KWS ELECTRONIC
HIGH FREQUENCY TEST EQUIPMENT

APPLICATION NOTE AN001

Fernsteuerung – SNMP-Remote-Control

KWS-Electronic GmbH
Tattenhausen
Sportplatzstrasse 1
83109 Großkarolinenfeld
Telefon: 0049 .8067 .9037-0
Telefax: 0049 .8067 .9037-99
Email: info@kws-electronic.
www.kws-electronic.de

Inhaltsverzeichnis

INHALTSVERZEICHNIS **1**

KAPITEL 1 **2**

Über dieses Dokument **2**

1.1 Revisionen 2

1.2 Referenzdokumente 2

1.3 Kontakt zum Hersteller 2

KAPITEL 2 **3**

Einstellungen am Messempfänger **3**

2.1 Freischaltung 3

2.2 Einstellung der IP-Konfiguration 3

KAPITEL 3 **4**

Eigenschaften von SNMP **4**

KAPITEL 4 **5**

AMA-MIB Struktur **5**

KAPITEL 5 **6**

Überwachung mit Trap-Nachrichten **6**

5.1 Auslösen von Traps 6

5.1.1 AmaEventTable 6

5.1.2 AmaAlarmTable 7

5.1.3 AmaTrapTable 8

5.2 Ein Beispiel 8

5.2.1 Konfiguration des Messempfängers 9

5.2.2 Überwachung des Empfangsstatus 9

5.2.3 Überwachung des Pegels 9

Kapitel 1

Über dieses Dokument

Dieses Dokument beinhaltet Informationen zur Softwareoption „Fernsteuerung - SNMP-Remote-Control“ von Antennenmessempfängern vom Typ AMA310.

1.1 Revisionen

V00.01 Juli 2010
Erste Veröffentlichung

1.2 Referenzdokumente

Diese Application Note bezieht sich auf folgende Dokumente:

- AMA310 Antennen-Messempfänger Bedienungsanleitung

1.3 Kontakt zum Hersteller

Für aktuelle Informationen zu Produkten von KWS-Electronic besuchen Sie unsere Homepage **www.kws-electronic.de**. Dort finden Sie auch alle Kontaktdaten.

Kapitel 2

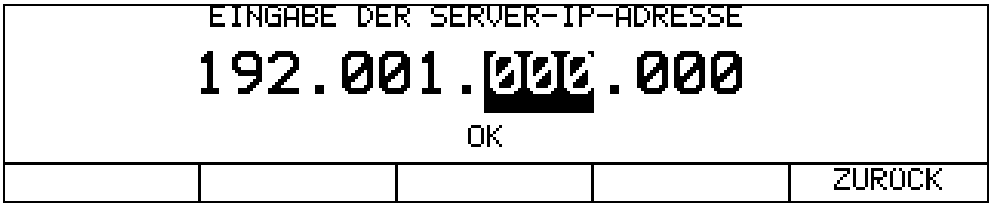
Einstellungen am Messempfänger

2.1 Freischaltung

Diese Option muss über einen 8-stelligen Schlüssel (Key-Code) im Messgerät aktiviert werden. Dieser ist beim Hersteller anzufordern. Weitere Informationen zur Eingabe des Key-Codes sind in der Bedienungsanleitung zum Messempfänger im Kapitel „Gerätemanagement“ im Abschnitt „Freigabe von Software-Optionen“ zu finden.

2.2 Einstellung der IP-Konfiguration

Bevor das Messgerät in einem Netzwerk betrieben werden kann, müssen die IP-Einstellungen vorgenommen werden. Dazu gehören IP-Adresse, Subnet-Maske und Standard-Gateway.
Diese Angaben können über **MODE** -> **EINSTELLU.** -> **IPCONFIG** -> **IP-ADR**, **SUBNETMASK**, bzw. **STDGATEWAY** eingegeben werden.



