

# Handbuch RFID-Server

**Release** 1.00, Juni 2007

Typ 95001  
ab Geräte-Firmware 2.10

**W&T**

© 06/2007 by Wiesemann und Theis GmbH  
Microsoft, MS-DOS, Windows, Winsock und Visual Basic  
sind eingetragene Warenzeichen der Microsoft Corporation

Irrtum und Änderung vorbehalten:

Da wir Fehler machen können, darf keine unserer Aussagen ungeprüft verwendet werden. Bitte melden Sie uns alle Ihnen bekannt gewordenen Irrtümer oder Missverständlichkeiten, damit wir diese so schnell wie möglich erkennen und beseitigen können.

Führen Sie Arbeiten an bzw. mit W&T Produkten nur aus, wenn Sie hier beschrieben sind und Sie die Anleitung vollständig gelesen und verstanden haben. Eigenmächtiges Handeln kann Gefahren verursachen. Wir haften nicht für die Folgen eigenmächtigen Handelns. Fragen Sie im Zweifel lieber noch einmal bei uns bzw. Ihrem Händler nach!

## **Einleitung**

Der W&T RFID-Server ist ein Komplettsystem mit integrierter Antenne und integriertem Netzwerkanschluss für die Verarbeitung von ISO15693-konformen RFID-Transpondern bis zu einer Reichweite von 35 cm. Speziell der intelligente Modus W&T Tag-Control entbindet den Anwender hierbei von der aufwändigen Einarbeitung in die ISO-Norm und erlaubt die ereignisgesteuerte Kommunikation der Tag-Daten. Parallel zu dieser Kommunikation kann der Leser über konfigurierte Vorfilter selbstständig Aktionen in Abhängigkeit des jeweiligen Tags, des Zeitpunktes und des Zustandes der digitalen Eingänge durchführen.

Neben der Konfiguration dieser Standardfunktionen beschreibt dieses Handbuch das vollständige Netzwerkprotokoll des RFID-Servers und erlaubt somit eine sehr systemnahe Einbindung in eigene Applikationen.

<b>1 Systemübersicht und Quickstart</b>	<b>7</b>
1.1 Quickstart	8
1.2 Systemübersicht	10
1.3 Die Werkseinstellungen	12
<b>2 Vergabe der IP-Adresse</b>	<b>13</b>
2. Konfiguration der Netzwerk-Parameter mit WuTility	14
2.2 Vergabe der IP mit Hilfe des ARP-Kommandos	17
2.3 IP-Vergabe per DHCP-Protokoll	19
2.3.1 Aktivierung/Deaktivierung von DHCP	19
2.3.2 System Name	20
2.3.3 Lease-Time	20
2.3.4 Reservierte IP-Adressen	21
2.3.5 Dynamische IP-Adressen	21
2.4 IP-Vergabe per BOOTP-Protokoll	23
2.4.1 Adressreservierung	23
2.5 IP-Vergabe über einen RARP-Server	25
<b>3 Montage und Antennenabgleich</b>	<b>27</b>
3.1 Montage des RFID-Servers	28
3.2 Antennenabgleich	30
<b>4 Anschlüsse und Anzeigen</b>	<b>31</b>
4.1 Spannungsversorgung	32
4.2 Netzwerkanschluss	33
4.3 Digitale Ein-/Ausgänge	35
4.3.1 Digitale Eingänge	36
4.3.2 Digitale Ausgänge	37
4.3.3 Relaisausgang	38
4.4 LED-Anzeigen	39
4.4.1 Power und Netzwerkstatus	39
4.4.2 RFID-Status	40
<b>5 Web-Based-Management - Grundlagen</b>	<b>43</b>
5.1 Start des Web Based Management	44
5.2 Web Based Management - Login und Navigation	45
5.2.2 Die Navigation	45
5.2.3 Speicherung und Aktivierung der Einstellungen	47

# W&T

<b>6</b>	<b>WBM - Allgemeine Konfiguration</b>	<b>49</b>
6.1	Session Control	50
6.1.1	Session Control >> Reset ...	50
6.1.2	Session Control >> New Password ...	50
6.2	Device	52
6.2.1	Device >> Network	52
6.2.2	Device >> Time and Date	55
6.2.3	Device >> Mode	56
6.3	Up-/Download - Konfigurationsprofile	57
6.4	Diagnose und Abgleich	58
<b>7</b>	<b>W&amp;T Tag-Control - Konfiguration</b>	<b>59</b>
7.1	Aufbau des W&T Tag Control	60
7.2	Filter TAG- Listen	63
7.3	Filter Time Condition	64
7.4	Filter Input Condition	66
7.5	Aktionen	67
7.6	Master (Filterset)	69
<b>8</b>	<b>W&amp;T Tag-Control - Netzwerkprotokoll</b>	<b>73</b>
8.1	Kommunikationsgrundlagen	74
8.2	Verbindungsaufbau	75
8.3	Definition der Protokoll-Strukturen	76
8.3.1	Filtermatch (0300)	78
8.3.2	Buffered Match (0301)	79
8.3.3	Clear Buffer (0302)	80
8.3.4	Buffer out of memory (030F)	80
8.3.5	Readflash (0320)	81
8.3.6	Writeflash (0321)	82
8.3.7	Get IO (0322)	84
8.3.8	Set Output (0323)	86
8.4	Fehlerbehandlung	88
8.4.1	Syntaxfehler (FF00)	88
8.4.2	Funktionale Fehler (FF02)	89

# W&T

<b>9 Kommunikation per OPC</b>	<b>91</b>
<b>10 Datenbankintegration per ODBC</b>	<b>93</b>
10.1 ODBC-Grundlagen	94
<b>11 Protocol Mode</b>	<b>95</b>
11.1 Funktionsbeschreibung	96
<b>Anhang</b>	<b>97</b>
Firmware-Update	98
Reset des RFID-Server über das Netzwerk	100
Verwendete Ports und Netzwerksicherheit	101
Hardware-Reset auf Werkseinstellungen	104
Zahlensysteme/Programmiergrundlagen	105
Technische Daten	108
Konformitätserklärung	109
Index	110

# **1 Systemübersicht und Quickstart**

Die folgenden Seiten vermitteln eine Übersicht des Kommunikations-Konzeptes und der Betriebsmodi des RFID-Servers. Darüberhinaus werden für bereits geübte Anwender die grundsätzlichen Schritte der Inbetriebnahme in Kurzform beschrieben. Detailinformationen können den folgenden Kapiteln entnommen werden.

