■ NO=Normally open, ist im Ruhezustand nicht mit COM verbunden. Wenn der Ausgang geschaltet wird, dann zieht das Relais an und wechselt vom Ruhezustand in den bestromten Zustand.
Ausgang 2	O2	Digitaler Ausgang (Open Drain), max. 12 V_{DC}, max. 100 mA (ohmsche Belastung) Wenn der Ausgang geschaltet wird, dann wird der Ausgang mit dem Massepotential verbunden.
Ausgang 3	O3	Digitaler Ausgang (Open Drain), max. 12 V_{DC}, max. 100 mA (ohmsche Belastung) Wenn der Ausgang geschaltet wird, dann wird der Ausgang mit dem Massepotential verbunden.

Sie können mit der Schaltfläche **LN auswählen** das Fenster "LN Auswahl zur I/O-Konfiguration" öffnen. Wählen Sie hier die LockNodes in Schließungen aus. Berechtigte Zutritte bzw. unberechtigte Zutrittsversuche an diesen Schließungen (LockNodes) werden an die LSM weitergeleitet.



In der LSM können Sie mit dem Ereignismanager auf das weitergeleitete Ereignis reagieren.

Sie können in der Dropdown-Liste ▼ **Ereignisse an Managementsystem übermitteln** einstellen, welche Ereignisse an den vorher markierten LockNodes an die LSM weitergeleitet werden:

"keine"	Standardeintrag. Es gibt kein Ereignis und keine Weiterleitungen.
"berechtigt"	Berechtigte Zutritte an den markierten Schließungen (LockNodes) werden an die LSM weitergeleitet (=Ereignis, das an die LSM weitergeleitet wird).
"unberechtigter Versuch"	Unberechtigter Zutrittsversuche an den markierten Schließungen (LockNodes) werden an die LSM weitergeleitet (=Ereignis, das an die LSM weitergeleitet wird).
"alle LN Ereignisse"	Berechtigte Zutritte und unberechtigte Zutrittsversuche an den markierten Schließungen (LockNodes) werden an die LSM weitergeleitet (=Ereignis, das an die LSM weitergeleitet wird).

Alternativ können Sie auch direkt an den LockNodes einstellen, ob die LockNodes Ereignisse an den RouterNode weiterleiten (siehe [LockNode \[92 \]](#)).

Wählen Sie hier das Ereignis aus, das die Weiterleitung an die LSM auslöst. Wenn das hier festgelegte Ereignis ("berechtigt", "unberechtigter Versuch" oder "alle LN Ereignisse") an den Schließungen (LockNodes), die Sie vorher bestimmt haben (**LN auswählen**) auftritt, dann wird das Ereignis an die LSM weitergeleitet.



HINWEIS

Selbes Ereignis zur Weiterleitung

Sie können LockNodes (und damit die Schließung, in die der LockNode eingebaut ist) nicht markieren und somit von der Ereignisweiterleitung ausnehmen. Wenn Sie die Ereignisweiterleitung nutzen, dann gilt dasselbe Ereignis für alle (in **LN auswählen**) markierten LockNodes.

Sie können zum Beispiel nicht für einen LockNode nur berechtigte Zutritte und für einen anderen nur unberechtigte Zutrittsversuche weiterleiten.

RouterNode: Digitaler Eingang

Sie können in der Dropdown-Liste ▼ **Eingang** einstellen, wie die LockNodes des RouterNodes auf ein am jeweiligen RouterNode-Eingang anliegendes Signal reagieren sollen. (=Anliegende Spannung ist höher als die fix eingestellte Vergleichsspannung).

Vergleichsspannungen (RN und RN2)

$< 0,9 V_{DC}$	LOW (kein Signal)
$> 2,1 V_{DC}$	HIGH (Signal)

"Eingang"	Standardeintrag. Der RouterNode reagiert nicht auf ein anliegendes Signal. Sie können die Signalwechsel aber an die LSM weiterleiten.
-----------	---

"Blockschloß"	Wenn am Eingang ein Signal anliegt (Inputereignis, Pegelwechsel Low zu High), dann sendet der RouterNode einen Broadcast an alle LockNodes. Sie können einstellen, ob die LockNodes auf den Broadcast reagieren sollen (siehe LockNode [► 92]). Die LockNodes deaktivieren dann für die Dauer des Inputereignisses die Schließungen, in denen sie eingebaut sind. Sie reagieren dann nicht mehr auf berechtigte Identifikationsmedien, es ist kein Zutritt möglich. Wenn das Signal nicht mehr anliegt (=kein Inputereignis mehr, Pegelwechsel High zu Low), dann werden die Schließungen wieder aktiviert. Wenn Sie durch eine Einbruchsmeldeanlage während der Scharfschaltung an den Eingang ein Signal anlegen, dann können Sie somit für die Dauer der Scharfschaltung der Alarmanlage die Schließungen der Außenhülle deaktivieren (und das ungewollte Auslösen der Alarmanlage verhindern). Sie können aber auch frei wählen, welche Schließungen Sie deaktivieren wollen. Mit den Ausgängen (siehe RouterNode: Digitaler Ausgang [► 81]) können Sie eine Quittung nach erfolgreicher Deaktivierung an die Einbruchsmeldeanlage zurückschicken. Die Verwendung dieser Funktion ist nicht VdS-konform.
---------------	---

"Amokfunktion"	Ähnlich der Blockschlossfunktion: Wenn am Eingang ein Signal anliegt (Pegelwechsel Low zu High), dann sendet der Router-Node einen Broadcast an alle LockNodes. Sie können einstellen, ob die LockNodes auf den Broadcast reagieren sollen (siehe LockNode [► 92]). Dieser Broadcast deaktiviert die Schließungen, in denen der LockNode eingebaut ist. Sie weisen dann alle Identifikationsmedien (auch normalerweise berechnete) ab, der einmalige Zutritt ist nur mit speziellen Identifikationsmedien möglich (rote Ebene). Der Unterschied zur Blockschlossfunktion ist, dass die Schließungen auch nach dem Ende des Inputereignisses deaktiviert bleiben. Sie müssen die Schließungen explizit mit einem Aktivierungsbefehl wieder aktivieren: ■ WaveNet (Reaktion "Aktivierung" verwenden) ■ LSM ■ Aktivierungstransponder bzw. -karte Wenn Sie einen Notknopf an einen Eingang anschließen (siehe Eingang (Taster) [► 94]) und diesen mit der Amokfunktion verbinden, dann können Sie mit dem Notknopf alle erreichten Schließungen blockieren und verhindern, dass Räume betreten (oder im Falle eines freidrehenden Zylinders auch verlassen) werden können, bis sie explizit wieder aktiviert werden.
"Notfreischaltung"	Entgegengesetzt zur Amokfunktion: Wenn am Eingang ein Signal anliegt (Pegelwechsel Low zu High), dann sendet der RouterNode einen Broadcast an alle LockNodes. Sie können einstellen, ob die LockNodes auf den Broadcast reagieren sollen (siehe LockNode [► 92]). Dieser Broadcast kuppelt alle Schließungen, in die die LockNodes eingebaut sind, dauerhaft ein. Die Schließungen bleiben auch nach dem Ende des Inputereignisses eingekuppelt. Sie müssen die Notfreischaltung der Schließungen mit einem Fernöffnungsbefehl beenden (die Schließungen kuppeln unmittelbar nach dem Eintreffen des Fernöffnungsbefehls wieder aus): ■ WaveNet (Reaktion "Fernöffnung" verwenden) ■ LSM Wenn Sie durch eine Brandmeldeanlage an den Eingang ein Signal anlegen (siehe Einsatzbeispiele [► 94]), dann können Sie somit alle Schließungen öffnen, um Rettungskräften den Zugriff zu ermöglichen.

"Fernöffnung"	Wenn am Eingang ein Signal anliegt (Pegelwechsel Low zu High), dann sendet der RouterNode einen Broadcast an alle LockNodes. Sie können einstellen, ob die LockNodes auf den Broadcast reagieren sollen (siehe LockNode [► 92]). Dieser Broadcast führt eine Fernöffnung durch. Die Schließung kuppelt für die in der LSM eingestellte Pulsdauer ein (Impulsöffnung). Das gilt auch für Schließungen im Flip-Flop-Betrieb.
"Aktivierung"	Wenn am Eingang ein Signal anliegt (Pegelwechsel Low zu High), dann sendet der RouterNode einen Broadcast an alle LockNodes. Sie können einstellen, ob die LockNodes auf den Broadcast reagieren sollen (siehe LockNode [► 92]). Dieser Broadcast aktiviert die Schließungen, in die die LockNodes eingebaut sind. Sie können dann zuvor deaktivierte Schließungen wieder verwenden. Diese Reaktion funktioniert nur mit I/O-RouterNodes vom Typ RN2 ab Firmwareversion 40.8 zusammen mit der WaveNet-Manager-Version 2.6.6 oder neuer.



HINWEIS

Dauerhafte Notöffnung

Ein Brand kann das Inputkabel oder andere Teile beschädigen. Damit würden die Schließungen wieder schließen, obwohl es brennt. Personen könnten im Brandbereich eingesperrt werden und Rettungskräfte am Zutritt gehindert werden.

Deshalb bleiben alle Schließungen im Zustand Notöffnung (und damit passierbar), bis ein expliziter Fernöffnungsbefehl die Schließungen wieder schließt.

Wenn Sie eine Reaktion auf ein Ereignis festlegen, dann müssen Sie zusätzliche Angaben machen.

1. Wählen Sie die LockNodes aus, die reagieren sollen.
2. Geben Sie die Protokollgeneration (G1, G1+G2, G2) so an, wie sie in den Einstellungen der Schließanlage eingetragen ist.
3. Geben Sie das Schließanlagenpasswort an.

Ein am Eingang anliegendes Signal ist ein Inputereignis und kann auch durch das eingebaute Relais geschaltet werden, siehe ▼ **Ausgang** in [RouterNode: Digitaler Ausgang \[► 81\]](#). Wenn der RouterNode auf das Inputereignis reagiert hat und zum Beispiel einen Broadcast durchgeführt hat, kann er somit als Bestätigung das Relais schalten.

Sie können in der Dropdown-Liste ▼ **Verzögerung [s]** einstellen, wie lange der RouterNode warten soll, bis der entsprechende Eingang auf ein Ereignis reagiert.

"0 s"	Standardeintrag. Der Eingang reagiert sofort auf ein Ereignis.
"8 s"	Der Eingang reagiert nach 8 Sekunden auf ein Ereignis
"16 s"	Der Eingang reagiert nach 16 Sekunden auf ein Ereignis
"24 s"	Der Eingang reagiert nach 24 Sekunden auf ein Ereignis
"32 s"	Der Eingang reagiert nach 32 Sekunden auf ein Ereignis
"RingCast"	Ein Ereignis am Eingang löst einen RingCast aus (siehe <i>RingCast</i> [▶ 103]).

Auslösende Ereignisse an die LSM weiterleiten

Sie können mit der Checkbox ☒ Ereignisse an Managementsystem übermitteln einstellen, ob die Signale (Inputereignisse), am jeweiligen Eingang an die LSM weitergeleitet werden sollen. In der LSM können Sie (zusätzlich) mit dem Ereignismanager auf diese Ereignisse reagieren.

Nicht alle Ereignisse werden weitergeleitet (siehe Tabelle):

Reaktion	Weiterleitbare Signale (Ereignisse)
■ "Amokfunktion" ■ "Notfreischaltung" ■ "Fernöffnung" ■ "Aktivierung"	■ Pegelwechsel Low zu High
■ "Eingang" ■ "Blockschloß"	■ Pegelwechsel Low zu High ■ Pegelwechsel High zu Low

Nur Ereignisse, die die Reaktionen "Eingang" oder "Blockschloß" werden an die LSM weitergeleitet. Alle anderen Ereignisse werden nicht an die LSM weitergeleitet.

LockNodes für Reaktion auswählen

Sie können mit der Schaltfläche **LN auswählen** einstellen, welche LockNodes die eingestellte Reaktion durchführen. Sie haben zwei Möglichkeiten zur Einstellung:

(Unterschiedliche) Einstellungen für einzelne Eingänge des RouterNodes	Gleiche Einstellung für alle Eingänge des RouterNodes
Klicken Sie auf die Schaltfläche des jeweiligen Eingangs (Für Input 1, 2 oder 3). Das Fenster des Eingangs öffnet sich. Markieren Sie im die LockNodes, die auf die Ereignisse dieses Eingangs reagieren sollen. Gehen Sie bei den anderen Eingängen ebenso vor. Hier markierte LockNodes reagieren auf alle Ereignisse an diesem Eingang. Sie führen die Reaktion aus, die Sie für diesen Eingang festgelegt haben.	Klicken Sie auf die Schaltfläche für alle Eingänge und wählen Sie die LockNodes aus. Hier markierte LockNodes reagieren auf alle Ereignisse an den Eingängen. Sie führen die Reaktion aus, die Sie für den jeweiligen Eingang festgelegt haben.

Das nachstehende Beispiel veranschaulicht das Verhalten je nach Einstellung:

Für Ereignisse an Input 1 und 2 wird "Fernöffnung" als Reaktion angenommen.

Beispiel für Einstellungen				
	Alle Eingänge	Input 1	Input 2	Input 3
LockNode 1	✓			
LockNode 2		✓		
LockNode 1 reagiert auf alle Ereignisse. LockNode 2 reagiert nur auf Ereignisse des Inputs 1. Anders gesagt: Mit einem Tastendruck an Input 1 erhalten alle Schließungen einen Fernöffnungsbefehl. Mit einem Tastendruck an Input 2 erhält nur die Schließung mit LockNode 1 einen Fernöffnungsbefehl.				

Alternativ können Sie auch direkt an den LockNodes einstellen, ob sie Reaktionen durchführen (siehe [LockNode \[92 \]](#)).

Sie geben mit dem Dropdown-Menü ▼ **Protokollgeneration** die Protokollgeneration der Schließanlage an.

Die LockNodes sprechen mit dem Schließanlagenpasswort die Schließungen an. Geben Sie deshalb Ihr Schließanlagenpasswort an.

Klicken Sie auf die Schaltfläche **Passwort unsichtbar**, um zu verhindern, dass Ihr Passwort während der Eingabe im Klartext angezeigt wird.

RouterNode: Analoger Eingang

Konfiguration analoger Eingang

Eventverarbeitung :

Kein Ereignis ▼

Schwellwert [mV] :

Unterschreitung :

999

Überschreitung :

1199

Abtastintervall [s]:

60

Sie können in der Dropdown-Liste ▼ **Eventverarbeitung** einstellen, wann eine Spannungsänderung am analogen Eingang des RouterNodes ein Ereignis (siehe *RouterNode: Digitaler Ausgang* [▶ 81]) auslöst.

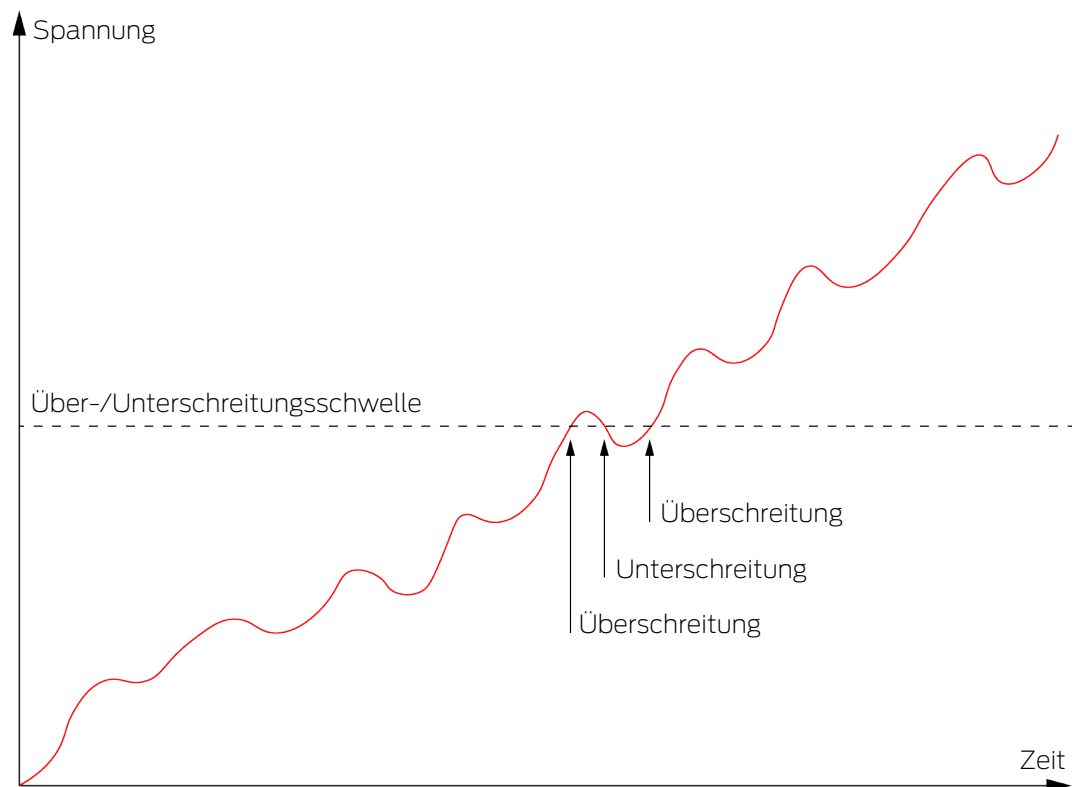
"Kein Ereignis"	Standardeintrag. Der RouterNode reagiert nicht auf ein anliegendes Signal.
"Bei Überschreitung"	Wenn die anliegende Spannung steigt, dann überschreitet sie irgendwann den Schwellwert zur Überschreitung. In diesem Moment wird das Ereignis ausgelöst.
"Bei Unterschreitung"	Wenn die anliegende Spannung sinkt, dann unterschreitet sie irgendwann den Schwellwert zur Unterschreitung. In diesem Moment wird das Ereignis ausgelöst.
"Bei Überschreitung / Unterschreitung"	Wenn sich die anliegende Spannung verändert und folgende Szenarien eintreten, dann wird das Ereignis ausgelöst. ■ Spannung sinkt und unterschreitet den Schwellwert zur Unterschreitung ■ Spannung steigt und überschreitet den Schwellwert zur Überschreitung

Sie können mit dem Abtastintervall angeben, wie oft das anliegende Signal mit den Schwellwerten verglichen wird.

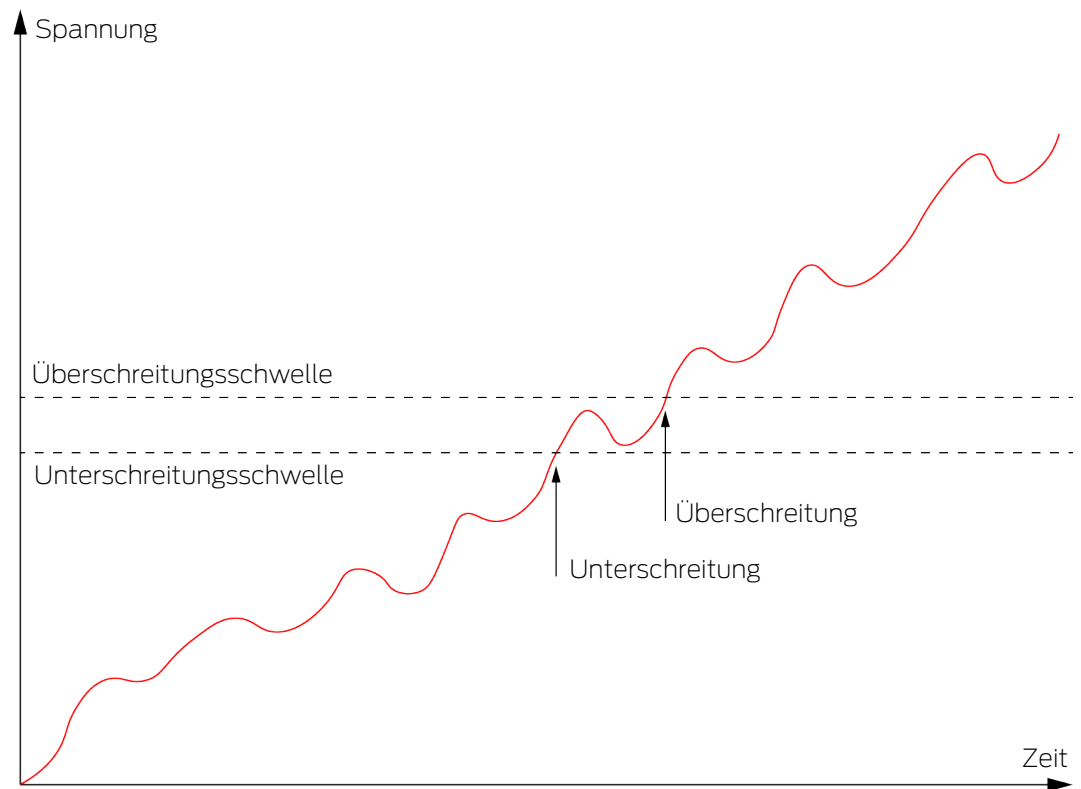
**HINWEIS****200-mV-Hystereseband**

Das anliegende Analogsignal kann je nach Beschaffenheit störungsanfällig sein und geringfügig schwanken. Wenn die Schwellwerte zu dicht beieinander liegen würden, dann würden bereits geringe Änderungen der Spannung mehrere unbeabsichtigte Ereignisse nacheinander auslösen.

Der WaveNet-Manager stellt den Schwellwert für die Unterschreitung automatisch um 200 mV niedriger als den Schwellwert für die Überschreitung ein (Hysteresis). Die Betriebssicherheit des RouterNodes wird so erhöht.



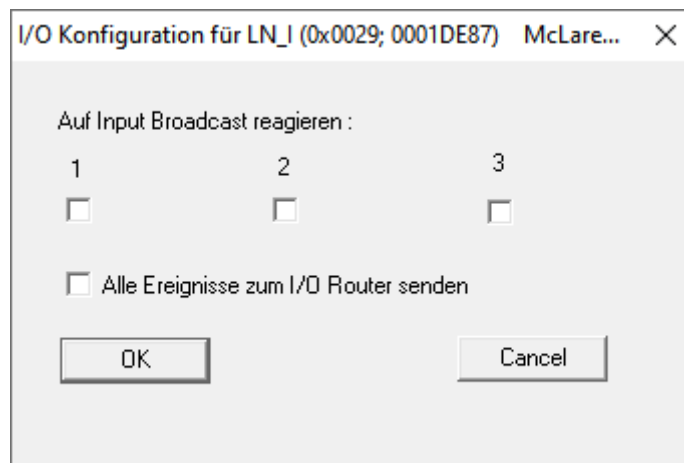
Ohne Hysteresis löst derselbe Spannungsverlauf zweimal eine Überschreitung aus.



Mit Hysterese löst derselbe Spannungsverlauf genau eine Überschreitung aus. Die Überschreitung wird erst wieder erkannt, nachdem die Unterschreitungsschwelle unterschritten wurde.

LockNode

- ✓ WaveNet-Manager über LSM geöffnet (siehe *Best Practice: Aus der LSM-Software* [► 40]).
- ✓ LockNodes erreichbar (siehe *Erreichbarkeit testen (WaveNet)* [► 195]).
- Klicken Sie mit der rechten Maustaste auf den Eintrag des LockNodes, dessen IO-Konfiguration Sie verändern wollen.
 - ↳ Fenster "I/O Konfiguration" öffnet sich (Fenster und Einstellungen versionsabhängig, Bild beispielhaft).



→ Sie können die IO-Konfiguration einstellen.

Reaktionen aktivieren

Wenn der RouterNode an einem seiner digitalen Eingänge ein Inputereignis erkennt und eine Reaktion eingestellt ist (siehe *RouterNode: Digitaler Eingang* [▶ 84]), dann sendet der RouterNode für einen Broadcast. Sie stellen mit der oberen Reihe von Checkboxes für jeden der drei Eingänge einzeln ein, ob der ausgewählte LockNode auf den Broadcast, der durch das Ereignis am jeweiligen Eingang verursacht wurde, reagiert.

Alternativ können Sie die Reaktion auch für mehrere LockNodes gleichzeitig aktivieren. Rufen Sie dazu das IO-Konfigurationsmenü des RouterNodes auf (siehe *RouterNode: Digitaler Eingang* [▶ 84]).

Ereignisweiterleitung aktivieren

Der RouterNode kann

- auf bestimmte Ereignisse reagieren (siehe *RouterNode: Digitaler Ausgang* [▶ 81])
- und/oder diese Ereignisse an die LSM weiterleiten.

Sie können direkt am LockNode einstellen, ob dieser die Ereignisse an den RouterNode weiterleitet. Aktivieren Sie die Checkbox ☒ Alle Ereignisse zum I/O-Router senden, um alle Ereignisse an den RouterNode weiterzuleiten. Auf diese Ereignisse können Sie entweder mit dem RouterNode (siehe *RouterNode: Digitaler Ausgang* [▶ 81]) oder in der LSM reagieren.

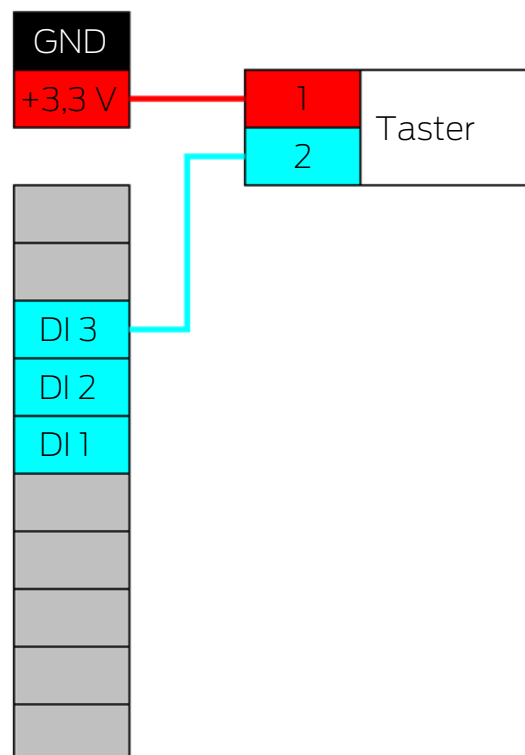
Alternativ können Sie die Ereignisweiterleitung auch für mehrere LockNodes eines RouterNodes gleichzeitig aktivieren. Rufen Sie dazu das IO-Konfigurationsmenü des RouterNodes auf (siehe *RouterNode: Digitaler Ausgang* [▶ 81]).

6.4.4.2 Einsatzbeispiele

Die folgenden Beispiele beschreiben den Anschluss am RouterNode 2. Die Beschaltung an der älteren RouterNode-Generation ist ähnlich.

Eingang (Taster)

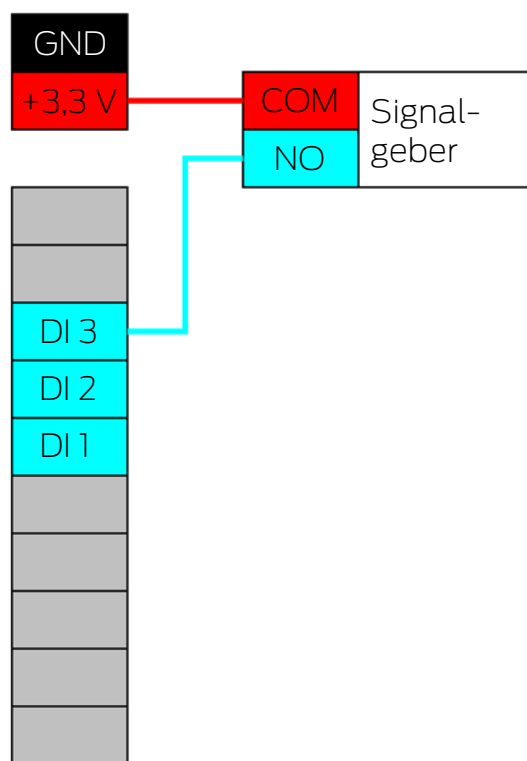
Verwenden Sie diesen Aufbau, um mit einem Taster einen Eingang zu schalten. Sie können so manuell einen Eingang schalten.



1. Verbinden Sie einen Kontakt des Tasters mit Kontakt auf der Platine, der neben dem IO-Connector liegt und für +3,3 V_{DC} vorgesehen ist.
2. Verbinden Sie den anderen Kontakt des Tasters mit einem der digitalen Eingänge DI1, DI2 oder DI3.

Eingang (Relaiskontakt)

Verwenden Sie diesen Aufbau, um mit einem Relaiskontakt einen Eingang zu schalten. Der Relaiskontakt kann durch ein Fremdsystem gesteuert werden. Sie können so ein Fremdsystem an das WaveNet anschließen.

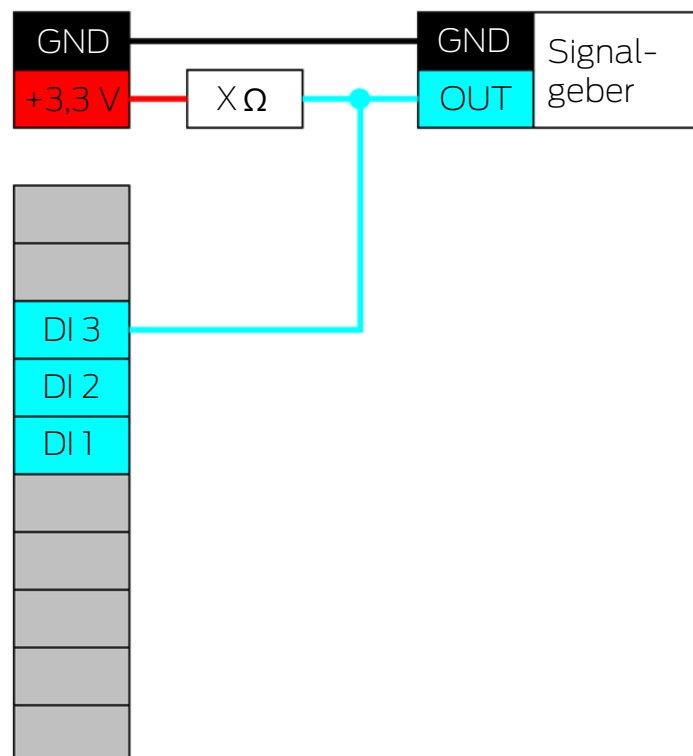


1. Verbinden Sie den COM-Anschluss des Relais mit dem Pluspol des Stromanschlusses neben dem IO-Connector.
2. Verbinden Sie den NO-Anschluss des Relais mit einem der digitalen Eingänge DI1, DI2 oder DI3.

Eingang (Open-Drain)

Verwenden Sie diesen Aufbau, um mit einem Open-Drain-Ausgang einen Eingang zu schalten. Der Open-Drain-Ausgang kann durch ein Fremdsystem gesteuert werden. Sie können so ein Fremdsystem an das WaveNet anschließen. Beachten Sie, dass das Schaltverhalten invertiert wird:

- Open-Drain des Signalgebers offen/ungeschaltet: Pull-Up-Widerstand "zieht" den digitalen Eingang auf +3,3 V_{DC} (High-Level). Ein Ereignis wird für diesen Input erkannt.
- Open-Drain des Signalgebers geschlossen/geschaltet: Eingang wird mit Masse kurzgeschlossen (Low-Level).



1. Verbinden Sie die Massepotentiale des Signalgebers und des RouterNodes.
2. Verbinden Sie den Pluspol des Stromanschlusses neben dem IO-Connector über den Pull-Up-Widerstand X mit dem Open-Drain-Ausgang des Signalgebers.
3. Verbinden Sie zusätzlich den Open-Drain-Ausgang des Signalgebers mit einem der digitalen Eingänge DI1, DI2 oder DI3.

Der Pull-Up-Widerstand ist abhängig vom Open-Drain-Ausgang des Signalgebers. Ein möglicher Wert ist 1 kΩ.

ACHTUNG**Berechnung des Pull-Up-Widerstands**

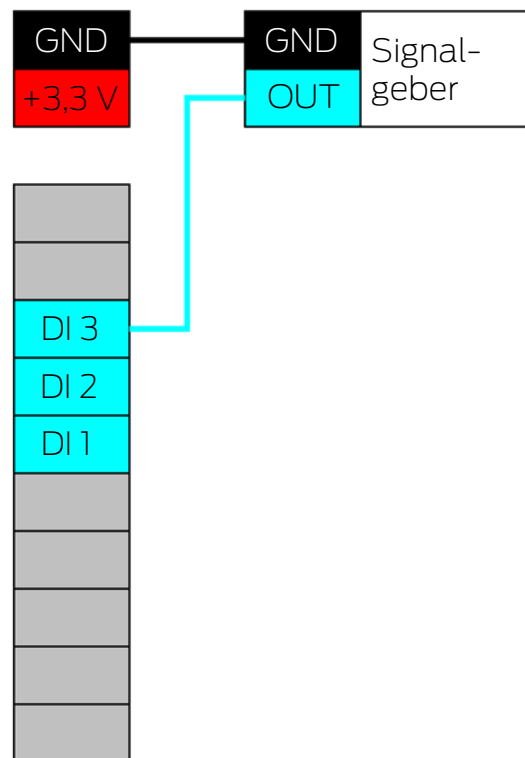
Zu kleine Pull-Up-Widerstände können den Stromanschluss neben dem IO-Connector beschädigen und den Open-Drain-Anschluss des Signalgebers überfordern. Zu große Pull-Up-Widerstände machen das Signal un sauber.

Der Pull-Up-Widerstand muss so klein wie möglich und so groß wie nötig sein.

1. Wählen Sie keinen Wert unter 16,5 Ω .
2. Wählen Sie keine unnötig großen Werte.

Eingang (Push-Pull)

Verwenden Sie diesen Aufbau, um mit einem Push-Pull-Ausgang einen Eingang zu schalten. Der Push-Pull-Ausgang kann durch ein Fremdsystem gesteuert werden. Sie können so ein Fremdsystem an das WaveNet anschließen.



1. Verbinden Sie die Massepotentiale des Signalgebers und des RouterNodes.
2. Verbinden Sie den Push-Pull-Ausgang des Signalgebers mit einem der digitalen Eingänge DI1, DI2 oder DI3.

ACHTUNG

Spannungsbereiche der digitalen Eingänge

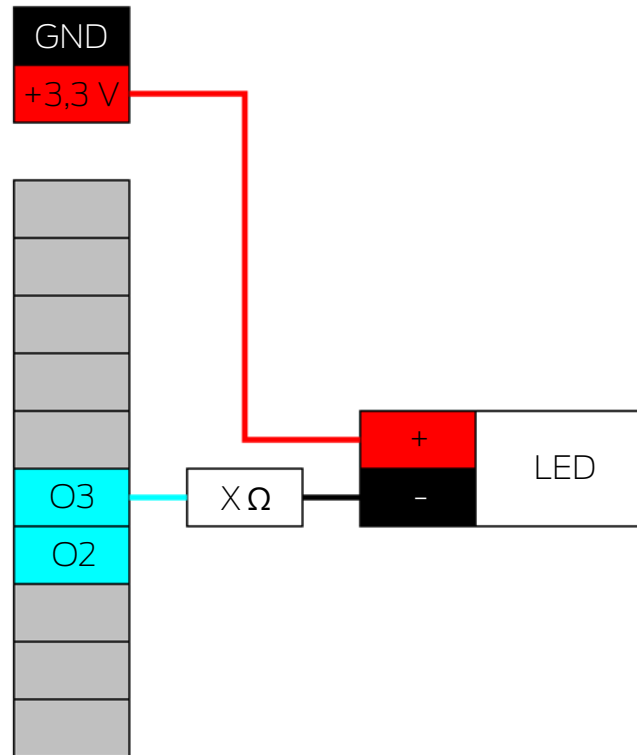
Der Push-Pull-Ausgang kann mit ungeeigneten Spannungen arbeiten. Damit das Signal verlässlich als HIGH und LOW erkannt wird, muss es sich je nach Signalpegel ober- oder unterhalb der Vergleichsspannungen befinden. Die maximale Ausgangsspannung des Push-Pull-Ausgangs darf $3,3\text{ V}_{\text{DC}}$ nicht überschreiten.

1. Verwenden Sie keine Push-Pull-Ausgänge, deren Spannungswerte für HIGH und LOW nicht zu den Vergleichsspannungen des RouterNode 2 passen.
2. Verwenden Sie keine Push-Pull-Ausgänge, deren maximale Ausgangsspannung $3,3\text{ V}_{\text{DC}}$ überschreitet.

Vergleichsspannungen (RN und RN2)	
$< 0,9 V_{DC}$	LOW (kein Signal)
$> 2,1 V_{DC}$	HIGH (Signal)

Ausgang (LED)

Schließen Sie die LED an O2 oder O3 an, um damit den zweiten oder dritten Ausgang anzuzeigen.



1. Verbinden Sie die Kathode der LED (-) über den Vorwiderstand X mit O3 oder O2.
2. Verbinden Sie die Anode (+) mit dem Pluspol des Stromanschlusses neben dem IO-Connector.

Der Wert des Vorwiderstands X hängt von der verwendeten LED ab.

ACHTUNG

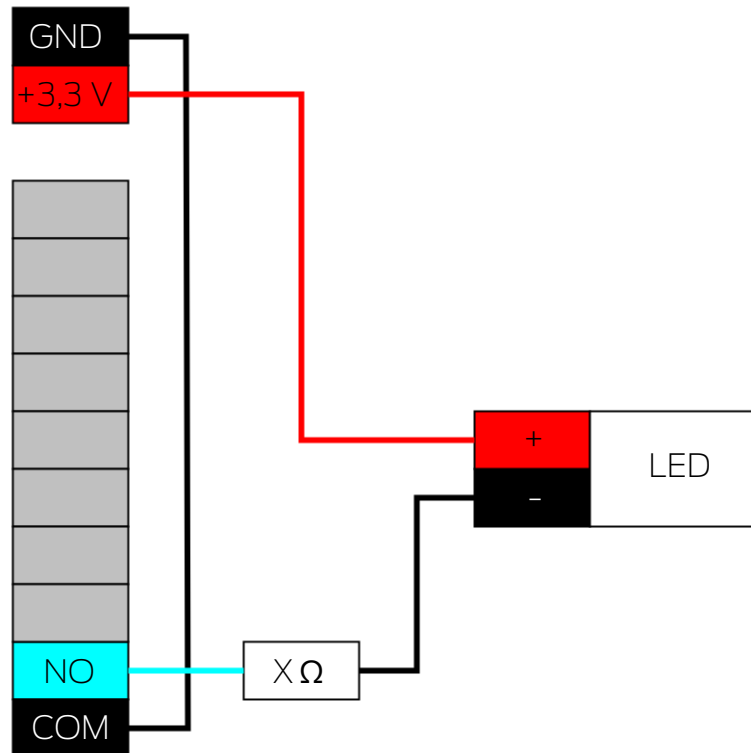
Strombelastbarkeit

Der Stromanschluss neben dem IO-Connector liefert zwischen 3,0 V_{DC} und 3,3 V_{DC} und darf mit maximal 200 mA belastet werden.

- Verwenden Sie den Anschluss nicht, um Geräte zu betreiben, die diese Spezifikationen überschreiten.

Ausgang (LED an Relais)

Schließen Sie die LED an das Relais an, um damit den ersten Ausgang anzuzeigen.



1. Verbinden Sie NO mit der Masse des RouterNodes.
2. Verbinden Sie dann die Kathode der LED (-) über den Vorwiderstand X mit COM.
3. Verbinden Sie die Anode (+) mit dem Pluspol des Stromanschlusses neben dem IO-Connector.

Der Wert des Vorwiderstands X hängt von der verwendeten LED ab.

ACHTUNG

Strombelastbarkeit

Der Stromanschluss neben dem IO-Connector liefert zwischen 3,0 V_{DC} und 3,3 V_{DC} und darf mit maximal 200 mA belastet werden.

Ausgang (Leuchte mit erhöhtem Strombedarf)

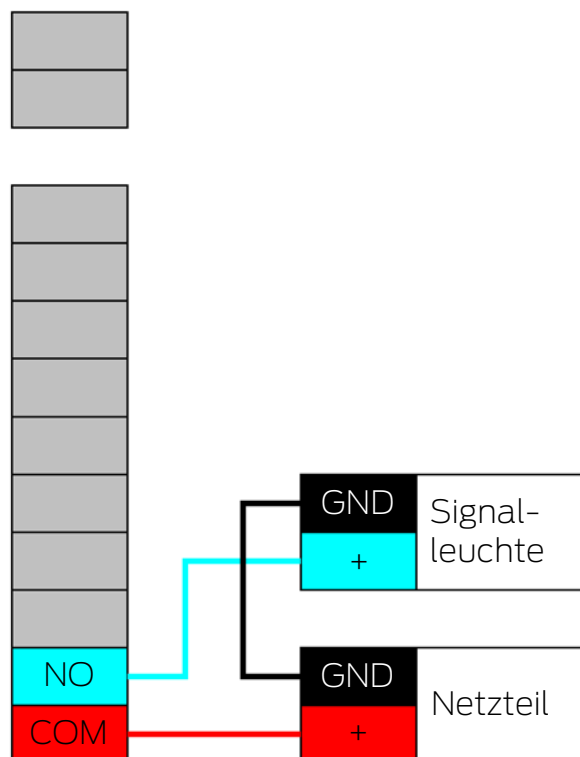
Leuchten mit erhöhtem Strombedarf sind in diesem Zusammenhang Lichtquellen, die mit mehr als 3,3 V_{DC} und/oder 200 mA betrieben werden. Schließen Sie diese Leuchten nicht an den Stromanschluss neben dem IO-Connector an, sondern verwenden Sie ein geeignetes Netzteil.