Die Eingabe geschieht über die Zehnertastatur. Nach Eingabe einer Stelle ist die Taste **ENTER** zu betätigen, woraufhin der Cursor auf die nächste Position springt. Ist die letzte Stelle eingegeben, steht der Cursor auf OK. Jetzt wird durch eine abschließende Betätigung der Taste **ENTER** die Einstellung abgespeichert.

Nach einer Veränderung der IP-Konfiguration **muss** das Messgerät einmal aus- und eingeschaltet werden, damit der TCP-IP-Stack mit der neuen Einstellung initialisiert wird.

Kapitel 3

Eigenschaften von SNMP

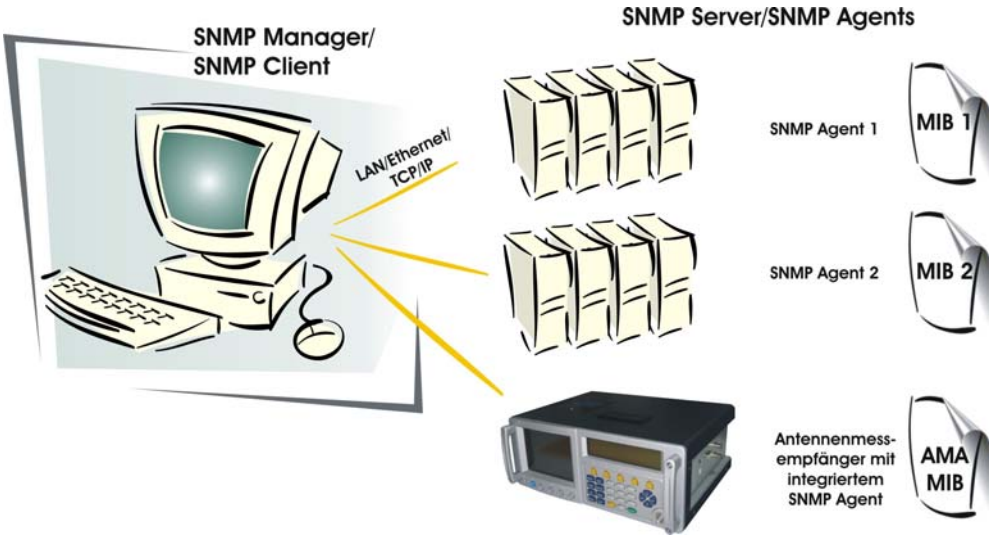
SNMP setzt auf das Internetprotokoll (IP) auf und existiert in drei Versionen. Die Standards zum Internet sind in Request-For-Comments-Dokumenten (RFCs) festgehalten. Dabei ist z.B. die Version 1 des SNMP-Standards (SNMPv1) in den Dokumenten RFC1155, RFC1156 und RFC1157 beschrieben. Die SNMP Option des Messempfängers verwendet SNMPv1.

Ein PC oder Netzwerkgerät auf welchem eine SNMP-fähige Netzwerk Management Software installiert ist, wird SNMP Manager oder SNMP Client genannt. Das zu überwachende Netzwerkgerät, z.B. ein Messempfänger, wird als SNMP Agent oder SNMP Server bezeichnet. Die Client-Server-Bezeichnung bezieht sich darauf, dass das zu überwachende Netzwerkgerät als Server Daten zur Verfügung stellt und das Überwachungsprogramm als Client diese Daten abfragt. Im weiteren Verlauf wird das Netzwerk Management System als SNMP Manager und das zu überwachende Gerät als SNMP Agent bezeichnet.

Um ein Netzwerkgerät zu steuern, werden Einstellungen vorgenommen und ausgelesen. Des Weiteren kann ein Netzwerkgerät so genannte Events anstoßen, um über bestimmte Ereignisse zu informieren. Bei SNMP erfolgt die Steuerung hauptsächlich über Set- (um Einstellungen vorzunehmen) und Get-Anweisungen (um Einstellungen, Messwerte und Parameter auszulesen). Die ausgelösten Ereignisse die z.B. zur Überwachung verwendet werden sind so genannte Traps. Die Objekte (meist Variablen), welche für die Steuerung und Überwachung benötigt werden, werden durch eine eindeutige Object Identity (OID) repräsentiert.