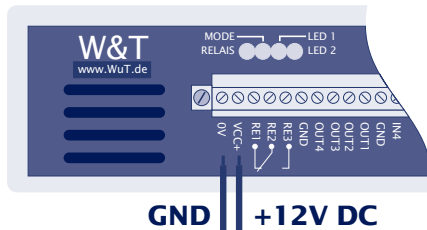
## 1.1 Quickstart

### Einsatzort

Der Betrieb des RFID-Servers kann in beliebiger Lage erfolgen. Zur Erzielung der optimalen Erfassungs-Reichweite, sollte die mit der Antenne gekennzeichnete Gehäusesseite in Leserichtung ausgerichtet sein. Die Lüftungsschlitze an den Gehäuse-Schmalseiten dürfen nicht verdeckt sein.

### Spannungsversorgung

Der RFID-Server wird mit einer geregelten Gleichspannung von 12V/ $\pm$ 5% versorgt. Schließen Sie diese in der abgebildeten Polarität an die steckbare Schraubklemme an.

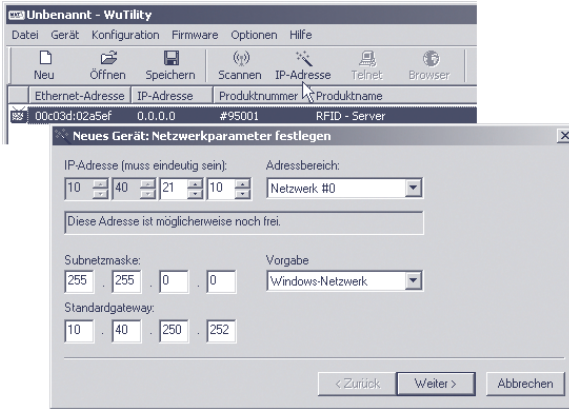


### Netzwerkinstallation

Der Netzwerkanschluss an den Hub oder Switch erfolgt über ein 1:1 verdrahtetes RJ45-Kabel. Ab Werk ist der DHCP-Client des RFID-Servers aktiviert, so dass die Zuteilung von IP-Adresse, Subnet-Mask und Gateway in einer entsprechenden Netzwerkumgebung automatisch erfolgt.

In Netzwerkumgebungen ohne DHCP, installieren Sie zunächst das Windows-Tool *WuTility* von der beiliegenden Produkt-CD und starten dieses auf einem PC im gleichen Subnetz des RFID-Servers. Markieren Sie den RFID-Server in der angezeigten Liste, betätigen dann den Button *IP-Adresse* und folgen dem anschließenden Dialog.





Nach der IP-Vergabe startet der RFID-Server den Modus W&T Tag-Control und arbeitet mit den eingestellten Filterregeln. Mit der Werkseinstellung wird hierbei Erfassung und Verlust jedes Tags mit einem kurzen Signalton quittiert. Ist ein TCP-Client mit dem W&T Tag-Control Serverport verbunden, erhält dieser ein Datenpaket des Typs 0x300 (Direct Filtermatch).

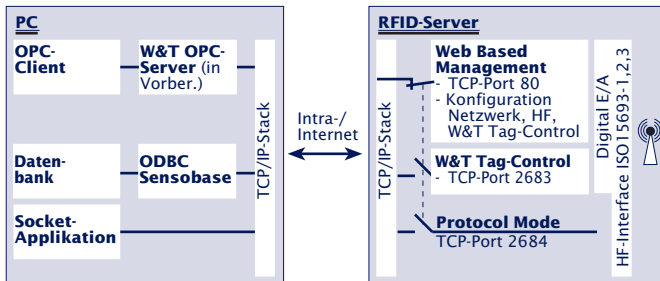
Die gesamte weitere Konfiguration des RFID-Servers inklusive des automatischen Antennen-Abgleiches erfolgt über das Web Based Management mit Hilfe eines Standard Internet-Browsers.



*Zur Erzielung der maximalen Antennen-Reichweite, muss nach der Inbetriebnahme oder einem Reset auf die Werkseinstellungen am Einsatzort mit Hilfe des Web Based Management ein Abgleich der HF-Schnittstelle erfolgen.*

## 1.2 Systemübersicht

Der RFID-Server ist ein Midrange Komplettsystem für die Verarbeitung von ISO15693-konformen Transpondern im 13,56MHz-Bereich. Die zentrale Kommunikations-Schnittstelle des RFID-Servers ist der Netzwerk-Anschluss, welcher TCP-Server-Dienste für die Erfassung und Verarbeitung von ISO15693-konformen Transpondern sowie zur Konfiguration des Systems per Internet-Browser zur Verfügung stellt.



### Modus Web Based Management (Default-Port TCP 80)

Die gesamte Konfiguration der Netzwerk- und HF-Parameter sowie der einzelnen Betriebsarten erfolgt mit Hilfe eines Standard Internet Browsers. Während einer aktiven Konfigurations-Session ist der RFID-Server nicht in der Lage Transponder zu verarbeiten. Die TCP-Server der *W&T Tag-Control* sowie des *Protocol Modes* sind deaktiviert.