ACHTUNG

Belastbarkeit des Relais

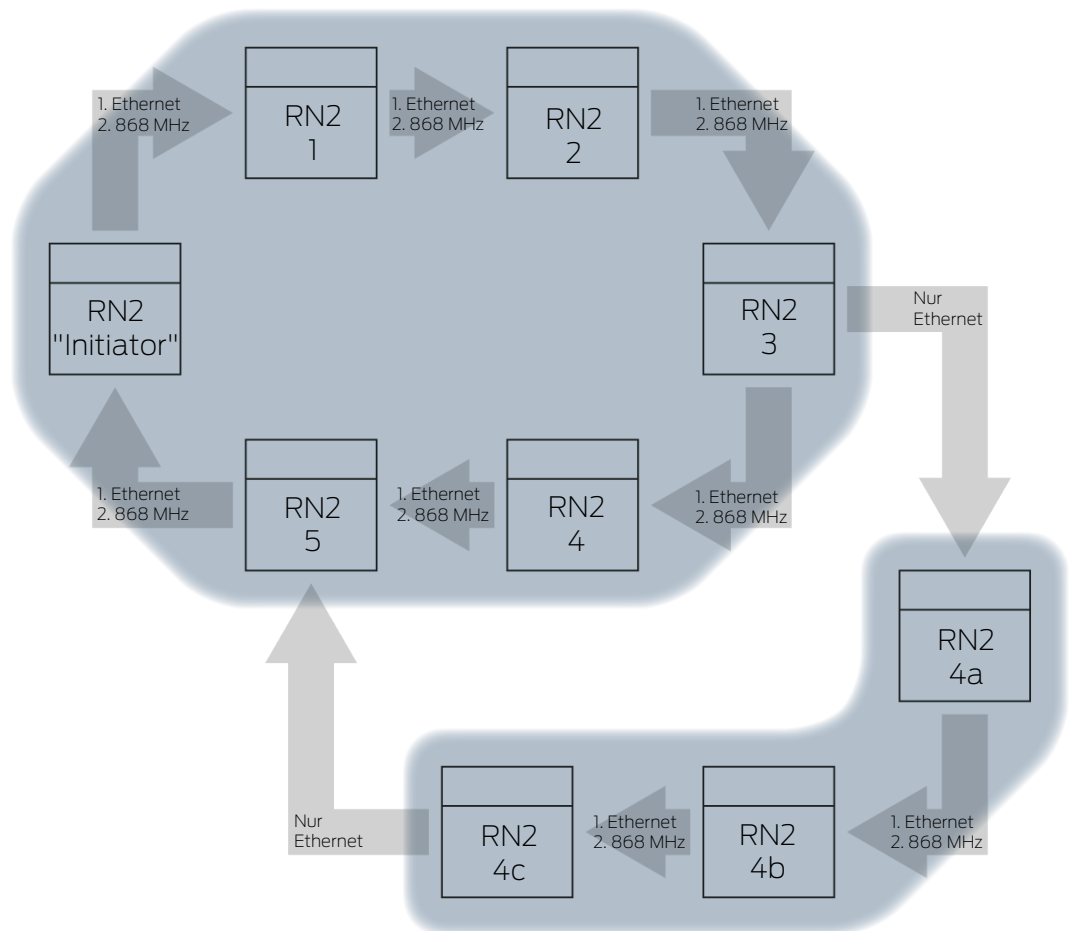
Das Relais im RouterNode 2 darf mit maximal 650 mA Dauerstrom und 12 V_{DC} Schaltspannung belastet werden (siehe auch Technische Daten im RouterNode-2-Handbuch).

- Verwenden Sie das Relais nicht, um Geräte zu betreiben, die diese Spezifikationen überschreiten.



1. Verbinden Sie die Masseanschlüsse des Netzteils und der Signalleuchte.
2. Verbinden Sie den Pluspol des Netzteils mit O1.COM.
3. Verbinden Sie den Pluspol der Signalleuchte mit O1.NO.

6.4.5 RingCast



Einzelne Funktionen sind je nach Firmwarestand der Router- und LockNodes nicht verfügbar (siehe *Firmware-Informationen* [► 42]).

**HINWEIS****Versionsabhängige Verfügbarkeit von RingCast im WaveNet-Manager**

Der WaveNet-Manager unterstützt ab Version 2.6.7 alle beschriebenen RingCast-Funktionen.

```

RingCast
├── RingCast(0)
│   ├── CN_UR (0x000E_0x0101; 0001E0CE)
│   └── RN_ER (0x0012_0x0301; 0002013F)
│       └── CN_UR (0x000E_0x0101; 0001E0CE) ###
    
```

Mit dem RingCast kann ein Inputsignal von einem bestimmten RouterNode ("Initiator") an alle vernetzten RouterNodes weitergegeben werden, ohne alle Inputs der RouterNodes verkabeln zu müssen. Wenn am Initiator an einem Eingang mit einem RingCast ein Signal ankommt, dann wird an alle an den RingCast angeschlossenen RouterNodes das Signal weitergeleitet und die RouterNodes reagieren so, als ob an ihrem Eingang tatsächlich ein Signal anliegen würde.

Bedeutung des Initiators	Der "Initiator" ist der wichtigste RouterNode im RingCast. Verbinden Sie den "Initiator" und die RouterNodes in der näheren Umgebung mit Ethernet, auch wenn sich die RouterNodes kabellos erreichen würden. Sie schaffen damit ein Backup und ermöglichen dem RouterNode eine Rückfallebene zur Weitergabe des Signals.
Drei Eingänge, drei RingCasts	Sie können für jeden der drei Eingänge eines RouterNodes einen eigenen RingCast erstellen, aber von einem Eingang nicht mehrere RingCasts starten. Daraus folgt, dass Sie einen RouterNode mit maximal drei RingCasts verbinden können. Hinsichtlich des gesamten WaveNets besteht diese Einschränkung nicht, Sie können mehr als drei RingCasts anlegen.
RingCast-Berechnung	Nachdem Sie den RingCast angelegt haben führt der WaveNet-Manager einen Funk-Scan durch. Anschließend berechnet er aus den Ergebnissen des Funk-Scans eine dreidimensionale Struktur.
Broadcast	RouterNodes, die ein Inputsignal erhalten haben und für dieses Inputsignal eine Reaktion gespeichert haben, führen einen Broadcast an alle mit diesem RouterNode vernetzten Schließungen durch. Innerhalb eines RingCasts können diese Reaktionen an den beteiligten Schließungen unterschiedlich sein (abhängig von der eingestellten Reaktion an den jeweiligen RouterNodes (siehe <i>RouterNode: Digitaler Eingang</i> [▶ 84])). Der RouterNode wiederholt je nach Einstellung den Broadcast bis zu drei Mal (insgesamt vier Versuche). Diese Einstellungen sind entscheidend für die Wiederholung des Broadcasts: ■ Ausgewählte Reaktion: "Blockschloß" oder "Aktivierung" ■ Input-Quittungen müssen aktiviert sein: "Input Quittung kurz" oder "Input Quittung statisch" Der WaveNet-Manager achtet bei der Berechnung der Struktur darauf, dass möglichst viele RouterNodes gleichzeitig einen Broadcast durchführen können, ohne sich gegenseitig zu stören. Damit können Sie mit einem RingCast Ihre LockNodes schnellstmöglich ansprechen. Nachdem der RouterNode seine Broadcasts abgeschlossen hat, leitet er das Signal in einem Datenpaket an seine Zielpartner weiter. Sobald die LockNodes den Broadcast empfangen haben, führt die Schließung mit dem LockNode die eingestellte Reaktion aus.
Schutzfunktionen	Ein Anwendungszweck ist zum Beispiel die Reaktion auf eine Brandmeldeanlage. Wenn die Brandmeldeanlage ein Signal an einen RouterNode schickt, dann sollen alle vernetzten Schließungen geöffnet werden und solange geöffnet bleiben, bis sie explizit per Fernöffnung geschlossen werden. Sie können aber auch andere Funktionen über einen RingCast verwenden, darunter: ■ Blockschlossfunktion

❑ Amokfunktion

❑ Fernöffnung

Datenpaket

Je nach Übertragungsweg hat ein RouterNode dabei einen oder mehrere andere RouterNodes als Zielpartner. Sendende RouterNodes übermitteln ein Datenpaket, bestehend aus:

❑ Zielpartner, die das Datenpaket empfangen sollen

❑ Inputsignal, das weitergeleitet werden soll

❑ Zählerstand des entsprechenden Inputs am Initiator

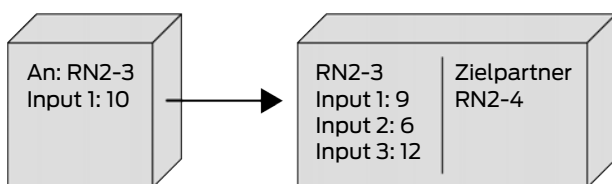
Standalone

Die Information, welche RouterNodes welche Zielpartner haben, ist auch in den RouterNodes selbst gespeichert. Der RingCast funktioniert deshalb unabhängig von angeschlossenen Computern.

6.4.5.1 Ablauf am einzelnen RouterNode betrachtet

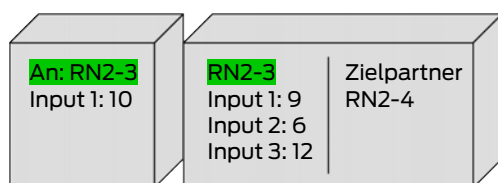
Ablauf des RingCasts an einem RouterNode 2:

1. Datenpaket empfangen



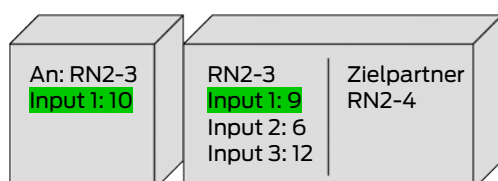
2. Datenpaket prüfen: **Ist Zielpartner**

Bei fehlgeschlagener Prüfung wird das Datenpaket verworfen

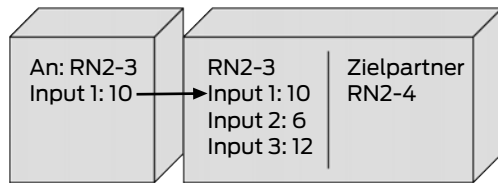


3. Datenpaket prüfen: **Input-Zählerstand im Datenpaket > aktuell gespeicherter Input-Zählerstand**

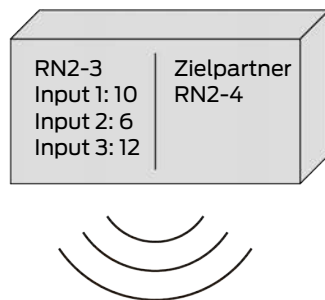
Bei fehlgeschlagener Prüfung wird das Datenpaket verworfen



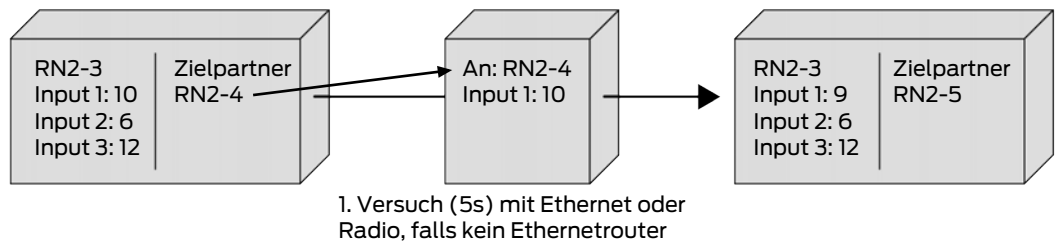
4. Input-Zählerstand des Pakets speichern



5. Broadcast durchführen: Fünf Sekunden (Eine Sekunde bei Unterstützung von Fast Wake-Up, siehe *Firmware-Informationen* [▶ 42])



6. Datenpaket mit Inputsignal und Input-Zählerstand weiterleiten (Ethernet bzw. Radio, falls RouterNode keinen Ethernetanschluss hat): Max. fünf Sekunden, danach Abbruch



HINWEIS

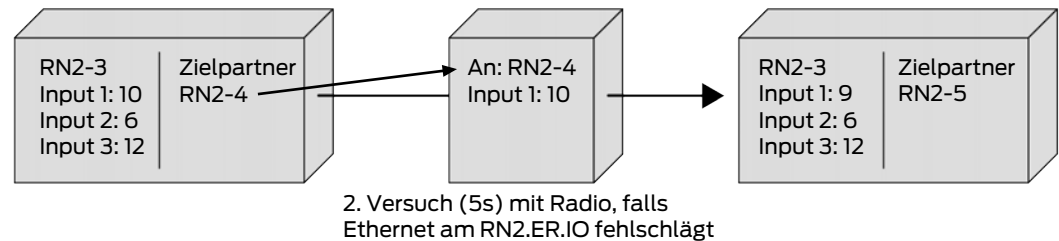
RingCast-Start nur mit vorhandener Funkverbindung

Der RingCast wird nach Funkerreichbarkeit aufgebaut. Wenn der Initiator keinen anderen RouterNode über Funk erreichen kann, dann wird das Datenpaket über Ethernet nur an die zugewiesenen Zielpartner gesendet. Auch wenn die Zielpartner weitere RouterNodes über Funk erreichen könnten, senden Sie das Datenpaket nicht weiter.

Der RingCast endet dann an den per Ethernet erreichbaren Zielpartnern des Initiators.

- Stellen Sie sicher, dass der Initiator eines RingCasts immer mindestens eine kabellose Verbindung zu einem anderen RouterNode des RingCasts aufbauen kann.

7. Datenpaket mit Inputsignal und Input-Zählerstand weiterleiten (Radio, nur nach fehlgeschlagenem Ethernetverbindungsversuch des RN2.ER.IO): Max. fünf Sekunden, danach Abbruch



Bedingungen, die für die Weiterleitung und den Broadcast erfüllt sein müssen:

1. **Ist Zielpartner:** Der RouterNode prüft, ob er in den Zielpartnern des Datenpakets aufgelistet ist.
2. **Input-Zählerstand im Datenpaket > aktuell gespeicherter Input-Zählerstand:** Der Initiator zählt, wie oft er nach einem Inputereignis das Inputsignal über den RingCast weitergeleitet hat und erhöht den Zählerstand bei jedem erneuten Senden. Das gesendete Datenpaket enthält diesen Zählerstand. Wenn ein RouterNode ein Datenpaket empfängt, dann gibt es zwei Möglichkeiten.

Zählerstand des empfangenen Pakets ist höher als der eigene Zählerstand: Das empfangene Paket ist neu und wurde noch nicht verarbeitet (andernfalls wäre der gespeicherte Zählerstand gleich).

Zählerstand des empfangenen Pakets ist kleiner oder gleich dem eigenen Zählerstand: Das empfangene Paket wurde bereits verarbeitet.

Wenn der Initiator ein Datenpaket empfängt, dessen Input-Zählerstand gleich seinem eigenen Zählerstand ist, dann gilt der RingCast als abgeschlossen.



HINWEIS

Signalverbreitung nach Abschlusserkennung des RingCasts

Die Abschlusserkennung bedeutet, dass der kürzestmögliche intakte Pfad des RingCasts durchlaufen ist und alle RouterNodes auf diesem Pfad das Inputsignal erhalten haben.

Wenn bei redundanten Pfaden nicht alle Pfade intakt sind, dann wird der RingCast trotzdem als abgeschlossen erkannt.

Die Abschlusserkennung sagt deshalb nichts darüber aus, ob alle beteiligten RouterNodes das Inputsignal erhalten haben.

Sendeverhalten nach Abschlusserkennung des RingCasts

Die Abschlusserkennung bedeutet, dass der kürzestmögliche intakte Pfad des RingCasts durchlaufen ist und alle RouterNodes auf diesem Pfad das Inputsignal erhalten haben.

Auf (längeren) redundanten Pfaden oder Verzweigungen kann trotzdem noch gesendet werden. Die Abschlusserkennung sagt deshalb nichts darüber aus, ob beteiligte RouterNodes noch senden.

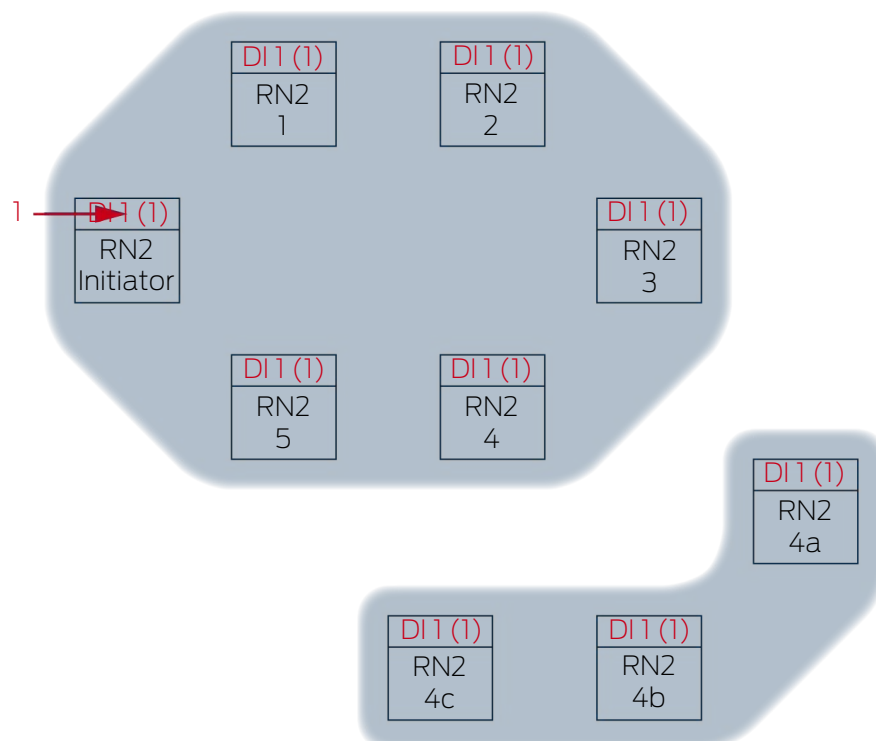
6.4.5.2 Ablauf an mehreren RouterNodes betrachtet

Sie können mit diesem Beispiel den Ablauf eines RingCasts nachvollziehen. Dieser RingCast beinhaltet:

- Verzweigungen
- Redundante Pfade unterschiedlicher Länge

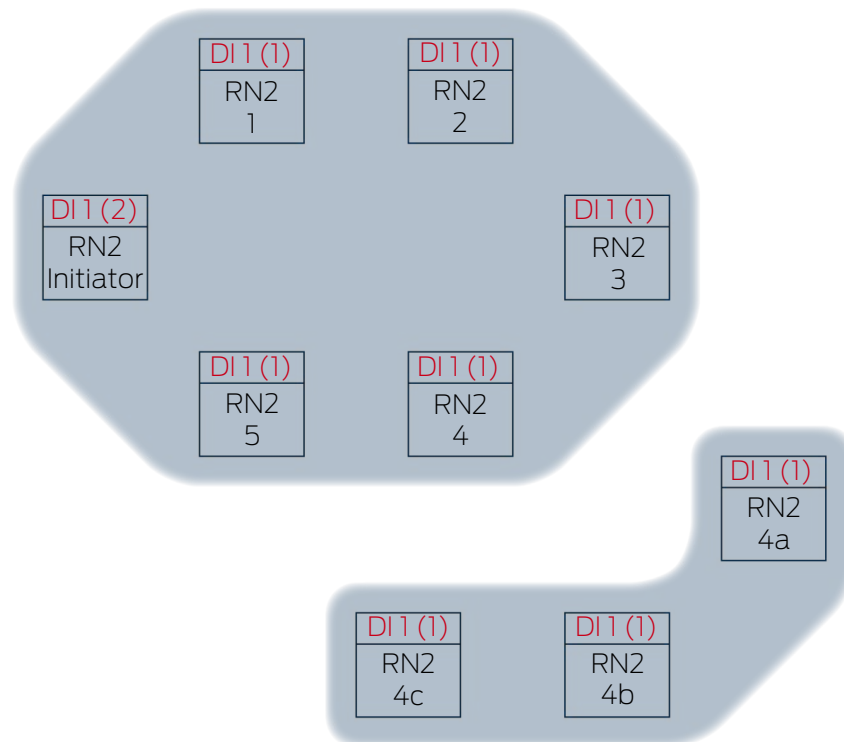
Das Inputsignal ist in diesem Beispiel mit **1** dargestellt.

Ausbreitung 1



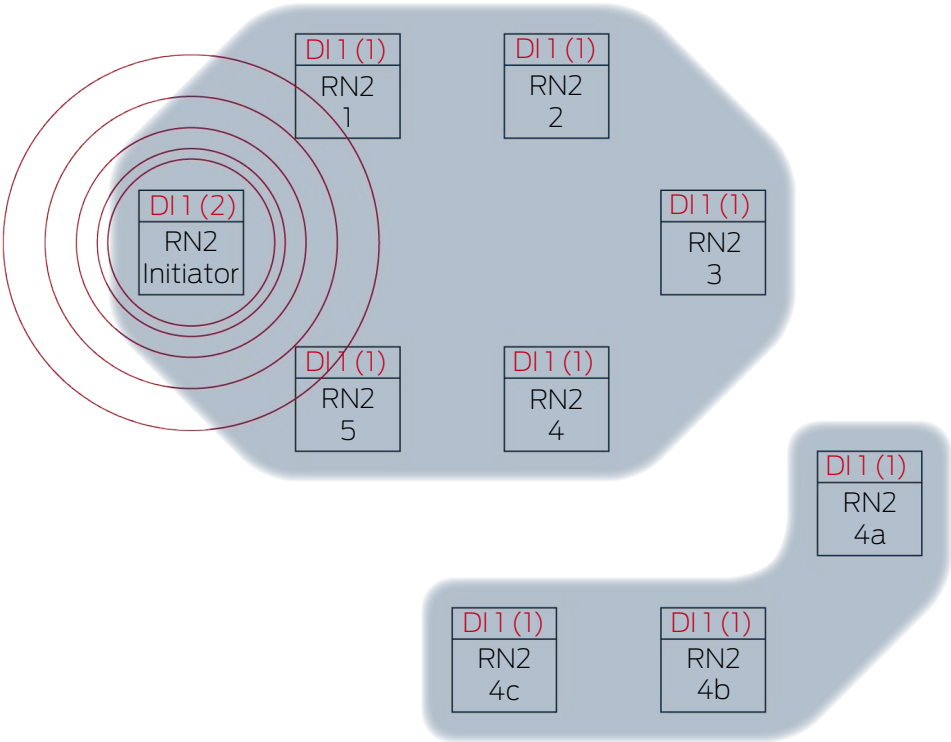
Inputsignal **1** am RN2-"Initiator".

Ausbreitung 2



Dies ist im Beispiel das zweite Mal, dass der "Initiator" über einen RingCast das Inputsignal 1 verbreitet. Der Input-Zählerstand im Initiator ist deshalb 2. Alle anderen RouterNodes im RingCast haben das Inputsignal erst einmal über einen RingCast empfangen und deshalb den Input-Zählerstand 1.

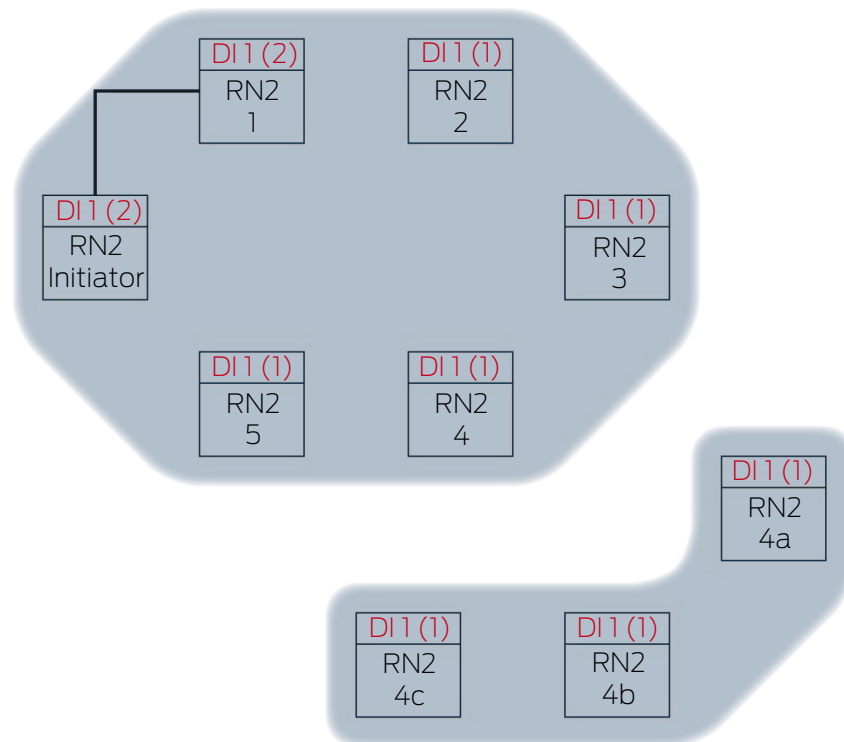
Ausbreitung 3



RN2-"Initiator" sendet Datenpaket aus (Kabelverbindung bzw. bei fehlgeschlagener/nicht vorhandener Kabelverbindung Funkverbindung).

Zielpartner	Inputsignal und Input-Zählerstand
RN2-1	1 (2)

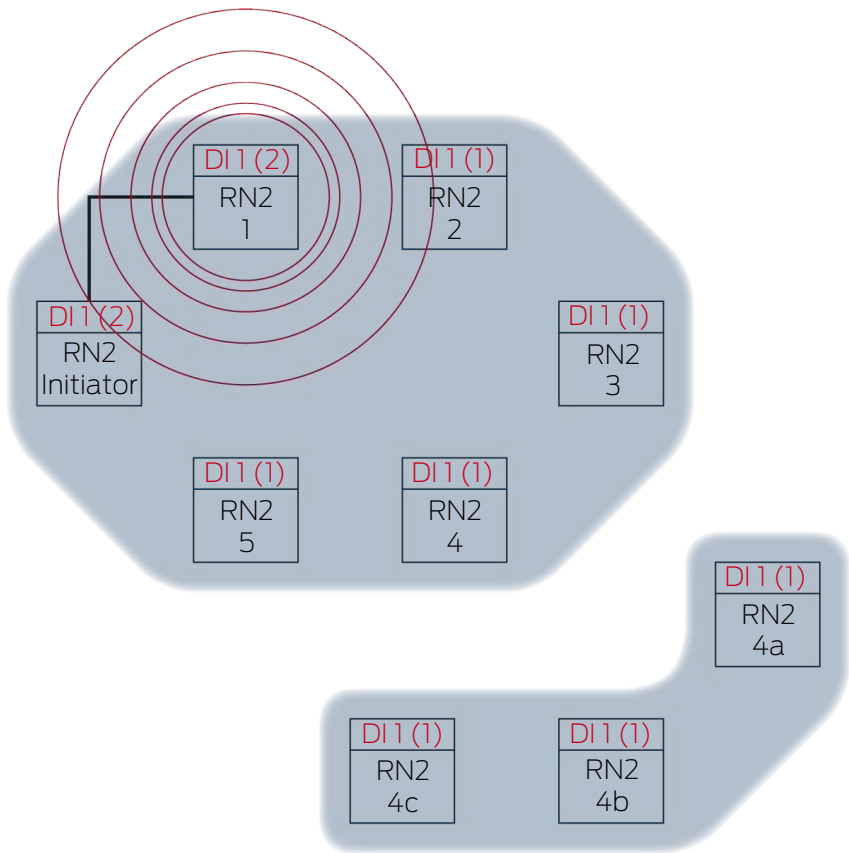
Ausbreitung 4



RN2-1 empfängt Datenpaket und prüft nacheinander die Bedingungen **Ist Zielpartner** und **Input-Zählerstand im Datenpaket > aktuell gespeicherter Input-Zählerstand**. Beide Bedingungen sind erfüllt → RN2-1 akzeptiert das Datenpaket und speichert den Input-Zählerstand des Datenpakets in seinen eigenen Input-Zählerstand.

Wenn das Datenpaket kabellos übertragen wird, dann empfangen andere RouterNodes in Reichweite das Datenpaket ebenfalls. Die Bedingung **Ist Zielpartner** ist aber nicht erfüllt, deshalb verwerfen diese RouterNodes das Datenpaket.

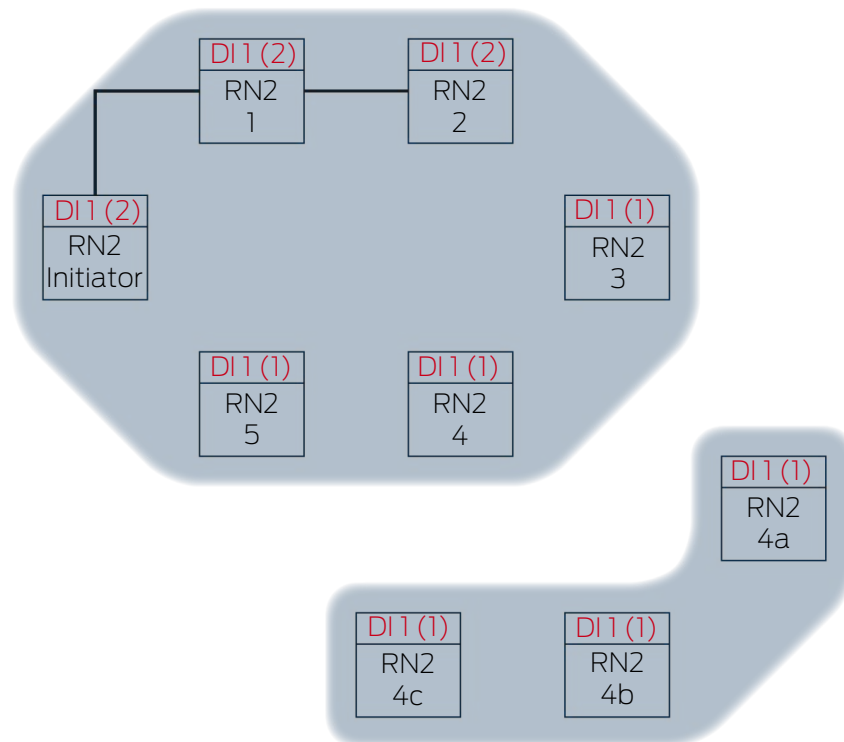
Ausbreitung 5



RN2-1 sendet Datenpaket aus (Kabelverbindung bzw. bei fehlgeschlagener/nicht vorhandener Kabelverbindung Funkverbindung).

Zielpartner	Inputsignal und Input-Zählerstand
RN2-2	1 (2)

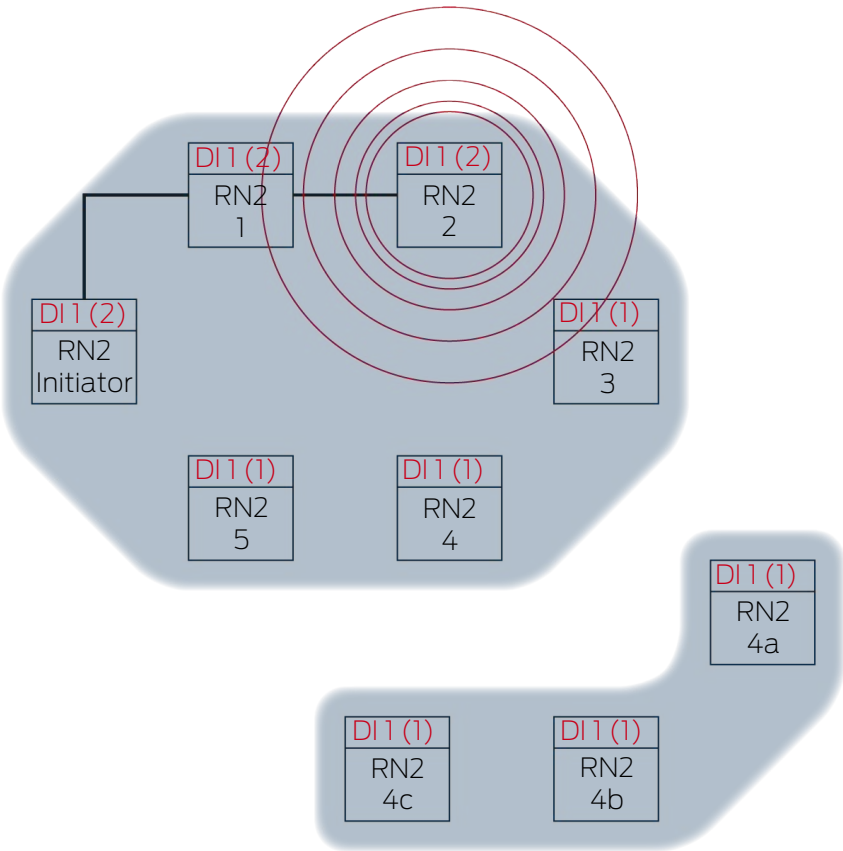
Ausbreitung 6



RN2-2 empfängt Datenpaket und prüft nacheinander die Bedingungen **Ist Zielpartner** und **Input-Zählerstand im Datenpaket > aktuell gespeicherter Input-Zählerstand**. Beide Bedingungen sind erfüllt → RN2-2 akzeptiert das Datenpaket und speichert den Input-Zählerstand des Datenpakets in seinen eigenen Input-Zählerstand.

Wenn das Datenpaket kabellos übertragen wird, dann empfangen andere RouterNodes in Reichweite das Datenpaket ebenfalls. Die Bedingung **Ist Zielpartner** ist aber nicht erfüllt, deshalb verwerfen diese RouterNodes das Datenpaket.

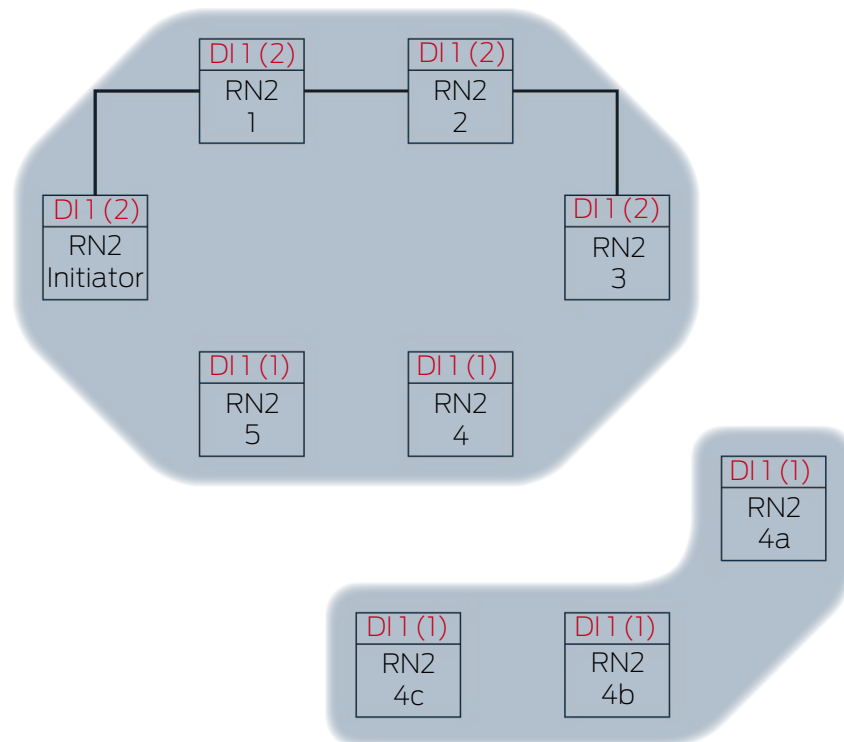
Ausbreitung 7



RN2-2 sendet Datenpaket aus (Kabelverbindung bzw. bei fehlgeschlagener/nicht vorhandener Kabelverbindung Funkverbindung).

Zielpartner	Inputsignal und Input-Zählerstand
RN2-3	1 (2)

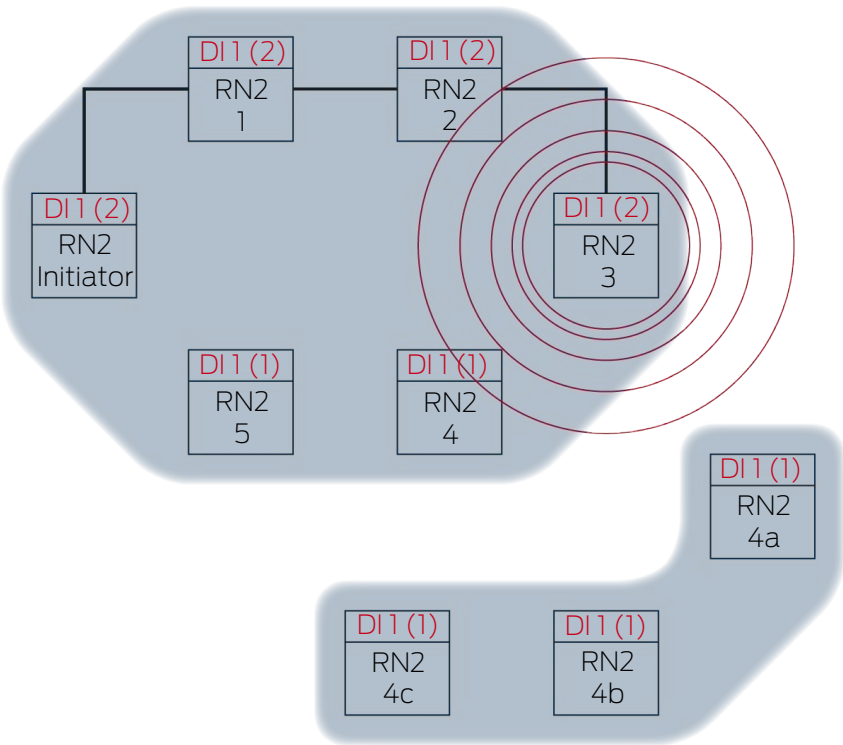
Ausbreitung 8



RN2-3 empfängt Datenpaket und prüft nacheinander die Bedingungen **Ist Zielpartner** und **Input-Zählerstand im Datenpaket > aktuell gespeicherter Input-Zählerstand**. Beide Bedingungen sind erfüllt → RN2-3 akzeptiert das Datenpaket und speichert den Input-Zählerstand des Datenpakets in seinen eigenen Input-Zählerstand.

Wenn das Datenpaket kabellos übertragen wird, dann empfangen andere RouterNodes in Reichweite das Datenpaket ebenfalls. Die Bedingung **Ist Zielpartner** ist aber nicht erfüllt, deshalb verwerfen diese RouterNodes das Datenpaket.

Ausbreitung 9

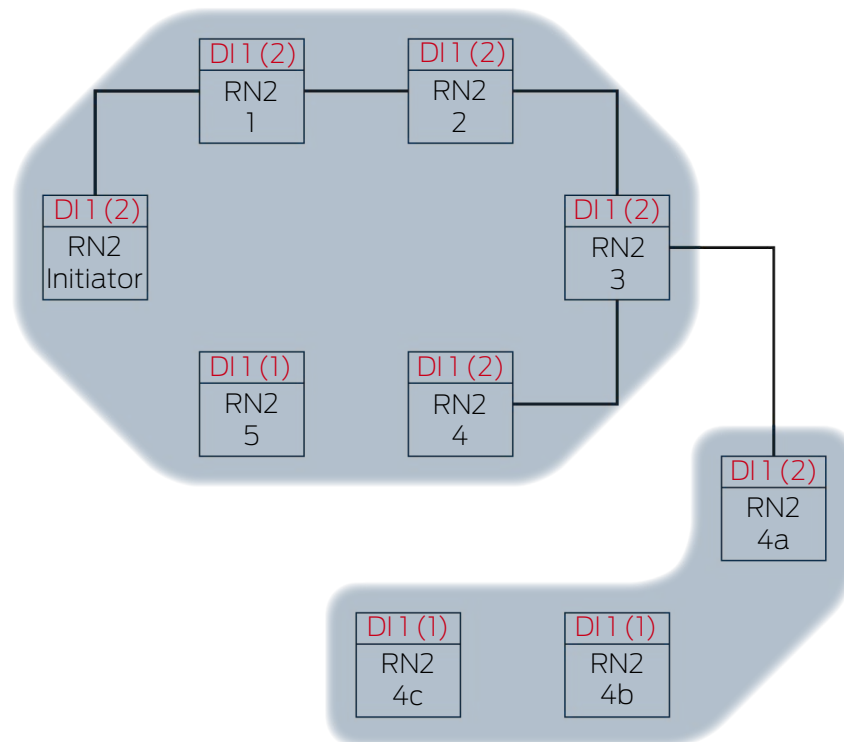


RN2-3 sendet Datenpaket aus (Kabelverbindung bzw. bei fehlgeschlagener/nicht vorhandener Kabelverbindung Funkverbindung).