Alle OIDs werden in einer Management Information Base (MIB) aufgelistet. Die MIB besitzt eine Baumstruktur, wobei jeder Knoten im MIB-Baum einen Namen sowie eine Nummer trägt und eine OID alle Namen bzw. Nummern bis zum eigentlichen Objekt enthält. Bestimmte MIB-Elemente sind standardisiert, jedoch kann z.B. eine Firma bei der Internet Assigned Numbers Authority (IANA) eine Private Enterprise Number (PEN) beantragen. Die Knoten bis zu den PENs sind laut Standard .iso(1).org(3).dod(6).internet(1).private(4).enterprise(1).

Der Hersteller hat z.B. die PEN 35128 und die OID für das MER-Objekt von Messempfängern ist „.1 .3 .6 .1 .4 .1 .35128 .ama(1) .measuredValues(2) .amaMER(4)“. Die Vergabe der OIDs hinter der PEN bleibt dem PEN-Besitzer selbst überlassen und wird in einer gerätespezifischen MIB festgehalten. Bei dieser MIB handelt es sich genau genommen um eine Unter-MIB und sie kann in der Regel vom Gerätehersteller angefragt werden. Eine (Unter-) MIB wird in einer Textdatei mit der Dateiendung .mib beschrieben und der Dateiinhalt folgt einer vorgegebenen Syntax. Damit ist gewährleistet, dass einem SNMP-Manager durch Einlesen einer MIB ein SNMP-Agenttyp bekannt gemacht werden kann. Der SNMP-Manager kann dann alle SNMP-Agents verwalten, für welche die eingelesene MIB gilt. Ein bestimmtes Netzwerkgerät wird dabei über dessen IP-Adresse angesprochen.



Kapitel 4

AMA-MIB Struktur

Die AMA-MIB ist in fünf Bereiche aufgeteilt.

- control:
In dieser Kategorie befinden sich alle Objekte, die für die Abstimmung des Messempfängers benötigt werden. Je nach Messbereich etc. sind unterschiedliche Objekte zu verwenden. Die Reihenfolge in der die Einstellungen vorgenommen werden, ist analog zur Bedienung des Messempfängers. Des Weiteren müssen einige der Objekte in bestimmten Konfigurationen nicht gesetzt werden, da diese Parameter dann vom Messempfänger automatisch ermittelt werden.

- measuredValues:
Die Objekte aus diesem Bereich geben die Messwerte zurück. Die Anzahl der Objekte mit gültigen Messwerten unterscheidet sich je nach Messbereich. Das Objekt amaLevel liefert bei abgestimmtem Messgerät immer einen Messwert für den Pegel.

- receivedParameters:
Hierbei handelt es sich um Parameter die vom Messempfänger automatisch ermittelt werden. Auch hier unterscheidet sich die Anzahl der Objekte mit gültigen Werten je nach Messbereich.

- trapControl :
In diesem Bereich werden die Einstellungen für das Senden von Trap-Nachrichten vorgenommen. Hierfür stehen die drei Tabellen amaEventTable, amaAlarmTable und amaTrapTable zur Verfügung. In der amaEventTable können alle Einstellungen über den Empfänger der Ereignisse vorgenommen werden. Die amaAlarmTable beinhaltet alle Angaben zu den zu überwachenden Messgrößen und die amaTrapTable dient der Überwachung von Zuständen, z.B. von amaState.

- traps:
Hier werden die Traps aufgelistet, die vom Messempfänger bei Auftreten bestimmter Ereignisse gesendet werden.

Um Messwerte und Parameter empfangen zu können, muss der Messempfänger abgestimmt und somit mindestens ein Control-Objekt via SNMP-Befehl gesetzt worden sein. Mit Setzen eines Control-Objekts wird die SNMP Funktionalität im Messempfänger aktiviert und Messwerte und Parameter können ausgelesen werden.