### Modus W&T Tag-Control (Default-Port TCP 2683)

*W&T Tag-Control* ist die Standard-Betriebsart für das Erfassen und die Verarbeitung von RFID-Tags. Inklusive der Kollisionserkennung und -behandlung, übernimmt der RFID-Server hierbei selbstständig die komplette Abwicklung des HF-Protokolls der ISO15693-Norm. Erfassung und Verlust von Transpondern stellen Ereignisse dar, die zuvor konfigurierte Filterketten durchlaufen. Als Ergebnis dieser Vorfilterung kann zum Beispiel das mit Zeitstempel versehene Senden der TAG-ID an eine Netzwerkapplikation sein. Darüberhinaus können unabhängig von einer bestehenden Netzwerkverbindung auch direkt die digitalen Aus-

gänge geschaltet werden, wodurch ein völlig autarker Offline-Betrieb des RFID-Servers möglich ist.

Der Modus W&T Tag-Control wird von allen W&T RFID-Tools genutzt.

**Protocol Mode (Default-Port TP 2684)**

Als Alternative zur Nutzung des Modus W&T Tag-Control, bietet der Protocol Mode die Möglichkeit des transparenten Zugriffs auf die Kommandos des Standards ISO15693-3. Die netzwerkseitige Anwendung muss hierbei sowohl den Start der Inventarisierungszyklen veranlassen, wie auch die Behandlung von Kollisionen bei mehreren gleichzeitig erfassten Tags übernehmen.

Detaillierte Informationen zu den einzelnen Betriebsarten finden Sie in den entsprechenden Kapiteln dieses Handbuchs.

## 1.3 Die Werkseinstellungen

Die Liste enthält eine Übersicht der wichtigsten Werkseinstellungen. Detailinformationen zu den einzelnen Parametern und deren Konfiguration, finden Sie in den entsprechenden Kapiteln dieses Handbuchs:

### Netzwerkparameter

Hardware-Anschluss:	Auto-Negotiating
IP-Adresse:	0.0.0.0
Gateway-Adresse:	0.0.0.0
Subnet-Mask:	255.0.0.0
DHCP-Protokoll:	Aktiv



*Zur Vermeidung ungewollter Adressvergaben oder Adressänderungen empfehlen wir, die Protokolle DHCP und BOOTP zu deaktivieren, sofern diese nicht ausdrücklich in der jeweiligen Netzwerkkumgebung genutzt werden.*

### Passwörter

System- und Userpasswort sind leer.

### HF-Schnittstelle

Betriebsart:	W&T Tag-Control
Filterset 1:	Aktiv (Signalton bei Erfassung/Verlust von Tags)
Filtersets 2-8:	Deaktiv

### TCP-Ports

Web Based Management:	80
W&T Tag-Control:	2683
Protocol-Mode:	2684



*Zur Erzielung der maximalen Antennen-Reichweite, muss nach der Inbetriebnahme oder einem Reset auf die Werkseinstellungen am Einsatzort mit Hilfe des Web Based Management ein Abgleich der HF-Schnittstelle erfolgen.*

## 2 Vergabe der IP-Adresse

Der RFID-Server hat ab Werk die IP-Adresse 0.0.0.0. Vor der Vergabe müssen Sie von Ihrem jeweiligen Systembetreuer eine zu Ihrem Netzwerk passende IP-Adresse erhalten. In kleineren, ungerouteten Netzen verwenden Sie die IP-Adresse Ihres PCs und ändern lediglich die letzte Stelle. Beachten Sie jedoch immer, dass IP-Adressen innerhalb eines Netzwerkes eindeutig sein müssen.

- Vergabe von IP-Adresse, Subnet-Mask und Gateway-Adresse mit dem Management-Tool *WuTility*
- IP-Vergabe mit Hilfe des ARP-Kommandos
- Einstellung von IP-Adresse, Subnet-Mask und Gateway-Adresse per DHCP-/BOOTP-Protokoll
- IP-Vergabe per RARP-Protokoll

## 2. Konfiguration der Netzwerk-Parameter mit *WuTility*

Das Windows-Tool *WuTility* ermöglicht ab der Version 3.0 neben der Inventarisierung aller W&T Netzwerkgeräte auch die komfortable Vergabe/Änderung der folgenden netzwerkseitigen Basisparameter des RFID-Servers

- IP-Adresse
- Subnet-Mask
- Gateway-Adresse
- Aktivierung/Deaktivierung BOOTP/DHCP

Für die Vergabe müssen sich PC und RFID-Server im gleichen Subnetz befinden. Ein gegebenenfalls eingestelltes Systempasswort, muss bekannt sein.

### **Download und Installation von *WuTility***

*WuTility* befindet sich auf der Produkt-CD und kann von dort direkt installiert werden. Die jeweils aktuellste Version ist auch stets auf unseren Webseiten unter folgender Adresse veröffentlicht:

<http://www.wut.de>

Sie navigieren von dort aus am einfachsten mit Hilfe des Menübaumes auf der linken Seite:

*Zubehör: Downloads → RFID-Server*

Nach dem Entpacken der ZIP-Datei erfolgt die Installation über einen Doppelklick auf die Datei *setup\_de.exe*. Der Start von *WuTility* erfolgt über

*Start → Programme → W&T Software Toolkit → WuTility*

### **Start des Vergabe-Dialoges**

Stellen Sie sicher, dass sowohl der RFID-Server als auch der verwendete Rechner an das Netzwerk angeschlossen sind und sich im gleichen Subnetz befinden. Beim Start durchsucht *WuTility* automatisch das lokale Netzwerk nach angeschlossenen W&T-Netzwerkgeräten und erzeugt eine Inventarliste. Dieser Suchvor-

gang lässt sich manuell beliebig oft durch Betätigung des Buttons *Scannen* wiederholen:



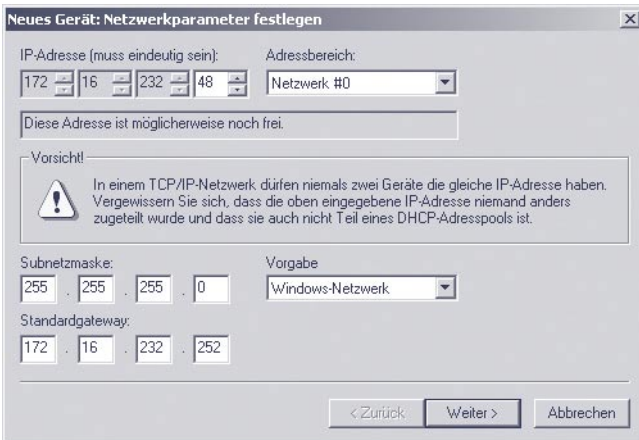
Innerhalb der Inventarliste können Sie den gewünschten RFID-Server anhand seiner MAC-Adresse identifizieren. Bei Erstinstallationen lautet dessen IP-Adresse immer 0.0.0.0.



Markieren sie den RFID-Server und betätigen dann den Button *IP-Adresse*:

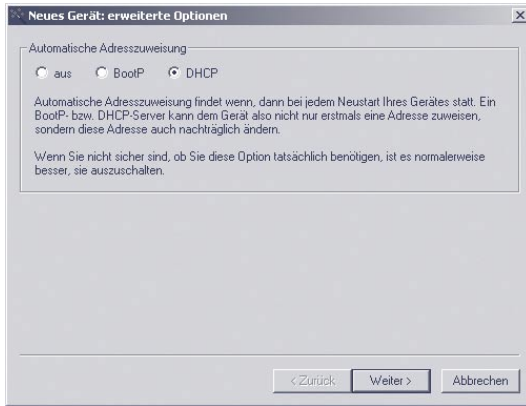


Geben Sie in die Eingabefelder des folgenden Fensters die gewünschten Werte für IP-Adresse, Subnet-Mask sowie Gateway-Adresse ein und betätigen den Button *Weiter*.



*Jede IP-Adresse muss immer netzwerkweit eindeutig sein.*

In dem folgenden Dialog können der DHCP- und BOOTP/RARP-Client des RFID-Servers aktiviert/deaktiviert werden.



*Zur Vermeidung ungewollter Adressvergaben oder Adressänderungen, empfehlen wir die Protokolle DHCP, BOOTP und RARP zu deaktivieren, sofern diese nicht ausdrücklich in der jeweiligen Netzwerkumgebung genutzt werden. RFID-Server mit fälschlich zugeteilter IP-Adresse können nachträglich mit Hilfe der Scan-Funktion des Managementtools WuTility komfortabel gefunden und neu konfiguriert werden.*

Mit Betätigung des Buttons *Weiter* werden dem RFID-Server die Netzwerkparameter zugewiesen. Alle Spalten der Geräte-liste in WuTility werden mit Informationen gefüllt.

Die netzwerkseitige Inbetriebnahme des RFID-Servers ist hiermit abgeschlossen. Die gesamte weitere Konfiguration erfolgt mit Hilfe eines Standard Internet-Browsers. Aus WuTility heraus ist der Start durch Betätigen des Buttons *Browser* möglich:



*Das Ändern der Netzwerkparameter ist durch das Systempasswort geschützt. Um mißbräuchliche Zugriffe zu verhindern, empfehlen wir bei in Betrieb befindlichen RFID-Servern ein Systempasswort zu vergeben.*

Weitere Informationen hierzu finden Sie im Kapitel *Allgemeine Konfiguration*.



## 2.2 Vergabe der IP mit Hilfe des ARP-Kommandos



*Diese Methode ist nur ausführbar, wenn der RFID-Server noch keine IP-Adresse hat, der Eintrag also 0.0.0.0 lautet. Verwenden Sie zum Ändern einer IP-Adresse eine der anderen in diesem Kapitel beschriebenen Methoden oder das Web Based Management des Gerätes.*

Weitere Voraussetzung ist ein Computer, der sich im gleichen Netzwerksegment des RFID-Servers befindet und auf dem das TCP/IP-Protokoll installiert ist. Lesen Sie die Ethernet-Adresse des RFID-Servers von dem Aufkleber an der Gehäusefront ab:



Fügen Sie jetzt mit der folgenden Befehlszeile der ARP-Tabelle des Rechners einen statischen Eintrag hinzu:

```
arp -s [IP-Adresse] [MAC-Adresse]
```

Beispiel unter Windows:

```
arp -s 172.16.231.10 00-C0-3D-00-12-FF
```

Beispiel unter SCO UNIX:

```
arp -s 172.16.231.10 00:C0:3D:00:12:FF
```

Führen Sie abschließend mit der folgenden Befehlszeile unter **Start** → **Ausführen** ein Ping auf den RFID-Server mit der gewünschten IP-Adresse aus:

```
ping [IP-Adresse] [Return]
```



*In Windows-Umgebungen darf die Eingabe von IP-Adressen nur ohne führende Nullen erfolgen. Ansonsten wird die Eingabe vom System falsch interpretiert und dem RFID-Server wird eine falsche IP-Adresse zugewiesen.*

Der RFID-Server übernimmt die IP-Adresse des ersten an ihn gesendeten Netzwerkpaketes als seine eigene und speichert die-



*Jede IP-Adresse muss immer netzwerkweit eindeutig sein.*



*Ältere Windows-Systeme akzeptieren einen statischen Eintrag nur dann, wenn bereits ein dynamischer vorhanden ist. Führen Sie hier zunächst ein PING auf einen anderen Netzwerkteilnehmer durch.*

se nichtflüchtig ab. Anschließend werden die Pings beantwortet.