Zielpartner	Inputsignal und Input-Zählerstand
RN2-4 RN2-4A	1 (2)

Der WaveNet-Manager erkennt, dass sich die Funknetze von RN2-4 und RN2-4A gegenseitig nicht beeinflussen und deshalb gleichzeitig das Inputsignal weiterverbreiten können. Das beschleunigt den RingCast.

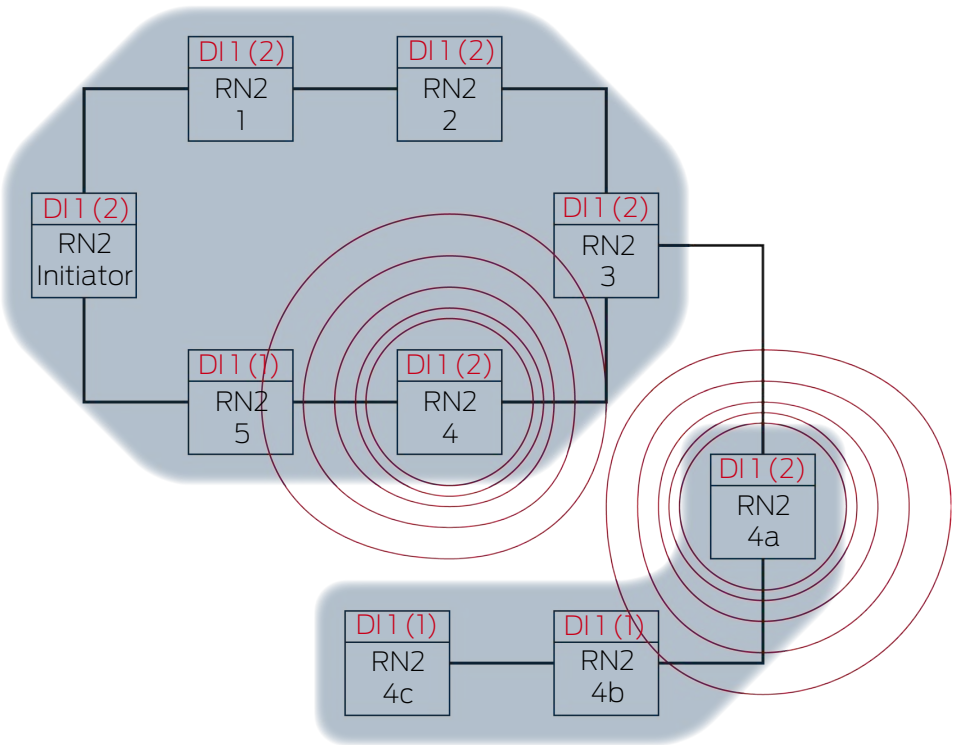
Ausbreitung 10



RN2-4 und RN2-4A empfangen Datenpaket und prüfen nacheinander die Bedingungen **Ist Zielpartner** und **Input-Zählerstand im Datenpaket > aktuell gespeicherter Input-Zählerstand**. Beide Bedingungen sind erfüllt → RN2-4 und RN2-4A akzeptieren das Datenpaket und speichern den Input-Zählerstand des Datenpakets in ihren eigenen Input-Zählerstand.

Wenn das Datenpaket kabellos übertragen wird, dann empfangen andere RouterNodes in Reichweite das Datenpaket ebenfalls. Die Bedingung **Ist Zielpartner** ist aber nicht erfüllt, deshalb verwerfen diese RouterNodes das Datenpaket.

Ausbreitung 11



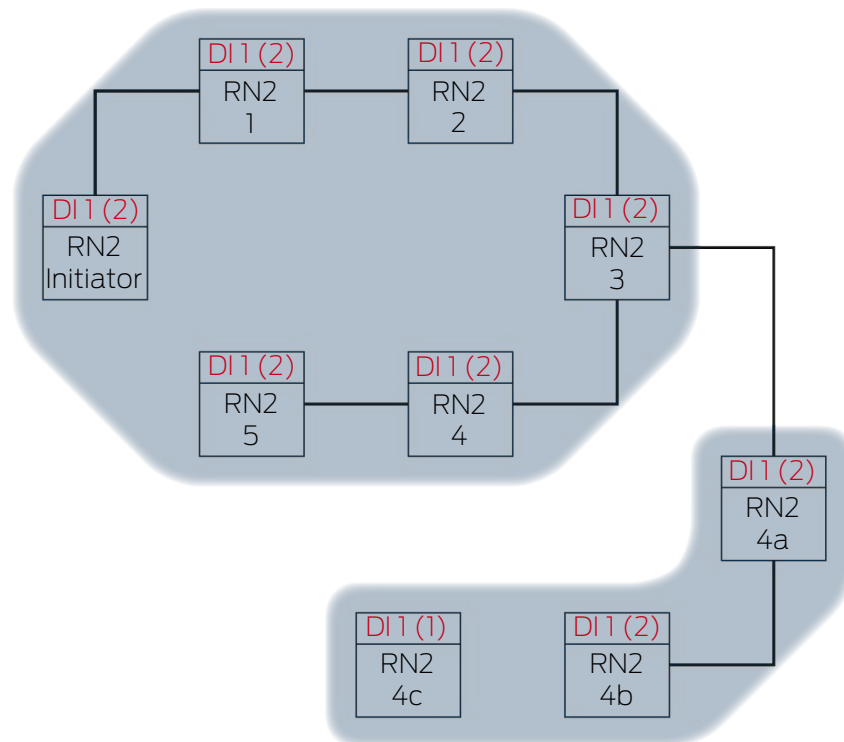
RN2-4 sendet Datenpaket aus (Kabelverbindung bzw. bei fehlgeschlagener/nicht vorhandener Kabelverbindung Funkverbindung).

Zielpartner	Inputsignal und Input-Zählerstand
RN2-5	1 (2)

RN2-4A sendet Datenpaket aus (Kabelverbindung bzw. bei fehlgeschlagener/nicht vorhandener Kabelverbindung Funkverbindung).

Zielpartner	Inputsignal und Input-Zählerstand
RN2-4B	1 (2)

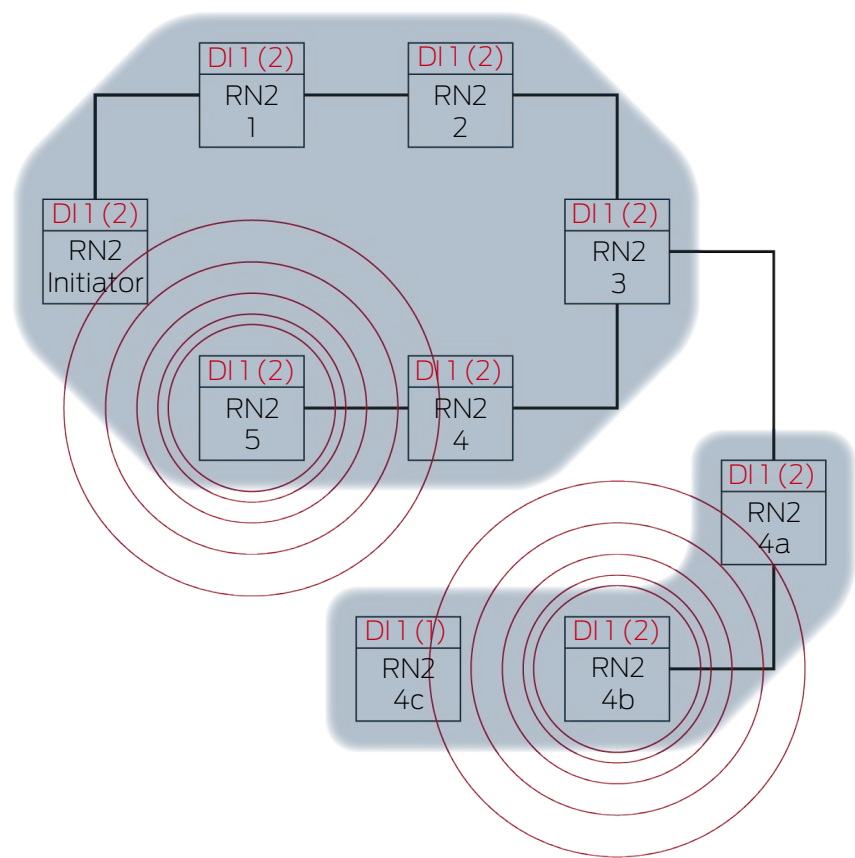
Ausbreitung 12



RN2-5 und RN2-4B empfangen Datenpaket und prüfen nacheinander die Bedingungen **Ist Zielpartner** und **Input-Zählerstand im Datenpaket > aktuell gespeicherter Input-Zählerstand**. Beide Bedingungen sind erfüllt → RN2-5 und RN2-4B akzeptieren das Datenpaket und speichern den Input-Zählerstand des Datenpakets in ihren eigenen Input-Zählerstand.

Wenn das Datenpaket kabellos übertragen wird, dann empfangen andere RouterNodes in Reichweite das Datenpaket ebenfalls. Die Bedingung **Ist Zielpartner** ist aber nicht erfüllt, deshalb verwerfen diese RouterNodes das Datenpaket.

Ausbreitung 13



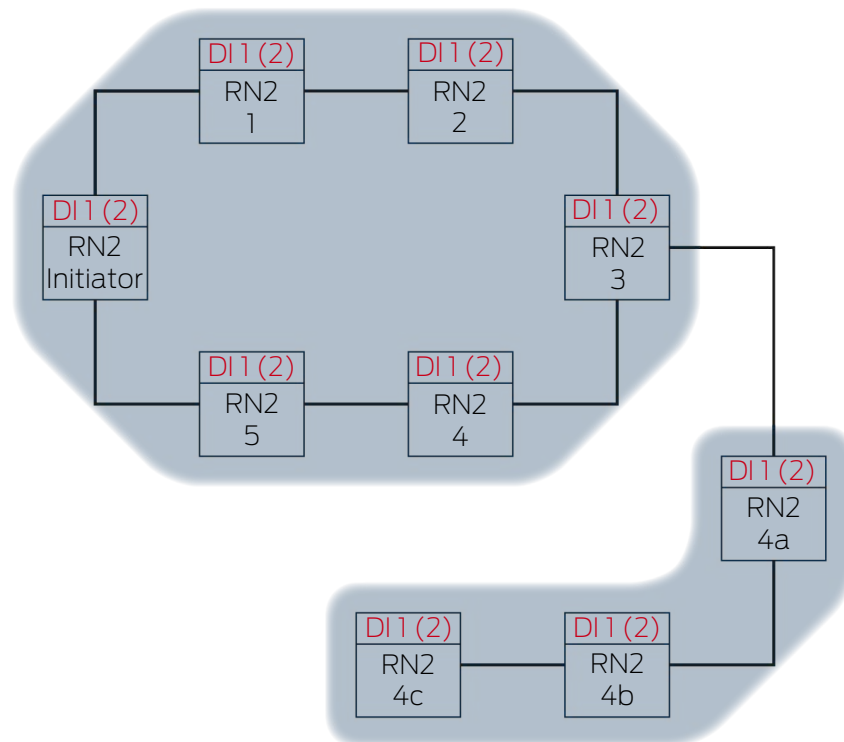
RN2-5 sendet Datenpaket aus (Kabelverbindung bzw. bei fehlgeschlagener/nicht vorhandener Kabelverbindung Funkverbindung).

Zielpartner	Inputsignal und Input-Zählerstand
RN2-"Initiator"	1 (2)

RN2-4B sendet Datenpaket aus (Kabelverbindung bzw. bei fehlgeschlagener/nicht vorhandener Kabelverbindung Funkverbindung).

Zielpartner	Inputsignal und Input-Zählerstand
RN2-4C	1 (2)

Ausbreitung 14

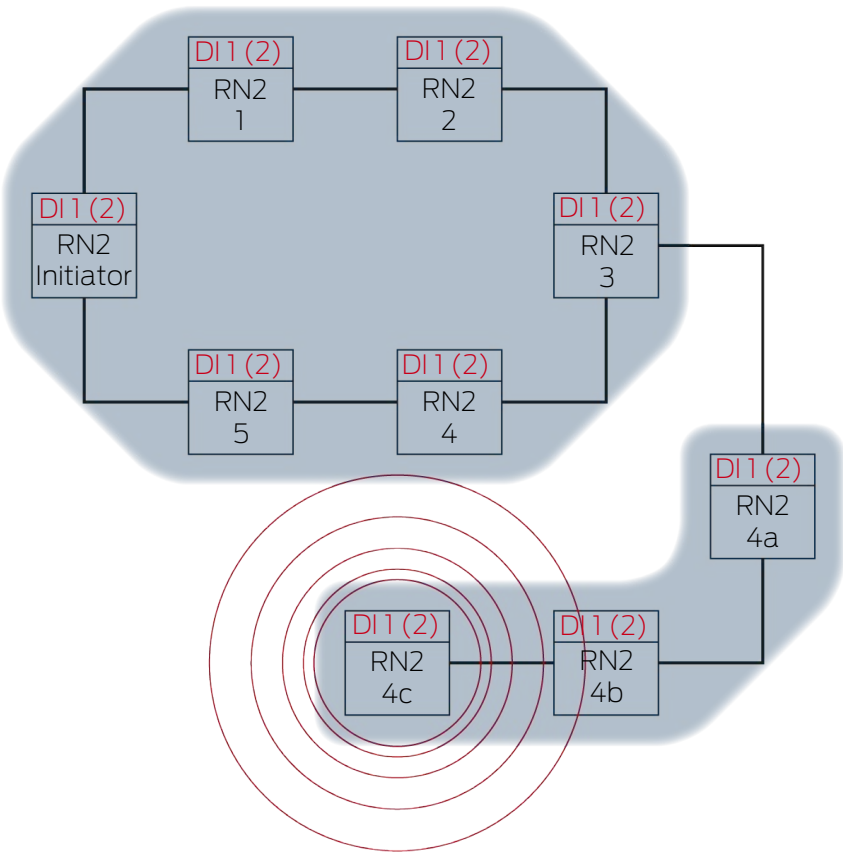


RN2-"Initiator" empfängt das Datenpaket und prüft nacheinander die Bedingungen **Ist Zielpartner** und **Input-Zählerstand im Datenpaket > aktuell gespeicherter Input-Zählerstand**. Die Bedingung **Input-Zählerstand im Datenpaket > aktuell gespeicherter Input-Zählerstand** ist nicht erfüllt (gleicher Input-Zählerstand) → RN2-"Initiator" akzeptiert das Datenpaket nicht und schließt den RingCast als "Initiator"-RouterNode ab.

RN2-4C empfängt Datenpaket und prüft nacheinander die Bedingungen **Ist Zielpartner** und **Input-Zählerstand im Datenpaket > aktuell gespeicherter Input-Zählerstand**. Beide Bedingungen sind erfüllt → RN2-4C akzeptiert das Datenpaket und speichert den Input-Zählerstand des Datenpakets in seinem eigenen Input-Zählerstand.

Wenn das Datenpaket kabellos übertragen wird, dann empfangen andere RouterNodes in Reichweite das Datenpaket ebenfalls. Die Bedingung **Ist Zielpartner** ist aber nicht erfüllt, deshalb verwerfen diese RouterNodes das Datenpaket.

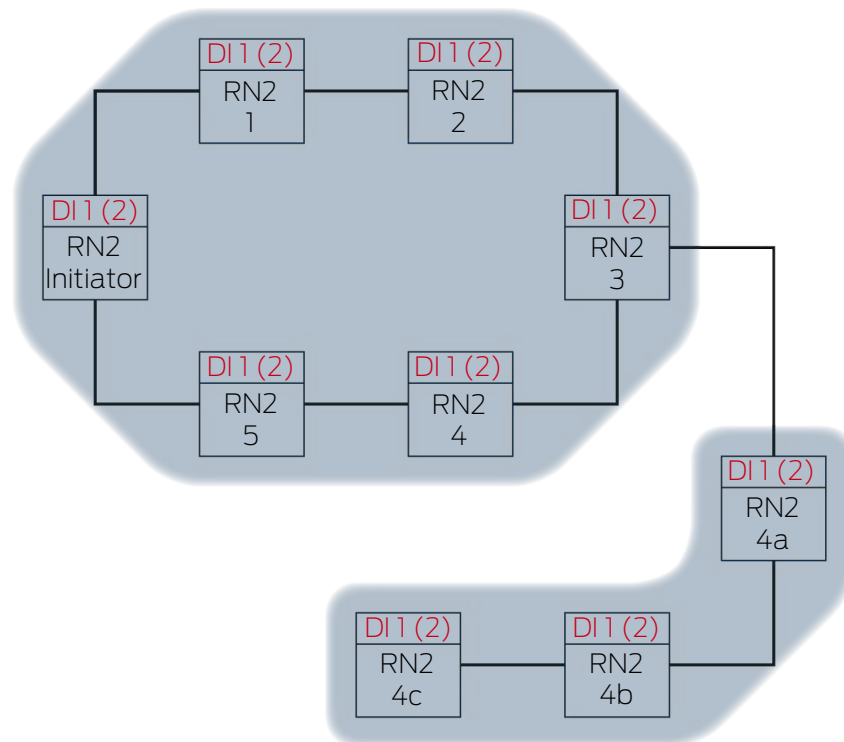
Ausbreitung 15



RN2-4C sendet Datenpaket aus (Kabelverbindung).

Zielpartner	Inputsignal und Input-Zählerstand
RN2-5	1 (2)

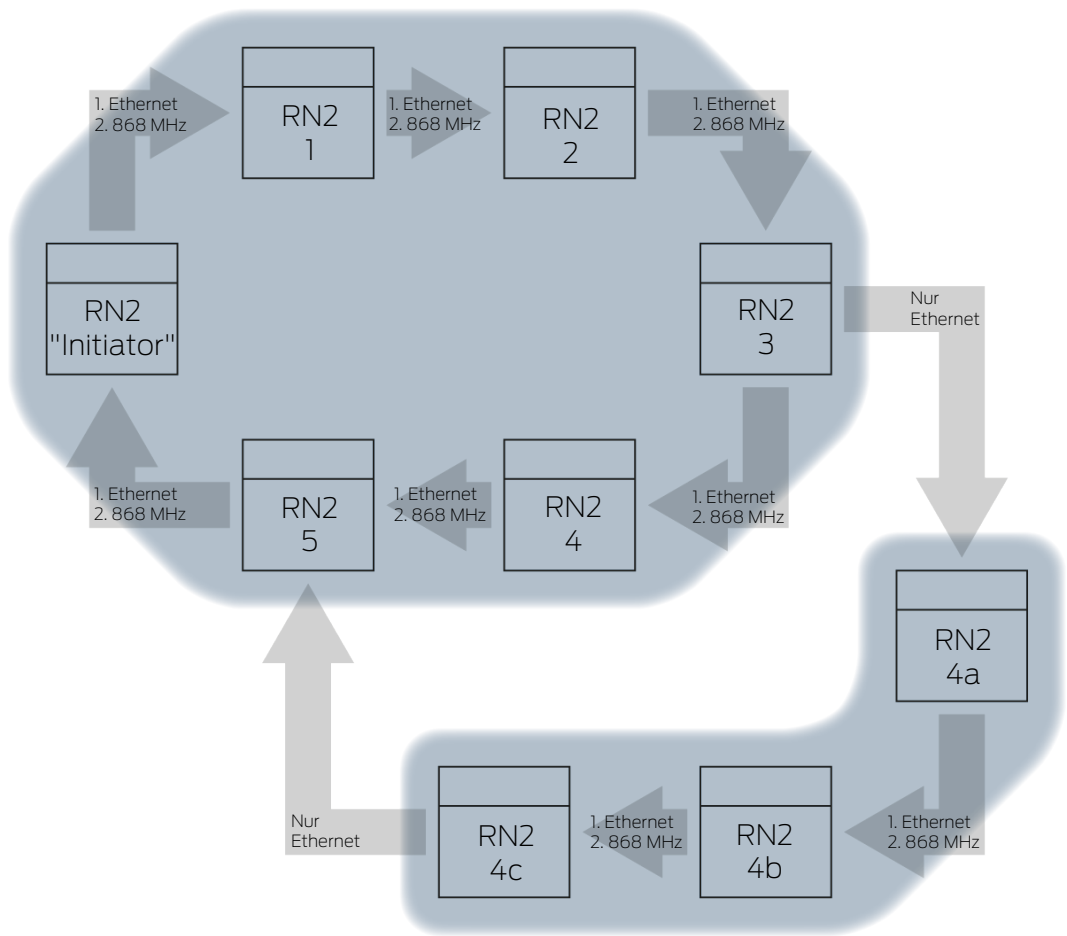
Ausbreitung 16



RN2-5 empfängt Datenpaket und prüft nacheinander die Bedingungen **Ist Zielpartner** und **Input-Zählerstand im Datenpaket > aktuell gespeicherter Input-Zählerstand**. Die Bedingung **Inputsignal nicht als empfangen gespeichert** ist nicht erfüllt (gleicher Input-Zählerstand) → RN2-5 verwirft das Datenpaket.

Wenn das Datenpaket kabellos übertragen wird, dann empfangen andere RouterNodes in Reichweite das Datenpaket ebenfalls. Die Bedingung **Ist Zielpartner** ist aber nicht erfüllt, deshalb verwerfen diese RouterNodes das Datenpaket.

6.4.5.3 Redundanzen im RingCast



Redundanz durch Übertragungsmedien

Wenn Sie Ethernet-RouterNodes der zweiten Generation (=RN2) verwenden, dann verwenden die RouterNodes zuerst die Ethernetverbindung und als Backup die kabellose Verbindung.

Wenn der WaveNet-Manager bei der Berechnung des RingCasts feststellt, dass sich mehrere RouterNodes gleichzeitig kabellos erreichen (im Beispiel "Initiator", 1, 2, 3, 4, 5 bzw. 4a, 4b und 4c), dann ordnet er innerhalb dieser "Funkwolke" jedem RouterNode genau einen Zielpartner zu.

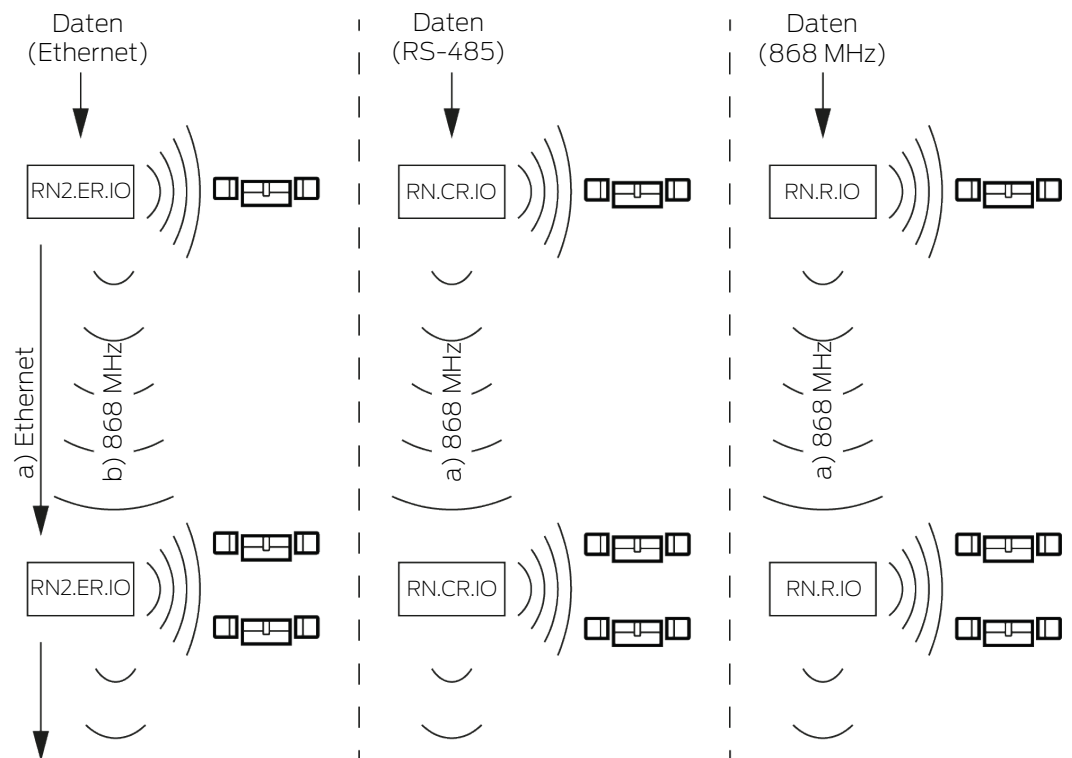
RouterNode	1. Übertragungsmedium im RingCast	2. Übertragungsmedium (Backup) im RingCast
RN2.ER.IO (Ethernet und Radio)	Ethernet	Radio (868 MHz)
RN.CR.IO (RS-485 und Radio)	Radio (868 MHz)	
RN.R.IO (Radio)	Radio (868 MHz)	



HINWEIS

Sendereichweite

Die Reichweite der Funkverbindung beträgt bis zu 30 m (abhängig von der Gebäudestruktur).



Wenn der Ethernet-RouterNode bei einem RingCast über die Ethernetverbindung seinen Zielpartner nach fünf Sekunden nicht erreicht, dann versucht er den Zielpartner über die kabellose Verbindung zu erreichen. Da der RouterNode bei einer kabellosen Verbindung physikalisch bedingt nicht gezielt seine Zielpartner ansprechen kann, empfangen alle RouterNodes in Reichweite das Datenpaket. Anschließend prüfen alle RouterNodes, die das Datenpaket empfangen haben, ob die Bedingung **Ist Zielpartner** erfüllt ist. Wenn die Bedingung nicht erfüllt ist, dann verwerfen die RouterNodes, die nicht Zielpartner des sendenden RouterNodes sind, das Paket wieder.

Wenn der RouterNode auch über die kabellose Verbindung seinen Zielpartner nicht erreicht, dann wird der RingCast an dieser Stelle unterbrochen.

Redundanz durch Verzweigungen

Unabhängig vom Übertragungsmedium ist es möglich, dass der WaveNet-Manager bei der Berechnung des RingCasts mehrere Verbindungen zwischen zwei RouterNodes aufbaut. Wenn eine dieser Verbindungen ausfällt oder gestört ist, dann kann der RingCast über die intakten

Verbindungen teilweise weiterlaufen. Das Datenpaket mit dem gleichen Input-Zählerstand wie dem im Initiator gespeicherten Input-Zählerstand kommt wieder am Initiator an und der RingCast wird als abgeschlossen erkannt.

Redundanz der Stromversorgung

Unterbrechung des RingCasts durch Ausfall der Stromversorgung

Die Stromversorgung in Gebäuden kann ausfallen. Wenn RouterNodes nicht mit Strom versorgt sind, dann können Sie ihre Datenpakete nicht weiterleiten und der RingCast ist unterbrochen.

- Setzen Sie eine unterbrechungsfreie Stromversorgung (USV) ein, um die RouterNodes vor einem Ausfall der Stromversorgung zu schützen.

Redundanz durch Events in der LSM



HINWEIS

Ereignismanagement nur in LSM Business

Dieses Kapitel beschreibt die Verwendung des Ereignismanagers. Der Ereignismanager ist nur in der LSM Business/Professional verfügbar.

Verschiedene Einflüsse können die Funkübertragung (temporär) stören (siehe [Funknetzwerk \[► 23\]](#) und [Signalqualität \[► 25\]](#)). Falls die Störung während eines Broadcasts auftritt, dann werden möglicherweise nicht alle LockNodes und damit nicht alle Schließungen erreicht.

Sie können eine zusätzliche Übertragung mithilfe der LSM nachschalten. Da Sie Inputereignisse bei bestehender Verbindung zur LSM auch an die LSM weiterleiten können (siehe [RouterNode: Digitaler Ausgang \[► 81\]](#)), können Sie auch in der LSM darauf reagieren (| Netzwerk | - [Ereignismanager](#)). Aktivieren Sie dazu im Fenster "I/O Konfiguration" die Checkbox ☒ Ja.

Ereignisse an Managementsystem übermitteln : ☒ Ja ☒ Ja ☒ Ja

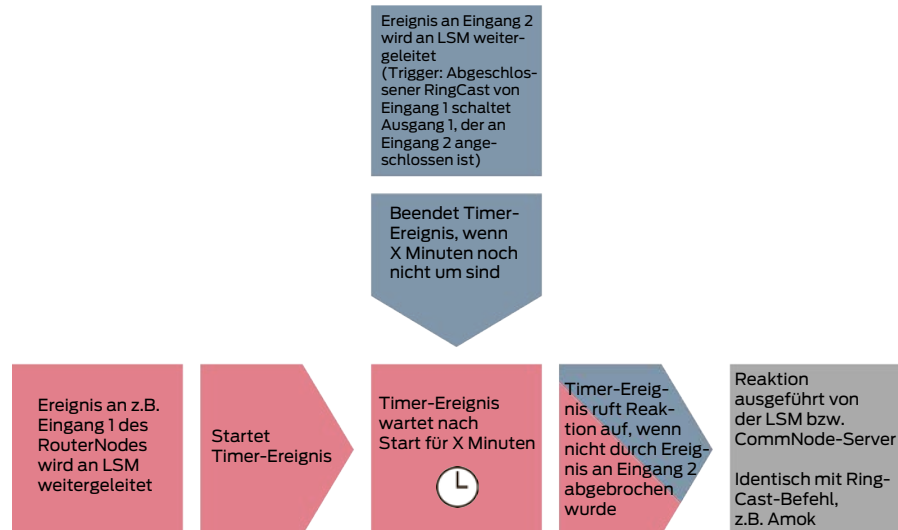
Diese zusätzliche Übertragung setzt Folgendes voraus:

- Initiator und zentraler Output-Router sind dasselbe Gerät
- Im RingCast sind nur Ethernet-RouterNodes beteiligt

Wenn Sie einen zentralen Output-Router verwenden und dessen Inputquittung an die LSM weiterleiten, dann können Sie die zusätzliche Übertragung auch abbrechen (In der LSM als Reaktion den Timer abbrechen). Verbinden Sie dazu den Ausgang der Inputquittung (z.B. 1) mit einem freien Eingang (z.B. 2).

Das Ereignis in der LSM wird in drei Teilen verarbeitet.

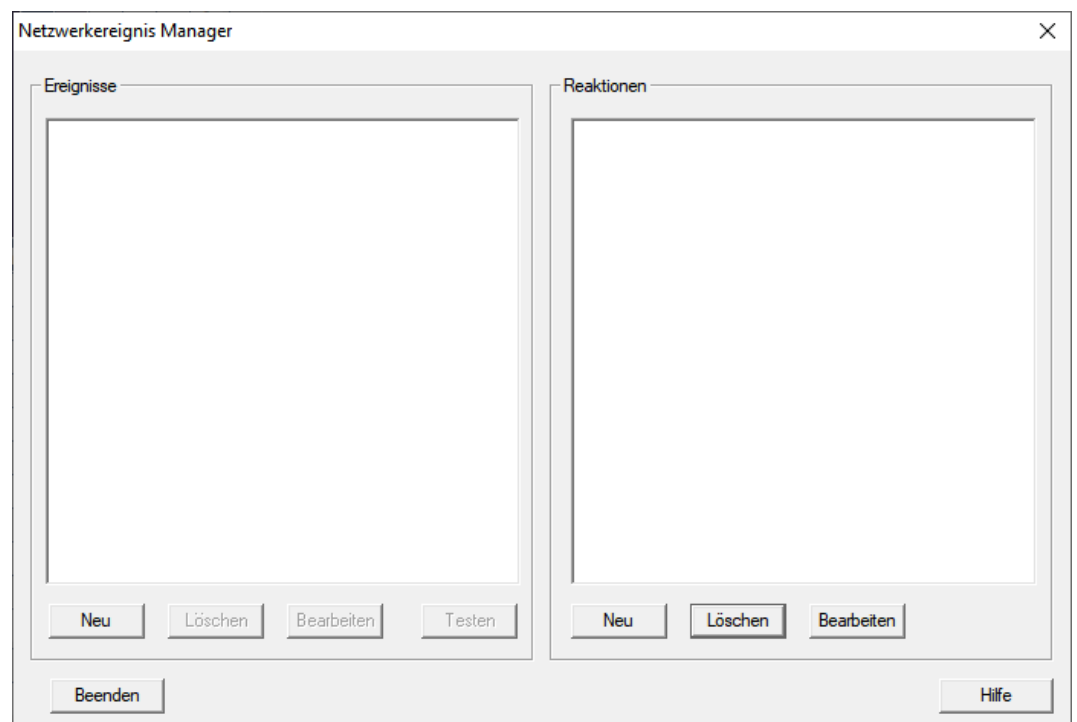
1. WaveNet-Input startet Timer-Ereignis.
2. Timer-Ereignis startet nach Ablauf Ereignis und startet Reaktion.
3. Reaktion sendet den Befehl des RingCasts an alle angegebenen Schließungen.



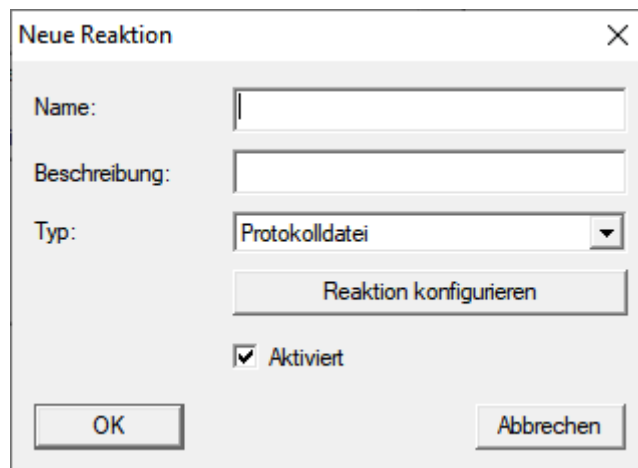
Broadcast wiederholen

✓ LSM geöffnet.

1. Wählen Sie über | Netzwerk | den Eintrag **Ereignismanager**.
↳ Fenster "Netzwerkereignis Manager" öffnet sich.



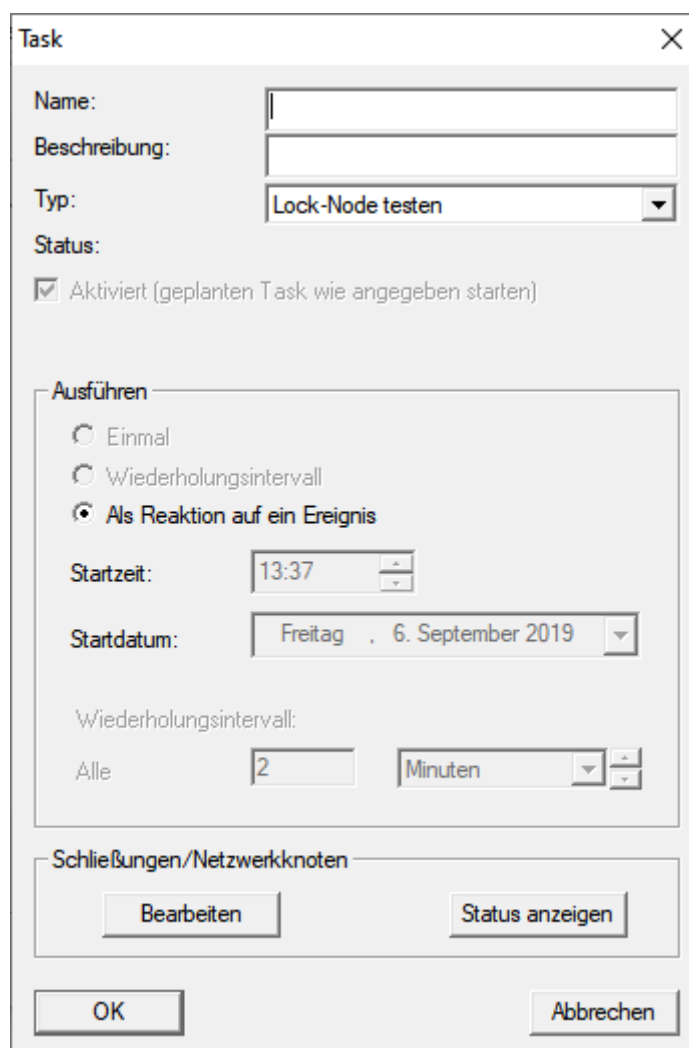
2. Klicken Sie im Bereich "Reaktionen" auf die Schaltfläche **Neu**.
↳ Fenster "Neue Reaktion" öffnet sich.



The 'Neue Reaktion' dialog box contains the following fields and controls:

- Name:** A text input field.
- Beschreibung:** A text input field.
- Typ:** A dropdown menu with 'Protokolldatei' selected.
- Reaktion konfigurieren:** A button located below the 'Typ' dropdown.
- ☒ **Aktiviert**
- OK** and **Abbrechen** buttons at the bottom.

3. Geben Sie einen Namen (z.B. "Broadcast") und eine Beschreibung ein.
4. Wählen Sie im Dropdown-Menü ▼ **Typ:** den Eintrag "Netzwerkaufgabe".
5. Klicken Sie auf die Schaltfläche **Reaktion konfigurieren**.
 - ↳ Fenster "Task" öffnet sich.

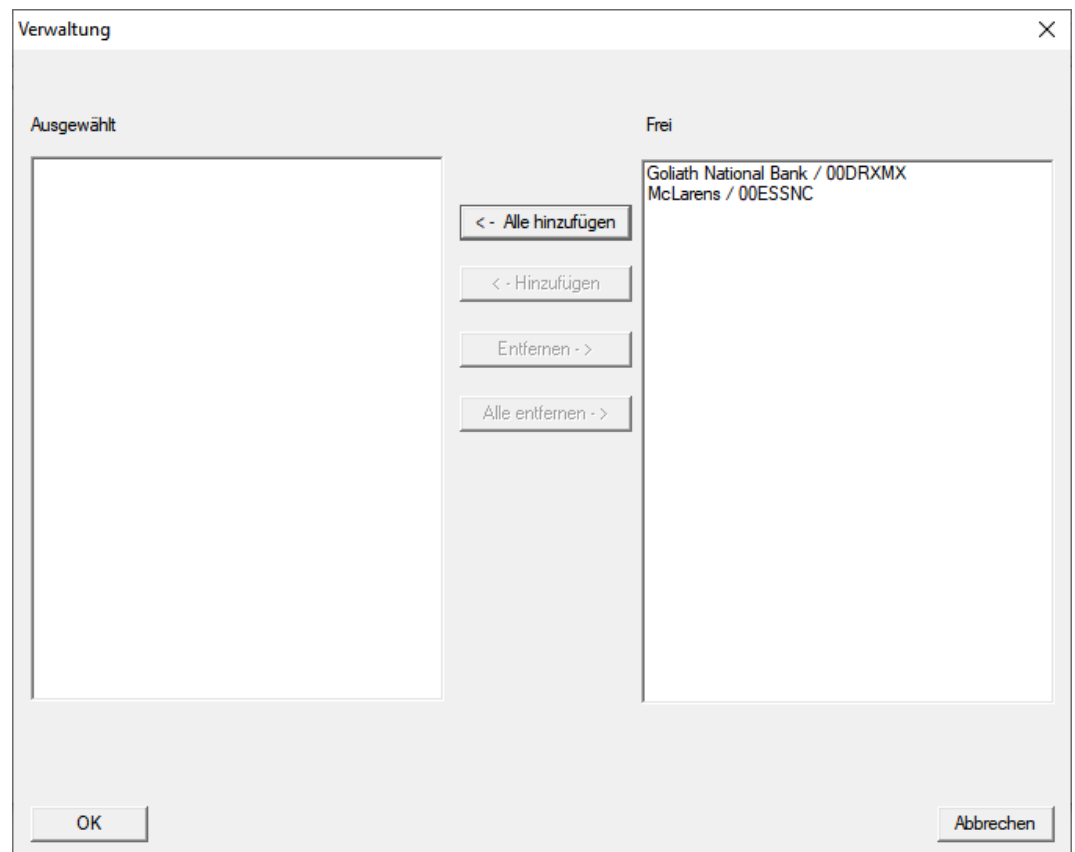


The 'Task' dialog box contains the following fields and controls:

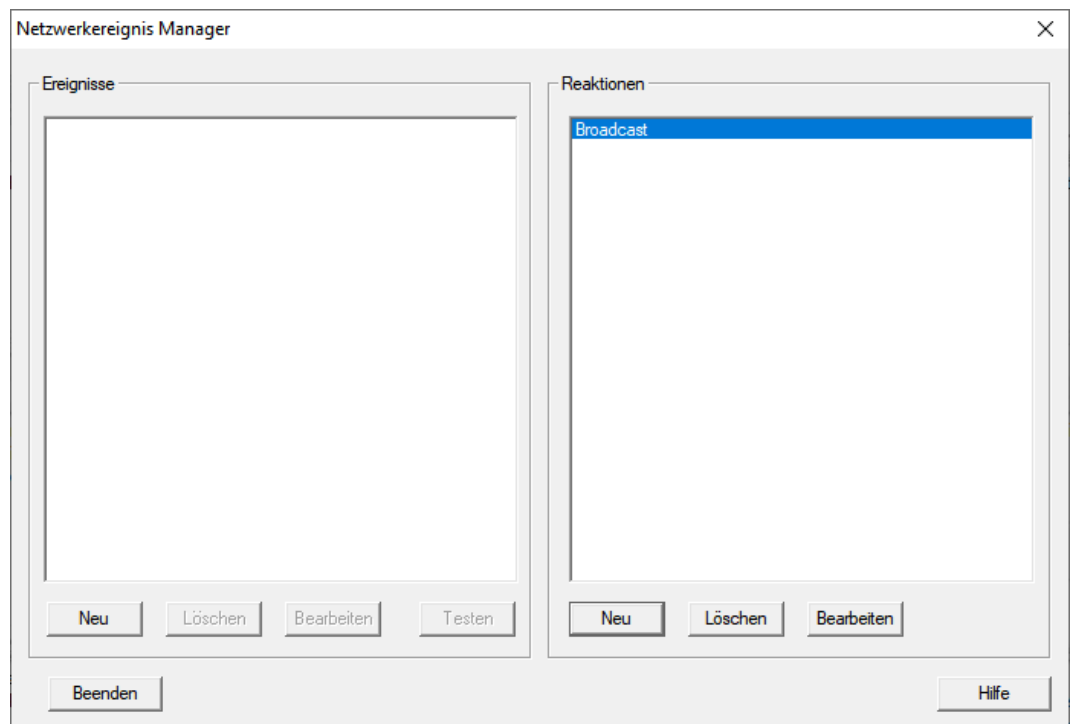
- Name:** A text input field.
- Beschreibung:** A text input field.
- Typ:** A dropdown menu with 'Lock-Node testen' selected.
- Status:**
 - ☒ **Aktiviert** (geplanten Task wie angegeben starten)
- Ausführen:**
 - ☐ Einmal
 - ☐ Wiederholungsintervall
 - ☒ **Als Reaktion auf ein Ereignis**
 - Startzeit:** A time picker set to 13:37.
 - Startdatum:** A date picker set to Freitag, 6. September 2019.
 - Wiederholungsintervall:**
 - Alle
- Schließungen/Netzwerkknoten:**
 - Bearbeiten** and **Status anzeigen** buttons.
- OK** and **Abbrechen** buttons at the bottom.