Kapitel 5

Überwachung mit Trap-Nachrichten

5.1 Auslösen von Traps

Wie bereits erwähnt, kann ein SNMP-Agent durch Auslösen eines Traps einen SNMP-Manager über ein aufgetretenes Ereignis informieren. Das vereinfacht für den SNMP-Manager die Überwachung von SNMP-Agents, da bestimmte Objekte nicht zyklisch abgefragt werden müssen. Ein SNMP-Agent meldet sich selbstständig beim SNMP-Manager. Vom Messempfänger können bestimmte Messwerte und Zustände überwacht werden. Genauere Informationen zu den einzelnen Objekten sind in der AMA-MIB enthalten.

Entsprechend dem Überwachungsprogramm des Messempfängers (siehe Kapitel „Überwachungsprogramm“ in der Bedienungsanleitung zum Messempfänger) können je nach Messbereich verschiedene Messgrößen überwacht werden:

Bereich	Betriebsart	Überwachte Größen
SAT		
	ATV	Pegel, S/N (nur mit Option S/N)
	DVB-S	Pegel, MER, CBER, VBER, PE (Packet Errors)
	DVB-S2	Pegel, MER, CBER, LBER, PE (Packet Errors)
TV		
	ATV	Pegel, S/N (nur mit Option S/N)
	DVB-C	Pegel, MER, BER, PE (Packet Errors)
	DVB-T	Pegel, MER, CBER, VBER, PE (Packet Errors)
	EUDOCSIS	Pegel, MER, BER, PE (Packet Errors)
	USDOCSIS	Pegel, MER, VBER, PE (Packet Errors)
FM		Pegel
RK		Pegel

Des Weiteren kann bei digitalem Empfang der Status locked/unlocked kontrolliert werden.

5.1.1 AmaEventTable

Zunächst muss der SNMP-Manager den SNMP-Agent für das Senden von Traps konfigurieren. Um einem SNMP-Agent mitzuteilen an welchen SNMP-Manager und in welcher Form Traps gesendet werden sollen, erfolgt ein Eintrag in die amaEventTable.

amaEventTable			
OID	**Zugriff**	**Werte mit Index 0**	**Werte mit Index 1**
amaEventIndex	Lese~	0	1
amaEventDescription	Lese~/Schreib~	Beschreibung über den Trap-Empfänger	…
amaEventType	Lese~/Schreib~	snmptrap(3)	
amaEventCommunity	Lese~/Schreib~	Community-String	
amaEventLastTimeSent	Lese~	Immer 0 (noch nicht implementiert)	
amaEventOwner	Lese~/Schreib~	IP-Adresse des Trap-Empfängers	
amaEventStatus	Lese~/Schreib~	valid(1), [createRequest(2), underCreation(3)], invalid(4)	

Durch Abfrage des amaEventIndex kann ein freier Index ermittelt werden, da ein nicht verwendeter Index den Fehler „no such value“ (zu deutsch „dieser Wert existiert nicht“) zurückgibt.
Die notwendigen Einträge sind amaEventCommunity und amaEventOwner, die übrigen Angaben sind freiwillig, da der amaEventType grundsätzlich „snmptrap“ ist. Sind alle Angaben vollständig, werden die Einträge durch Setzen von amaEventStatus auf „valid“ (zu deutsch „gültig“) für abgeschlossen erklärt. Der verwendete Event-Index wird anschließend für die Einträge in der amaAlarmTable und amaTrapTable benötigt, um den Trap-Empfänger anzugeben. Soll ein SNMP-Manager keine Traps mehr empfangen, muss der amaEventStatus mit dem entsprechenden Index auf „invalid“ (zu deutsch „ungültig“) gesetzt werden. Alle Einträge in amaAlarmTable und amaTrapTable, welche diesen Event-Index angeben, werden damit ebenfalls auf „invalid“ gesetzt.

Nachdem ein Trap-Empfänger angelegt ist, können gewünschte Traps durch Einträge in die amaAlarmTable und amaTrapTable angegeben werden. Auch hier kann durch Abfrage von amaAlarmIndex bzw. amaTrapIndex ein freier Index ermittelt werden.