Die gesamte weitere Konfiguration erfolgt mit Hilfe eines Standard Internet-Browsers. Aus WuTility heraus ist der Start durch Betätigen des Buttons *Browser* möglich.

## 2.3 IP-Vergabe per DHCP-Protokoll

Viele Netzwerke nutzen für die zentralisierte und dynamische Vergabe der Netzwerkparameter DHCP (**D**ynamic **H**ost **C**onfiguration **P**rotocol) oder auch das im folgenden Kapitel beschriebene Vorgängerprotokoll BOOTP. Mit den Werkseinstellungen ist das DHCP-Protokoll aktiviert, so dass es in Netzwerkumgebungen mit dynamischer IP-Vergabe ausreicht, den RFID-Server an das Netzwerk anzuschliessen. Die folgenden Parameter können mit Hilfe von DHCP zugewiesen werden:

- IP-Adresse
- Subnet-Mask
- Gateway-Adresse
- Lease-Time



*Zur Vermeidung ungewollter Adressvergaben oder Adressänderungen, empfehlen wir die Protokolle DHCP, BOOTP und RARP zu deaktivieren, sofern diese nicht ausdrücklich in der jeweiligen Netzwerkumgebung genutzt werden. RFID-Server mit fälschlich zugeteilter IP-Adresse können nachträglich mit Hilfe der Scan-Funktion des Managementtools WuTility komfortabel gefunden und neu konfiguriert werden.*

### 2.3.1 Aktivierung/Deaktivierung von DHCP

Mit der Werkseinstellung ist das DHCP-Protokoll aktiviert. Zur Deaktivierung oder auch zum späteren Wiedereinschalten stehen die folgenden Möglichkeiten zur Verfügung.

- **Management-Tool WuTility**  
Markieren Sie in der Geräteliste den gewünschten RFID-Server und betätigen den Button *IP-Adresse*. In dem ersten Dialogfenster tragen Sie die neu zu vergebenden Netzwerkparameter ein und betätigen dann *Weiter*. Deaktivieren Sie in dem folgenden Dialogfenster die Optionen *BOOTP* und

*DHCP*. Mit *Weiter* werden jetzt abschließend die neuen Konfigurationsdaten an den RFID-Server übertragen.

- **Web Based Management**

Im Menüzweig *Home* → *Config* → *Device* → *Network* können die Protokolle einzeln aktiviert bzw. deaktiviert werden.

### 2.3.2 System Name


Zur Unterstützung einer eventuell automatisierten Aktualisierung des DNS-Systems durch den DHCP-Server, identifiziert sich der RFID-Server innerhalb des DHCP-Protokolls mit seinem System Namen. In der Werkseinstellung lautet dieser *RFID-Server*- gefolgt von den letzten drei Stellen der Ethernet-Adresse. Zum Beispiel lautet der werksseitig eingestellte Systemname eines RFID-Servers mit der Ethernet-Adresse 00:c0:3d:01:02:03 *RFID-SERVER-010203*. Der Systemname des RFID-Servers kann im Menüzweig *Home* → *Config* → *Device* → *Network* geändert werden.

### 2.3.3 Lease-Time

Die vom DHCP-Server bestimmte und übermittelte Lease-Time legt die Gültigkeitsdauer der zugewiesenen IP-Adresse fest. Nach Ablauf der halben Lease-Time versucht der RFID-Server bei dem zuweisenden DHCP-Server die Gültigkeit zu verlängern bzw. die Adresse zu aktualisieren. Ist dieses bis zum Ablauf der Lease-Time nicht möglich, zum Beispiel weil der DHCP-Server nicht mehr erreichbar ist, löscht der RFID-Server die IP-Adresse und startet eine zyklische Suche nach alternativen DHCP-Servern zwecks Zuweisung einer neuen IP-Adresse.

Nach dem Neustart erfolgt eine Aktualisierungsanfrage bei dem ursprünglichen DHCP-Server. Sollte dieser zu diesem Zeitpunkt nicht erreichbar sein, löscht der RFID-Server die IP-Adresse und startet eine zyklische Suche nach alternativen DHCP-Servern.

Ist DHCP aktiviert, wird die verbleibende Lease-Time zusammen mit der aktuellen IP-Adresse im Untermenü *Home* → *Config* → *Device* → *Network* der Web-Konfiguration angezeigt.

 *Sollte nach Ablauf der zugewiesenen Lease-Time der DHCP-Server nicht erreichbar sein, löscht der RFID-Server seine IP-Adresse. Alle bestehenden TCP-Verbindungen zwischen dem RFID-Server und anderen Netzwerkteilnehmern werden hierdurch unterbrochen. Um Störungen dieser Art zu vermeiden, empfehlen wir, die zu vergebende Lease-Time im DHCP-Server möglichst auf unendlich zu konfigurieren.*

### 2.3.4 Reservierte IP-Adressen

Der RFID-Server stellt als TCP-Server Dienste zur Verfügung, die andere Teilnehmer (Clients) im Netzwerk nach Bedarf in Anspruch nehmen können. Für die Verbindungsaufnahme wird von diesen natürlich die aktuelle IP-Adresse des RFID-Servers benötigt, so dass es in diesen Anwendungsfällen sinnvoll ist, auf dem DHCP-Server eine bestimmte IP-Adresse für den RFID-Server zu reservieren. In der Regel erfolgt dieses durch die Bindung der IP-Adresse an die weltweit einmalige Ethernet-Adresse des RFID-Servers, welche dem Aufkleber an der Gehäusefront entnommen werden kann.