6. Geben Sie einen Namen und eine Beschreibung ein.

7. Wählen Sie im Dropdown-Menü ▼ **Typ:** den Befehl aus, den Ihr Ring-Cast sendet.
8. Klicken Sie im Bereich "Schließungen/Netzwerkknoten" auf die Schaltfläche **Bearbeiten**.
 - ➔ Fenster "Verwaltung" öffnet sich.

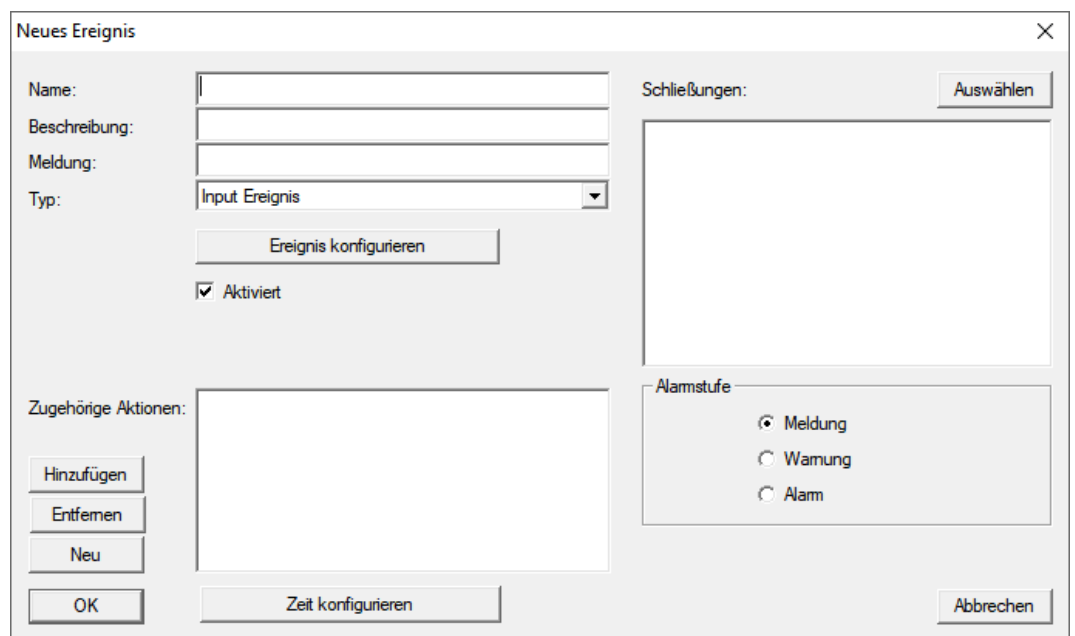


9. Markieren Sie alle Schließungen, die durch den RingCast gesteuert werden.
10. Klicken Sie auf die Schaltfläche **Hinzufügen**.
11. Klicken Sie auf die Schaltfläche **OK**.
 - ➔ Fenster "Verwaltung" schließt sich.
12. Klicken Sie auf die Schaltfläche **OK**.
 - ➔ Fenster "Task" schließt sich.
13. Klicken Sie auf die Schaltfläche **OK**.
 - ➔ Fenster "Neue Reaktion" schließt sich.
 - ➔ Reaktion ist im Bereich "Reaktionen" gelistet.

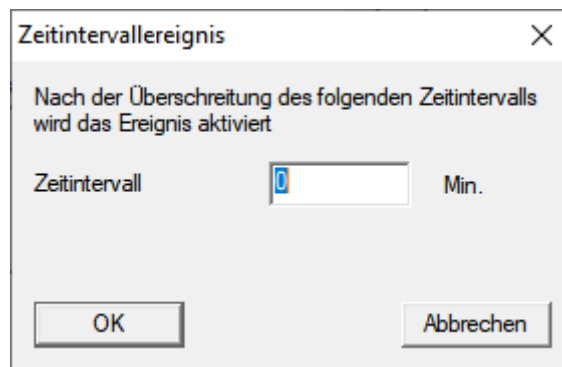


Timer abwarten

1. Klicken Sie im Bereich "Ereignisse" auf die Schaltfläche **Neu**.
↳ Fenster "Neues Ereignis" öffnet sich.



2. Geben Sie einen Namen (z.B. Timer für Broadcast-Wiederholung") und eine Beschreibung (z.B. "Wartet die nötige Verzögerung ab") ein.
3. Wählen Sie im Dropdown-Menü ▼ **Typ:** den Eintrag "Zeitintervall".
4. Klicken Sie auf die Schaltfläche **Ereignis konfigurieren**.
↳ Fenster "Zeitintervallereignis" öffnet sich.



5. Geben Sie die Zeitverzögerung zwischen RingCast-Start und LSM-Backupstart an.



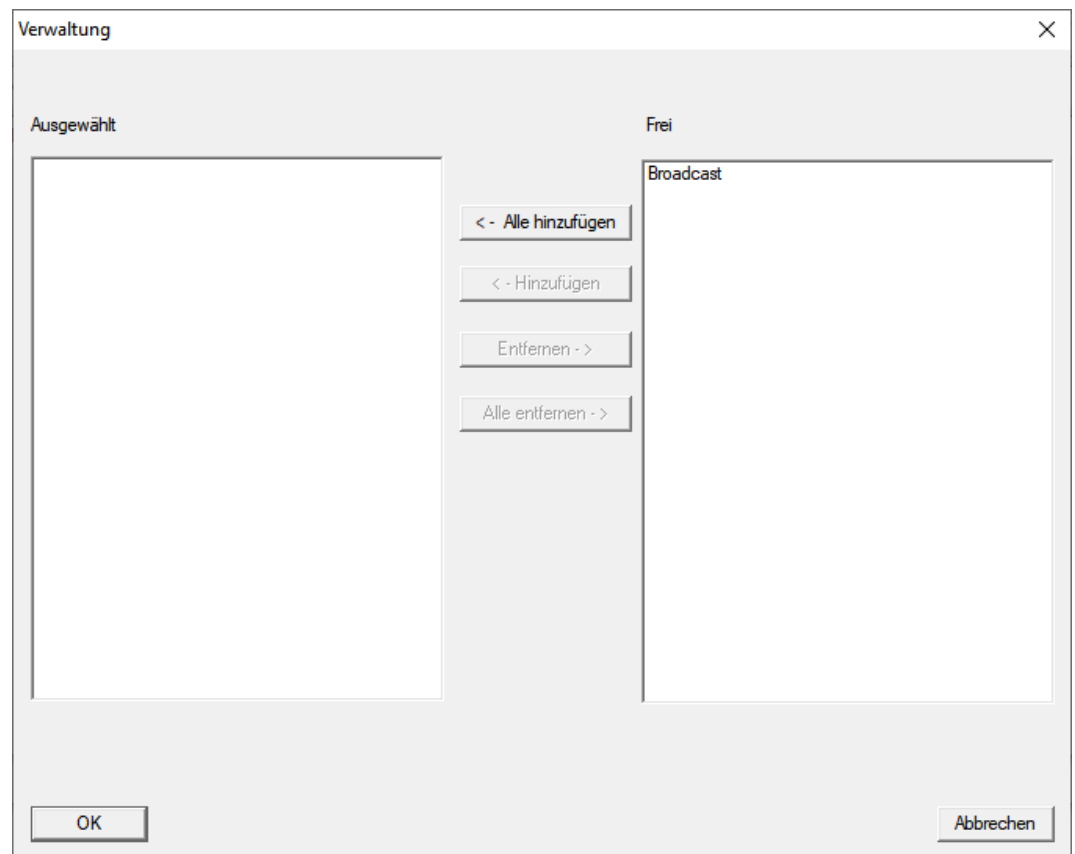
HINWEIS

Störung des RingCasts durch Parallelsendung

Wenn die LSM die Reaktion sofort ausführt, dann senden die betroffenen RouterNodes schon, während der RingCast noch nicht abgeschlossen ist. Dadurch kann der RingCast unterbrochen werden.

- Stellen Sie eine Verzögerung ein, die eine Minute länger als die maximale Übertragungsdauer des RingCasts ist (siehe *Maximale Übertragungsdauer im RingCast* [► 138]).

6. Klicken Sie auf die Schaltfläche **OK**.
 - ↳ Fenster "Zeitintervallereignis" schließt sich.
7. Klicken Sie auf die Schaltfläche **Hinzufügen**.
 - ↳ Fenster "Verwaltung" öffnet sich.



8. Markieren Sie die Reaktion, die Sie vorhin erstellt haben und die ausgelöst werden soll, wenn das Timer-Ereignis abläuft, ohne unterbrochen zu werden.
9. Klicken Sie auf die Schaltfläche **Hinzufügen**.
10. Klicken Sie auf die Schaltfläche **OK**.
 - Fenster "Verwaltung" schließt sich.
 - Aktion wird in der Liste der zum Ereignis gehörenden Aktionen angezeigt.

The 'Neues Ereignis' dialog box is used to create a new event. It contains the following fields and controls:

- Name:** Text field containing 'Timer für Broadcast-Wiederholung'.
- Beschreibung:** Text field containing 'Wartet die nötige Verzögerung ab'.
- Meldung:** Text field.
- Typ:** Dropdown menu set to 'Zeitintervall'.
- Schließungen:** Section with an 'Auswählen' button and an empty list box.
- Ereignis konfigurieren:** Button.
- Aktiviert:** Checked checkbox.
- Zugehörige Aktionen:** List box containing 'Broadcast'. To its left are buttons: 'Hinzufügen', 'Entfernen', 'Neu', and 'OK'.
- Alarmstufe:** Radio buttons for 'Meldung' (selected), 'Warnung', and 'Alarm'.
- Zeit konfigurieren:** Button.
- Abbrechen:** Button.

11. Klicken Sie auf die Schaltfläche **OK**.
 - Fenster "Neues Ereignis" schließt sich.
 - "Reaktionen" erhält zwei Zusatzeinträge mit den Endungen "entschärfen" und "scharfstellen".

The 'Netzwerkereignis Manager' window displays a list of events and their associated reactions.

- Ereignisse (Events):** A list box containing 'Timer für Broadcast-Wiederholung'. Below it are buttons: 'Neu', 'Löschen', 'Bearbeiten', and 'Testen'.
- Reaktionen (Reactions):** A list box containing:
 - Broadcast
 - Timer für Broadcast-Wiederholung entschärfen
 - Timer für Broadcast-Wiederholung scharfstellenBelow it are buttons: 'Neu', 'Löschen', and 'Bearbeiten'.
- Beenden:** Button at the bottom left.
- Hilfe:** Button at the bottom right.

Timer starten

1. Klicken Sie im Bereich "Ereignisse" auf die Schaltfläche **Neu**.
 - Fenster "Neues Ereignis" öffnet sich.

The 'Neues Ereignis' dialog box contains the following fields and controls:

- Name:** Text input field.
- Beschreibung:** Text input field.
- Meldung:** Text input field.
- Typ:** Dropdown menu with 'Input Ereignis' selected.
- Ereignis konfigurieren:** Button.
- Aktiviert:** Checked checkbox.
- Zugehörige Aktionen:** List box with buttons 'Hinzufügen', 'Entfernen', and 'Neu' on the left.
- OK:** Button.
- Zeit konfigurieren:** Button.
- Schließungen:** Section with an 'Auswählen' button and a large empty list box.
- Alarmstufe:** Radio buttons for 'Meldung' (selected), 'Warnung', and 'Alarm'.
- Abbrechen:** Button.

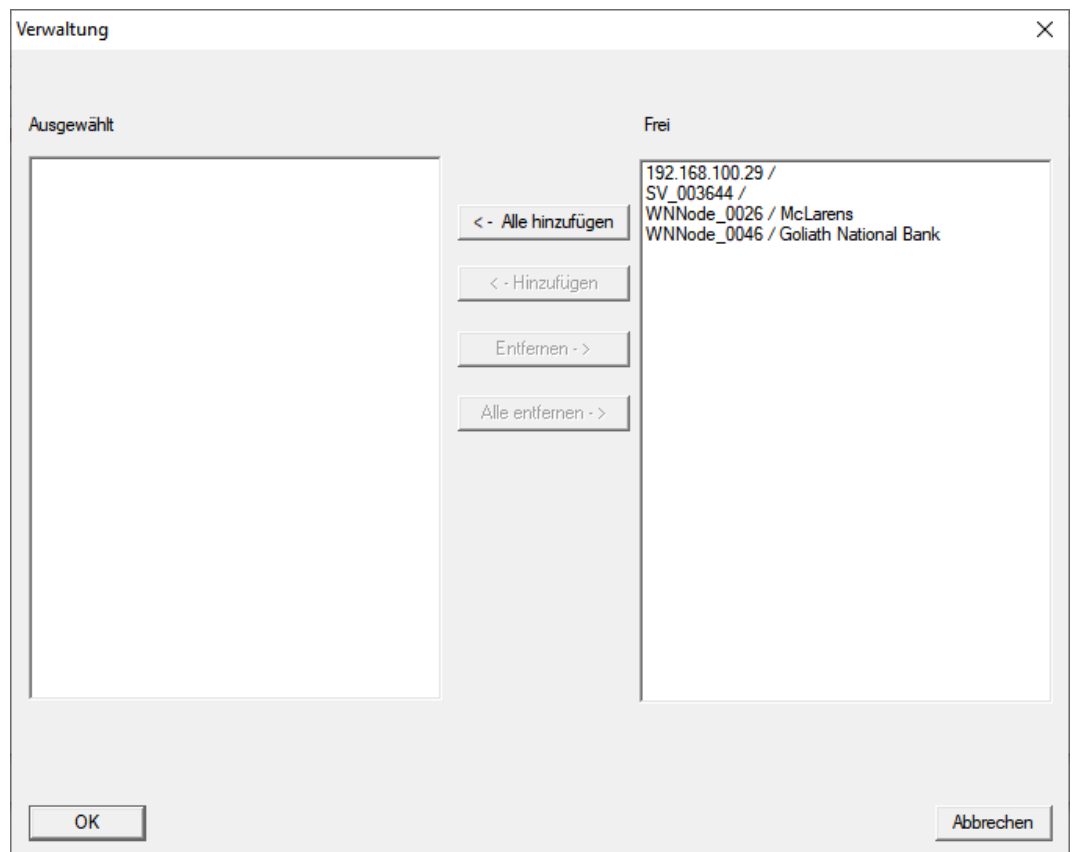
2. Geben Sie einen Namen (z.B. "Verzögerungstimer") und eine Beschreibung (z.B. "Wartet die Verzögerung des RingCasts ab") ein.
3. Wählen Sie im Dropdown-Menü ▼ **Typ:** den Eintrag "Input Ereignis".
4. Klicken Sie auf die Schaltfläche **Ereignis konfigurieren**.
→ Fenster "Input Ereignis" öffnet sich.

The 'Input Ereignis' dialog box contains the following sections and controls:

- Die Inputs eines Lock-Nodes sollen folgendermaßen berücksichtigt werden:** Instructional text.
- Input auswählen:** Radio buttons for 'Input 1' (selected), 'Input 2', and 'Input 3'.
- Input ändert sich:** Radio buttons for 'von 0 auf 1' (selected), 'von 1 auf 0', and 'beides'.
- OK:** Button.
- Abbrechen:** Button.

5. Wählen Sie im Bereich "Input auswählen" den Input aus, der Ihren Ring-Cast auslöst.
6. Wählen Sie im Bereich "Input ändert sich" aus, wann Ihr Input Ihren RingCast startet.
 - Von 0 auf 1: RingCast startet, wenn das Signal anliegt.

- Von 1 auf 0: RingCast startet, wenn das Signal nicht mehr anliegt.
 - beides: RingCast startet, wenn das Signal anliegt und wenn es nicht mehr anliegt.
7. Klicken Sie auf die Schaltfläche **OK**.
 - ➔ Fenster "Input Ereignis" schließt sich.
 8. Klicken Sie auf die Schaltfläche **Auswählen**.
 - ➔ Fenster "Verwaltung" öffnet sich.



9. Markieren Sie den Router, der in Ihrem RingCast der Initiator ist (den RouterNode, der den Input als erstes bekommt).
10. Klicken Sie auf die Schaltfläche **Hinzufügen**.
 - ➔ Fenster "Verwaltung" schließt sich.
 - ➔ RouterNode wird in der Liste der zum Ereignis gehörenden Schließungen angezeigt.

Neues Ereignis

Name: Verzögerungstimer

Beschreibung: Wartet die Verzögerung des RingCasts ab

Meldung:

Typ: Input Ereignis

Ereignis konfigurieren

☒ Aktiviert

Schließungen: Auswählen

SV_003644 /

Alarmstufe

☒ Meldung

☐ Warnung

☐ Alarm

Zugehörige Aktionen:

Hinzufügen

Entfernen

Neu

OK

Zeit konfigurieren

Abbrechen

11. Klicken Sie auf die Schaltfläche **Hinzufügen**.
 - ↳ Fenster "Verwaltung" öffnet sich.
12. Markieren Sie aus den vorhin erstellten Reaktionen diejenige mit der Endung "scharfstellen".
13. Klicken Sie auf die Schaltfläche **Hinzufügen**.
14. Klicken Sie auf die Schaltfläche **OK**.
 - ↳ Fenster "Verwaltung" schließt sich.
 - ↳ Aktion wird in der Liste der zum Ereignis gehörenden Aktionen angezeigt.

Neues Ereignis

Name: Verzögerungstimer

Beschreibung: Wartet die Verzögerung des RingCasts ab

Meldung:

Typ: Input Ereignis

Ereignis konfigurieren

☒ Aktiviert

Schließungen: Auswählen

SV_003644 /

Alarmstufe

☒ Meldung

☐ Warnung

☐ Alarm

Zugehörige Aktionen:

Timer für Broadcast-Wiederholung scharfstellen

Hinzufügen

Entfernen

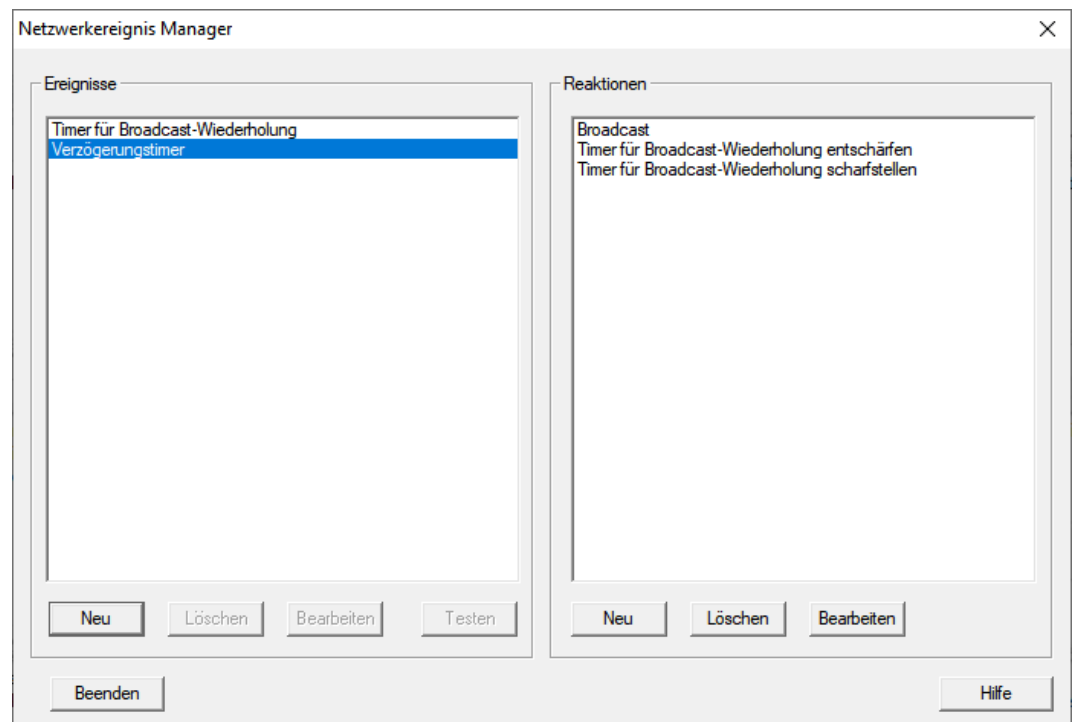
Neu

OK

Zeit konfigurieren

Abbrechen

15. Klicken Sie auf die Schaltfläche **OK**.
 - ↳ Fenster "Neues Ereignis" schließt sich.
 - ↳ LSM-Backup ist eingerichtet.



Timer abbrechen

- ✓ Am zentralen Output-Router ist mindestens ein digitaler Ausgang auf "Input Quittung kurz" oder "Input Quittung statisch" eingestellt (siehe *RouterNode: Digitaler Ausgang* [▶ 81]).
1. Verbinden Sie am zentralen Output-Router einen freien Input-Eingang mit einem digitalen Ausgang mit Inputquittung (siehe *Zentraler Output-Router* [▶ 145]).
 2. Wählen Sie über | Netzwerk | den Eintrag **Ereignismanager**.
 - ↳ Fenster "Netzwerkereignis Manager" öffnet sich.
 3. Klicken Sie im Bereich "Ereignisse" auf die Schaltfläche **Neu**.
 - ↳ Fenster "Neues Ereignis" öffnet sich.
 4. Geben Sie einen Namen für das Ereignis ein, z.B. "Backup Abbruch".
 5. Wählen Sie im Dropdown-Menü ▼ **Typ**: den Eintrag "Input Ereignis".
 6. Klicken Sie auf die Schaltfläche **Ereignis konfigurieren**.
 - ↳ Fenster "Input Ereignis" öffnet sich.
 7. Wählen Sie im Bereich "Input auswählen" den Input aus, an den die Quittung des zentralen Output-Routers angelegt wird.
 8. Wählen Sie im Bereich "Input ändert sich" die Option ☒ Von 1 auf 0 aus.
 9. Klicken Sie auf die Schaltfläche **OK**.
 - ↳ Fenster "Input Ereignis" schließt sich.

10. Klicken Sie auf die Schaltfläche **Hinzufügen**.
 - ↳ Fenster "Verwaltung" öffnet sich.
 11. Markieren Sie aus den vorhin erstellten Reaktionen diejenige mit der Endung "entschärfen".
 12. Klicken Sie auf die Schaltfläche **□ Hinzufügen**.
 - ↳ Reaktion wird
 13. Klicken Sie auf die Schaltfläche **OK**.
 - ↳ Fenster "Verwaltung" schließt sich.
 - ↳ Aktion wird in der Liste der zum Ereignis gehörenden Aktionen angezeigt.
 14. Klicken Sie auf die Schaltfläche **OK**.
 - ↳ Fenster "Netzwerkereignis Manager" schließt sich.
- ↳ LSM-Backup-Abbruch ist eingerichtet.

Übertragen Sie die Änderungen an den Kommunikationsknoten, der Ihrem RouterNode zugeordnet ist (siehe [LSM-Import \[► 69\]](#)).

Weitere Informationen zur Einrichtung eines Ereignisses und einer Reaktion finden Sie im LSM-Handbuch.

6.4.5.4 Maximale Übertragungsdauer im RingCast

Der RingCast überträgt Daten mitunter kabellos. Die kabellose Übertragung ist naturgemäß langsamer als die Ethernet-Schnittstelle. Abhängig von der gewählten Schutzfunktion wird der Broadcast an die Schließungen auch wiederholt. Daraus resultiert eine Gesamt-Übertragungsdauer für den RingCast. Sie können die maximale Übertragungsdauer Ihres RingCasts mit folgender Formel berechnen:

Übertragungsdauer = Anzahl der RouterNodes im RingCast * Broadcast-Dauer * Anzahl der Broadcasts pro RouterNode + Weiterleitungszeit * Anzahl der RouterNodes im RingCast

Anzahl der RouterNodes	Sie sehen die Anzahl der RouterNodes in der Übersicht (siehe Übersicht [► 190]) bzw. beim Anlegen und Bearbeiten des RingCasts (siehe RingCast anlegen [► 141]).
Broadcast-Dauer	Die Dauer des Broadcasts beträgt fünf Sekunden. Wenn im RingCast sowohl alle LockNodes als auch alle RouterNodes Fast Wake-Up unterstützen (siehe Firmware-Informationen [► 42]), dann beträgt die Broadcast-Dauer eine Sekunde. Sobald ein Gerät Fast Wake-Up nicht unterstützt, müssen Sie für die Berechnung fünf Sekunden annehmen.

Anzahl der Broadcasts pro RouterNode (abhängig von in ▼ Eingang eingestellter Reaktion)	"Eingang"	Kein Broadcast
	"Blockschloß"	1x (wenn Inputquittung nicht aktiv) 4x (wenn Inputquittung aktiv)
	"Amokfunktion"	1x
	"Notfreischaltung"	1x
	"Fernöffnung"	1x
	"Aktivierung"	1x (wenn Inputquittung nicht aktiv) 4x (wenn Inputquittung aktiv)
Weiterleitungszeit	Die Weiterleitungszeit beträgt maximal fünf Sekunden. Die Weiterleitungszeit ist vom Übertragungsmedium abhängig (siehe <i>Übertragungswege</i> [► 14]) und kann kürzer sein.	

Berechnungsbeispiel (50 RouterNodes) mit langer Broadcast-Dauer und Blockschoß mit Inputquittung

Übertragungsdauer = 50 RouterNodes im RingCast * 5 s * 4 Broadcasts + 5 s * 50 RouterNodes im RingCast

Die Übertragungsdauer beträgt bis zu 1000 Sekunden.

Berechnungsbeispiel (50 RouterNodes) mit kurzer Broadcast-Dauer und Blockschoß ohne Inputquittung

Übertragungsdauer = 50 RouterNodes im RingCast * 1 s * 1 Broadcast + 5 s * 50 RouterNodes im RingCast

Die Übertragungsdauer beträgt bis zu 300 Sekunden.

6.4.5.5 RouterNode für RingCast vorbereiten



HINWEIS

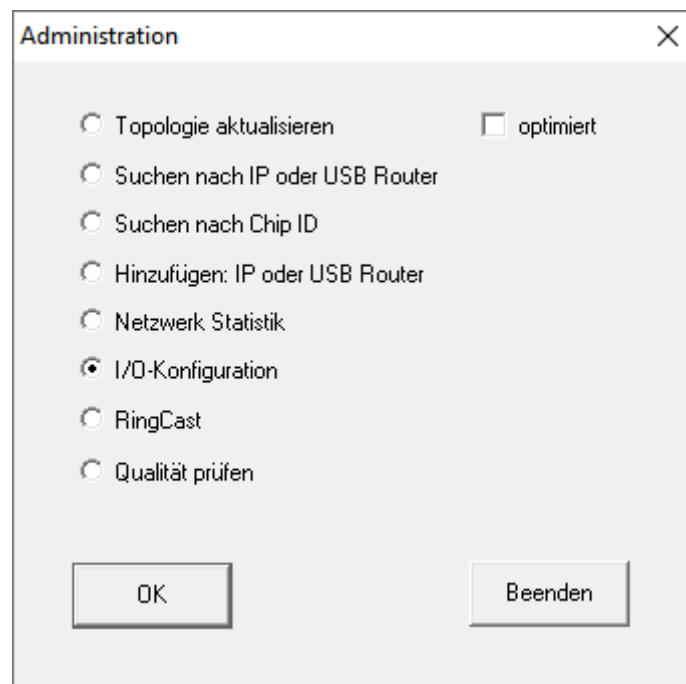
Firmwareabhängige Verfügbarkeit von RingCast für RouterNodes

Die Unterstützung von RingCast ist firmwareabhängig (siehe *Firmware-Informationen* [► 42]).

- Aktualisieren Sie ggfs. die Firmware (siehe *Firmware aktualisieren* [► 34]).

Bereiten Sie die RouterNodes für den RingCast vor:

- ✓ Im Wavenet-Funknetzwerk sind mindestens zwei verschiedene ringcastfähige RouterNodes konfiguriert und "online" (siehe *Firmware-Informationen* [► 42]).
 - ✓ Jedem RouterNode des geplanten RingCasts ist mindestens eine Schließung zugewiesen. Beide Schließungen sind "online".
1. Öffnen Sie den WaveNet-Manager.
 2. Klicken Sie mit der rechten Maustaste auf den ersten RouterNode 2.
 - ↳ Fenster "Administration" öffnet sich.



3. Wählen Sie die Option ☒ I/O-Konfiguration.
4. Klicken Sie auf die Schaltfläche **OK**.
 - ↳ Fenster "Administration" schließt sich.
 - ↳ Fenster "I/O Konfiguration" öffnet sich.
5. Optional: Wählen Sie beispielsweise für ▼ **Ausgang** 1 "Input Quittung statisch", um während der Deaktivierung ein Signalgerät ansteuern zu können.
6. Wählen Sie im Dropdown-Menü ▼ **Eingang** des gewünschten Eingangs den Eintrag der entsprechenden Reaktion aus (siehe *RouterNode: Digitaler Eingang* [► 84]).
7. Wählen Sie im Dropdown-Menü ▼ **Verzögerung** [s] den Eintrag "Ring-Cast" aus.
8. Klicken Sie auf die Schaltfläche **LN auswählen**.
9. Prüfen Sie, ob alle gewünschten LockNodes ausgewählt sind. (*Beim erstmaligen Einrichten der I/O-Konfiguration des Routers werden alle LockNodes mit einbezogen.*)

10. Wählen Sie im Dropdown-Menü ▼ **Protokollgeneration** Ihre Protokollgeneration.



HINWEIS

Protokollgeneration in der LSM

Die Protokollgeneration wird Ihnen in der LSM in den Schließanlageneseigenschaften in der Registerkarte [Name] im Bereich "Protokollgeneration" angezeigt.

11. Geben Sie das Schließanlagenepasswort ein.
12. Klicken Sie auf die Schaltfläche **OK**.
13. Nehmen Sie die selben Einstellungen auch an den weiteren RouterNodes 2 vor.

6.4.5.6 RingCast anlegen

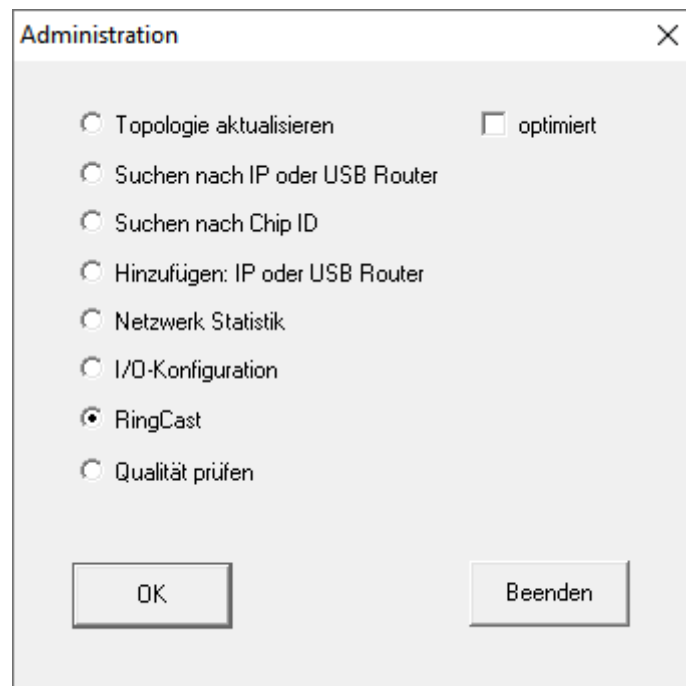


HINWEIS

Neuberechnung des RingCasts

Wenn Sie einen RouterNode im RingCast ersetzen, löschen oder dessen RingCast-relevante IO-Konfiguration ändern, dann wird der RingCast nach dem Speichern der Änderungen und dem Bestätigen der Nachfrage automatisch neu berechnet.

- ✓ WaveNet-Manager über LSM geöffnet (siehe *Best Practice: Aus der LSM-Software* [► 40]).
 - ✓ RouterNodes und LockNodes an Stromversorgung angeschlossen.
 - ✓ RouterNodes und LockNodes in WaveNet-Topologie importiert (siehe *Geräte finden und hinzufügen* [► 52]).
 - ✓ RouterNodes für RingCast vorbereitet (siehe *RouterNode für RingCast vorbereiten* [► 139]).
1. Klicken Sie mit der rechten Maustaste auf den Eintrag WaveNet XX_X.
↳ Fenster "Administration" öffnet sich.



2. Wählen Sie die Option ☒ RingCast.
3. Klicken Sie auf die Schaltfläche **OK**.
 - ➔ Fenster "Administration" schließt sich.
 - ➔ Fenster "Funkdomänen bearbeiten" öffnet sich.

Funkdomänen bearbeiten. [X]

Erstelle spezielle Funkdomänen.

Wähle Domäne :

Name :

Input :

Output Router :

Aktualisieren ☐

ausgewählte Router :

freie Router :

4. Wählen Sie im Dropdown-Menü ▼ **Wähle Domäne** einen Eingang aus, für den Sie bei ▼ **Verzögerung [s]** den "RingCast" gewählt haben.

▼

Input1

neu

- Im Feld "ausgewählte Router" erscheinen alle RouterNode2, bei denen Sie an diesem Eingang bei ▼ **Verzögerung [s]** den Eintrag "RingCast" gewählt haben (=Domäne).

Funkdomänen bearbeiten. [X]

Erstelle spezielle Funkdomänen.

Wähle Domäne :

Name :

Input :

Output Router :

Aktualisieren ☒

ausgewählte Router :

RN_ER (0x0006_0x0021; 89003644)
RN_ER (0x000E_0x0041; 0002A8B2)

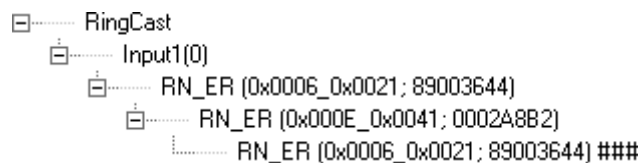
freie Router :

5. Klicken Sie auf die Schaltfläche **Speichern**.
6. Klicken Sie auf die Schaltfläche **Beenden**.
 - ↳ Fenster "Funkdomänen bearbeiten" schließt sich.
 - ↳ Fenster "WaveNetManager" öffnet sich.

WaveNetManager [X]

 Es wurden Änderungen vorgenommen. Möchten Sie die Funkdomänen aktualisieren ?

7. Klicken Sie auf die Schaltfläche **Ja**.
 - ↳ Fenster "WaveNetManager" schließt sich.
 - ↳ Änderungen werden aktualisiert.
- ↳ Der RingCast wird angelegt und ist nach kurzer Zeit im WaveNet-Manager sichtbar.



Speichern Sie die neuen Einstellungen und beenden Sie den WaveNet-Manager.

6.4.5.7 Zentraler Output-Router

Die Verfügbarkeit dieser Funktion ist firmwareabhängig (siehe *Firmware-Informationen* [► 42]).

Sie können die Firmwareversion Ihres RouterNodes über die Browserschnittstelle (siehe *Browserschnittstelle* [► 157]) oder das OAM-Tool (siehe *Firmware aktualisieren* [► 34]) auslesen.

Zentralen Output-Router hinzufügen

Sie können im RingCast einen beliebigen RouterNode der zweiten Generation (mit Ethernet-Schnittstelle, WNM.RN2.ER.IO ab Firmwareversion 40.10) als zentralen Output-Router konfigurieren. Der zentrale Output-Router sammelt zunächst die empfangenen Input-Quittungen aller anderen im RingCast beteiligten Ethernet-RouterNodes (ER) und setzt erst dann seine eigene Input-Quittung ab bzw. setzt den Output, wie er bei *RouterNode: Digitaler Ausgang* [► 81] eingestellt wurde. Alle anderen RouterNodes setzen die Input-Quittung / den Output wie vorher eingestellt.

Die Übertragung erfolgt über Ethernet. Sein Output wird also immer als letzter Output des gesamten RingCasts geschaltet und zeigt an, dass alle via Ethernet-RouterNodes am RingCast beteiligten Schließungen den Befehl erhalten haben.



HINWEIS

Zentraler Output-Router im RingCast mit R/CR-RouterNodes

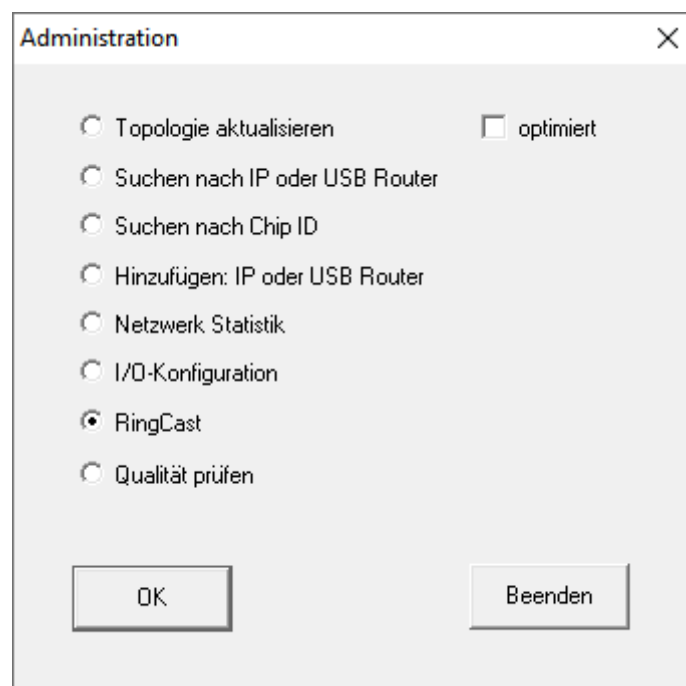
Der zentrale Output-Router erhält die Inputquittung der beteiligten RouterNodes ausschließlich über eine Ethernetverbindung. Der zentrale Output-Router ignoriert deshalb den Status von RouterNodes, die keine Ethernet-RouterNodes (.ER) sind. Wenn Sie den zentralen Output-Router verwenden und Ihr RingCast auch RouterNodes ohne Ethernetschnittstelle enthält,

dann bedeutet die Inputquittung des zentralen Output-Routers nur, dass alle Schließungen, die einem Ethernet-RouterNode zugewiesen sind, den Befehl empfangen haben.