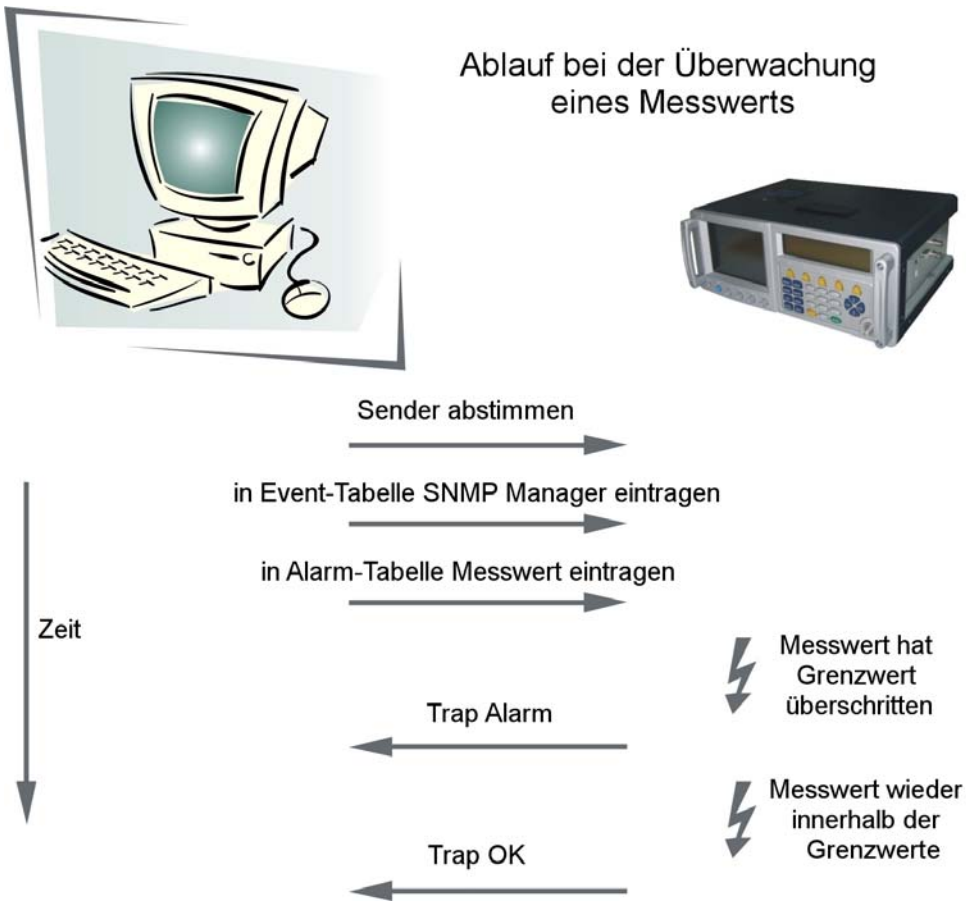
5.1.2 AmaAlarmTable

In der Alarmtabelle sind die Einträge amaAlarmVariable, amaAlarmSampleType, amaAlarmRisingThreshold oder amaAlarmFallingThreshold und amaAlarmEventIndex zwingend erforderlich. Der obere (amaAlarmRisingThreshold) und der untere Grenzwert (amaAlarmFallingThreshold) können entweder einzeln oder zusammen angegeben werden. In bestimmten Fällen macht die Angabe einer der beiden Grenzwerte keinen Sinn und kann entfallen.

amaAlarmTable			
OID	**Zugriff**	**Werte mit Index 0**	**Werte mit Index 1**
amaAlarmIndex	Lese~	0	1
amaAlarmVariable	Lese~/Schreib~	OID des zu überwachenden Messwertes	…
amaAlarmSampleType	Lese~/Schreib~	absoluteValue(1), deltaValue(2)	
amaAlarmValue	Lese~	Messwert zum Zeitpunkt der Grenzwertüberschreitung	
amaAlarmRisingThreshold	Lese~/Schreib~	Oberer Grenzwert	
amaAlarmFallingThreshold	Lese~/Schreib~	Unterer Grenzwert	
amaAlarmEventIndex	Lese~/Schreib~	Index des zugehörigen Event-Tabellen-Eintrages	
amaAlarmStatus	Lese~/Schreib~	valid(1), [createRequest(2), underCreation(3)], invalid(4)	

Bei amaAlarmEventIndex handelt es sich um den Index des Event-Tabelleneintrags, welcher den gewünschten Trap-Empfänger beschreibt. Um die Einträge abzuschließen muss auch hier das Statusobjekt, in diesem Fall amaAlarmStatus, auf „valid“ gesetzt werden.