### 2.3.5 Dynamische IP-Adressen

Eine völlig dynamische Adress-Vergabe, bei welcher der RFID-Server mit jedem Neustart oder auch nach Ablauf der Lease-Zeit eine andere IP-Adresse bekommt, ist nur in Netzwerkumgebungen mit automatisierter Querverbindung zwi-

schen den Diensten DHCP und DNS sinnvoll. Das heißt, bei der Neuzuteilung einer IP-Adresse an den RFID-Server, aktualisiert der DHCP-Server automatisch auch das DNS-System. Dem jeweiligen Domain-Namen wird hierbei die neue Adresse zugeordnet. Für diesbezügliche Detailinformationen zu Ihrer Netzwerkumgebung, wenden Sie sich im Zweifel an Ihren Systemadministrator.

## 2.4 IP-Vergabe per BOOTP-Protokoll

Viele Netzwerke nutzen für die zentralisierte und dynamische Vergabe von IP-Adressen BOOTP als Vorgänger des DHCP-Protokolls. Mit den Werkseinstellungen des RFID-Servers ist BOOTP abgeschaltet. Die Aktivierung kann im Zuge der IP-Vergabe mit *WuTility* über das Konfigurationstool *RFID-Explorer* erfolgen. Die folgenden Parameter können übergeben werden:

- IP-Adresse
- Subnetmask
- Gateway-Adresse



*Zur Vermeidung ungewollter Adressvergaben oder Adressänderungen, empfehlen wir die Protokolle DHCP, BOOTP und RARP zu deaktivieren, sofern diese nicht ausdrücklich in der jeweiligen Netzwerkumgebung genutzt werden. RFID-Server mit fälschlich zugeteilter IP-Adresse können nachträglich mit Hilfe der Scan-Funktion des Managementtools WuTility komfortabel gefunden und neu konfiguriert werden.*

### 2.4.1 Adressreservierung

Das BOOTP-Protokoll basiert auf festen Reservierungen von festen IP-Adressen für bestimmte Ethernet-Adressen. Das heißt, ein an das Netzwerk angeschlossener RFID-Server erhält nur dann eine IP-Adresse, wenn diese zuvor im BOOTP-Server entsprechend hinterlegt wurde. Für das Anlegen der Reservierung wenden Sie sich bitte an den zuständigen Systemadministrator. Die hierfür benötigte Ethernet-Adresse des RFID-Servers kann dem an der Gehäusefront befindlichen Aufkleber entnommen werden.



Nachdem die notwendigen Eintragungen vom Administrator vorgenommen wurden, bezieht der RFID-Server nach jedem Reset automatisch die gewünschte IP-Adresse. Um die Erreichbarkeit des RFID-Servers auch bei ausgefallenem BOOTP-Server zu gewährleisten, wird bei ausbleibender Antwort die bisherige IP-Adresse beibehalten.



## 2.5 IP-Vergabe über einen RARP-Server

Besonders UNIX-Umgebungen bedienen sich für eine zentralisierte Zuweisung von IP-Adressen häufig des RARP-Protokolls. Hierbei senden TCP/IP-Geräte, die eine IP-Adresse beziehen möchten, RARP-Requests mit Ihrer Ethernet-Adresse als Broadcast in das Netzwerk.

Aktivieren Sie den RARP-Server auf dem UNIX-System, und tragen Sie in der Datei `/etc/ethers` die Ethernet-Adresse des RFID-Servers sowie in der Datei `/etc/hosts` die IP-Adresse ein.



Der RFID-Server muss sich im gleichen Subnetz wie der RARP-Server befinden.

### Beispiel

Ihr RFID-Server hat die MAC-Adresse EN= 00C03D0012FF (Sticker auf dem Gerät). Er soll die IP-Adresse 172.16.231.10 und den Aliasnamen WT\_1 erhalten:

- Eintrag in der Datei `/etc/hosts`:  
172.16.231.10 WT\_1
- Eintrag in der Datei `/etc/ethers`:  
00:C0:3D:00:12:FF WT\_1

RARP-Broadcasts werden mit der Werkseinstellung nach jedem Reset des RFID-Servers erzeugt. Die Antwort eines RARP-Servers überschreibt die aktuelle IP-Adresse des RFID-Servers. Wir empfehlen aus diesem Grund, die Protokolle DHCP, und BOOTP/RARP zu deaktivieren, sofern diese nicht ausdrücklich benötigt werden. Nutzen Sie hierfür die Funktion *IP-Adresse* in *WuTility*. Die Deaktivierung von BOOTP/RARP kann auch über die Web-Konfiguration im Untermenü *Home* → *Config* → *Device* → *Network* erfolgen.