- Prüfen Sie den Status von anderen RouterNodes R/CR) unabhängig vom zentralen Output-Router manuell (siehe *Erreichbarkeit testen (LSM)* [► 198] und *RouterNodes* [► 195] bzw. *IO-Status und LockNode-Reaktionsfähigkeit* [► 200]).

Wenn der zentrale Output-Router seine Input-Quittung nicht setzt bzw. sein Output nicht schaltet, dann kann dies unter anderem diese Gründe haben:

- Ein oder mehrere RouterNodes haben das Datenpaket nicht empfangen.
 - Ein oder mehrere RouterNodes haben einen oder mehrere LockNodes nicht erreicht.
 - Ethernetverbindung zu einem oder mehreren RouterNodes ist unterbrochen. Die RouterNodes könnten das Datenpaket zwar kabellos empfangen haben, aber ihre Inputquittungen wegen der unterbrochenen Ethernetverbindung nicht mehr zurückmelden.
1. Klicken Sie mit der rechten Maustaste auf den Eintrag "WaveNet_xx_x" im Wavenet-Manager.
 - ↳ Fenster "Administration" öffnet sich.



2. Wählen Sie die Option ☒ RingCast.
3. Klicken Sie auf die Schaltfläche .
- ↳ Fenster "Administration" schließt sich.

➞ Fenster "Funkdomänen bearbeiten" öffnet sich.

Funkdomänen bearbeiten.

Erstelle spezielle Funkdomänen.

Wähle Domäne :

Name :

Input :

Output Router :

Aktualisieren ☒

ausgewählte Router :

- RN_ER (0x0006_0x0021; 89003644)
- RN_ER (0x000E_0x0041; 0002A8B2)

freie Router :

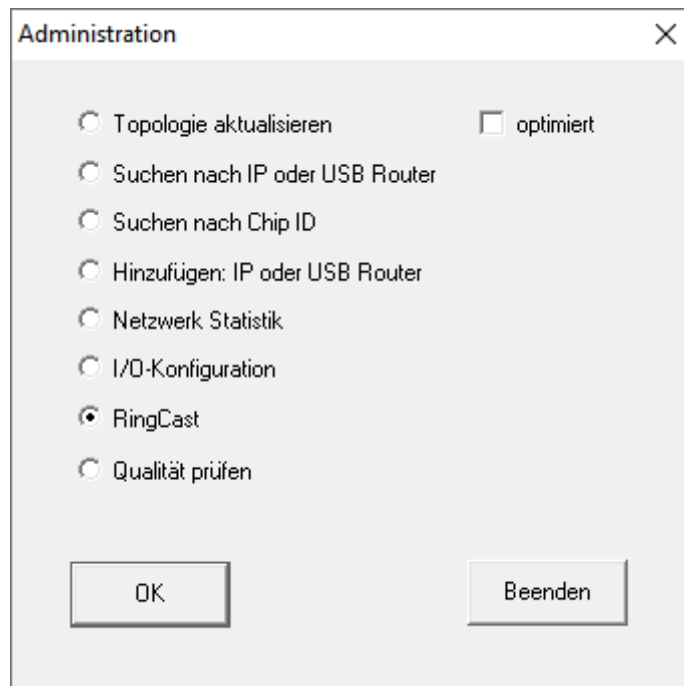
4. Wählen Sie in der Dropdown-Liste ▼ **Wähle Domäne** den Namen der Domäne aus, deren zentralen Output-Router Sie festlegen wollen.
 5. Markieren Sie den RouterNode, den Sie als zentralen Output-Router festlegen wollen.
 6. Klicken Sie auf die Schaltfläche **Setzen**.
 7. Klicken Sie auf die Schaltfläche **Save**.
 8. Klicken Sie auf die Schaltfläche **Beenden**.
- ➞ Zentraler Output-Router ist festgelegt.

Zentralen Output-Router löschen

Ohne zentralen Output-Router setzen alle RouterNodes (einschließlich dem ehemaligen zentralen Output-Router) die Inputquittung / den Output wie vorher eingestellt.

1. Klicken Sie mit der rechten Maustaste auf den Eintrag "WaveNet_xx_x" im Wavenet-Manager.

↳ Fenster "Administration" öffnet sich.



2. Wählen Sie die Option ☒ RingCast.
3. Klicken Sie auf die Schaltfläche **OK**.
 - ↳ Fenster "Administration" schließt sich.
 - ↳ Fenster "Funkdomänen bearbeiten" öffnet sich.

Funkdomänen bearbeiten. [X]

Erstelle spezielle Funkdomänen.

Wähle Domäne :

Name :

Input :

Output Router :

Aktualisieren ☒

ausgewählte Router :

RN_ER (0x0006_0x0021; 89003644)
RN_ER (0x000E_0x0041; 0002A8B2)

freie Router :

4. Klicken Sie auf die untere Schaltfläche **Löschen**.

↳ Zentraler Output-Router ist zur Löschung vorgemerkt.

5. Klicken Sie auf die Schaltfläche **Save**.

6. Klicken Sie auf die Schaltfläche **Beenden**.

↳ Zentraler Output-Router ist gelöscht. Der Abschluss des RingCasts wird nicht mehr angezeigt.

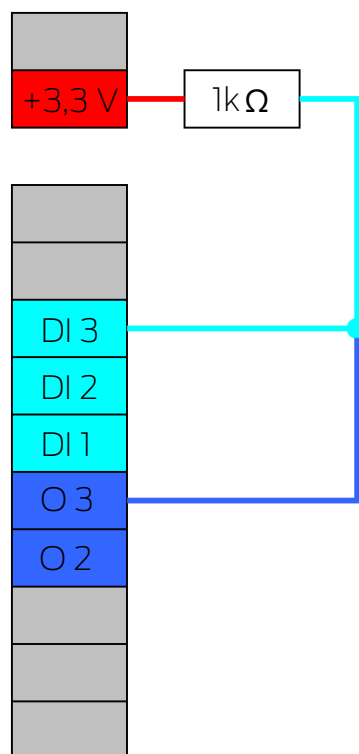
Abschluss des RingCasts an die LSM melden

RouterNodes können die Input-Quittung (bzw. das Schalten eines Ausgangs) nicht direkt an die LSM melden. Verwenden Sie dazu einen digitalen Eingang und leiten Sie dessen Status an die LSM weiter (siehe

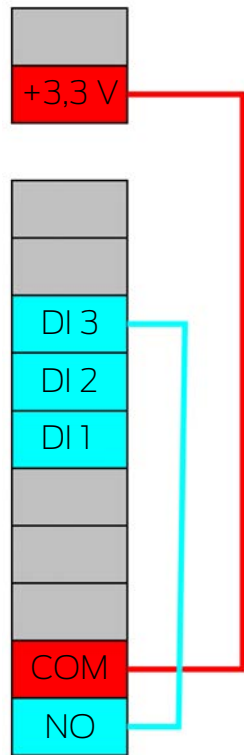
RouterNode: Digitaler Eingang [► 84]). Damit können Sie im Ereignismanager auf den erfolgreichen Abschluss eines RingCasts reagieren.

Diese Grafik zeigt die Beschaltung, wenn die Input-Quittung auf O3 oder O2 ausgegeben wird. Verbinden Sie O3/O2 wie gezeigt mit einem freien digitalen Eingang und leiten Sie diesen an die LSM weiter. Das Schaltverhalten ist durch den Pull-Up-Widerstand invertiert:

- Inputquittung aktiv: Pegel am digitalen Eingang 0 (Low)
- Inputquittung nicht aktiv: Pegel am digitalen Eingang 1 (High)



Diese Grafik zeigt die Beschaltung, wenn die Input-Quittung auf O1 ausgegeben wird. Verbinden Sie O1 wie gezeigt mit einem freien digitalen Eingang und leiten Sie diesen an die LSM weiter.



6.4.5.8 RingCast-Funktionstest

Der RingCast hat keine Selbstprüffunktion.



WARNUNG

Beeinträchtigung oder Ausfall von Schutzfunktionen durch geänderte Bedingungen

Die Aktivierung der Schutzfunktionen im RingCast basiert auf kabellosen Verbindungen und Ethernetverbindungen. Insbesondere kabellose Verbindungen können durch sich ändernde Umgebungsbedingungen beeinflusst werden (siehe *Funknetzwerk* [► 23] und *Herausforderungen in Funknetzwerken* [► 27]). Damit wird auch die Aktivierung der Schutzfunktionen im RingCast beeinflusst und die Sicherheit von Personen und Sachwerten, die beispielsweise durch die Schutzfunktionen im RingCast zusätzlich abgesichert werden, kann gefährdet sein.

1. Testen Sie die Schutzfunktionen mindestens einmal pro Monat (siehe *RingCast-Funktionstest* [► 151]).
2. Beachten Sie ggfs. auch weitere Richtlinien bzw. Verordnungen, die für Ihre Schließanlage relevant sind (insbesondere für Flucht- und Rettungswege sowie Brandschutz. Sie stellen die Erfüllung dieser Richtlinien und Verordnungen in Eigenverantwortung sicher.).

Veränderung des Ablaufs von Notfallfunktionen durch Fehlfunktionen

SimonsVoss und "Made in Germany" stehen für höchste Sicherheit und Zuverlässigkeit. In Einzelfällen können Fehlfunktionen Ihrer Geräte dennoch nicht ausgeschlossen werden. Damit wird möglicherweise die Sicherheit von Personen und Sachwerten, die durch die Schutzfunktionen im RingCast zusätzlich abgesichert werden, gefährdet.

1. Testen Sie Ihre Geräte mindestens einmal pro Monat (siehe *Geräte-Funktionstest* [▶ 199]. Nach anderen Vorschriften bezüglich Ihres Gesamtsystems können auch kürzere Abstände erforderlich sein).
2. Testen Sie die Schutzfunktionen mindestens einmal pro Monat (siehe *RingCast-Funktionstest* [▶ 151]).

Schalten Sie am Initiator den entsprechenden Eingang und überprüfen Sie:

- ob die Schließungen wie gewünscht reagieren (siehe auch *RouterNode: Digitaler Eingang* [▶ 84]).
- ob der ggfs. eingestellte Ausgang am RouterNode die Quittung wie gewünscht durch Schalten anzeigt (siehe auch *RouterNode: Digitaler Ausgang* [▶ 81]).

Test mit zentralem Output-Router



HINWEIS

Zentraler Output-Router im RingCast mit R/CR-RouterNodes

Der zentrale Output-Router erhält die Inputquittung der beteiligten RouterNodes ausschließlich über eine Ethernetverbindung. Der zentrale Output-Router ignoriert deshalb den Status von RouterNodes, die keine Ethernet-RouterNodes (.ER) sind. Wenn Sie den zentralen Output-Router verwenden und Ihr RingCast auch RouterNodes ohne Ethernetschnittstelle enthält, dann bedeutet die Inputquittung des zentralen Output-Routers nur, dass alle Schließungen, die einem Ethernet-RouterNode zugewiesen sind, den Befehl empfangen haben.

- Prüfen Sie den Status von anderen RouterNodes R/CR) unabhängig vom zentralen Output-Router manuell (siehe *Erreichbarkeit testen (LSM)* [▶ 198] und *RouterNodes* [▶ 195] bzw. *IO-Status und LockNode-Reaktionsfähigkeit* [▶ 200]).

Die Verwendung eines zentralen Output-Routers (siehe *Zentraler Output-Router* [▶ 145]) vereinfacht den Test des RingCasts erheblich. Schalten Sie am Initiator den entsprechenden Eingang und prüfen Sie, ob der zentrale Output-Router eine Inputquittung absetzt bzw. den entsprechenden Ausgang schaltet. Wenn der Ausgang nicht schaltet, dann prüfen Sie, welche RouterNodes Probleme verursacht haben:

- ✓ WaveNet-Manager über LSM geöffnet (siehe *Best Practice: Aus der LSM-Software* [▶ 40]).
- 1. Klicken Sie mit der rechten Maustaste auf den Eintrag des RingCasts, den Sie testen wollen.
- 2. Wählen Sie im Dropdown-Menü ▼ **Wähle Domäne** den Input aus, dessen RingCast Sie testen wollen.
 - ↳ Fenster "Funkdomänen bearbeiten" öffnet sich.

Funkdomänen bearbeiten.

Erstelle spezielle Funkdomänen.

Wähle Domäne :

Name :

Input :

Output Router :

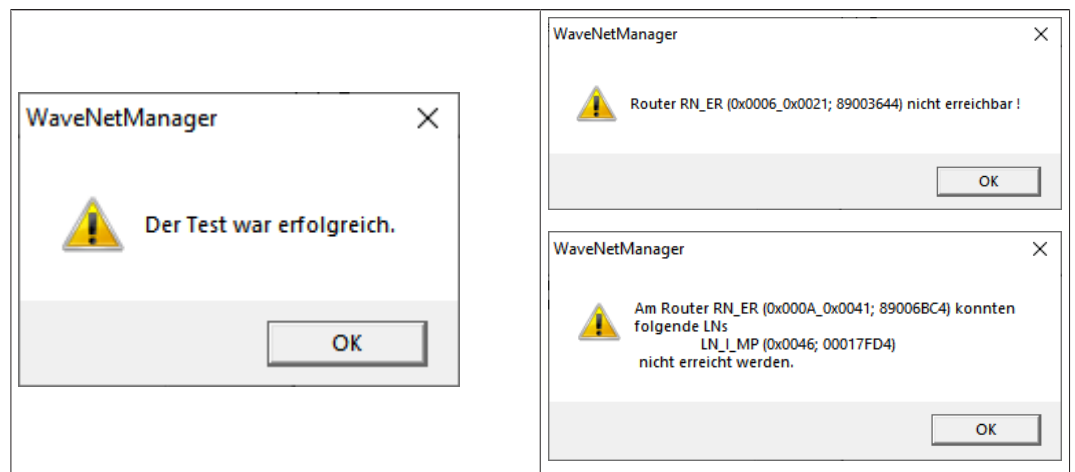
Aktualisieren ☒

ausgewählte Router :

- RN_ER (0x0006_0x0021; 89003644)
- RN_ER (0x000E_0x0041; 0002A8B2)

freie Router :

3. Klicken Sie auf die Schaltfläche **Status**.
 - ↳ RingCast wird getestet.



Der RingCast konnte alle Schließungen ansprechen.	Der RingCast konnte nicht abgeschlossen werden. Mögliche Ursachen (siehe auch <i>Zentraler Output-Router</i> [► 145]): ■ Ein oder mehrere RouterNodes haben das Datenpaket nicht empfangen. ■ Ein oder mehrere RouterNodes haben einen oder mehrere LockNodes nicht erreicht. ■ Ethernetverbindung zu einem oder mehreren RouterNodes ist unterbrochen. Die RouterNodes könnten das Datenpaket zwar kabellos empfangen haben, aber ihre Inputquittungen wegen der unterbrochenen Ethernetverbindung nicht mehr zurückmelden. 1. Prüfen Sie die Erreichbarkeit der genannten RouterNodes (siehe <i>RouterNodes</i> [► 195] und <i>Erreichbarkeit testen (LSM)</i> [► 198]). 2. Prüfen Sie die Erreichbarkeit der LockNodes (siehe <i>LockNodes</i> [► 197] und <i>Erreichbarkeit testen (LSM)</i> [► 198]). 3. Prüfen Sie die letzten Reaktionen der LockNodes (siehe <i>IO-Status und LockNode-Reaktionsfähigkeit</i> [► 200]).
--	--

6.4.5.9 RingCast löschen

- ✓ WaveNet-Manager über LSM geöffnet (siehe *Best Practice: Aus der LSM-Software* [► 40]).
 - ✓ RouterNodes und LockNodes an Stromversorgung angeschlossen.
1. Klicken Sie in der Übersicht mit der rechten Maustaste auf den obersten Eintrag des RingCast, den Sie löschen wollen.
 - ➞ Fenster "Funkdomänen bearbeiten" öffnet sich.

Funkdomänen bearbeiten. X

Erstelle spezielle Funkdomänen.

Wähle Domäne : neu ▼

Name : Löschen

Input : 1 ▼

Output Router : Löschen Status

Aktualisieren ☐

ausgewählte Router :

freie Router :

Speichern Beenden

2. Wählen Sie im Dropdown-Menü ▼ **Wähle Domäne** die Domäne (Eingang) aus, deren RingCast Sie löschen wollen.
3. Klicken Sie auf die Schaltfläche **Löschen** unterhalb der Dropdown-Menüs ▼ **Wähle Domäne**.
 - ➔ RingCast der Domäne ist zur Löschung vorgemerkt.
4. Klicken Sie auf die Schaltfläche **Save**.
5. Klicken Sie auf die Schaltfläche **Beenden**.
 - ➔ RingCast der Domäne ist gelöscht und wird in der Übersicht nicht mehr angezeigt.

Wiederholen Sie die Schritte, bis Sie alle gewünschten RingCasts gelöscht haben. Anschließend können Sie die IO-Konfiguration der RouterNodes an den entsprechenden Eingängen neu konfigurieren (siehe [RouterNode: Digitaler Eingang \[► 84\]](#)).

6.4.6 Gerätespezifische Einstellungen

6.4.6.1 RouterNodes

Sie können die IO-Konfiguration für jeden RouterNode individuell einstellen (siehe *I/O-Konfiguration und Schutzfunktionen* [► 74]) und routerspezifische Einstellungen (Oberflächenpasswort und IP-Änderung durch das OAM-Tool) in der Browserschnittstelle einstellen (siehe *Browserschnittstelle* [► 157]).

Browserschnittstelle

Sie können für RouterNodes, GatewayNodes und SmartBridges mit Ethernet-Schnittstelle über den Browser unter anderem einstellen:

- Änderungen über das OAM-Tool erlauben
- Passwort für die Weboberfläche
- IP-Adresse/DHCP-Betrieb
- SNMP-Port öffnen und schließen

Aufruf

Sie erhalten das Gerät mit folgender werkseitiger Konfiguration:

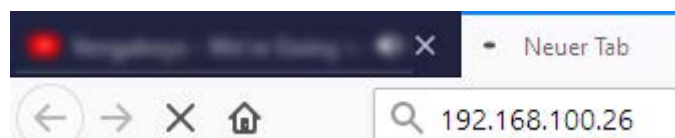
IP-Adresse	192.168.100.100 (falls kein DHCP-Server gefunden wird)
Subnetz-Maske	255.255.0.0
Benutzername	SimonsVoss
Passwort	SimonsVoss

Der Ablauf ist für RouterNodes beschrieben. Verfahren Sie für SmartIntego-GatewayNodes und MobileKey-SmartBridges ebenso.

Ändern Sie nach dem ersten Aufruf das Standardpasswort.

- ✓ IP des RouterNodes bekannt (siehe *IP-Adresse ermitteln und einstellen* [► 53]).
- ✓ Browser geöffnet.
- ✓ Zugangsdaten zur Browserschnittstelle (Name und Passwort) bekannt.

1. Geben Sie in das Adressfeld Ihres Browsers die IP-Adresse ein.



2. Bestätigen Sie die Eingabe mit der Enter-Taste.

- ➔ Fenster "Authentifizierung erforderlich" öffnet sich.

Authentifizierung erforderlich

?

http://192.168.100.26 verlangt einen Benutzernamen und ein Passwort. Ausgabe der Website: "protected area"

Benutzername:

Passwort:

OK

Abbrechen

3. Geben Sie die Zugangsdaten ein.

4. Klicken Sie auf die Schaltfläche **OK**.

→ Systemübersicht der Browserschnittstelle ist sichtbar.

ÜBERSICHT
WAVENET
VERBINDUNG

System Information: Übersicht

Version:

Firmware Version: 40.11.00

Netzwerkconfiguration:

MAC Adresse:	94:50:89:00:36:44
Host Name:	SV_003644
DHCP:	Ein
IP-Adresse:	192.168.100.26
Subnetzmaske:	255.255.255.0
Gateway:	192.168.100.1
DNS-Server1:	192.168.100.1
DNS-Server2:	0.0.0.0
SV Port:	2101
SV SecPort:	2153



HINWEIS

Weboberfläche ab Firmware 40.12 nicht mehr mit Standardpasswort nutzbar

Ab Firmwareversion 40.12 bleibt die Browserschnittstelle solange gesperrt, bis das Standardpasswort geändert wurde.

■ Ändern Sie das Standardpasswort.

→ Browserschnittstelle wird entsperrt und Einstellungen können geändert werden.

**HINWEIS****Unbefugter Zugriff mit Standard-Zugangsdaten**

1. Ändern Sie das frei einsehbare Webserver-Standardpasswort. Unbefugte können zwar keinen Zutritt erlangen, aber die Konfiguration ändern. In diesem Fall erreichen Sie das Gerät nicht mehr und müssen es zurücksetzen.
2. Verwenden Sie keine Leerzeichen am Anfang oder am Ende (werden von manchen Browsern nicht übertragen).

Änderung der IP-Adresse über das OAM-Tool sperren/erlauben

Solange Sie die ▼ **OAM-Tool erlauben** nicht erlauben, können Sie auch keine Updates über das OAM-Tool einspielen.

- ✓ Browserschnittstelle geöffnet.
- 1. Öffnen Sie über | KONFIGURATION | die Registerkarte [PORT].
 - ➔ Sie sehen die Übersicht der TCP-Port-Einstellungen des RouterNode
- 2.

NETZWERK
PORT
ETHERNET SCHNITTSTELLE
WAVENET

Konfiguration: Port-Einstellungen ändern**TCP-Port Einstellungen:**

SV Port:	2101
SV SecPort:	2153
SV Zeitabschaltung [s]:	30
HTTP:	Ein
Telnet:	Aus
OAM-Tool erlauben:	Ja

2. Wählen Sie im Dropdown-Menü ▼ **OAM-Tool erlauben** den Eintrag "Ja" (Änderung der IP durch OAM-Tool erlauben) bzw. "Nein" (Änderung der IP durch OAM-Tool sperren) aus.
3. Klicken Sie auf die Schaltfläche **Save**.
 - ➔ Änderung der IP-Adresse über das OAM-Tool ist gesperrt/erlaubt.

Passwort ändern

Einige Browser übertragen keine Leerzeichen, die am Anfang des Passworts stehen. Beginnen Sie das Passwort deshalb nicht mit Leerzeichen.

✓ Browserschnittstelle geöffnet.

1. Öffnen Sie über | ADMINISTRATION | die Registerkarte [PASSWORT].

PASSWORT
ZERTIFIKATE
WERKSEINSTELLUNG
NEUSTART

Administration: Passwort ändern

Neues Passwort:

Neues Passwort:	
Passwort bestätigen:	
Passwort speichern	

2. Geben Sie Ihr neues Passwort ein.

3. Wiederholen Sie Ihr neues Passwort.

4. Klicken Sie auf die Schaltfläche **Passwort speichern**.

➞ Passwort ist geändert.

SNMP-Port schließen und öffnen

Der SNMP-Port ist ab Werk und nach jedem Zurücksetzen geöffnet. Nicht benötigte Ports sollten generell geschlossen werden. Wenn Sie den SNMP-Port schließen, dann findet das OAM-Tool den RouterNode 2 nicht mehr.

✓ Browserschnittstelle geöffnet.

1. Öffnen Sie über | KONFIGURATION | die Registerkarte [PORT].

➞ Sie sehen die Übersicht der TCP-Port-Einstellungen des RouterNode 2.

NETZWERK
PORT
ETHERNET SCHNITTSTELLE
WAVENET

Konfiguration: Port-Einstellungen ändern

TCP-Port Einstellungen:

SV Port:	2101
SV SecPort:	2153
SV Zeitabschaltung [s]:	30
HTTP:	Ein ▼
Telnet:	Aus ▼
OAM-Tool erlauben:	Ja ▼
Speichern	

2. Wählen Sie im Dropdown-Menü ▼ **SNMP-Port** den Eintrag "Ja" (SNMP-Port öffnen) bzw. "Nein" (SNMP-Port schließen) aus.

3. Klicken Sie auf die Schaltfläche **Save**.

→ SNMP-Port ist geöffnet bzw. geschlossen.

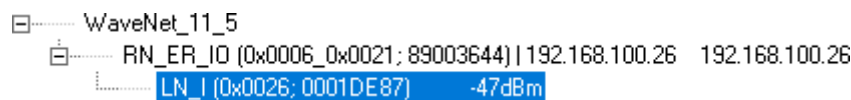
6.4.6.2 LockNodes

Sie können für jeden LockNode individuell einstellen, ob er auf Broadcasts reagiert (siehe auch *I/O-Konfiguration und Schutzfunktionen* [► 74] und *LockNode* [► 92]).

6.5 Fehlerbehebung

6.5.1 Signalqualität verbessern

Sie sehen die Signalstärke in der Übersicht des WaveNet-Managers (siehe auch *Signalqualität prüfen* [► 192]).



The screenshot shows a hierarchical tree view of the WaveNet system. The root node is 'WaveNet_11_5'. Under it is 'RN_ER_IO (0x0006_0x0021; 89003644)' with IP addresses '192.168.100.26' and '192.168.100.26'. Below that is a node 'LN_I (0x0026; 0001DE87)' which is highlighted in blue and shows a signal strength of '-47dBm'.

Einheit der Signalstärke

Der WaveNet-Manager gibt die Signalstärke als RSSI-Wert (Received Signal Strength) in dBm an. Dieser Wert ist:

- Logarithmisch: Eine Verbesserung um 10 dBm bedeutet in der Praxis die doppelte Signalstärke.
- Negativ: Der theoretische Bestwert beträgt 0 dBm und wird nur durch Kabelverbindungen erreicht. Je näher der Wert an 0 dBm ist (je kleiner also der Betrag ist), desto besser ist der Empfang.

Externe Antenne

Eine externe Antenne (siehe *Zubehör* [► 19]) verbessert bei richtiger Positionierung den Empfang. Schließen Sie die Antenne am vorgesehenen Steckplatz an und richten Sie die Antenne so aus, dass die Signalstärke am LockNode verbessert wird.

6.5.1.1 LockNodes einem anderen RouterNode zuweisen

Die Signalqualität der Funkstrecke zwischen RouterNodes und LockNodes (und anderen RouterNodes) wird unter anderem durch folgendes beeinflusst:

- Umgebungsbedingungen (Störsignale, Baumaterialien)
- Entfernung

Sie können diese Bedingungen und damit Signalqualität der Funkstrecke zwischen RouterNodes und LockNodes verbessern, indem Sie den LockNode einem näher oder störungsärmer gelegenen RouterNode zuweisen.

Solange Sie den LockNode innerhalb desselben CentralNode-/Ethernet-RouterNode-Segments verschieben, können Sie den LockNode wie nachfolgend beschrieben einfach neu zuweisen. Andernfalls setzen Sie den LockNode im WaveNet-Manager zurück und fügen ihn am geplanten RouterNode neu ein (siehe *Best Practice: Reset mit WaveNet-Manager* [► 178] und *LockNodes dem WaveNet hinzufügen* [► 64]).

Einzelnen LockNode einem RouterNode neu zuweisen

- ✓ WaveNet-Manager über LSM geöffnet (siehe *Best Practice: Aus der LSM-Software* [► 40]).
- 1. Klicken Sie mit der rechten Maustaste auf den Eintrag des LockNodes, den Sie einem anderen RouterNode zuweisen wollen.
 - ↳ Fenster "Administration" öffnet sich.

Administration von LN_I (0x0026; 0001DE87) -47dBm

Konfiguration

Name :

☐ Ersetzen mit Chip ID

☐ Zurücksetzen/Löschen

☒ Verschieben in ein anderes Mastersegment

☐ I/O-Konfiguration

Wartung

☐ Mastersegment durchsuchen ☐ nur bekannt

☐ Zweig aktualisieren ☐ optimiert

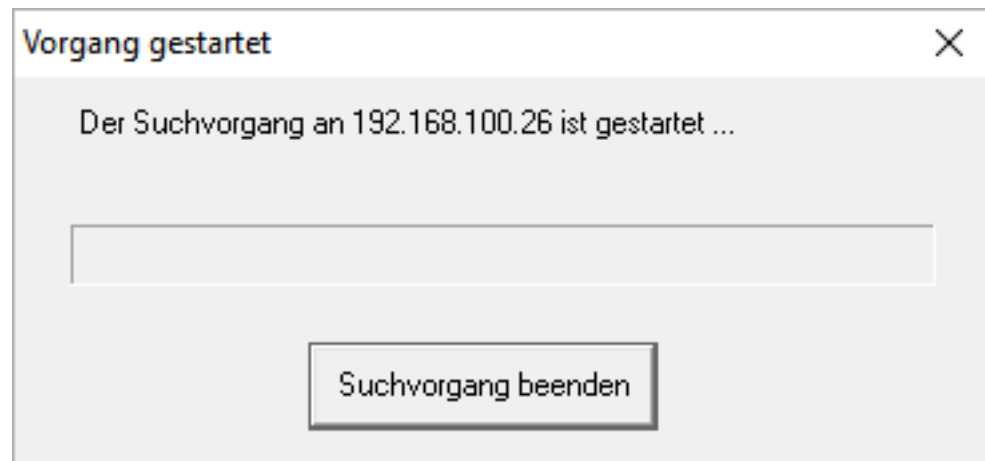
☐ Suchen nach Chip ID

☐ Ping

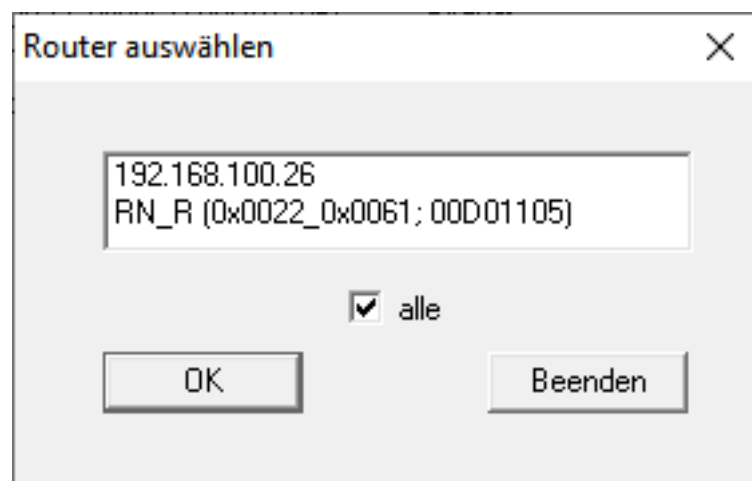
☐ Neu starten

OK Beenden

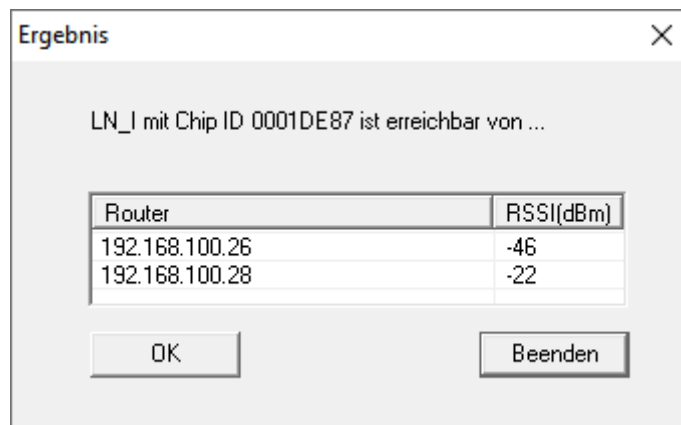
2. Wählen Sie im Bereich "Konfiguration" die Option  Verschieben in ein anderes Mastersegment aus.
3. Klicken Sie auf die Schaltfläche **OK**.
 - ↳ Fenster "Vorgang gestartet" öffnet sich vorübergehend.



- ↳ Fenster "Router auswählen" öffnet sich (Wenn sich direkt das Ergebnisfenster öffnet, dann gibt es keine anderen Router-/CentralNodes im Segment. Sie müssen den LockNode zurücksetzen und an einem anderen RouterNode neu hinzufügen).



4. Markieren Sie die Router-/CentralNodes, die für die Verschiebung des LockNodes infrage kommen. (Aktivieren Sie ggfs. die Checkbox ☒ alle.)
5. Klicken Sie auf die Schaltfläche **OK**.
 - ↳ Signalqualität zwischen LockNode und ausgewählten RouterNodes wird gemessen.
 - ↳ Fenster "Ergebnis" öffnet sich. Sie sehen die Liste der zuvor ausgewählten RouterNodes mit Messwerten.



6. Markieren Sie den RouterNode, dem Sie Ihren LockNode zuordnen wollen.



HINWEIS

Beste Signalqualität

Markieren Sie aus den möglichen RouterNodes den RouterNode, dessen RSSI-Wert am nächsten bei 0 (0 = Theoretischer Bestwert) liegt.



HINWEIS

Ausrufezeichen vor RouterNodes in der Liste

Bei bestimmten Netzwerkstrukturen können Sie den ausgewählten Lock-Node nur bestimmten RouterNodes zuordnen. RouterNodes, denen Sie den ausgewählten LockNode nicht zuordnen können, sind mit einem Ausrufezeichen vor dem Eintrag markiert (z.B. wenn die maximale Anzahl der Lock-Nodes für diesen RouterNode bereits erreicht ist). Diese RouterNodes werden nur der Vollständigkeit halber angezeigt.

7. Klicken Sie auf die Schaltfläche **OK**.

→ Fenster "Ergebnis" schließt sich.

→ LockNode ist dem gewünschten RouterNode zugeordnet.

Mehrere LockNodes einem RouterNode neu zuweisen

- ✓ WaveNet-Manager über LSM geöffnet (siehe *Best Practice: Aus der LSM-Software* [▶ 40]).
 - ✓ LockNodes und RouterNodes an Stromversorgung angeschlossen.
 - ✓ LockNodes und RouterNodes mit WaveNet verbunden (Test siehe *Erreichbarkeit testen (WaveNet)* [▶ 195]).
 - ✓ LockNodes mit aktuell schlechter Verbindung bekannt (siehe *Signalqualität prüfen* [▶ 192]).
1. Klicken Sie mit der rechten Maustaste auf den RouterNode, dem Sie LockNodes neu zuweisen wollen.
 - ➔ Fenster "Administration" öffnet sich.

Administration von RN_ER_IO (0x0006_0x0021; 89003644)

Konfiguration

Name :

☐ Ersetzen mit ...

☐ Zurücksetzen/Löschen

☐ Verschieben in ein anderes Mastersegment

☐ I/O-Konfiguration

Wartung

☒ Mastersegment durchsuchen ☐ nur bekannt

☐ Zweig aktualisieren ☐ optimiert

☐ Suchen nach Chip ID

☐ Ping

☐ Neu starten

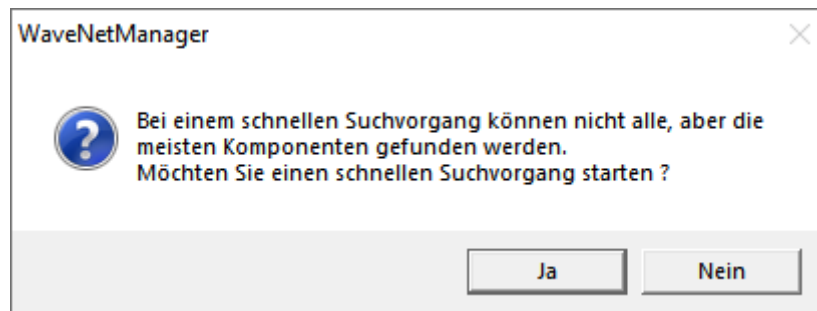
☐ Ausgang setzen und I/O-Status

☐ Qualität prüfen

Das Mastersegment besteht aus 2/25 LN_(X) und aus 0/4 Routern.

2. Wählen Sie im Bereich "Wartung" die Option ☒ Mastersegment durchsuchen.
3. Aktivieren Sie die Checkbox ☒ bekannt.
4. Klicken Sie auf die Schaltfläche .
- ➔ Fenster "Administration" schließt sich.

→ Fenster "WaveNetManager" öffnet sich.



5. Klicken Sie auf die Schaltfläche **Ja** (Schneller Suchvorgang) oder **Nein** (Normaler Suchvorgang).



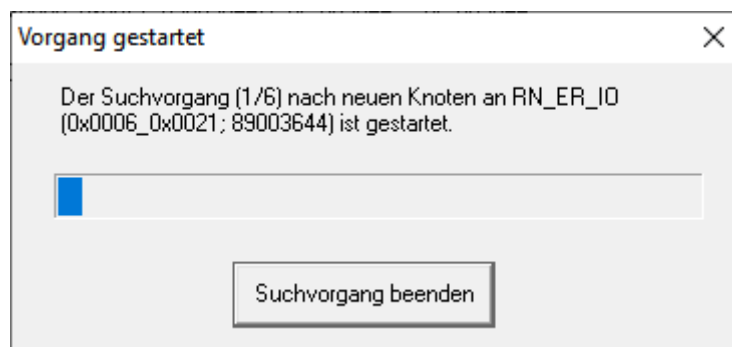
HINWEIS

Schneller Suchvorgang

Wenn Sie einen schnellen Suchvorgang durchführen, dann sendet der RouterNode nur einen einzigen Broadcast. Wenn Sie einen normalen Suchvorgang durchführen, dann sendet der RouterNode insgesamt sechs Broadcasts. Der schnelle Suchvorgang ist schneller abgeschlossen, dafür ist der normale Suchvorgang gründlicher und findet auch LockNodes, die bei einem schnellen Suchvorgang nicht erreicht wurden.

→ Fenster "WaveNetManager" schließt sich.

→ Fenster "Vorgang gestartet" öffnet sich vorübergehend.



→ Fenster "Ergebnis des Suchvorganges" öffnet sich.

Ergebnis des Suchvorganges

RN_ER (0x0006_0x0021; 89003644)

Knoten in diesem Segment:

Knoten	RSSI(dBm)
LN_I_MP(00017FD7)	-78
LN_I_MP(00017FD4)	-32
LN_I(0003BA7D)	-68
LN_I(0001DE87)	-46

Knoten von anderen Segmenten:

Knoten	RSSI(dBm)
LN_I_SH(00029DE1)	-73
LN_I(000183E4)	-82

neue Knoten:

Knoten	RSSI(dBm)

Sortieren nach RSSI

Beenden

Sie sehen eine Übersichtstabelle der LockNodes, die der RouterNode während der Suche gefunden hat. Diese Tabelle hat drei Spalten:

Knoten in diesem Segment	Knoten von anderen Segmenten	Neue Knoten
Diese LockNodes befinden sich in der WaveNet-Topologie und sind dem RouterNode bereits zugeordnet.	Diese LockNodes befinden sich in der WaveNet-Topologie, sind aber einem anderen RouterNode zugeordnet.	Diese RouterNodes befinden sich nicht in der WaveNet-Topologie.

Jede Spalte enthält zwei Unterspalten:

Knoten	RSSI
Name des LockNodes	Signalstärke der Verbindung des LockNodes zum suchenden Router-Node

Einheit der Signalstärke

Der WaveNet-Manager gibt die Signalstärke als RSSI-Wert (Received Signal Strength) in dBm an. Dieser Wert ist:

- Logarithmisch: Eine Verbesserung um 10 dBm bedeutet in der Praxis die doppelte Signalstärke.
- Negativ: Der theoretische Bestwert beträgt 0 dBm und wird nur durch Kabelverbindungen erreicht. Je näher der Wert an 0 dBm ist (je kleiner also der Betrag ist), desto besser ist der Empfang.

1. Markieren Sie die Ihnen bekannten LockNodes mit schlechter Verbindung in der mittleren Spalte (Knoten von anderen Segmenten), wenn der RSSI-Wert besser ist.
Sie sehen die aktuellen RSSI-Werte im Hauptfenster des WaveNet-Managers.

2. Verschieben Sie die LockNodes mithilfe von Drag-and-Drop in die linke Spalte (Knoten in diesem Segment), um sie dem aktuellen RouterNode (mit dem Sie gesucht haben) zuzuweisen.

↳ LockNodes werden dem aktuellen RouterNode zugewiesen.



HINWEIS

Dauer der Zuweisung

Wenn Sie LockNodes neu zuweisen, dann kommuniziert der WaveNet-Manager mit den LockNodes, um die Konfiguration zu übertragen und den LockNode zu prüfen. Diese Prüfung dauert einige Sekunden.

3. Bestätigen Sie ggfs. die IO-Konfiguration des LockNodes mit einem Klick auf die Schaltfläche **OK** (Sie können die IO-Konfiguration jederzeit ändern, siehe *I/O-Konfiguration und Schutzfunktionen* [► 74]).

↳ LockNodes sind dem RouterNode zugewiesen.

6.5.2 Geräteneustart

6.5.2.1 RouterNodes

Ethernet-RouterNodes über die Browserschnittstelle neustarten

✓ Browserschnittstelle geöffnet (siehe *Browserschnittstelle* [► 157]).

1. Öffnen Sie über | ADMINISTRATION | die Registerkarte [NEUSTART].

↳ Sie sehen das Neustartmenü.