Einträge in der Alarmtabelle lösen beim Auftreten einer Grenzwertüber- bzw. Grenzwertunterschreitung amaTrapAlarms aus. Fällt ein überwachter Messwert wieder in den Bereich innerhalb der Grenzwerte zurück, wird vom Messempfänger ein amaTrapOK-Trap gesendet. Soll ein Messwert nicht mehr überwacht werden, muss der entsprechende Eintrag in der Alarmtabelle durch Setzen von amaAlarmStatus auf „invalid“ gelöscht werden.



5.1.3 *AmaTrapTable*

Um Zustände des Messempfängers zu überwachen, müssen amaTrapVariable und amaTrapEventIndex in die Trap-Tabelle eingetragen werden. Auch hier handelt es sich bei amaTrapEventIndex um den Index des Event-Tabelleneintrags, welcher den gewünschten Trap-Empfänger beschreibt. Des Weiteren werden hier ebenfalls die Einträge für einen Index abgeschlossen, indem das Statusobjekt amaTrapStatus auf „valid“ gesetzt wird. Die Angabe von Grenzwerten ist für die Überwachung eines Zustands nicht notwendig, stattdessen wird ein amaTrapState-Trap ausgelöst, wenn sich der zu überwachende Zustand ändert. Soll ein Zustand nicht mehr überwacht werden, muss der entsprechende Eintrag in der Trap-Tabelle durch Setzen von amaTrapStatus auf „invalid“ gelöscht werden.

amaTrapTable			
OID	**Zugriff**	**Werte mit Index 0**	**Werte mit Index 1**
amaTrapIndex	Lese~	0	1
amaTrapVariable	Lese~/Schreib~	OID des zu überwachenden Status	…
amaTrapValue	Lese~	Status zum Zeitpunkt der Änderung	
amaTrapEventIndex	Lese~/Schreib~	Index des zugehörigen Event-Tabellen-Eintrages	
amaEventStatus	Lese~/Schreib~	valid(1), [createRequest(2), underCreation(3)], invalid(4)	

5.2 *Ein Beispiel*

Nachfolgend werden konkrete Beispiele gegeben, wie das Gerät zum Senden von Traps eingestellt werden muss. Um die Einstellungen vornehmen zu können, wird ein SNMP-/Netzwerk-Management-Programm benötigt, bei welchem die AMA-MIB eingelesen wurde.

Für den Empfang von Traps muss der IP-Port 162 freigegeben sein, der eventuell von einer Firewall gesperrt wurde.
Des Weiteren muss ein Trap-Empfangs-Programm zur Darstellung der eingegangenen Traps aktiviert werden. Meist handelt es sich dabei um Tools bzw. Funktionen des Management-Programms die lediglich gestartet werden müssen, nachdem alle Einstellungen vorgenommen wurden.

Zunächst wird der Messempfänger für die folgenden Beispiele auf einen digitalen Sender abgestimmt. Dies geht am Schnellsten mit einem Set-Befehl für die OID amaRecall auf einen Abstimmspeicherplatz an dem ein digitaler Sender gespeichert ist. Mit Get-Befehlen kann überprüft werden, ob das Abstimmen erfolgreich war.