## **3 Montage und Antennenabgleich**

- Installations-/Betriebs-Umgebung
- Antennenausrichtung
- Antennenabgleich

### 3.1 Montage des RFID-Servers

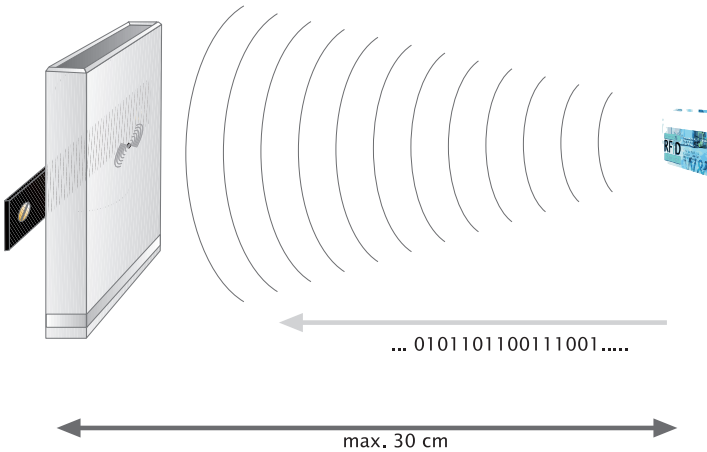
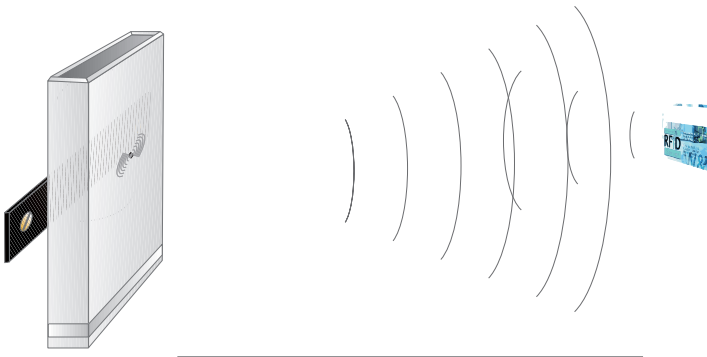
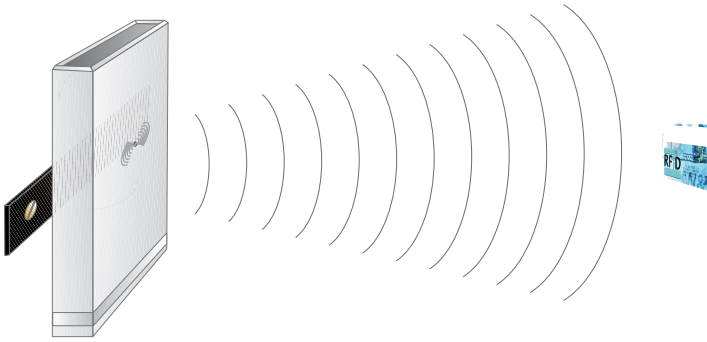
Der RFID-Server ist sowohl für den Einsatz als Tischgerät sowie mit Hilfe des optionalen Montagekits 95201 auch zur Wandmontage geeignet. Die integrierte Antenne des RFID-Servers befindet sich unter der entsprechend gekennzeichneten Gehäuseseite. Zur Erzielung einer möglichst großen Erfassungs-Reichweite, sollte die Antennenseite möglichst in Leserichtung ausgerichtet sein.

Bei der Auswahl des Einsatz- bzw. Montageortes muss lediglich die unmittelbarer Nähe (<15cm) *geschlossener* Metallflächen vermieden werden. Nicht geschlossene metallische Strukturen wie z.B. in Stahlbeton oder Trockenbauwänden werden durch einen Abgleich des RFID-Servers kompensiert.

Um eine einwandfreie Luftzirkulation zu gewährleisten, dürfen die Lüftungsschlitze an den Frontseiten des Gehäuses nicht verdeckt werden.

# RFID-Server

# Transponder



## 3.2 Antennenabgleich

Für eine optimale Anpassung an das magnetische Umfeld am jeweiligen Einsatzort, muss ein Abgleich der integrierten Antenne erfolgen. Nach der ersten Inbetriebnahme in der jeweiligen Umgebung, erfolgt dieser Erstabgleich über die Web-Konfiguration des RFID-Servers. Detaillinformationen hierzu finden Sie im Kapitel *WBM - Allgemeine Funktionen*.



*Während des Abgleichs dürfen sich keine Tags in der Erfassungsreichweite des RFID-Servers befinden. Ggf. ist der Abgleich nach Entfernen des/der Tags zu wiederholen.*

Für den späteren produktiven Dauerbetrieb im Modus W&T Tag-Control, besteht darüberhinaus die Möglichkeit, einen zyklischen, automatischen Abgleich zu aktivieren. Hierdurch wird verhindert, dass sich Änderungen des magnetischen Umfeldes oder auch gravierende Schwankungen der Umgebungstemperatur negativ auf die Erfassungsreichweite auswirken.

Führt der Betrieb im nicht abgeglichenem Zustand oder auch die dauerhafte Überschreitung der zulässigen Umgebungstemperatur von 50°C zur Überhitzung der HF-Endstufe, schaltet der RFID-Server diese selbstständig ab. In der Betriebsart W&T Tag-Control wird dieses durch Blinken der LED *MODE* signalisiert. Netzwerkseitig verbundene Anwendungen erhalten ein entsprechendes Error-Paket. Nach Abkühlung führt der RFID-Server einen automatischen Neuabgleich durch und versucht den eingestellten Betriebsmodus W&T Tag-Control oder Protocol Mode neu zu starten.



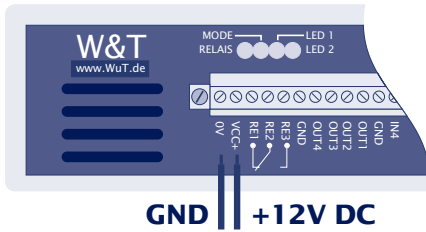
*Während eines automatisch oder auch manuell angestossenen Abgleichs der Antenne ist der RFID-Server für ca. 2s nicht in der Lage Tags zu erfassen.*

## **4 Anschlüsse und Anzeigen**

- Spannungsversorgung
- Der Netzwerkanschluss
- Digitale Ein-/Ausgänge
- LED-Anzeigen

## 4.1 Spannungsversorgung

Die Spannungsversorgung des RFID-Servers erfolgt über die 16 polige Schraubklemme an der Gehäusefrontseite mit folgender Polarität:



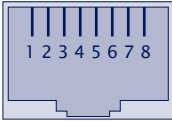
Die Versorgungsspannung muss 12V DC +/-5% betragen.