PASSWORT
ZERTIFIKATE
WERKSEINSTELLUNG
NEU START

Administration: Router neu starten

Neustart

Information: Für den Neustart werden ca. 10 Sekunden benötigt.

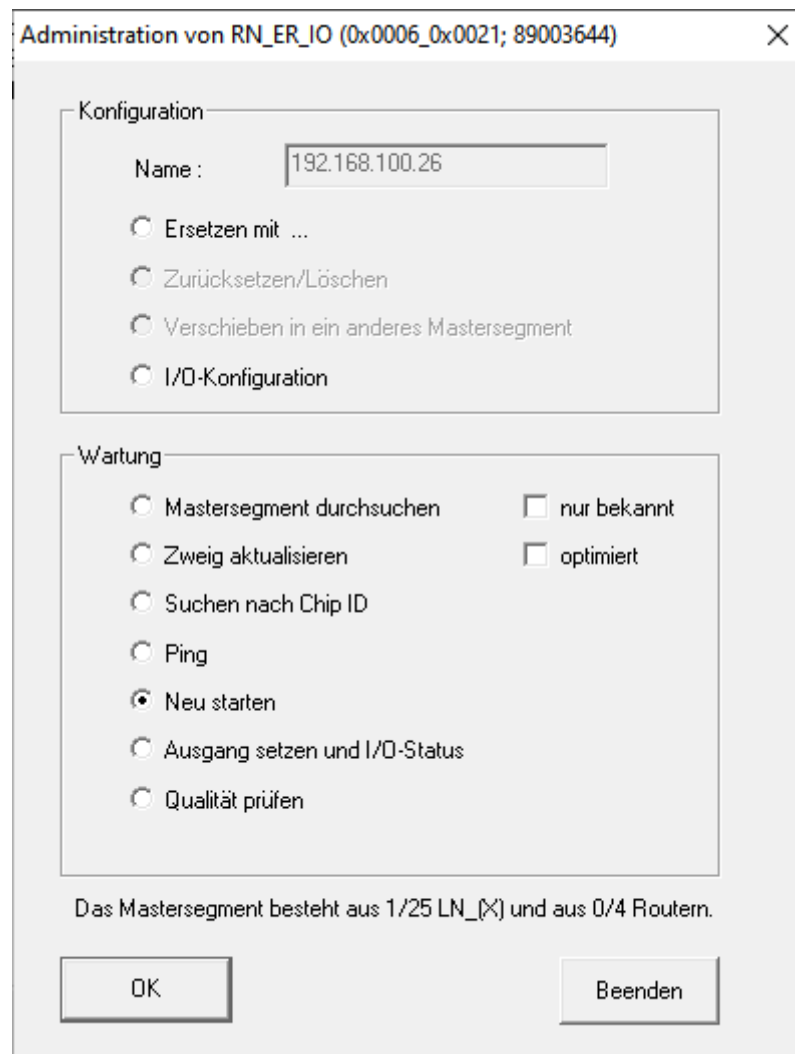
2. Klicken Sie auf die Schaltfläche **Neustart**.

↳ Neustart wird durchgeführt.

↳ Ethernet-RouterNode ist neu gestartet.

RouterNodes im WaveNet-Manager neustarten

- ✓ WaveNet-Manager über LSM geöffnet (siehe *Best Practice: Aus der LSM-Software* [▶ 40]).
 - ✓ RouterNode mit WaveNet verbunden (siehe *RouterNode dem WaveNet hinzufügen* [▶ 57]).
1. Klicken Sie mit der rechten Maustate auf den Eintrag des RouterNodes, den Sie neu starten wollen.
 - ↳ Fenster "Administration" öffnet sich.



2. Wählen Sie im Bereich "Wartung" die Option  Neu starten.
 3. Klicken Sie auf die Schaltfläche .
- ↳ Fenster "Vorgang gestartet" öffnet sich vorübergehend.



- ↳ RouterNode wird neu gestartet.
- ↳ RouterNode ist neu gestartet.

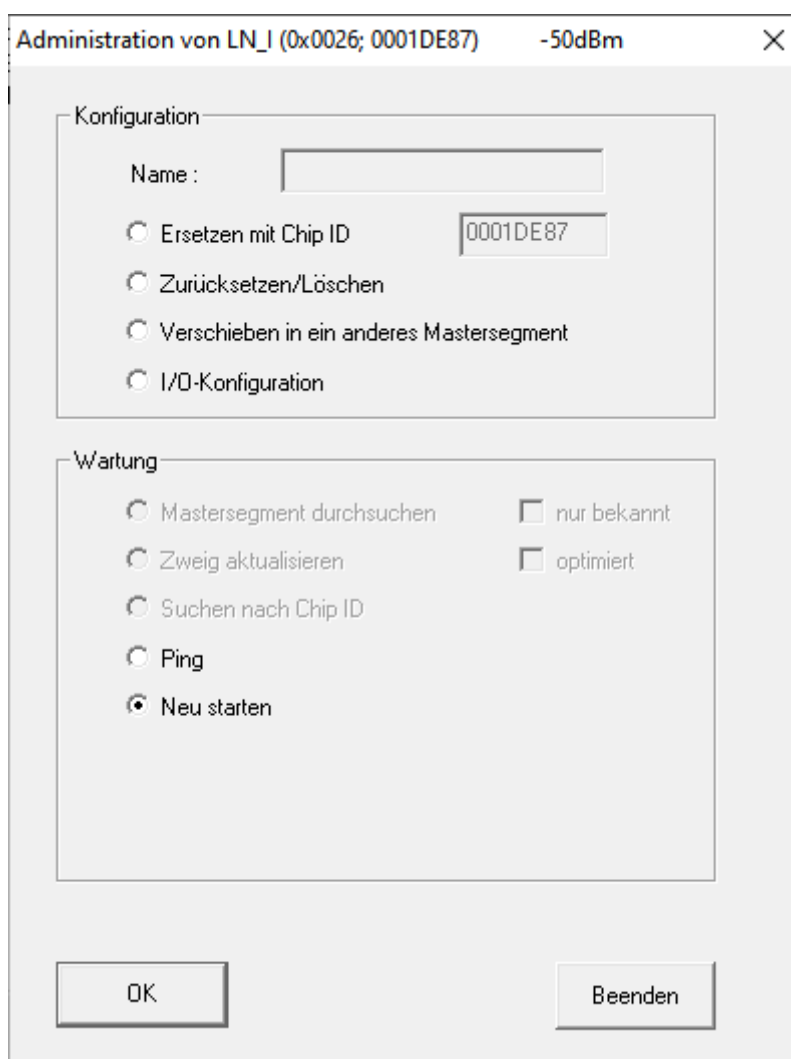
RouterNodes über Stromanschluss neustarten

Ihre RouterNodes starten neu, wenn Sie die Stromversorgung trennen, etwa eine halbe Minute warten und wieder anschließen.

6.5.2.2 LockNodes

LockNodes im WaveNet-Manager neustarten

- ✓ WaveNet-Manager über LSM geöffnet (siehe *Best Practice: Aus der LSM-Software* [► 40]).
 - ✓ LockNode mit WaveNet verbunden (siehe *LockNodes dem WaveNet hinzufügen* [► 64]).
1. Klicken Sie mit der rechten Maustaste auf den Eintrag des LockNodes, den Sie neu starten wollen.
 - ↳ Fenster "Administration" öffnet sich.



2. Wählen Sie im Bereich "Wartung" die Option ☒ Neu starten.
3. Klicken Sie auf die Schaltfläche **OK**.
 - ↳ Fenster "Vorgang gestartet" öffnet sich vorübergehend.



- ↳ LockNode wird neu gestartet.
- ↳ LockNode ist neu gestartet.

LockNodes über Stromanschluss neustarten

Ihre LockNodes werden zurückgesetzt und starten neu, wenn Sie die Stromversorgung trennen (bzw. den LNI ausbauen), eine halbe Minute warten und wieder anschließen (bzw. den LNI wieder einbauen). Nach dem Neustart piepen die LockNodes vier Mal.

6.5.3 Gerät neu programmieren oder ersetzen

Wenn Sie Probleme mit einem Gerät haben, dann versuchen Sie vor dem Ersetzen Folgendes:

- Gerät neu programmieren
- Gerät zurücksetzen und neu programmieren (siehe [Zurücksetzen/Löschen](#) [► 177])

Gerät neu programmieren

Das Blitzsymbol in der Übersicht signalisiert ein Problem mit Ihrem Gerät. Versuchen Sie die Konfiguration auf demselben Gerät neu zu programmieren. Führen Sie dazu den Ersetzvorgang wie beschrieben (siehe [RouterNodes](#) [► 173] und [LockNodes](#) [► 175]) mit derselben IP-Adresse bzw. Chip-ID des Geräts durch, das Sie neu programmieren wollen. Sie übertragen die Konfiguration des Geräts, das ersetzt werden soll, auf das Gerät, das die genannte Chip-ID hat. Wenn das dieselbe Chip-ID ist, dann wird die Konfiguration auf dem Gerät neu programmiert.

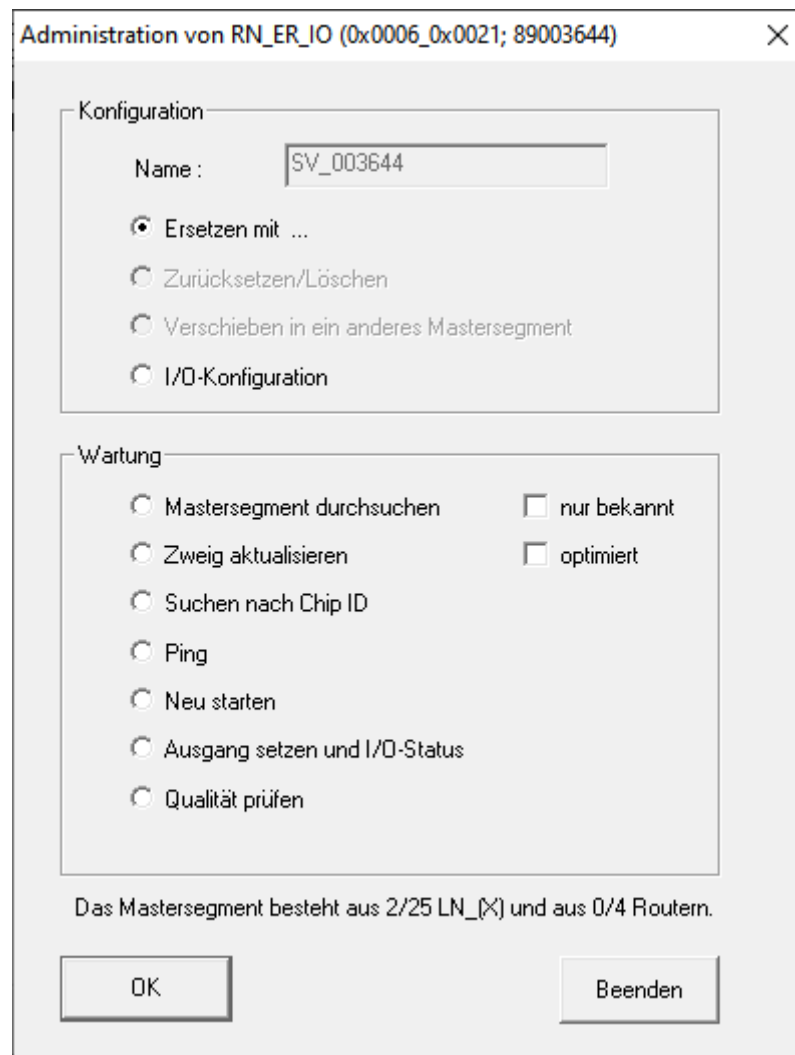
Gerät ersetzen

Sie können im WaveNet Geräte ersetzen, falls ein Gerät zum Beispiel aus folgenden Gründen nicht mehr verwendet werden soll:

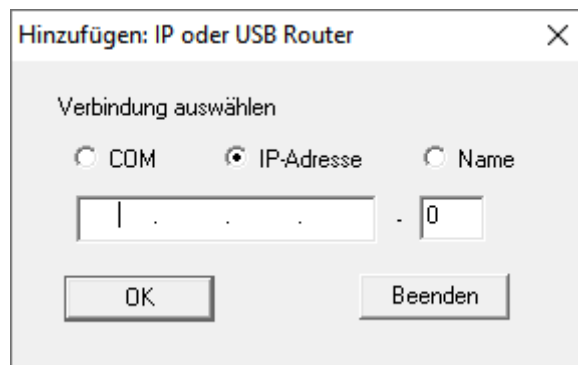
- Austausch
 - Vandalismus
 - Diebstahl
 - Defekte
 - ✓ Ersatz-RouterNode bzw. Ersatz-LockNode bereits am endgültigen Betriebsort aufgestellt.
 - ✓ Ersatz-RouterNode bereits über gültige IP-Adresse/Hostnamen auflösbar (IP-Adresse ermitteln/einstellen siehe [IP-Adresse ermitteln und einstellen](#) [► 53])
1. Verwenden Sie für die Neuprogrammierung anstelle derselben IP-Adresse/Chip-ID die IP-Adresse/Chip-ID des Ersatzgerätes.
 2. Gehen Sie wie bei der Neuprogrammierung einer WaveNet-Konfiguration auf einem Gerät vor (siehe [RouterNodes](#) [► 173] und [LockNodes](#) [► 175]).
- ➞ Gerät ersetzt.

6.5.3.1 RouterNodes

- ✓ WaveNet-Manager über LSM geöffnet (siehe *Best Practice: Aus der LSM-Software* [▶ 40]).
- 1. Klicken Sie mit der rechten Maustaste auf den Eintrag des RouterNodes, den Sie ersetzen wollen.
 - ↳ Fenster "Administration" öffnet sich.



- 2. Wählen Sie im Bereich "Konfiguration" die Option ☒ Ersetzen mit....
- 3. Klicken Sie auf die Schaltfläche **OK**.
 - ↳ Fenster "Administration" schließt sich.
 - ↳ Fenster "Hinzufügen: IP oder USB Router" öffnet sich.



4. Wählen Sie die Option ☒ IP-Adresse bzw. ☒ Name.
5. Prüfen Sie die IP-Adresse bzw. den Namen (und korrigieren Sie diese ggfs.).
6. Klicken Sie auf die Schaltfläche **OK**.
 - ↳ Fenster "Hinzufügen: IP oder USB Router" schließt sich.
 - ↳ Falls Sie im zu ersetzenden RouterNode die IO-Funktionen verwenden: Fenster "I/O Konfiguration" öffnet sich.

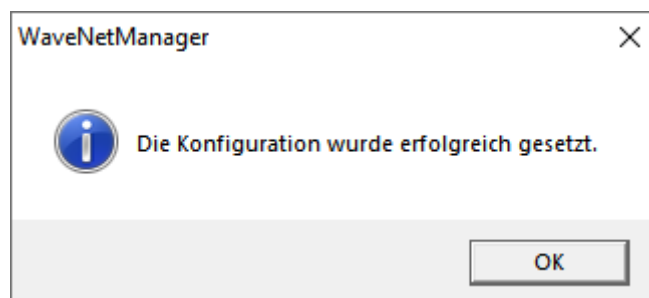


HINWEIS

IO-Konfiguration prüfen

Prüfen Sie die IO-Konfiguration. Sie können die IO-Konfiguration auch später einstellen (siehe *I/O-Konfiguration und Schutzfunktionen* [► 74]).

7. Klicken Sie auf die Schaltfläche **OK**.
 - ↳ Fenster "I/O Konfiguration" schließt sich.
 - ↳ Fenster "WaveNetManager" öffnet sich.



8. Klicken Sie auf die Schaltfläche **OK**.
 - ↳ Fenster "WaveNetManager" schließt sich.
 - ↳ RouterNode ist ersetzt.

6.5.3.2 LockNodes

- ✓ WaveNet-Manager über LSM geöffnet (siehe *Best Practice: Aus der LSM-Software* [▶ 40]).
- 1. Klicken Sie mit der rechten Maustaste auf den Eintrag des LockNodes, den Sie ersetzen wollen.
 - ↳ Fenster "Administration" öffnet sich.

Administration von LN_I_MP (0x0027; 00017FD4) Goliath Nationa... X

Konfiguration

Name : Goliath National Bank

☒ Ersetzen mit Chip ID 00017FD4

☐ Zurücksetzen/Löschen

☐ Verschieben in ein anderes Mastersegment

☐ I/O-Konfiguration

Wartung

☐ Mastersegment durchsuchen ☐ nur bekannt

☐ Zweig aktualisieren ☐ optimiert

☐ Suchen nach Chip ID

☐ Ping

☐ Neu starten

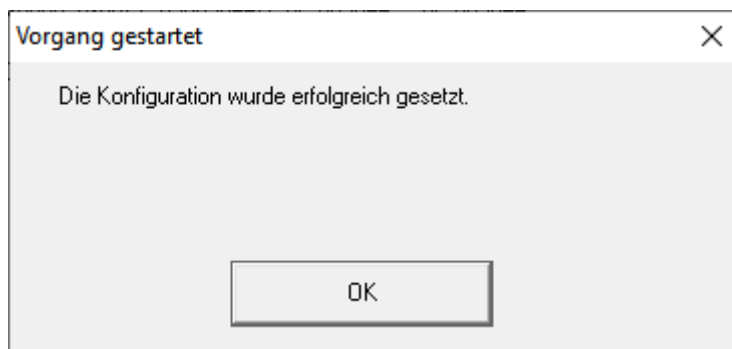
OK Beenden

2. Wählen Sie im Bereich "Konfiguration" die Option ☒ Ersetzen mit Chip-ID.
3. Geben Sie die Chip-ID des neuen LockNodes an (Sie finden die Chip-ID auf der Verpackung des LockNodes oder auf dem LockNode selbst).
4. Klicken Sie auf die Schaltfläche **OK**.
 - ↳ Fenster "Administration" schließt sich.
 - ↳ Fenster "I/O Konfiguration" öffnet sich.

**HINWEIS****IO-Konfiguration prüfen**

Prüfen Sie die IO-Konfiguration. Sie können die IO-Konfiguration auch später einstellen (siehe *I/O-Konfiguration und Schutzfunktionen* [► 74]).

5. Klicken Sie auf die Schaltfläche **OK**.
 - ↳ Fenster "I/O Konfiguration" schließt sich.
 - ↳ Fenster "Vorgang gestartet" öffnet sich.



6. Klicken Sie auf die Schaltfläche **OK**.
 - ↳ Fenster "Vorgang gestartet" schließt sich.
 - ↳ LockNode ist ersetzt.

Verwenden Sie ersetzte LockNodes nicht mehr in Reichweite des WaveNets.

6.5.4 netcfg.xml löschen

Wenn Sie Probleme mit falschen Einträgen oder Ihrem WaveNet haben, dann löschen Sie die netcfg.xml, bevor Sie den WaveNet-Manager starten. In der netcfg.xml können insbesondere dann, wenn Sie mit mehreren WaveNet-Netzwerken arbeiten, falsche Einträge stehen.

✓ WaveNet-Manager nicht geöffnet.

1. Navigieren Sie in das Verzeichnis des WaveNet-Managers.

	appcfg.xml	10.09.2019 12:56	XML-Dokument	1 KB
	boost_threadmon.dll	23.07.2002 19:15	Anwendungserwe...	24 KB
	msgcfg.xml	10.09.2019 12:56	XML-Dokument	1 KB
	netcfg.xml	10.09.2019 12:56	XML-Dokument	3 KB
	Readme.txt	08.03.2019 07:09	Textdokument	2 KB
	WaveNetManager.exe	07.03.2019 11:38	Anwendung	804 KB
	WNIPDiscoveryLib.dll	17.10.2014 09:21	Anwendungserwe...	32 KB
	WNM_Handbook.pdf	14.12.2016 16:02	Adobe Acrobat D...	1.571 KB
	WNM_move_node	08.08.2019 15:28	Datei	1 KB
	WNM_Ring_report	06.09.2019 10:57	Datei	1 KB
	WNM_RSSI_report	10.09.2019 12:57	Datei	1 KB
	WNMManager	10.09.2019 12:57	Datei	1 KB

2. Löschen Sie die Datei **netcfg.xml**.

➔ Sie können den WaveNet-Manager starten (siehe *Best Practice: Aus der LSM-Software* [► 40]).

6.5.5 Zurücksetzen/Löschen

Zurückgesetzte Geräte werden aus Ihrer WaveNet-Topologie gelöscht und nicht mehr in der Übersicht angezeigt.

Das Zurücksetzen des gesamten WaveNets besteht aus vier Teilen:

1. LockNodes zurücksetzen (siehe *LockNodes* [► 178])
2. RouterNodes zurücksetzen (siehe *RouterNodes* [► 180])
3. Kommunikationsknoten bearbeiten (siehe *WaveNet* [► 183])
4. Leere Segmente aus der LSM löschen, falls nicht durch Import der leeren Topologie geschehen (siehe *WaveNet* [► 183])

Generell sollten Sie Ihre Geräte im WaveNet-Manager zurücksetzen und anschließend die Topologie importieren. Somit kann der WaveNet-Manager der LSM mitteilen, welche Geräte tatsächlich im WaveNet vorhanden sind und Sie halten die Daten synchron.

Sie können LockNodes und RouterNodes aber auch unabhängig von den anderen Teilen zurücksetzen.

**HINWEIS****LockNodes nach Zurücksetzen nicht erreichbar**

Wenn Sie einen RouterNode zurücksetzen, dann können Sie dessen LockNodes danach nicht mehr erreichen.

- Setzen Sie mit dem RouterNode verbundene LockNodes vorher zurück (siehe *LockNodes* [► 161]).

Wenn Sie die LockNodes nicht mehr erreichen, dann können Sie die LockNodes auch mit einem Hardware-Reset zurücksetzen (Trennen und Wiederherstellen der Stromversorgung, siehe *LockNodes* [► 170]).

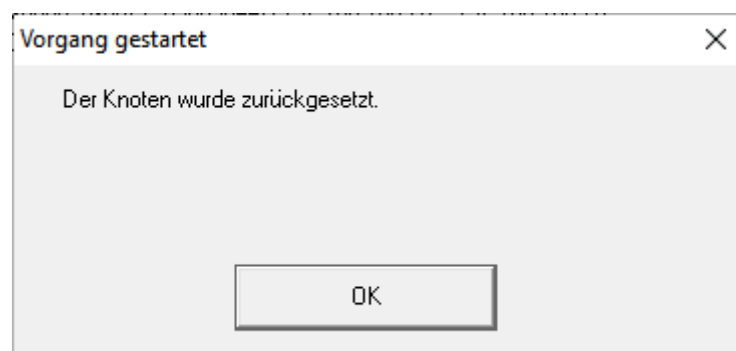
6.5.5.1 LockNodes

Best Practice: Reset mit WaveNet-Manager

- ✓ WaveNet-Manager über LSM geöffnet (siehe *Best Practice: Aus der LSM-Software* [► 40]).
 - ✓ LockNode mit WaveNet verbunden (siehe *LockNodes dem WaveNet hinzufügen* [► 64]).
1. Klicken Sie mit der rechten Maustaste auf den Eintrag des Locknodes, den Sie zurücksetzen wollen.
 - ➔ Fenster "Administration" öffnet sich.



2. Wählen Sie im Bereich "Konfiguration" die Option ☒ Zurücksetzen/Löschen.
3. Klicken Sie auf die Schaltfläche **OK**.
 - ↳ Fenster "Vorgang gestartet" öffnet sich.



4. Klicken Sie auf die Schaltfläche **OK**.
 - ↳ Fenster "Vorgang gestartet" schließt sich.
5. Klicken Sie auf die Schaltfläche **Speichern**.
 - ↳ LockNode ist zurückgesetzt und aus der WaveNet-Topologie gelöscht.

Hardware-Reset externer LockNodes

Sie können WaveNet-Manager-fähige LockNodes (erkennbar an WNM in der Artikelnummer) zurücksetzen:

1. Trennen Sie den LockNode von der Stromversorgung bzw. bauen Sie die Batterien aus.
2. Warten Sie ca. 20 Sekunden.
3. Drücken und halten Sie den Init-Taster.
4. Schließen Sie die Stromversorgung wieder an bzw. setzen Sie die Batterien wieder ein.
 - ↳ LED leuchtet konstant rot.
5. Lassen Sie den Init-Taster los, während die LED konstant rot leuchtet.
 - ↳ Alle WaveNet-Informationen im LockNode sind gelöscht.

Sie können den LockNode wieder in Ihr WaveNet einbinden (siehe WaveNet-Handbuch).

Die SmartIntego-Variante (SI.N.IO) kann nur im SmartIntego-Manager zurückgesetzt werden.

Hardware-Reset interner LockNodes

Interne LockNodes werden vollständig zurückgesetzt, wenn Sie den LockNode in eine Schließung einer anderen Schließanlage einbauen.

1. Bauen Sie den LockNode aus (siehe Handbuch/Kurzanleitung des LockNodes oder der Schließung).
2. Bauen Sie den LockNode in einer programmierten Schließung einer anderen Schließanlage wieder ein.
 - ↳ Schließung piept/blinkt viermal.
 - ↳ LockNode ist zurückgesetzt.

Sie können den LockNode danach wieder aus der Schließung der anderen Schließanlage ausbauen. Anschließend ist der LockNode wieder in Ihrem WaveNet einsetzbar.

6.5.5.2 RouterNodes



HINWEIS

LockNodes nach Zurücksetzen nicht erreichbar

Wenn Sie einen RouterNode zurücksetzen, dann können Sie dessen LockNodes danach nicht mehr erreichen.

- Setzen Sie mit dem RouterNode verbundene LockNodes vorher zurück (siehe *LockNodes* [▶ 161]).

Zurückgesetzte RouterNodes haben die Funk-Standardkonfiguration:

Netzwerk-ID	DDDD Diese ID wird bei Inbetriebnahme immer geändert. Stellen Sie diese ID deshalb nicht im WaveNet-Manager oder in der LSM ein.
Funkkanal	Kanal 0 (868,1 MHz)

Best Practice: RouterNodes im WaveNet-Manager zurücksetzen



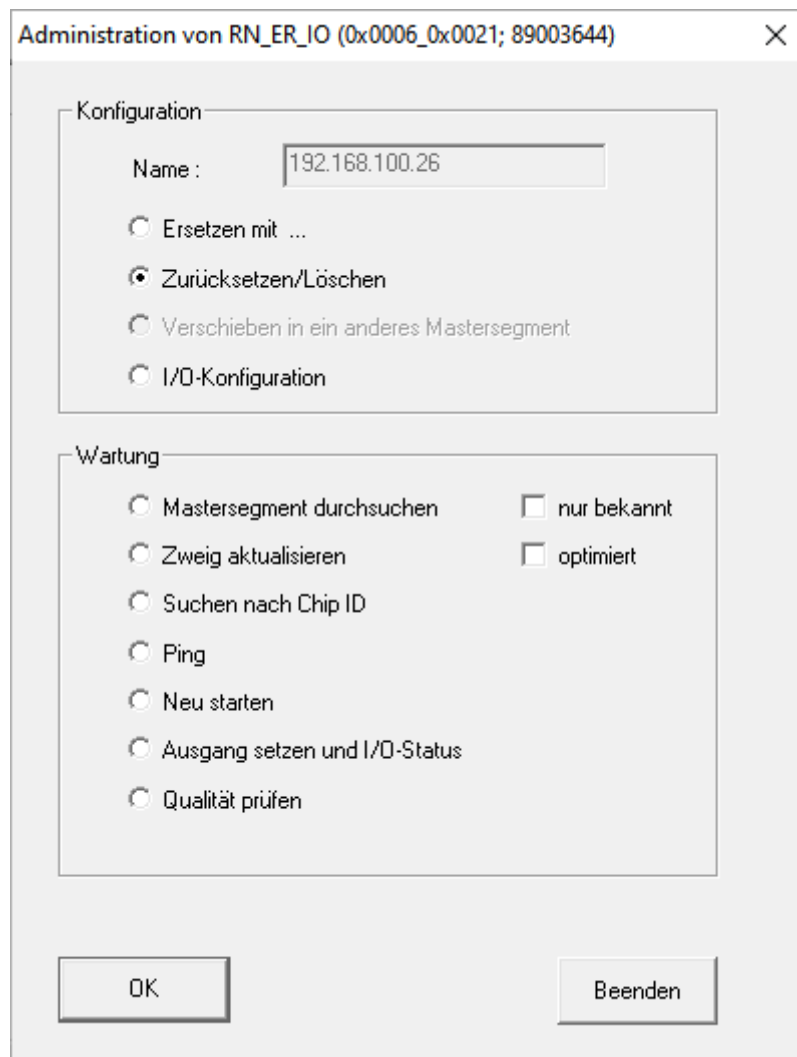
HINWEIS

Zurücksetzen gesperrt

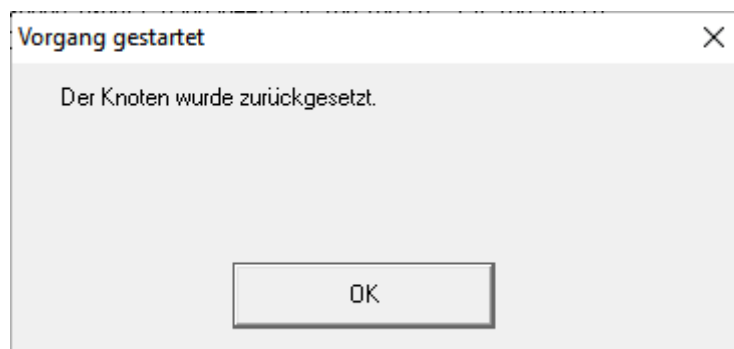
LockNodes, die dem RouterNode zugewiesen sind, sind nach dem Zurücksetzen des RouterNodes nicht mehr erreichbar. Deshalb ist die Option  Zurücksetzen/Löschen gesperrt, wenn noch LockNodes dem RouterNode zugewiesen sind.

- Setzen Sie zuerst alle LockNodes zurück, die dem RouterNode zugewiesen sind (siehe *LockNodes* [► 178]) bzw. löschen Sie sie.

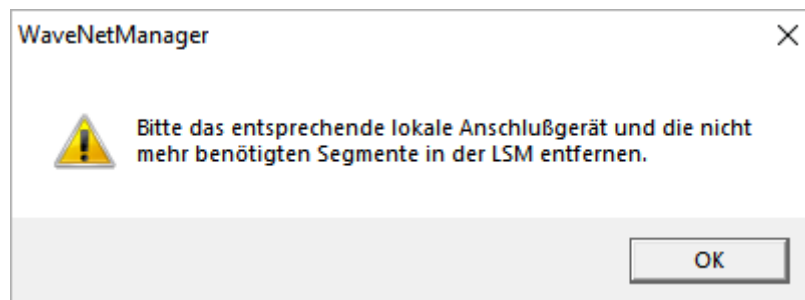
- ✓ WaveNet-Manager über LSM geöffnet (siehe *Best Practice: Aus der LSM-Software* [► 40]).
 - ✓ RouterNode mit WaveNet verbunden (siehe *RouterNode dem WaveNet hinzufügen* [► 57]).
1. Klicken Sie mit der rechten Maustaste auf den Eintrag des RouterNodes, den Sie zurücksetzen wollen.
 - ↳ Fenster "Administration" öffnet sich.



2. Wählen Sie im Bereich "Konfiguration" die Option ☒ Zurücksetzen/Löschen.
3. Klicken Sie auf die Schaltfläche **OK**.
 - ↳ Fenster "Vorgang gestartet" öffnet sich.



4. Klicken Sie auf die Schaltfläche **OK**.
 - ↳ Fenster "Vorgang gestartet" schließt sich.
 - ↳ Fenster "WaveNetManager" öffnet sich.



5. Klicken Sie auf die Schaltfläche **OK**.
 - ↳ Fenster "WaveNetManager" schließt sich.
6. Klicken Sie auf die Schaltfläche **Speichern**.
 - ↳ RouterNode ist zurückgesetzt und aus der WaveNet-Topologie gelöscht.

Ethernet-RouterNodes über die Browserschnittstelle zurücksetzen

✓ Browserschnittstelle geöffnet (siehe *Browserschnittstelle* [▶ 157]).

1. Öffnen Sie über | ADMINISTRATION | die Registerkarte [WERKSEINSTELLUNG].
 - ↳ Sie sehen das Wiederherstellungsmenü.

PASSWORT
ZERTIFIKATE
WERKSEINSTELLUNG
NEUSTART

Administration: Werkseinstellung wiederherstellen

Wiederherstellen

Information: Das Gerät ist nach der Wiederherstellung und einem Neustart evtl. nicht mehr erreichbar.

2. Klicken Sie auf die Schaltfläche **Wiederherstellen**.
 - ↳ Wiederherstellung wird durchgeführt.
 - ↳ Ethernet-RouterNode ist auf Werkseinstellung zurückgesetzt.

RouterNodes über die Hardware zurücksetzen

Alle RouterNodes unterstützen einen Hardware-Reset. Sie können diese RouterNodes mit dem Reset-Taster auf der Platine zurücksetzen. Weitere Informationen entnehmen Sie bitte dem Handbuch bzw. der Kurzanleitung des jeweiligen RouterNodes.

6.5.5.3 WaveNet

Der Import der WaveNet-Topologie entfernt zurückgesetzte LockNodes auch aus der LSM.

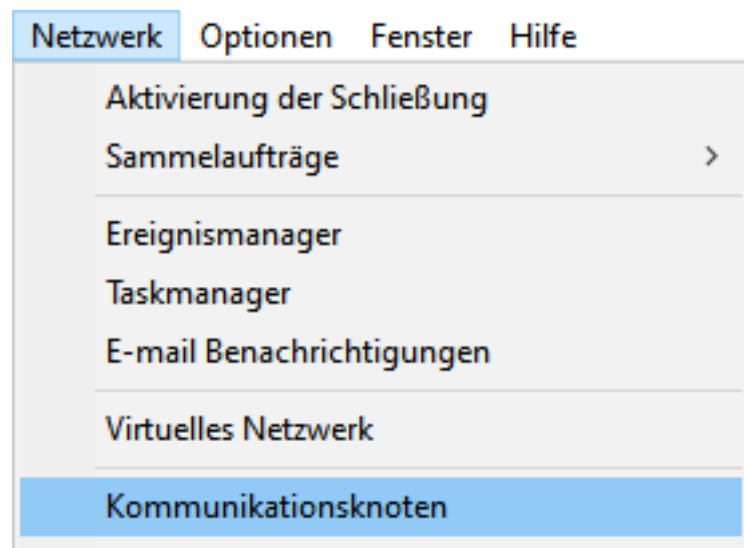
Die Segmente von RouterNodes und CentralNodes/RouterNodes mit Ethernet-Anschluss bleiben bestehen. Sie müssen diese nachträglich entfernen:

1. RouterNodes aus Kommunikationsknoten bzw. lokale Anschlüssen entfernen
2. Segmente entfernen

Kommunikationsknoten bearbeiten

Gehen Sie für lokale Anschlüsse analog vor (wenn Sie keinen CommNode-Server verwenden).

- ✓ RouterNodes und LockNodes im WaveNet-Manager zurückgesetzt (siehe *Best Practice: Reset mit WaveNet-Manager* [► 178] und *Best Practice: RouterNodes im WaveNet-Manager zurücksetzen* [► 181]).
 - ✓ WaveNet-Topologie importiert.
 - ✓ LSM geöffnet.
1. Wählen Sie über | Netzwerk | den Eintrag **Kommunikationsknoten**.



- ↳ Kommunikationsknoten-Übersicht öffnet sich.
2. Wählen Sie ggfs. mit den Schaltflächen ,  und  den für das WaveNet verwendeten Kommunikationsknoten aus.
- ↳ Sie sehen in der Übersicht die nicht gelöschten Einträge Ihrer RouterNodes.

Anschlüsse:

Typ	COM-Port	
IP-Schließung	192.168.100.22	
WN over TCP Central Node	192.168.100.26	
WN over TCP Central Node	192.168.100.29	

Buttons: Ping, Konfig-Dateien, Übertragen, Testen, Bearbeiten, Hinzufügen, Entfernen, Verschieben, Neu, Bearbeiten, Übernehmen, Beenden, Hilfe

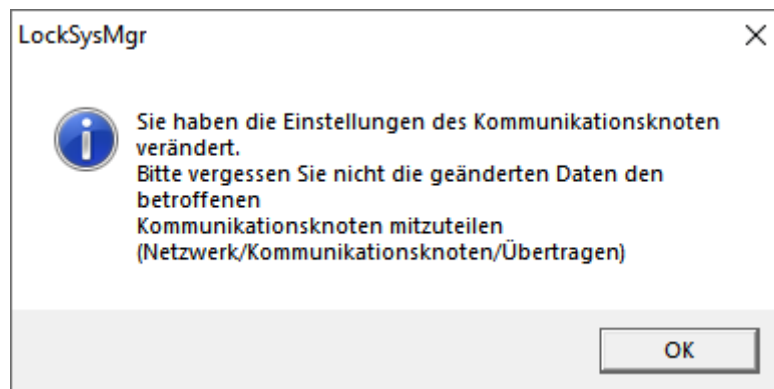
3. Markieren Sie Ihre RouterNodes.
4. Klicken Sie auf die Schaltfläche **Entfernen**.
↳ RouterNodes sind aus Liste entfernt.

Anschlüsse:

Typ	COM-Port	
IP-Schließung	192.168.100.22	

Buttons: Ping, Konfig-Dateien, Übertragen, Testen, Bearbeiten, Hinzufügen, Entfernen, Verschieben, Neu, Bearbeiten, Übernehmen, Beenden, Hilfe

5. Klicken Sie auf die Schaltfläche **Übernehmen**.
↳ Fenster "LockSysMgr" öffnet sich.

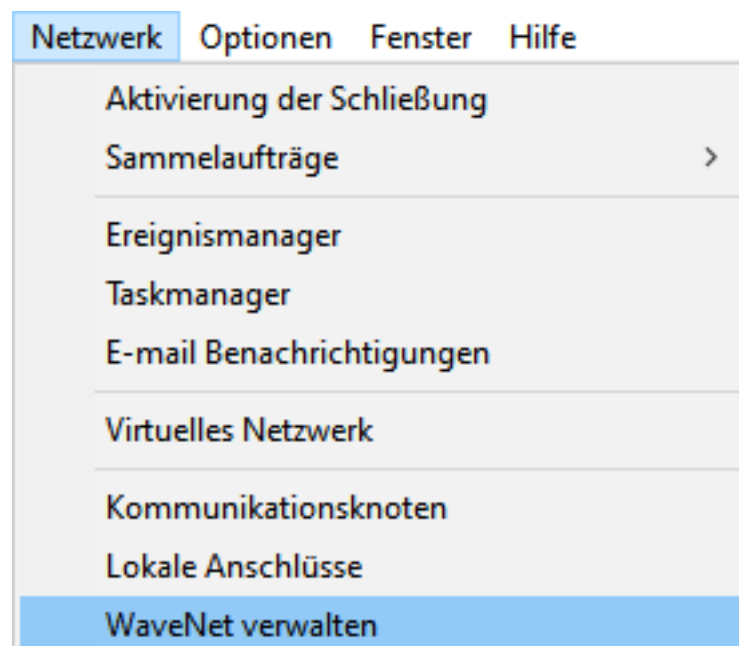


6. Klicken Sie auf die Schaltfläche **OK**.
 - ↳ Fenster "LockSysMgr" schließt sich.
7. Klicken Sie auf die Schaltfläche **Konfig-Dateien**.
8. Klicken Sie auf die Schaltfläche **OK**.
 - ↳ Rückfrage zum knotenspezifischen Speicherort öffnet sich.
9. Klicken Sie auf die Schaltfläche **Nein**.
 - ↳ Rückfrage zum knotenspezifischen Speicherort schließt sich.
 - ↳ Bestätigungsmeldung öffnet sich.
10. Klicken Sie auf die Schaltfläche **OK**.
 - ↳ Bestätigungsmeldung schließt sich.
11. Klicken Sie auf die Schaltfläche **Übertragen**.
 - ↳ Daten werden zum Kommunikationsknoten übertragen.
 - ↳ Bestätigungsmeldung öffnet sich.
12. Klicken Sie auf die Schaltfläche **OK**.
 - ↳ Bestätigungsmeldung schließt sich.