5.2.1 Konfiguration des Messempfängers

Um dem Messempfänger den Trap-Empfänger bekannt zu machen, werden in der amaEventTable folgende Einträge gemacht:

- **amaEventCommunity mit Index 0** (also OID: .1.3.6.1.4.1.35128.1.4.1.1.4.0) **auf Wert 'public'**
- **amaEventOwner mit Index 0** (also OID: .1.3.6.1.4.1.35128.1.4.1.1.6.0) **auf IP-Adresse des Trap-Empfängers,** z.B. '192.1.1.0', die IP-Adresse eines Windows-PCs kann z.B. über die Eingabeaufforderung mit ipconfig abgefragt werden.
- **amaEventStatus mit Index 0** (also OID: .1.3.6.1.4.1.35128.1.4.1.1.7.0) **auf '1'** (valid), um die Einträge in dieser Tabellenzeile (Zeile 0, weil Index 0) abzuschließen.

Damit sind alle notwendigen Angaben zum Trap-Empfänger eingetragen.

5.2.2 Überwachung des Empfangsstatus

Um den Status locked/unlocked zu überwachen, werden in der amaTrapTable folgende Angaben eingetragen:

- **amaTrapVariable mit Index 0** (also OID: .1.3.6.1.4.1.35128.1.4.3.1.2.0) **auf zu überwachende OID '.1.3.6.1.4.1.35128.1.3.1.0'**, momentan nur möglich für amaState
- **amaTrapEventIndex mit Index 0** (also OID: .1.3.6.1.4.1.35128.1.4.3.1.4.0) **auf '0'**, entspricht dem Tabellenindex des Trap-Empfängers in der amaEventTable
- **amaTrapStatus mit Index 0** (.1.3.6.1.4.1.35128.1.4.3.1.5.0) **auf '1'** (valid), um die Einträge in dieser Tabellenzeile (Zeile 0, weil Index 0) abzuschließen.

Hiermit sind alle notwendigen Werte zur Überwachung des Status locked/unlocked gesetzt. Nun muss ein Trap-Empfangs-Programm/-Tool aktiviert werden. Wenn das Messgerät in den Zustand unlocked geht (z.B. durch Abstecken des Messkabels ausgelöst), kann eine Trap-Nachricht empfangen werden.

5.2.3 Überwachung des Pegels

Ein Messwert, z.B. der Pegel, wird überwacht indem in die amaAlarmTable Folgendes eingetragen wird:

- **amaAlarmVariable mit Index 0** (also OID: .1.3.6.1.4.1.35128.1.4.2.1.2.0) **auf zu überwachende OID '.1.3.6.1.4.1.35128.1.2.1.0'**, entspricht amaLevel
- **amaAlarmSampleType mit Index 0** (also OID: .1.3.6.1.4.1.35128.1.4.2.1.3.0) **auf '1'**, entspricht „absolute Value“ (zu deutsch „Absolutwert“)
- **amaAlarmFallingThreshold mit Index 0** (also OID: .1.3.6.1.4.1.35128.1.4.2.1.6.0) **auf '30.0dBµV'**, ein 'u' statt 'µ' ist ebenfalls möglich
- **amaAlarmEventIndex mit Index 0** (also OID: .1.3.6.1.4.1.35128.1.4.2.1.7.0) **auf '0'**, entspricht dem Tabellenindex des Trap-Empfängers in der amaEventTable
- **amaAlarmStatus mit Index 0** (also OID: .1.3.6.1.4.1.35128.1.4.2.1.8.0) **auf '1'** (valid), um die Einträge in dieser Tabellenzeile (Zeile 0, weil Index 0) abzuschließen.

Auf diese Weise sind alle notwendigen Angaben zur Überwachung einer Unterschreitung des Pegels unter 30,0dBµV gemacht worden. Ein Trap-Empfangs-Programm/-Tool muss auch hier aktiviert werden, um eine Trap-Nachricht empfangen zu können. Wenn der Pegel unter 30,0dBµV sinkt (auch hier z.B. ausgelöst durch Abstecken des Messkabels), sendet der Messempfänger eine Meldung. Selbstverständlich kann auch ein Wert für amaAlarmRisingThreshold eingetragen werden, wodurch eine Trap-Nachricht bei Überschreiten des angegebenen Werts ausgelöst wird.