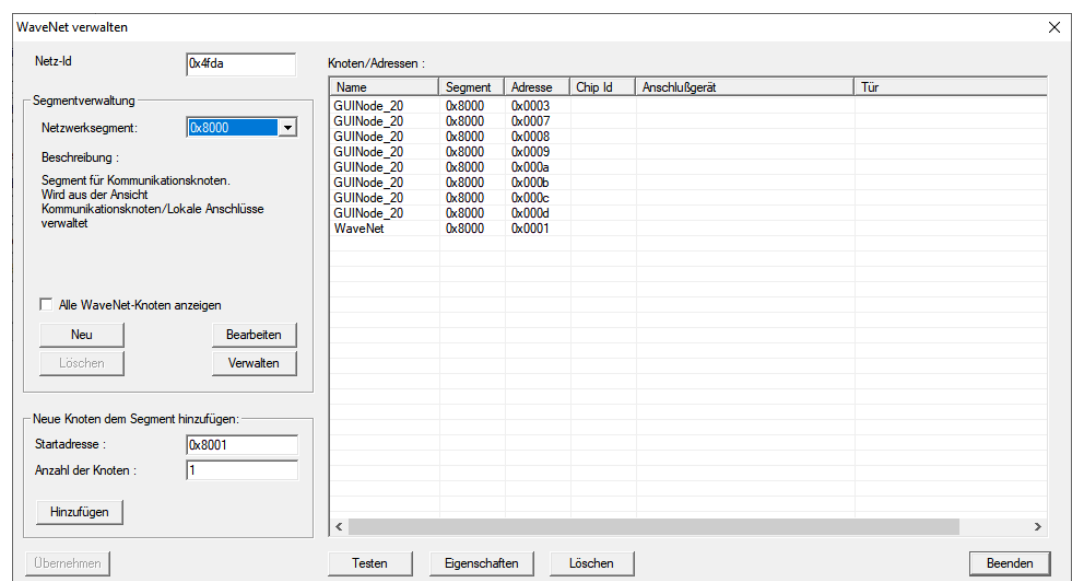
Segmente entfernen

- ✓ RouterNodes und LockNodes im WaveNet-Manager zurückgesetzt (siehe *Best Practice: Reset mit WaveNet-Manager* [► 178] und *Best Practice: RouterNodes im WaveNet-Manager zurücksetzen* [► 181]).
- ✓ WaveNet-Topologie importiert.
- ✓ RouterNodes aus Kommunikationsknoten bzw. aus lokalen Anschlüssen entfernt.
- ✓ LSM geöffnet.

1. Wählen Sie über | Netzwerk | den Eintrag **WaveNet verwalten**.



→ Fenster "WaveNet verwalten" öffnet sich.



2. Wählen Sie im Dropdown-Menü ▼ **Netzwerksegment** Ihr Netzwerksegment aus.
Sie erkennen das Segment daran, dass in der Tabelle keine Einträge mehr vorhanden sind.

3. Klicken Sie im Bereich "Segmentverwaltung" auf die Schaltfläche **Löschen**.
→ Fenster "LockSysMgr" öffnet sich.

4. Klicken Sie auf die Schaltfläche **OK**.
→ Fenster "LockSysMgr" schließt sich.
5. Klicken Sie auf die Schaltfläche **Übernehmen**.
→ Segment ist gelöscht.

6.5.6 Virtual Store überprüfen und beheben

Wenn Sie den WaveNet-Manager nicht mit Administratorrechten starten und zusätzlich mit wechselnden Windows-Benutzerkonten arbeiten, dann kann es vorkommen, dass die angezeigte WaveNet-Topologie veraltet ist.

Falls dieses Problem auftritt, dann wurden die erzeugten Netzwerkdaten des WaveNet-Managers nicht in dem beim Start angegebenen Ordner gespeichert. Änderungen in geschützten Ordnern (wie dem Windows-

Programmordner) benötigen Administratorrechte. Wenn der WaveNet-Manager keine Administratorrechte hat und im geschützten Programmordner speichern will, dann leitet Windows die erzeugten Daten in den Virtual Store um.

Wenn der WaveNet-Manager immer vom gleichen Windows-Benutzerkonto und (fälschlicherweise) über die LSM nicht als Administrator gestartet wird und auf die Netzwerkdaten zugreift, dann fängt Windows den Zugriff ab und leitet ihn auf die Datei im Virtual Store um. In dem Moment, in dem der WaveNet-Manager aber von einem anderen Windows-Benutzerkonto oder (korrekterweise) über die LSM als Administrator gestartet wird funktioniert diese Umleitung nicht mehr. Der WaveNet-Manager greift auf die veralteten Netzwerkdaten in dem angegebenen Ordner (also an dem Ort, an dem sie normalerweise auch gespeichert werden würden) zu und zeigt deshalb eine veraltete WaveNet-Topologie an.

1. Öffnen Sie folgenden Dateipfad: **C:\Users\Benutzername\AppData\Local\SimonsVoss**.
2. Suchen Sie nach dem Ordner WaveNetManager.
3. Öffnen Sie folgenden Dateipfad: **C:\Users\Benutzername\AppData\Local\VirtualStore\Program Files (x86)\SimonsVoss**.
4. Suchen Sie nach dem Ordner WaveNetManager.

Wenn Sie in den geprüften Verzeichnissen den Ordner WaveNetManager finden, dann wurde die Ausgabe der Netzwerkdaten mindestens einmal umgeleitet.

1. Fertigen Sie eine Backup-Kopie des aktuellen Speicherorts (angezeigt während des Starts, siehe [Start \[► 40\]](#)) des WaveNet-Managers an.
2. Verschieben Sie die Netzwerkdaten aus den geprüften Dateipfaden an den im WaveNet-Manager eingestellten Speicherort.
3. Starten Sie die LSM als Administrator.
4. Starten Sie aus der LSM den WaveNet-Manager.
5. Ändern Sie den Ausgabepfad auf einen Ort mit freien Schreibrechten.

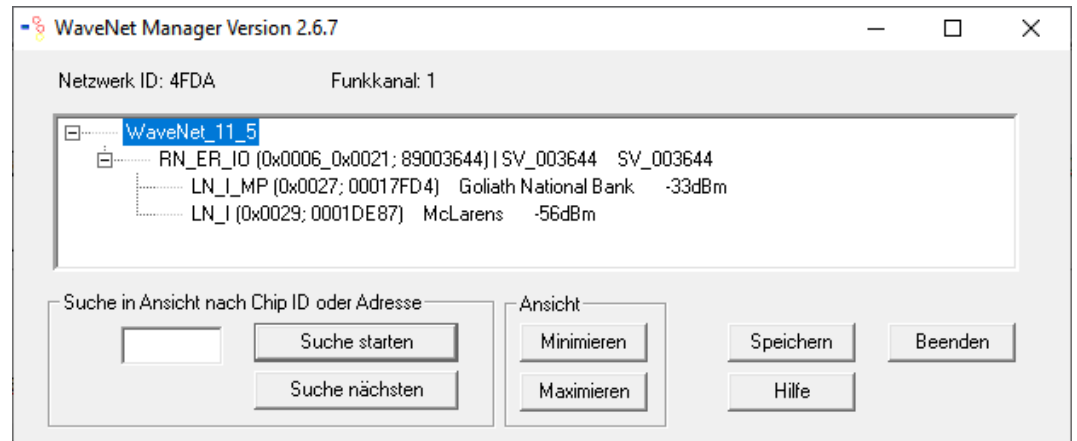
Beachten Sie zur Vermeidung dieses Fehlers auch die Hinweise zu den Verzeichnissen, siehe [Entpacken \[► 38\]](#).

6.6 Wartung

- Informationen zur Wartung eines RingCasts siehe [RingCast-Funktionstest \[► 151\]](#).
- Informationen zum Batteriezustand oder zum Batteriewechsel siehe [Batteriemanagement \[► 205\]](#).

6.6.1 Übersicht

Sie sehen die Topologie Ihres WaveNets im WaveNet-Manager auf der Startseite.



Die Übersicht stellt folgende Informationen bereit:

RouterNode

- RouterNode-Typ (z.B. RN_ER_IO)
- Eingangsadresse (z.B. 0x0006)
- Chip-ID (z.B. 89003644)
- Hostname (Wenn Sie keine Hostnamen verwenden, wird anstelle des Hostnamens die IP-Adresse angezeigt).
- RSSI-Wert (sofern nur Radio-Schnittstelle. Im Beispiel nicht verwendet)

LockNode

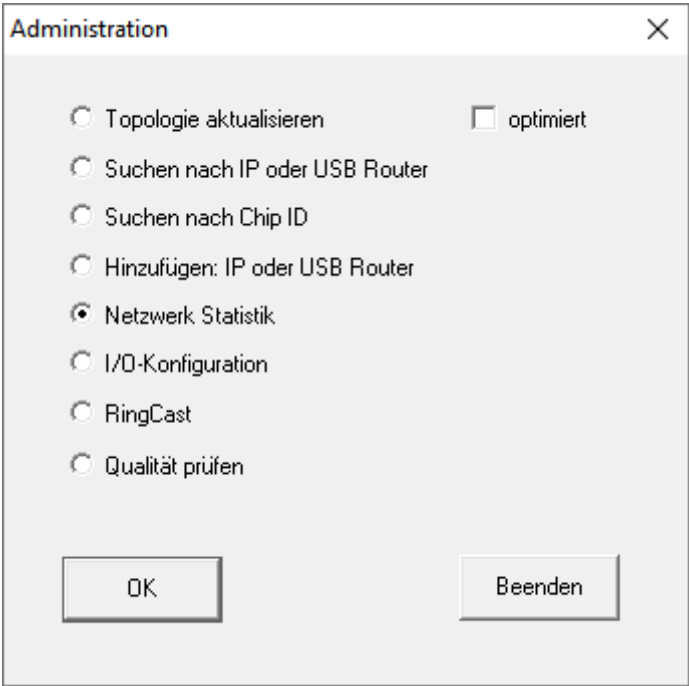
- LockNode-Typ (z.B. LN_I)
- Adresse (z.B. 0x0027)
- Chip-ID (z.B. 00017023)
- Name der verknüpften Schließung
- RSSI-Wert (z.B. -33 dBm)

Sie können mit der angezeigten Adresse die Segmente bestimmen (siehe [Adressierung \[▶ 45\]](#)).

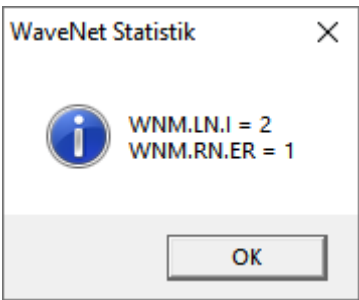
Anzahl der Gerätetypen

Der WaveNet-Manager bietet Ihnen eine Möglichkeit, die Anzahl der verschiedenen Gerätetypen anzuzeigen.

- ✓ WaveNet-Manager über LSM geöffnet (siehe *Best Practice: Aus der LSM-Software* [▶ 40]).
- 1. Klicken Sie mit der rechten Maustaste auf den Eintrag WaveNet_XX_X.
 - ↳ Fenster "Administration" öffnet sich.



2. Wählen Sie die Option **Netzwerk Statistik**.
3. Klicken Sie auf die Schaltfläche **OK**.
 - ↳ Fenster "Administration" schließt sich.
 - ↳ Fenster "WaveNet Statistik" öffnet sich. Sie sehen eine Aufzählung der Gerätetypen mit der Anzahl.



Speicherstatus

Sie erkennen in der Übersicht auch den Speicherzustand der Geräte.

Fett	Eintrag im WaveNet geändert, aber noch nicht gespeichert. Klicken Sie auf die Schaltfläche Speichern
Normal	Eintrag im WaveNet gespeichert

Konfigurationsstatus

Sie erkennen Probleme an der Konfiguration von RouterNodes oder LockNodes an einem schwarzen Blitz vor dem jeweiligen Eintrag. Wiederholen Sie die Konfiguration, indem Sie das Gerät neu programmieren (siehe [Gerät neu programmieren oder ersetzen](#) [► 172]).

6.6.2 Signalqualität prüfen

ACHTUNG

Empfohlene Signalstärke

Die Signalstärke im WaveNet-Manager sollte zwischen 0 dBm und -70 dBm liegen.

Wenn die Signalstärke nicht ausreicht, dann kann die Verbindung und Kommunikation zwischen den Geräten langsam oder unterbrochen werden und es kommt zudem zu einem höheren Stromverbrauch.

- Wenn die Signalstärke zwischen -75 dBm und -90 dBm liegt, kann es zu eingeschränkter Funktion kommen. Verbessern Sie die Signalqualität (siehe [Signalqualität verbessern](#) [► 161]).

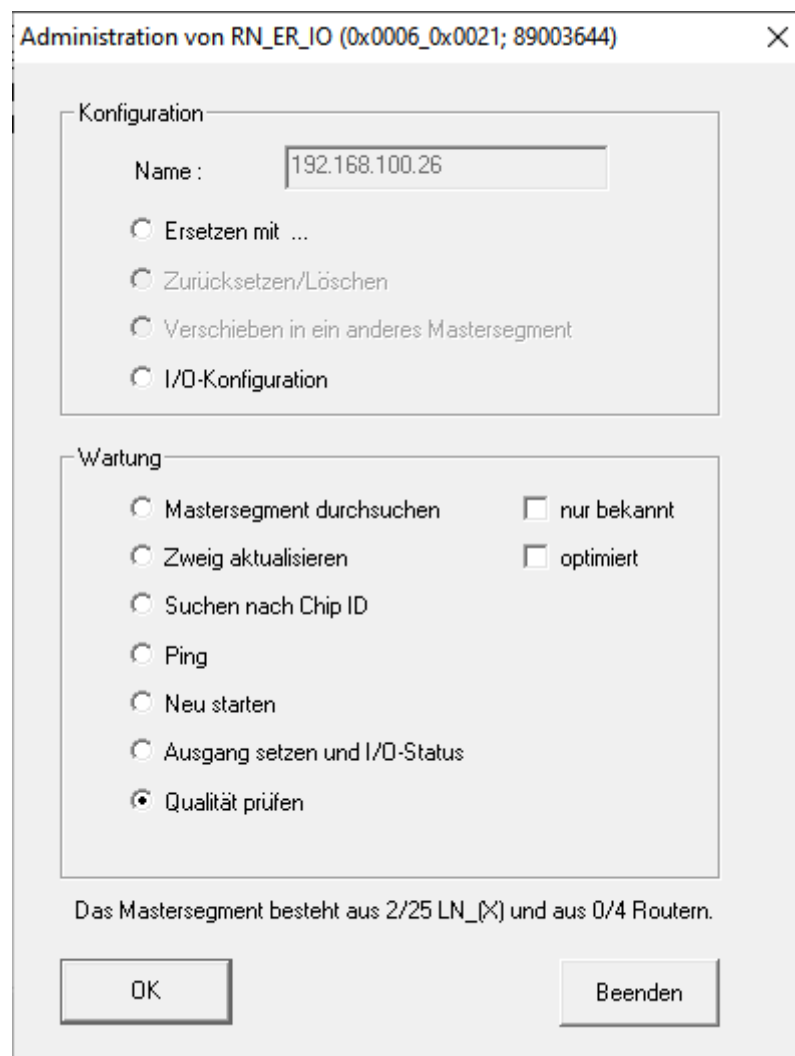
Einheit der Signalstärke

Der WaveNet-Manager gibt die Signalstärke als RSSI-Wert (Received Signal Strength) in dBm an. Dieser Wert ist:

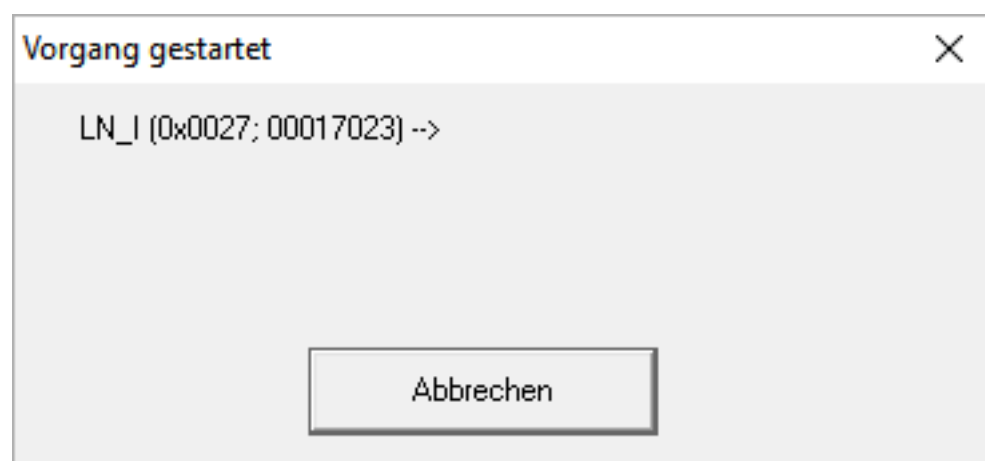
- Logarithmisch: Eine Verbesserung um 10 dBm bedeutet in der Praxis die doppelte Signalstärke.
- Negativ: Der theoretische Bestwert beträgt 0 dBm und wird nur durch Kabelverbindungen erreicht. Je näher der Wert an 0 dBm ist (je kleiner also der Betrag ist), desto besser ist der Empfang.

Einzelner RouterNode

- ✓ WaveNet-Manager über LSM geöffnet (siehe [Best Practice: Aus der LSM-Software](#) [► 40]).
 - ✓ RouterNodes und LockNodes mit WaveNet verbunden (siehe [Geräte finden und hinzufügen](#) [► 52]).
1. Klicken Sie mit der rechten Maustaste auf den Eintrag des RouterNodes, dessen Signalqualität zu seinen LockNodes Sie prüfen wollen.
 - ↳ Fenster "Administration" öffnet sich.



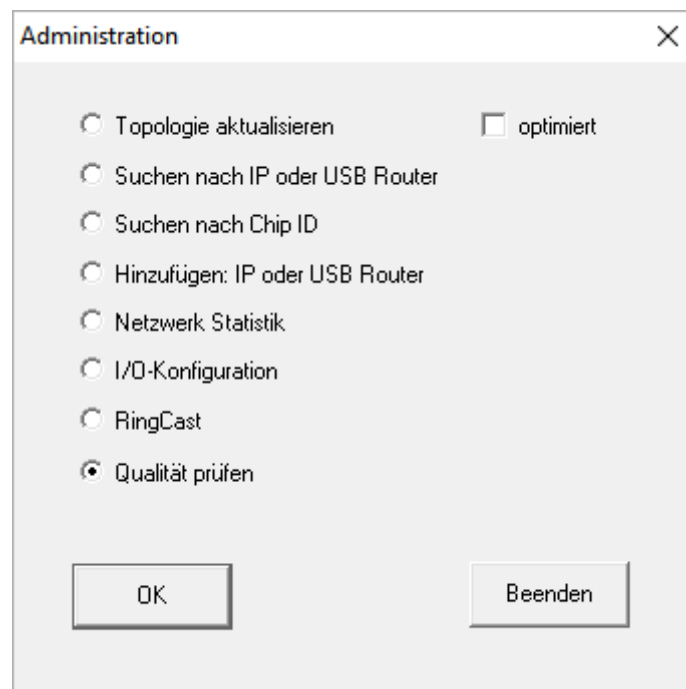
2. Wählen Sie die Option ☒ Qualität prüfen.
3. Klicken Sie auf die Schaltfläche **OK**.
 - ↳ Fenster "Administration" schließt sich.
 - ↳ Fenster "Vorgang gestartet" öffnet sich vorübergehend.



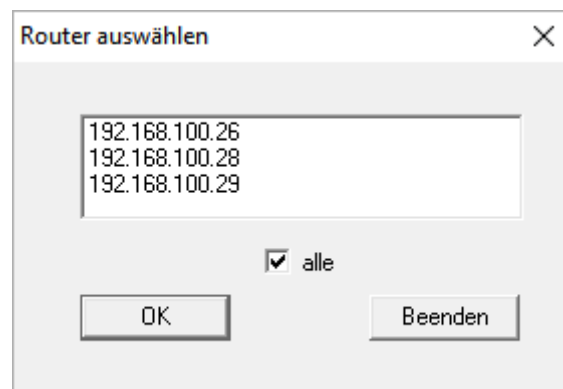
- ↳ RSSI-Werte in der Übersicht sind für den entsprechenden RouterNode aktualisiert.

Mehrere RouterNodes

- ✓ WaveNet-Manager geöffnet.
- ✓ RouterNodes und LockNodes mit WaveNet verbunden.
- 1. Klicken Sie mit der rechten Maustaste auf den Eintrag WaveNet_XX_X.
 - ↳ Fenster "Administration" öffnet sich.

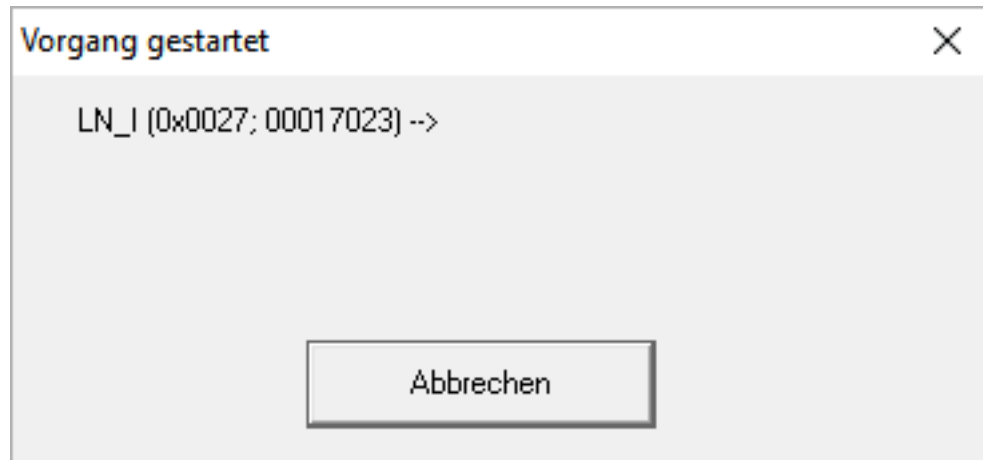


2. Wählen Sie die Option ☒ Qualität prüfen.
3. Klicken Sie auf die Schaltfläche **OK**.
 - ↳ Fenster "Administration" schließt sich.
 - ↳ Fenster "Router auswählen" öffnet sich. Sie sehen eine Liste der RouterNodes in Ihrem WaveNet.



4. Markieren Sie entweder alle gewünschten RouterNodes oder aktivieren Sie die Checkbox ☒ alle.
5. Klicken Sie auf die Schaltfläche **OK**.
 - ↳ Fenster "Router auswählen" schließt sich.

↳ Fenster "Vorgang gestartet" öffnet sich vorübergehend.



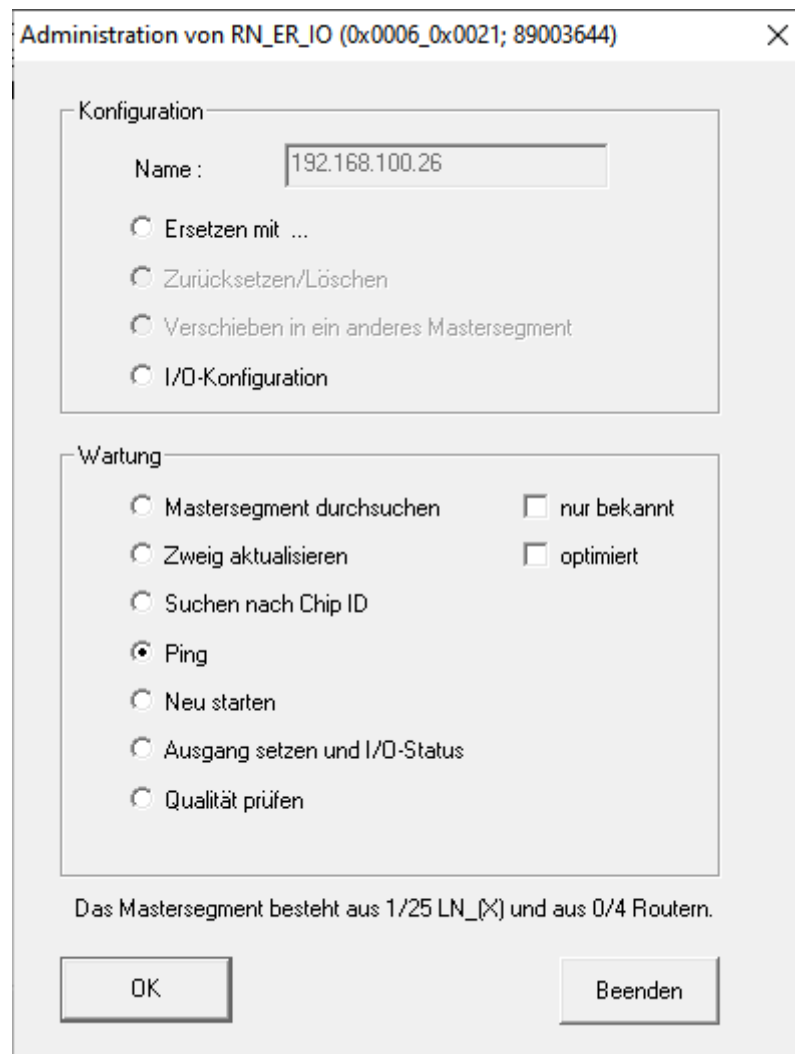
↳ RSSI-Werte in der Übersicht sind für die entsprechenden RouterNodes aktualisiert.

6.6.3 Erreichbarkeit testen (WaveNet)

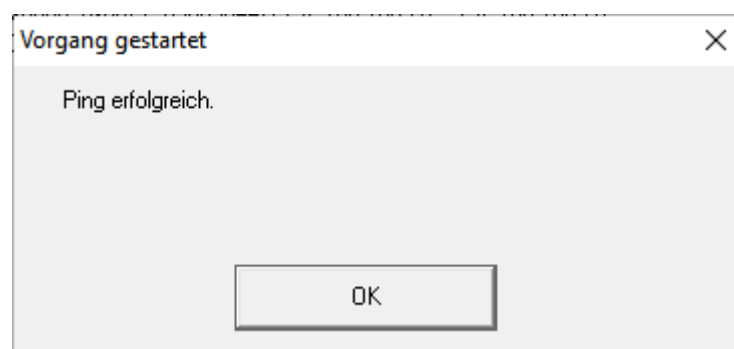
Sie können mit dem WaveNet-Manager testen, ob der WaveNet-Manager Ihre RouterNodes und LockNodes erreicht.

6.6.3.1 RouterNodes

- ✓ WaveNet-Manager über LSM geöffnet (siehe *Best Practice: Aus der LSM-Software* [▶ 40]).
 - ✓ RouterNode mit WaveNet verbunden (siehe *RouterNode dem WaveNet hinzufügen* [▶ 57]).
1. Klicken Sie mit der rechten Maustaste auf den Eintrag des RouterNodes, dessen Erreichbarkeit Sie testen wollen.
 - ↳ Fenster "Administration" öffnet sich.



2. Wählen Sie im Bereich "Wartung" die Option ☒ Ping.
3. Klicken Sie auf die Schaltfläche **OK**.
 - ↳ Fenster "Administration" schließt sich.
 - ↳ Fenster "Vorgang gestartet" öffnet sich.



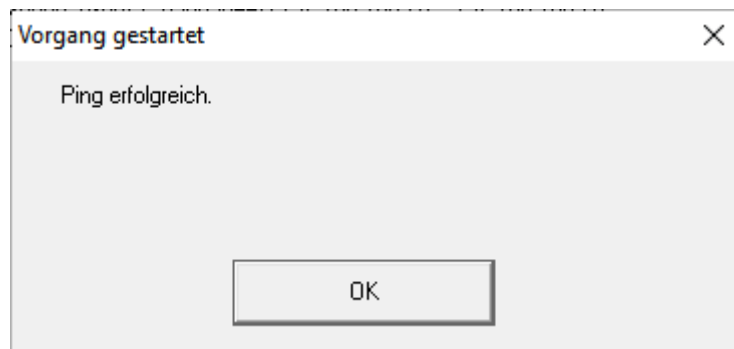
4. Klicken Sie auf die Schaltfläche **OK**.
 - ↳ Fenster "Vorgang gestartet" schließt sich.
 - ↳ WaveNet-Manager erreicht RouterNode.

6.6.3.2 LockNodes

- ✓ WaveNet-Manager über LSM geöffnet (siehe *Best Practice: Aus der LSM-Software* [▶ 40]).
 - ✓ LockNode mit WaveNet verbunden (siehe *LockNodes dem WaveNet hinzufügen* [▶ 64]).
1. Klicken Sie mit der rechten Maustaste auf den Eintrag des LockNodes, dessen Erreichbarkeit Sie testen wollen.
 - ↳ Fenster "Administration" öffnet sich.



2. Wählen Sie im Bereich "Wartung" die Option ☒ Ping.
3. Klicken Sie auf die Schaltfläche **OK**.
 - ↳ Fenster "Administration" schließt sich.
 - ↳ Fenster "Vorgang gestartet" öffnet sich.



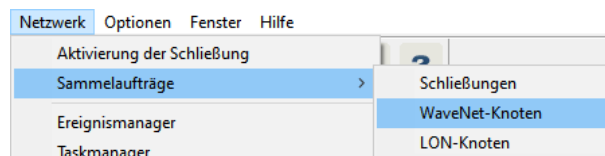
4. Klicken Sie auf die Schaltfläche **OK**.
 - ↳ Fenster "Vorgang gestartet" schließt sich.
 - ↳ WaveNet-Manager erreicht LockNode.

6.6.4 Erreichbarkeit testen (LSM)

Sie können mit der LSM testen, ob der Netzwerkknoten einer WaveNet-Schließung ordnungsgemäß funktioniert und für die LSM erreichbar ist.

- ✓ LSM geöffnet.
- ✓ WaveNet angelegt.
- ✓ WaveNet-Topologie importiert (siehe *LSM-Import* [▶ 69]).

1. Öffnen Sie die Zuweisung über | Netzwerk | - **Sammelaufträge** - **WaveNet-Knoten**.



- ↳ Fenster "Sammelauftrag für WaveNetknoten" öffnet sich.

**WARNUNG****Veränderung des Ablaufs von Notfallfunktionen durch Fehlfunktionen**

SimonsVoss und "Made in Germany" stehen für höchste Sicherheit und Zuverlässigkeit. In Einzelfällen können Fehlfunktionen Ihrer Geräte dennoch nicht ausgeschlossen werden. Damit wird möglicherweise die Sicherheit von Personen und Sachwerten, die durch die Schutzfunktionen im RingCast zusätzlich abgesichert werden, gefährdet.

1. Testen Sie Ihre Geräte mindestens einmal pro Monat (siehe *Geräte-Funktionstest* [▶ 199]. Nach anderen Vorschriften bezüglich Ihres Gesamtsystems können auch kürzere Abstände erforderlich sein).
2. Testen Sie die Schutzfunktionen mindestens einmal pro Monat (siehe *RingCast-Funktionstest* [▶ 151]).

Schließungen und Identifikationsmedien

1. Betätigen Sie die Schließung.
 - ↳ Schließung ist freilaufend.
2. Betätigen Sie ein berechtigtes Identifikationsmedium.
 - ↳ Schließung signalisiert berechtigten Zutritt (Oder Batteriewarnung, dann Batterien wechseln).
 - ↳ Schließung öffnet, wenn der Batteriezustand gut ist.
3. Warten Sie, bis die Schließung auskuppelt.
 - ↳ Schließung signalisiert Auskuppeln (Oder nichts, wenn die Batterie schwach ist).
4. Betätigen Sie ein unberechtigtes Identifikationsmedium.
 - ↳ Schließung signalisiert fehlende Berechtigung (Oder Batteriewarnung, dann Batterien wechseln).
5. Prüfen Sie den Batteriezustand (siehe *Batteriemanagement* [▶ 205]).

WaveNet-Geräte

1. Prüfen Sie die Signalqualität (siehe *Signalqualität prüfen* [▶ 192]).
2. Prüfen Sie die Erreichbarkeit (siehe *Erreichbarkeit testen (LSM)* [▶ 198] und *Erreichbarkeit testen (WaveNet)* [▶ 195]).
3. Prüfen Sie den Batteriezustand (siehe *Batteriemanagement* [▶ 205]).

6.6.6 IO-Status und LockNode-Reaktionsfähigkeit

Sie können Folgendes prüfen:

- Signal am jeweiligen Eingang
- Ergebnisse des letzten Broadcasts für jedes Gerät
- Status der Ausgänge

- Anliegende analoge Spannung

Zusätzlich können Sie die Ausgänge auch manuell schalten.



HINWEIS

Manuelles Schalten gesperrt

Sie können den Ausgang abhängig von Identifikationsmedien oder abgeschlossenen Reaktionen schalten (siehe *I/O-Konfiguration und Schutzfunktionen* [► 74]). Ausgänge, die durch die IO-Konfiguration gesteuert werden, können nicht manuell geschaltet werden.

- ✓ WaveNet-Manager über LSM geöffnet (siehe *Best Practice: Aus der LSM-Software* [► 40]).
 - ✓ RouterNode mit Strom versorgt.
 - ✓ RouterNode mit WaveNet verbunden (siehe *RouterNode dem WaveNet hinzufügen* [► 57]).
1. Klicken Sie mit der rechten Maustaste auf den Eintrag des RouterNodes, dessen IO-Status Sie auslesen wollen.
 - ➞ Fenster "Administration" öffnet sich.

Administration von RN_ER_IO (0x000A_0x0021; 89003644)

Konfiguration

Name : 192.168.100.26

☐ Ersetzen mit ...

☐ Zurücksetzen/Löschen

☐ Verschieben in ein anderes Mastersegment

☐ I/O-Konfiguration

Wartung

☐ Mastersegment durchsuchen ☐ nur bekannt

☐ Zweig aktualisieren ☐ optimiert

☐ Suchen nach Chip ID

☐ Ping

☐ Neu starten

☒ Ausgang setzen und I/O-Status

☐ Qualität prüfen

Das Mastersegment besteht aus 2/25 LN_(X) und aus 0/4 Routern.

OK Beenden

2. Wählen Sie im Bereich "Wartung" die Option ☒ Ausgang setzen und I/O-Status.
 - ↳ Fenster "Administration" schließt sich.
 - ↳ Fenster "I/O Status" öffnet sich.

I/O Status für RN_ER_IO (0x0006_0x0021; 89003644)

Status der Eingänge:

Eingang 1: An

Eingang 2: Aus

Eingang 3: Aus

Ergebnis vom letzten Broadcast :

Fehler

Keine Antwort

Erfolgreich

Knoten

0x29 (0xD)

Knoten

Knoten

0x27

Status bzw. Setzen der Ausgänge :

☐ Ausgang 1

☐ Ausgang 2

☐ Ausgang 3

Analogwert [mV]: 0

Setzen

Schließen

Status der Eingänge

Im Bereich "Status der Eingänge" sehen Sie den Status der Eingänge (gültig für RN und RN2):

Status der Eingänge	Bedeutung
Aus	Am Eingang liegt kein Signal an. Die anliegende Spannung ist niedriger als die Vergleichsspannung.
An	Am Eingang liegt ein Signal an. Die anliegende Spannung ist höher als die Vergleichsspannung.

Vergleichsspannungen (RN und RN2)	
$<0,9 V_{DC}$	LOW (kein Signal)
$>2,1 V_{DC}$	HIGH (Signal)

Status/Reaktionsfähigkeit der LockNodes

Im Bereich "Status der Eingänge" sehen Sie außerdem das Verhalten der LockNodes beim letzten Broadcast:

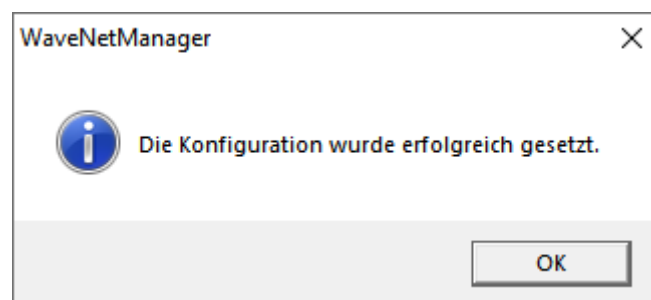
Fehler	Keine Antwort	Erfolgreich
Verarbeitung des Befehls im LockNode der Schließung fehlerhaft.	Hier gibt es zwei Möglichkeiten: ■ Schließung mit LockNode hat Befehl nicht empfangen und deshalb nicht geantwortet. ■ Schließung mit LockNode hat Befehl empfangen, RouterNode aber die Antwort nicht empfangen.	Die Schließung mit dem LockNode hat den Befehl empfangen und der RouterNode die Antwort empfangen.

Status der Ausgänge

Im Bereich "Status bzw. Setzen der Ausgänge" sehen Sie den Status der Ausgänge und können Ausgänge manuell schalten.

Status der Eingänge	Bedeutung
☒ Ausgang	Ausgang ist geschaltet.
☐ Ausgang	Ausgang ist nicht geschaltet.

1. Aktivieren Sie die Checkbox ☒ Ausgang des Ausgangs, den Sie schalten wollen bzw. deaktivieren Sie die Checkbox ☐ Ausgang, den Sie nicht mehr schalten wollen.
2. Klicken Sie auf die Schaltfläche **Setzen**.
 - ↳ Fenster "I/O Status" schließt sich.
 - ↳ Fenster "WaveNetManager" öffnet sich.



- ↳ Ausgang geschaltet.

7. Batteriemanagement

7.1 LockNodes

Sie erkennen ein Kommunikationsproblem (fehlgeschlagener Verbindungsversuch) an einem roten W in der LSM (siehe *Überwachung der Geräte im Netzwerk* [► 30]). Wenn das Kommunikationsproblem auch nach wiederholten Verbindungsversuchen besteht, dann kann dies eine Reihe von Ursachen haben:

- Funkschatten durch geöffnete Tür
- Routingproblem zwischen CommNode-Server und RouterNode
- Kommunikationsproblem zwischen CommNode-Server und RouterNode, z.B. durch blockierten Port 2101
- (Teilweiser) Netzerkausfall, z.B. durch defekte Switches
- Temporär ausgesetzte IP-Vergabe, z.B. durch Wartungsarbeiten im Netzwerk
- Schwache Batterien

Den Batteriezustand können Sie einfach selbst prüfen.

Signalisierung

Die Signalisierung des Batteriezustands hängt vom verwendeten LockNode ab (siehe *Signalisierung des Betriebszustands* [► 214]).

Warnungsmonitor (LSM)

Die LSM bringt einen Warnungsmonitor (| Berichte |, Eintrag **Warnungsmonitor**) mit. Sie sehen dort Batteriewarnungen aller in der Schließanlage verwendeten Schließungen. Zur sinnvollen Nutzung dieser Funktion brauchen Sie einen Task, der regelmäßig den Batteriezustand Ihrer vernetzten LockNodes testet.

Task

Name:

Beschreibung:

Typ: **Lock-Node testen**

Status:

☒ Aktiviert (geplanten Task wie angegeben starten)

Ausführen

☒ Einmal

☐ Wiederholungsintervall

☐ Als Reaktion auf ein Ereignis

Startzeit: 18:05

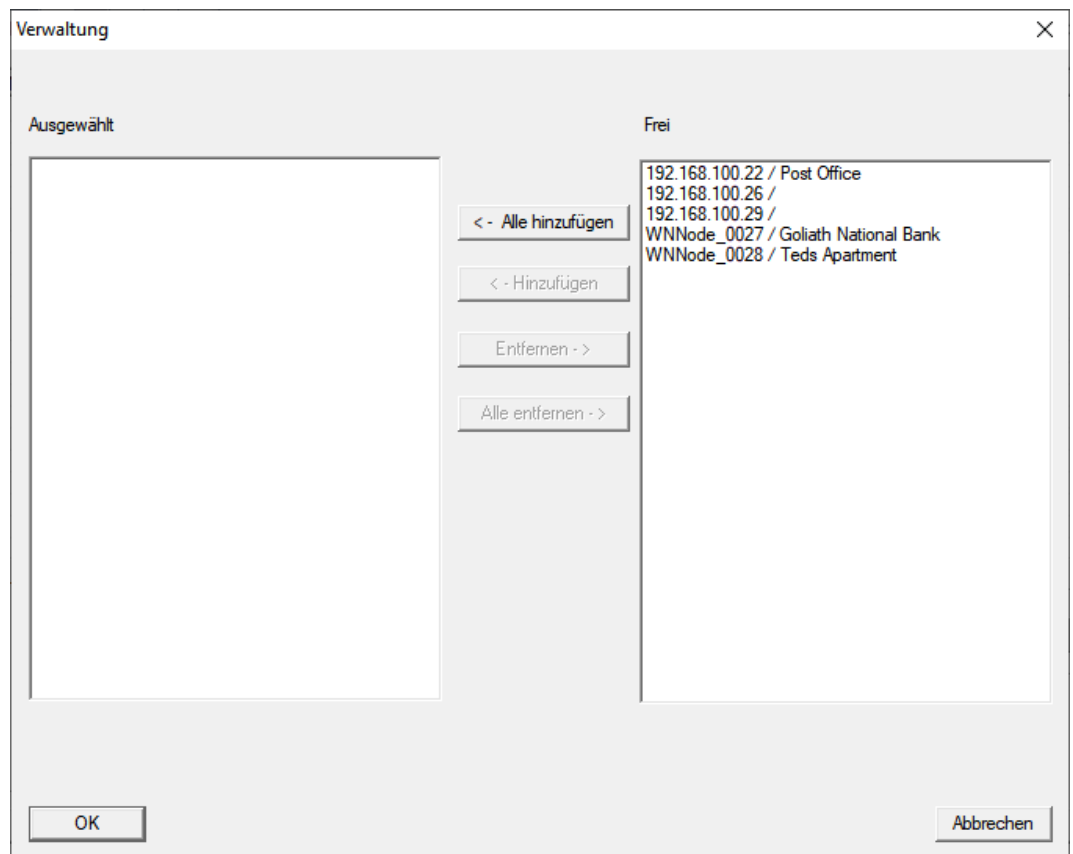
Startdatum: 13 January 2020

Wiederholungsintervall:

Alle 2 Minuten

Schließungen/Netzwerkknoten

3. Geben Sie einen Namen für den Task ein, z.B. "Batteriezustand testen".
4. Geben Sie ggfs. eine Beschreibung ein.
5. Wählen Sie im Dropdown-Menü ▼ **Typ** den Eintrag "LockNode testen".
6. Legen Sie das Wiederholungsintervall fest (z.B. wöchentlich=168 Stunden).
7. Klicken Sie im Bereich "Schließungen/Netzwerkknoten" auf die Schaltfläche **Bearbeiten**.
 - ↳ Fenster "Verwaltung" öffnet sich.



8. Markieren Sie alle Schließungen, deren Batteriezustand Sie überwachen wollen (in der Regel alle Schließungen, die mit einer Batterie betrieben werden und vernetzt sind).
9. Klicken Sie auf die Schaltfläche **Hinzufügen**.
 - ➞ Die markierten Schließungen sind jetzt in der linken Spalte.
10. Klicken Sie auf die Schaltfläche **OK**.
 - ➞ Fenster "Verwaltung" schließt sich.
11. Klicken Sie auf die Schaltfläche **OK**.
 - ➞ Fenster "Task" schließt sich.
12. Wählen Sie im Bereich "Taskdienst" im Dropdownmenü **Task- und Ereignisdienst werden auf folgendem CommNode Server betrieben** den CommNode aus, den Sie für das Testen der LockNodes verwenden wollen.
13. Klicken Sie auf die Schaltfläche **Übernehmen**.
14. Klicken Sie auf die Schaltfläche **Beenden**.
 - ➞ Erinnerungsfenster öffnet sich.
15. Klicken Sie auf die Schaltfläche **OK**.
 - ➞ Erinnerungsfenster schließt sich.
 - ➞ Fenster "Taskmanager" schließt sich.
- ➞ Task in LSM eingerichtet.

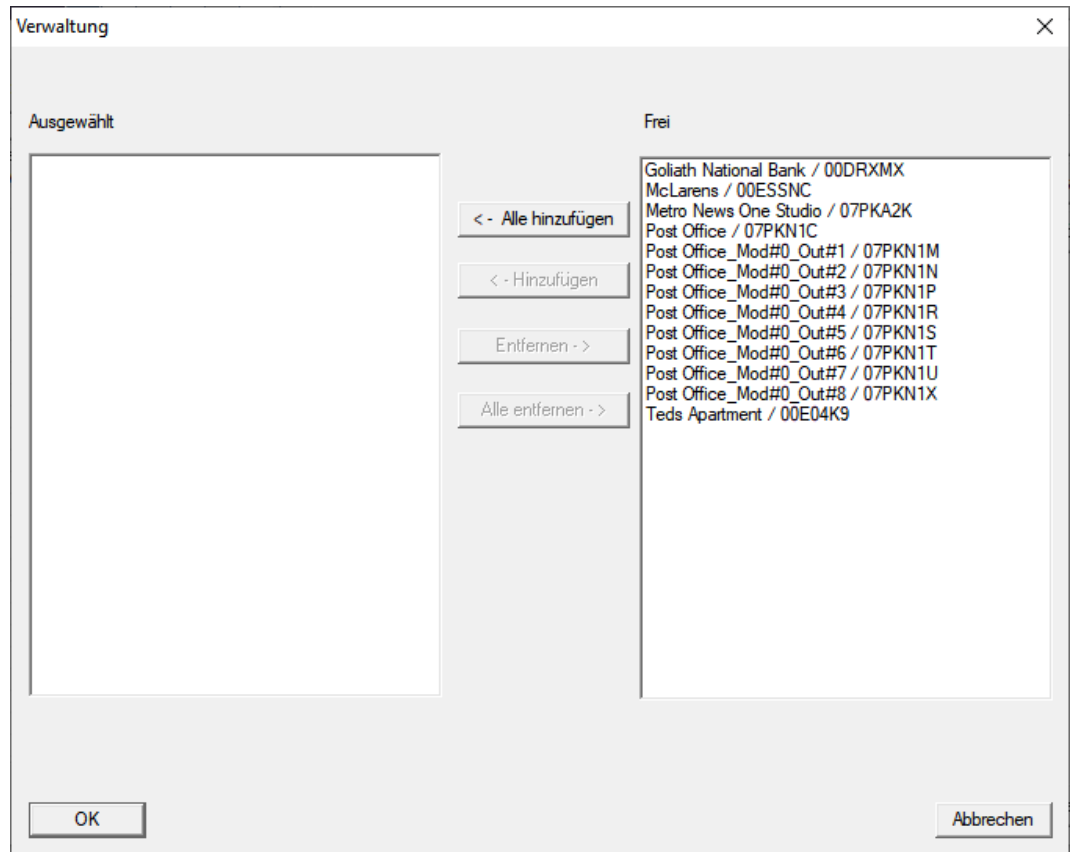
Auf Kommunikati-
onsknoten übertra-
gen

1. Wählen Sie über | Netzwerk | den Eintrag **Kommunikationsknoten**.
2. Stellen Sie sicher, dass Ihr eben verwendeter Kommunikationsknoten ausgewählt ist.
3. Klicken Sie auf die Schaltfläche **Konfig-Dateien**.
 - ↳ Windows-Ordnersuche öffnet sich.
4. Stellen Sie sicher, dass Ihr CommNode-Verzeichnis (CommNodeSvr_X_X) ausgewählt ist.
5. Klicken Sie auf die Schaltfläche **OK**.
 - ↳ Windows-Ordnersuche schließt sich.
 - ↳ Fenster "LockSysMgr" öffnet sich.
6. Klicken Sie auf die Schaltfläche **Nein**.
 - ↳ Fenster "LockSysMgr" schließt sich.
 - ↳ Fenster "LockSysMgr" öffnet sich.
7. Klicken Sie auf die Schaltfläche **OK**.
 - ↳ Fenster "LockSysMgr" schließt sich.
8. Klicken Sie auf die Schaltfläche **Übertragen**.
 - ↳ Daten werden zum Kommunikationsknoten übertragen.
9. Fenster "Programmierung" öffnet sich.
10. Klicken Sie auf die Schaltfläche **OK**.
11. Fenster "Programmierung" schließt sich.
 - ↳ Task ist auf Kommunikationsknoten übertragen.

Batteriewarnungen
anzeigen

- Sie müssen aber die zu überwachenden Schließungen selbst hinzufügen.
Sie können die Anzeige von Batteriewarnungen überprüfen und einstellen:
- ✓ LSM geöffnet.
1. Wählen Sie über | Berichte | den Eintrag **Warnungen verwalten**.
 - ↳ Fenster "Warnungen verwalten" öffnet sich.

4. Stellen Sie sicher, dass die Checkbox ☒ Aktiviert aktiviert ist.
5. Klicken Sie auf die Schaltfläche **Verwalten**.
 - ↳ Fenster "Verwaltung" öffnet sich.



6. Klicken Sie auf die Schaltfläche **Alle hinzufügen**.
 - ↳ Alle Schließungen werden hinzugefügt.
7. Klicken Sie auf die Schaltfläche **OK**.
 - ↳ Fenster "Verwaltung" schließt sich.
8. Klicken Sie auf die Schaltfläche **OK**.
 - ↳ Fenster "Warnung Eigenschaften" schließt sich.

7.1.1 Batteriewechsel bei integrierten LockNodes

LockNodes, die in der Schließung integriert sind (LockNode Inside), werden von der Schließung mit Strom versorgt. Wenn die Schließung batteriebetrieben ist, dann sinkt die Batteriespannung im Laufe der Zeit. Sobald die Batteriespannung einen bestimmten Wert unterschreitet, wird eine Batteriewarnung verschickt. Sinkt der Wert weiter, wird zum Schutz der Restkapazität der LockNode deaktiviert und die Schließung kann nicht mehr über das WaveNet angesprochen werden.

Wechseln Sie bei einer Batteriewarnung die Batterien der Schließung aus. Details dazu entnehmen Sie bitte der Kurzanleitung bzw. dem Handbuch der entsprechenden Schließung.

7.1.2 Batteriewechsel bei externen LockNodes

1. Bauen Sie externe LockNodes aus der Einbauposition aus (öffnen Sie zum Beispiel die Unterputzdose).
2. Entfernen Sie die hintere Abdeckung.
3. Entfernen Sie die alten Batterien.
4. Setzen Sie neue Batterien ein.
 - ↳ LED blinkt zweimal kurz (Power-On-Reset).
- ↳ LockNode ist betriebsbereit.



HINWEIS

Batterien im WN.LN.R

Der WN.LN.R enthält einen Kondensator zur Pufferung der Betriebsspannung. Nach dem Entfernen der Batterien hält dieser Kondensator die Betriebsspannung für einige Sekunden aufrecht. Während dieser Zeit wird kein Power-On-Reset ausgelöst und der neue Batteriezustand nicht erkannt. Wenn Sie eine Batterie verpolt einsetzen, dann entleeren Sie damit den Kondensator und lösen den Power-On-Reset aus.

1. Setzen Sie eine der neuen Batterien am WN.LN.R verpolt ein.
2. Warten Sie fünf Sekunden.
 - ↳ Kondensator entleert.
3. Entfernen Sie die Batterie wieder.
4. Setzen Sie alle Batterien korrekt ein.
 - ↳ Power-On-Reset wird ausgelöst.
- ↳ Neuer Batteriezustand wird erkannt.

7.2 Schließungen

LockNodes, die in die Schließungen integriert sind, beziehen ihren Strom aus den Batterien der Schließungen. Stellen Sie deshalb sicher, dass die Batterien Ihrer Schließungen nicht leer sind. Sie können den Batteriezustand Ihrer Schließungen in der LSM einsehen. Wenn ein Kommunikationsproblem (rotes W in der LSM, siehe auch *Überwachung der Geräte im Netzwerk* [▶ 30]) wiederholt besteht, dann kommen verschiedene Ursachen infrage, unter anderem:

- Funkschatten durch geöffnete Tür
- Routingproblem zwischen CommNode-Server und RouterNode
- Kommunikationsproblem zwischen CommNode-Server und RouterNode, z.B. durch blockierten Port 2101
- (Teilweiser) Netzerkausfall, z.B. durch defekte Switches

- Temporär ausgesetzte IP-Vergabe, z.B. durch Wartungsarbeiten im Netzwerk
- Schwache Batterien

Den Batteriezustand können Sie einfach selbst prüfen.

Weitere Informationen zum Batteriewechsel an Ihrer Schließung finden Sie in der Kurzanleitung bzw. dem Handbuch Ihrer Schließung.

8. Signalisierung des Betriebszustands

RouterNodes

Gerät	Signalisierung	Bedeutung	Reaktion
WNM.RN2.ER.IO	Blinken, ~1,5 Hz (grüne LED auf Deckel)	WaveNet-Konfiguration vorhanden, RouterNode ist betriebsbereit.	
	Blinken, ~0,3 Hz (grüne LED auf Deckel)	Keine WaveNet-Konfiguration vorhanden.	1. Fügen Sie den RouterNode Ihrem WaveNet hinzu (siehe <i>RouterNode dem WaveNet hinzufügen</i> [► 57]).
	Blinken, kurzzeitig (rote LED auf Deckel)	Power-On-Reset.	
	Flackern (grüne LED auf Deckel)	Datenübertragung.	
	Dauerleuchten (rote LED auf Deckel)	Soft- oder Hardwaredefekt.	1. Führen Sie einen Power-On-Reset durch (siehe <i>RouterNodes</i> [► 168]). 2. Tauschen Sie das Gerät aus (siehe <i>Gerät neu programmieren oder ersetzen</i> [► 172]).

Gerät	Signalisierung	Bedeutung	Reaktion
WNM.RN.R.IO WNM.RN.CC.IO WNM.RN.CR.IO WNM.RN.EC.IO	Blinken, ~1,5 Hz (grüne LED)	Empfangsbereit.	
	Blinken (grüne LED)	Datenübertragung.	
	Dauerleuchten (rote LED)	■ Softwareproblem ■ Problem mit der Spannungsversorgung ■ Hardwareproblem	1. Führen Sie einen Power-On-Reset durch (siehe <i>RouterNodes</i> [► 168]). 2. Prüfen Sie die Spannungsversorgung. 3. Tauschen Sie das Gerät aus (siehe <i>Gerät neu programmieren oder ersetzen</i> [► 172]).

LockNodes

Gerät	Signalisierung	Bedeutung	Reaktion
WNM.LN.I WNM.LN.I.MP	4x Piepen (nach Kontaktierung)	LockNode und Schließung verbunden.	
	Kein Signal (nach Kontaktierung)	LockNode und Schließung nicht verbunden.	1. Prüfen Sie die Batterien (siehe Beipackzettel Schließzylinder). 2. Setzen Sie den LockNode zurück (siehe <i>LockNodes</i> [► 178]).
WNM.LN.I.S2	4x Piepen (nach Kontaktierung)	LockNode und Schließung verbunden.	
	Kein Signal (nach Kontaktierung)	LockNode und Schließung nicht verbunden.	1. Prüfen Sie die Batterien (siehe Handbuch SmartHandle AX). 2. Setzen Sie den LockNode zurück (siehe <i>LockNodes</i> [► 178]).

Gerät	Signalisierung	Bedeutung	Reaktion
WNM.LN.I.SH	4x Piepen (nach Kontaktierung)	LockNode und Schließung verbunden.	
	Kein Signal (nach Kontaktierung)	LockNode und Schließung nicht verbunden.	1. Prüfen Sie die Batterien (siehe Handbuch SmartHandle). 2. Setzen Sie den LockNode zurück (siehe <i>LockNodes</i> [► 178]).
WNM.LN.I.SREL2.G2	4x Blinken (nach Kontaktierung)	LockNode und Smart-Relais verbunden.	
WNM.LN.I.SREL.G2	Kein Signal (nach Kontaktierung)	LockNode und Smart-Relais nicht verbunden.	1. Prüfen Sie die Stromversorgung des SmartRelais.

Gerät	Signalisierung	Bedeutung	Reaktion
CompactReader-LockNode (nicht nachrüstbar)	3x Blinken, gefolgt von 4x Blinken (nach Batteriewechsel)	Power-On-Reset CompactReader, LockNode und CompactReader verbunden.	
	3x Blinken (nach Batteriewechsel)	Power-On-Reset CompactReader, LockNode und CompactReader nicht verbunden.	LockNode und CompactReader sind fest verbunden. 1. Setzen Sie den CompactReader zurück. 2. Tauschen Sie das Gerät aus (siehe <i>Gerät neu programmieren oder ersetzen [► 172]</i>).
	4x Blinken (nach Konfigurieren)	LockNode im CompactReader konfiguriert.	
	Kein Signal (nach Konfigurieren)	LockNode im CompactReader nicht konfiguriert.	1. Prüfen Sie die Batterien (siehe Kurzanleitung CompactReader). 2. Setzen Sie den CompactReader zurück. 3. Tauschen Sie das Gerät aus (siehe <i>Gerät neu programmieren oder ersetzen [► 172]</i>).

Gerät	Signalisierung	Bedeutung	Reaktion
WNM.LN.R	Flimmern (Signal-LED)	Keine WaveNet-Konfiguration vorhanden.	1. Fügen Sie den RouterNode Ihrem WaveNet hinzu (siehe <i>RouterNode dem WaveNet hinzufügen</i> [► 57]).
	1x (Signal-LED)	Sende-/Empfangsleistung zwischen Lock-Node und WN.XN.XR schlecht (Prüfung durch Betätigung des Tasters, der mit <i>Init</i> markiert ist).	Verbessern Sie die Signalqualität (siehe <i>Signalqualität verbessern</i> [► 161]).
	2x (Signal-LED)	Sende-/Empfangsleistung zwischen Lock-Node und WN.XN.XR ausreichend (Prüfung durch Betätigung des Tasters, der mit <i>Init</i> markiert ist).	
	3x (Signal-LED)	Sende-/Empfangsleistung zwischen Lock-Node und WN.XN.XR optimal (Prüfung durch Betätigung des Tasters, der mit <i>Init</i> markiert ist).	
WNM.LN.C	2x kurz (rote LED)	Power-On-Reset.	
	Flimmern (rot und grün im Wechsel)	Datenübertragung von/zum LockNode.	

Abgekündigte Produkte

Gerät	Signalisierung	Bedeutung	Reaktion
WN.RN.XX	2x kurz (rote LED)	Power-On-Reset.	
	1x (Signal-LED)	Sende-/Empfangsleistung zwischen zwei WN.RN.R schlecht (Prüfung durch Tastertätigung auf Baseboard).	Verbessern Sie die Signalqualität (siehe <i>Signalqualität verbessern</i> [► 161]).
	2x (Signal-LED)	Sende-/Empfangsleistung zwischen zwei WN.RN.R ausreichend (Prüfung durch Tastertätigung auf Baseboard).	
	3x (Signal-LED)	Sende-/Empfangsleistung zwischen zwei WN.RN.R optimal (Prüfung durch Tastertätigung auf Baseboard).	
	Dauerleuchten (rote LED)	Soft- oder Hardwaredefekt.	1. Führen Sie einen Power-On-Reset durch (siehe <i>RouterNodes</i> [► 168]). 2. Tauschen Sie das Gerät aus (siehe <i>Gerät neu programmieren oder ersetzen</i> [► 172]).

Gerät	Signalisierung	Bedeutung	Reaktion
WN.LN.C	2x kurz (rote LED)	Power-On-Reset.	
	Dauerleuchten (rote LED)	Soft- oder Hardware-defekt.	1. Führen Sie einen Power-On-Reset durch (siehe <i>RouterNodes</i> [► 168]). 2. Tauschen Sie das Gerät aus (siehe <i>Gerät neu programmieren oder ersetzen</i> [► 172]).
WN.RN.R	Langsam blinkend (grüne LED)	Empfangsbereit.	
	Schnell blinkend (grüne LED)	Datenübertragung vom/zum LockNode.	
	Dauerleuchten (rote LED)	Soft- oder Hardware-defekt.	1. Führen Sie einen Power-On-Reset durch (siehe <i>RouterNodes</i> [► 168]). 2. Tauschen Sie das Gerät aus (siehe <i>Gerät neu programmieren oder ersetzen</i> [► 172]).

Gerät	Signalisierung	Bedeutung	Reaktion
WN.RN.XC (Master) WN.RN.CN.XC (Master)	Flackern (rote LED) und grüne LED aus	Kein Slave im Segment gefunden.	1. Prüfen Sie die Kabelverbindung zum Slave. 2. Prüfen Sie die Funktionsfähigkeit des Slaves.
	Dauerleuchten (rote LED)	Soft- oder Hardwaredefekt.	1. Führen Sie einen Power-On-Reset durch (siehe <i>RouterNodes</i> [► 168]). 2. Tauschen Sie das Gerät aus (siehe <i>Gerät neu programmieren oder ersetzen</i> [► 172]).
WN.RN.CX (Slave) WN.LN.C (Slave)	Flackern (rote LED) und grüne LED aus	Kein Master im Segment gefunden.	1. Prüfen Sie die Kabelverbindung zum Master. 2. Prüfen Sie die Funktionsfähigkeit des Masters.
	Dauerleuchten (rote LED)	Soft- oder Hardwaredefekt.	1. Führen Sie einen Power-On-Reset durch (siehe <i>RouterNodes</i> [► 168]). 2. Tauschen Sie das Gerät aus (siehe <i>Gerät neu programmieren oder ersetzen</i> [► 172]).

Gerät	Signalisierung	Bedeutung	Reaktion
WN.LN.R	2x kurz (rote LED)	Power-On-Reset.	
	1x (Signal-LED)	Sende-/Empfangsleistung zwischen Lock-Node und WN.XN.XR schlecht (Prüfung durch Tasterbetätigung auf Baseboard des LockNodes).	Verbessern Sie die Signalqualität (siehe <i>Signalqualität verbessern</i> [► 161]).
	2x (Signal-LED)	Sende-/Empfangsleistung zwischen Lock-Node und WN.XN.XR ausreichend (Prüfung durch Tasterbetätigung auf Baseboard des LockNodes).	
	3x (Signal-LED)	Sende-/Empfangsleistung zwischen Lock-Node und WN.XN.XR optimal (Prüfung durch Tasterbetätigung auf Baseboard des LockNodes).	
	1x kurz (rote LED)	Batterie voll (Prüfung nach Power-On-Reset).	
	1x lang (rote LED)	Batterie schwach (Prüfung nach Power-On-Reset).	1. Ersetzen Sie die Batterien (siehe <i>Batteriewechsel bei externen LockNodes</i> [► 212]).
	1x lang, vier Sekunden (rote LED)	Batterie sehr schwach (Prüfung nach Power-On-Reset).	1. Ersetzen Sie die Batterien (siehe <i>Batteriewechsel bei externen LockNodes</i> [► 212]).
	Dauerleuchten (rote LED)	Soft- oder Hardwaredefekt.	1. Führen Sie einen Power-On-Reset durch (siehe <i>RouterNodes</i> [► 168]). 2. Tauschen Sie das Gerät aus (siehe <i>Gerät neu prüfen</i> [► 168]).

Gerät	Signalisierung	Bedeutung	Reaktion
WN.RN.CC	1x lang (gelbe LED)	Power-On-Reset.	
	Leuchten (grüne LED)	Upstream-Datenübertragung (Slave sendet an Master).	
	Leuchten (dunkelgrüne LED)	Downstream-Datenübertragung (Master sendet an Slave).	
	Dauerleuchten (rote LED)	Soft- oder Hardwaredefekt.	1. Führen Sie einen Power-On-Reset durch (siehe <i>RouterNodes</i> [► 168]). 2. Tauschen Sie das Gerät aus (siehe <i>Gerät neu programmieren oder ersetzen</i> [► 172]).
WN.CN.UX	1x lang (gelbe LED)	USB korrekt erkannt und Power-On-Reset.	
	Blinken, langsam (grüne LED)	Empfangsbereit	
	Blinken, schnell (grüne LED)	Datenübertragung vom/zum LockNode.	
	Dauerleuchten (rote LED)	Soft- oder Hardwaredefekt.	1. Führen Sie einen Power-On-Reset durch (siehe <i>RouterNodes</i> [► 168]). 2. Tauschen Sie das Gerät aus (siehe <i>Gerät neu programmieren oder ersetzen</i> [► 172]).

Gerät	Signalisierung	Bedeutung	Reaktion
WN.RP.CC	Dauerleuchten (gelbe LED)	Stromversorgung vorhanden.	
	Leuchten (grüne LED)	Upstream_Datenübertragung.	
	Leuchten (dunkelgrüne LED)	Downstream-Datenübertragung.	
	Dauerleuchten (rote LED)	Soft- oder Hardwaredefekt.	1. Führen Sie einen Power-On-Reset durch (siehe <i>RouterNodes</i> [► 168]). 2. Tauschen Sie das Gerät aus (siehe <i>Gerät neu programmieren oder ersetzen</i> [► 172]).

Gerät	Signalisierung	Bedeutung	Reaktion
WN.RN2	Blinken (rot und grün im Wechsel)	Reset wird durchgeführt (firmwareabhängig).	
	Blinken, 1,5 s (grün)	Keine WaveNet-Konfiguration vorhanden.	1. Fügen Sie den RouterNode Ihrem WaveNet hinzu (siehe <i>RouterNode dem WaveNet hinzufügen [► 57]</i>).
	Blinken, 1 s	WaveNet-Konfiguration vorhanden, RouterNode ist betriebsbereit.	
	Blinken, 0,5 s	Datenübertragung.	
	Dauerleuchten (rote LED)	Soft- oder Hardwaredefekt.	1. Führen Sie einen Power-On-Reset durch (siehe <i>RouterNodes [► 168]</i>). 2. Tauschen Sie das Gerät aus (siehe <i>Gerät neu programmieren oder ersetzen [► 172]</i>).

8.1 In der LSM

Einige Informationen über den Betriebszustand können Sie direkt aus der LSM einsehen. Dazu gehören:

- Batteriezustand (Schließung auslesen)
- Status der Netzwerkverbindung (Matrix)
- Zustand der Schließung (DoorMonitoring) (Matrix bzw. Smart.Surveil)
- Batteriewarnungen der Schließungen mit LockNodes über Warnungsmonitor (| Berichte | - **Warnungsmonitor**), siehe *LockNodes [► 205]*. Zur sinnvollen Nutzung muss ein Task zum Testen des Batteriezustands eingerichtet mit dem Taskmanager eingerichtet werden. Diese Funktion ist nur in der LSM Business/Professional verfügbar.

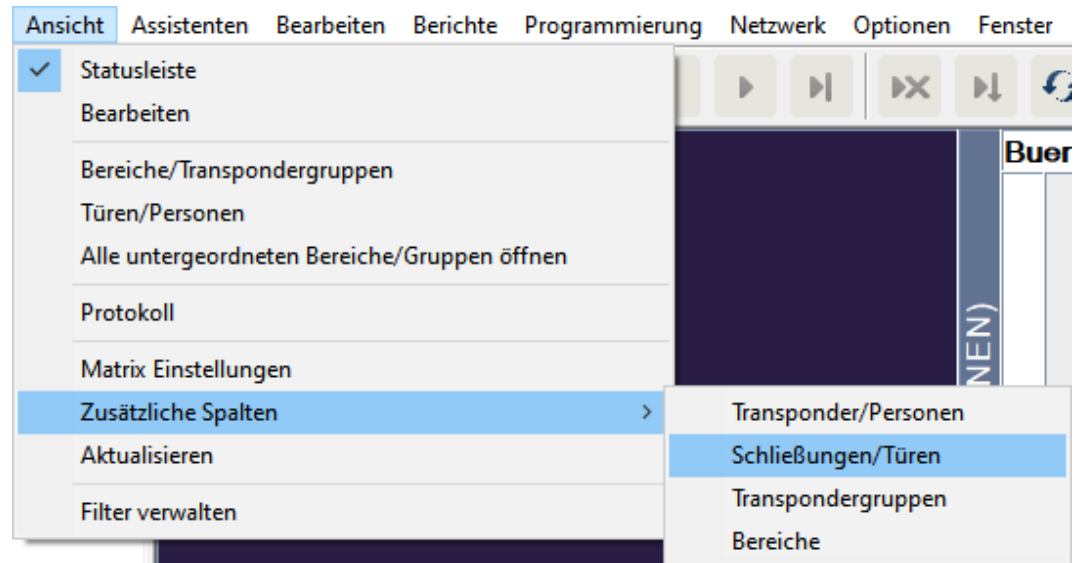
Mit der Schaltfläche  aktualisieren Sie die Ansicht.

Netzwerk- und DoorMonitoring-Status anzeigen

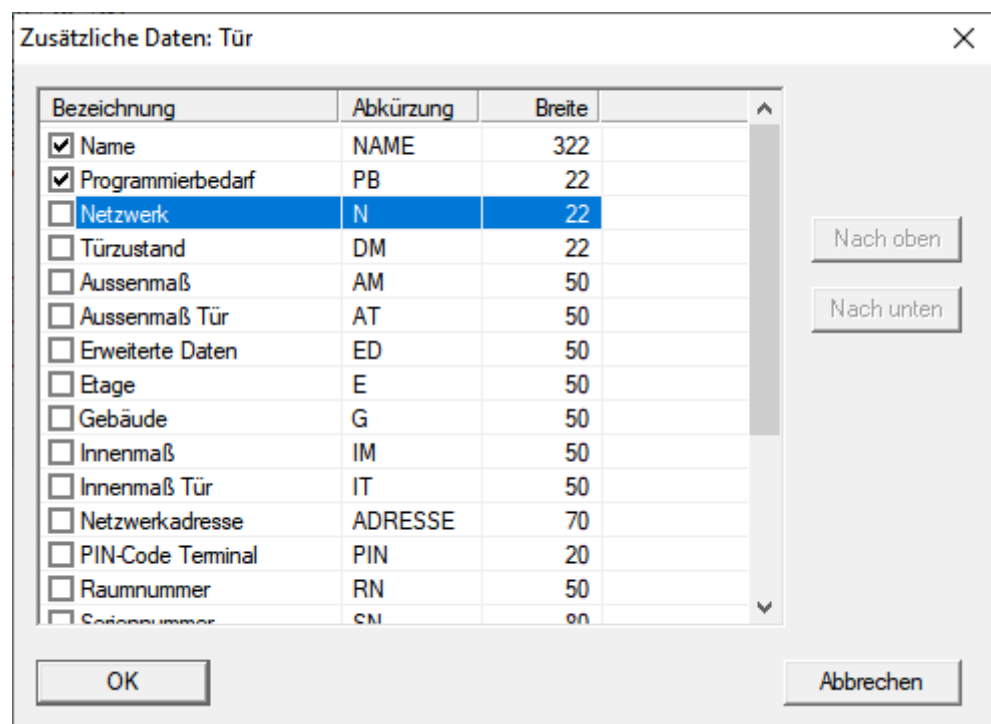
Der Status der Netzwerkverbindung wird nicht standardmäßig angezeigt. Aktivieren Sie die Anzeige des Netzwerkstatus wie folgt:

✓ LSM geöffnet.

1. Wählen Sie über | Ansicht | den Eintrag **Zusätzliche Spalten** und dort **Schließungen/Türen**.



→ Fenster "Zusätzliche Daten: Tür" öffnet sich.



2. Aktivieren Sie die Checkboxen ☒ Türzustand und ☒ Netzwerk.

9. Technische Daten

9.1 WaveNet allgemein

Anzahl Geräte

Siehe auch *Adressierung* [► 45].

Netzwerkmaske	Anzahl RouterNodes	Anzahl LockNodes
8_8	Max. 249	Max. 249 pro Router-Node
11_5	Max. 1790	Max. 25 pro RouterNode
12_4	Max. 3200	Max. 9 pro RouterNode

Übertragungswege

Unterschiedliche WaveNet-Geräte unterstützen unterschiedliche Übertragungswege (siehe *Artikelnummern* [► 15]).

25 kHz	B-Feld zur Kommunikation zwischen: ■ Transpondern und Schließungen ■ Externen LockNodes und Schließungen
868 MHz	SRD-Feld zur Kommunikation zwischen: ■ RouterNodes und LockNodes ■ RouterNodes und RouterNodes
Ethernet	Ethernetverkabelung zur Kommunikation zwischen: ■ Computer und RouterNodes
RS-485	Busverkabelung für die Anbindung an das Netzwerk: ■ RouterNodes ■ Verkabelte LockNodes

Funkfrequenzen im ISM-Band

Siehe auch *Funkkanal* [► 46].

Kanalnummer	Frequenzbereich	Empfohlene geographische Einsatzregion
0 (nur für Suche nach Komponenten)	868,1 MHz (Standardvariante)	Europa
	920,1 MHz (australische Variante)	Australien
1	868,3 MHz für (Standardvariante)	Europa
	920,3 MHz (australische Variante)	Australien
2	868,5 MHz (Standardvariante)	Europa
	920,5 MHz (australische Variante)	Australien
9	869,9 MHz	Europa
	921,9 MHz	Australien

Einstellbare Auslöser für Relaisausgang (RouterNode 2)

Siehe auch *I/O-Konfiguration und Schutzfunktionen* [► 74].

- Zutritt berechtigter Identifikationsmedien
- Zutrittsversuche unberechtigter Identifikationsmedien
- Zutritt berechtigter Identifikationsmedien oder Zutrittsversuche unberechtigter Identifikationsmedien
- Abgeschlossene Reaktionen (außer Aktivierung)

Auslöser für Ereignisse

Siehe auch *I/O-Konfiguration und Schutzfunktionen* [► 74].

- Schalten von Eingang 1
- Schalten von Eingang 2
- Schalten von Eingang 3

Ereignisse am analogen Eingang werden an die LSM weitergeleitet und dort ausgewertet:

- Überschreitung einer analogen Schwellwertspannung
- Unterschreiten einer analogen Schwellwertspannung
- Überschreiten oder Unterschreiten einer analogen Schwellwertspannung

Einstellbare Reaktionen auf Ereignisse (RouterNode 2)

Siehe auch *I/O-Konfiguration und Schutzfunktionen* [► 74].

- Blockschloss
- Amokfunktion
- Notfreischaltung
- Fernöffnung
- Aktivierung

Einstellbare Verzögerung zwischen Ereignis und Reaktion (RouterNode 2)

- 0 s
- 8 s
- 16 s
- 24 s
- 32 s
- RingCast (siehe *RingCast* [► 103])

9.2 RouterNodes**WNM.RN2.ER.IO**

Übertragungs- medien	Schnittstellen	Stromversorgung	Maße
■ 868 MHz ■ Ethernet	■ RJ45 (Netzwerk/PoE) ■ Rundstecker Ø 5,5 mm, Ø Stift 2,0 mm (Stromversorgung) ■ Schraubklemmblock 2-pol, Aderdurchmesser 0,14 mm² bis 1,5 mm² (IO-V_{out} für externe Anwendungen) ■ MCX-Buchse (optionale externe Antenne) ■ Federklemmblock 10-pol, Aderdurchmesser 0,14 (starr) bzw. 0,2 (flexibel) mm² bis 0,5 mm² (IO-Connector)	9 V_{DC} bis 32 V_{DC} oder PoE nach IEEE 802.3af, 3 W Stromversorgung über PoE und Rundstecker gleichzeitig möglich: Rundstecker > 12 VDC → Rundstecker verwendet, Rundstecker < 12 VDC → PoE verwendet	172,1×85,9×32,8 mm

WNM.RN.R.IO

Übertragungs- medien	Schnittstellen	Stromversorgung	Maße
■ 868 MHz	■ Anschlussklemmen für externes Steckernetzteil ■ FME-Buchse (Antenne) ■ Molex PicoBlade 10-pol (IO-Connector)	9 V _{DC} bis 24 V _{DC} , min. 3 VA (Nicht-IO-Versionen abweichend, siehe Kurzanleitung)	98×64×40 mm bzw. 98×64×130 mm mit Antenne

WNM.RN.CC.IO

Übertragungs- medien	Schnittstellen	Stromversorgung	Maße
■ RS-485	■ Anschlussklemmen für externes Steckernetzteil ■ Anschlussklemmen für RS-485 ■ Molex PicoBlade 10-pol (IO-Connector)	9 V _{DC} bis 24 V _{DC} , min. 3 VA (Nicht-IO-Versionen abweichend, siehe Kurzanleitung)	98×64×40 mm

WNM.RN.CR.IO

Übertragungs- medien	Schnittstellen	Stromversorgung	Maße
■ 868 MHz ■ RS-485	■ Anschlussklemmen für externes Steckernetzteil ■ Anschlussklemmen für RS-485 ■ FME-Buchse (Antenne) ■ Molex PicoBlade 10-pol (IO-Connector)	9 V _{DC} bis 24 V _{DC} , min. 3 VA (Nicht-IO-Versionen abweichend, siehe Kurzanleitung)	98×64×40 mm bzw. 98×64×130 mm mit Antenne

WNM.RN.EC.IO

Übertragungs- medien	Schnittstellen	Stromversorgung	Maße
■ Ethernet ■ RS-485	■ Anschlussklemmen für externes Steckernetzteil ■ Anschlussklemmen für RS-485 ■ RJ45-Buchse (Ethernet) ■ Molex PicoBlade 10-pol (IO-Connector)	9 V _{DC} bis 48 V _{DC} , min. 3 VA oder PoE nach IEEE 802.3af, 3 W (Nicht-IO-Versionen abweichend, siehe Kurzanleitung)	98×64×40 mm

9.3 LockNodes

WNM.LN.I

Übertragungs- medien	Schnittstellen	Stromversorgung	Maße
■ 868 MHz	Kontakte zur Schließung	Versorgung aus Schließung	Im Schließzylinder eingebaut

WNM.LN.I.S2

Übertragungs- medien	Schnittstellen	Stromversorgung	Maße
■ 868 MHz	Kontakte zur Schließung	Versorgung aus Schließung	Im SmartHandle AX eingebaut

WNM.LN.I.SH

Übertragungs- medien	Schnittstellen	Stromversorgung	Maße
■ 868 MHz	Kontakte zur Schließung	Versorgung aus Schließung	Im SmartHandle 3062 eingebaut

WNM.LN.I.SREL2.G2

Übertragungs- medien	Schnittstellen	Stromversorgung	Maße
■ 868 MHz	Kontakte zur Schließung	Versorgung aus Schließung	Im SmartRelais 2 (G2) eingebaut

WNM.LN.I.SREL.G2

Übertragungs- medien	Schnittstellen	Stromversorgung	Maße
■ 868 MHz	Kontakte zur Schließung	Versorgung aus Schließung	Im SmartRelais (G2) eingebaut

WNM.LN.R

Übertragungs- medien	Schnittstellen	Stromversorgung	Maße
■ 868 MHz ■ 25 kHz	■ 3 Eingänge (potentialfrei, Pulse im 2-Hz-Takt : 1 ms, 35 μ A) ■ Ausgang (Open Drain, max. 25 V _{DC} , max. 650 mA Dauerstrom (2 A Einschaltstrom - Kontaktwiderstand 0,5 Ω) IO-Kabel mit 6-pol-Molexstecker erforderlich (WNM.LN.SENSOR.CABLE)	2x CR ² / ₃ AA (Lithium 3,6V - Tadiran SL-761) Lebensdauer ca. 6 Jahre	37×Ø53 mm

WNM.LN.C

Übertragungs- medien	Schnittstellen	Stromversorgung	Maße
25 kHz	Anschlussklemmen für RS-485 Anschlussklemmen für externe Stromversorgung Ausgang (Open Drain, max. 25 V_{DC}, max. 650 mA Dauerstrom (2 A Einschaltstrom - Kontaktwiderstand 0,5 Ω) IO-Kabel mit 6-pol-Molexstecker erforderlich (WN.LN.SENSOR.CABLE)	9 V _{DC} bis 24 V _{DC} , ~15 mA	37×Ø53 mm

10. Hilfe und weitere Informationen

Infomaterial/Dokumente

Detaillierte Informationen zum Betrieb und zur Konfiguration sowie weitere Dokumente finden Sie auf der Homepage:

<https://www.simons-voss.com/de/dokumente.html>

Software und Treiber

Software und Treiber finden Sie auf der Website:

<https://www.simons-voss.com/de/service/software-downloads.html>

Konformitätserklärungen und Zertifikate

Konformitätserklärungen und Zertifikate finden Sie auf der Homepage:

<https://www.simons-voss.com/de/zertifikate.html>

Technischer Support

Unser technischer Support hilft Ihnen gerne weiter (Festnetz, Kosten abhängig vom Anbieter):

+49 (0) 89 / 99 228 333

E-Mail

Sie möchten uns lieber eine E-Mail schreiben?

support-simonsvoss@allegion.com

FAQ

Informationen und Hilfestellungen finden Sie im FAQ-Bereich:

<https://faq.simons-voss.com/otrs/public.pl>

Adresse

SimonsVoss Technologies GmbH
Muenchner Str. 16
D-85774 Unterfoehring
Deutschland



Das ist SimonsVoss

SimonsVoss, der Pionier funkgesteuerter, kabelloser Schließtechnik, bietet Systemlösungen mit breiter Produktpalette für die Bereiche SOHO, kleine und große Unternehmen sowie öffentliche Einrichtungen.

SimonsVoss-Schließsysteme verbinden intelligente Funktionalität, hohe Qualität und preisgekröntes Design Made in Germany.

Als innovativer Systemanbieter legt SimonsVoss Wert auf skalierbare Systeme, hohe Sicherheit, zuverlässige Komponenten, leistungsstarke Software und einfache Bedienung. Damit wird SimonsVoss als ein

Technologieführer bei digitalen Schließsystemen angesehen.

Mut zur Innovation, nachhaltiges Denken und Handeln sowie hohe Wertschätzung der Mitarbeiter und Partner sind Grundlage des wirtschaftlichen Erfolgs.

SimonsVoss ist ein Unternehmen der ALLEGION Group – ein global agierendes Netzwerk im Bereich Sicherheit. Allegion ist in rund 130 Ländern weltweit vertreten (www.allegion.com).

Made in Germany

Für SimonsVoss ist „Made in Germany“ ein ernsthaftes Bekenntnis: Alle Produkte werden ausschließlich in Deutschland entwickelt und produziert.

© 2026, SimonsVoss Technologies GmbH, Unterföhring

Alle Rechte vorbehalten. Texte, Bilder und Grafiken unterliegen dem Schutz des Urheberrechts.

Der Inhalt dieses Dokuments darf nicht kopiert, verbreitet oder verändert werden. Technische Änderungen vorbehalten.

SimonsVoss und MobileKey sind eingetragene Marken der SimonsVoss Technologies GmbH.

SimonsVoss
technologies

Made in Germany

A BRAND OF