Zur Einhaltung der EMV-Richtlinien muss in die Zuleitung der Versorgungsspannung des RFID-Servers einer der zum Lieferumfang gehörenden Ferrite möglichst nahe am Gerät eingeschleift werden. Hierbei muss Versorgungskabel mindestens mit vier Wicklungen durch den Ferrit laufen. An dem optional erhältlichen W&T Steckernetzteil 11083 sind sowohl der Ferrit als die steckbare Schraubklemme bereits vormontiert.



## 4.2 Netzwerkanschluss

Der RFID-Server verfügt über einen IEEE 802.3 kompatiblen Netzwerkanschluss auf einem geschirmten RJ45-Steckverbinder. Die Belegung entspricht einer MDI-Schnittstelle, so dass der Anschluss an den Hub oder Switch mit einem 1:1 verdrahteten und geschirmten Patchkabel erfolgt.



Pin	Richtung	Funktion
1	Out	Tx+
2	Out	Tx-
3	In	Rx+
4	--	nc
5	--	nc
6	In	Rx-
7	--	nc
8	--	nc

### Auto Negotiation

Der RFID-Server arbeitet netzwerkseitig in der Betriebsart *Auto-Negotiation*. Datenübertragungsgeschwindigkeit und Duplex-Verfahren werden mit dem angeschlossenen Switch/Hub automatisch verhandelt und entsprechend eingestellt. In modernen Infrastrukturen wird das Ergebnis in der Regel 100BaseT/Full-Duplex sein.

Soll in managbaren Umgebungen der RJ45-Port des jeweiligen Switches auf einen bestimmten Modus fixiert werden, so muss als Duplex-Verfahren Halb-Duplex konfiguriert werden.

### Galvanische Trennung

Der Netzwerkanschluss ist gegenüber der Versorgungsspannung mit mindestens  $500V_{rms}$  galvanisch getrennt.

### Link-Status

Den aktuellen Link-Status signalisiert die *Error*-LED an der Gerätefront an. Blinkt diese im Abstand von 1–2 Sekunden auf, ist die Verbindung zum Hub nicht vorhanden bzw. gestört.

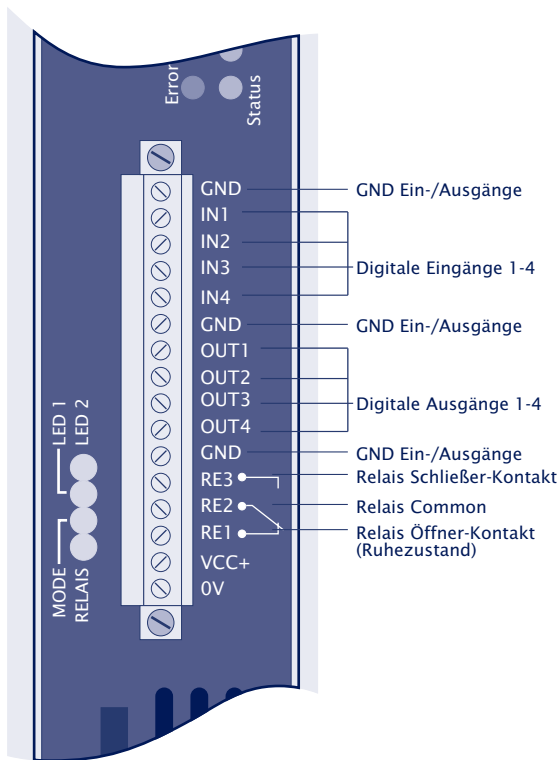


*Managebare Switches verfügen häufig über spezielle Protokolle (Spanning Tree Protocol, Port-Trunking, ...), wie sie z.B. für Uplinks zu anderen Switches oder den breitbandigen Anschluss von Servern benötigt werden. Diese Protokolle werden für die Anbindung gewöhnlicher Endgeräte wie den RFID-Server in der Regel nicht benötigt, verzögern den Kommunikationsaufbau nach einem Neustart unter Umständen aber erheblich. Wir empfehlen diese Protokolle und Funktionen, an dem für den RFID-Server verwendeten Port zu deaktivieren. Wenden Sie sich hierfür bitte an den zuständigen Netzwerk-administrator.*

### 4.3 Digitale Ein-/Ausgänge

Der RFID-Server verfügt über jeweils vier digitale Ein- und Ausgänge mit gemeinsamen Bezugspotential. Die galvanische Trennung gegenüber der Masse der Versorgungsspannung ist durch Optokoppler gewährleistet. Darüberhinaus steht ein potentialfreier Relais-Umschaltkontakt zur Verfügung. Alle Signale sind auf die an der Gehäusefront befindliche, steckbare Schraubklemme geführt.

Im Modus *W&T Tag-Control* erfolgt der Zugriff auf die Ein- und Ausgänge entweder autark durch die geräteeigenen Filterregeln oder die externe netzwerkseitige Anwendung. Detailinformationen hierzu enthalten die Kapitel *W&T Tag-Control-Konfiguration* und *W&T Tag-Control - Netzwerkprotokoll*.

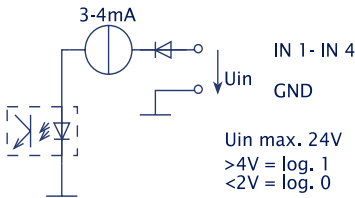


### 4.3.1 Digitale Eingänge

Der RFID-Server verfügt über vier digitale Eingänge mit folgenden Eckdaten:

- Eingangsspannung: 0-24VDC
- Eingangsstrom: 3-4mA über Stromquelle (Stromziehend)
- Schaltschwelle: 3V +/-1V (OFF: < 2V / ON: > 4V)

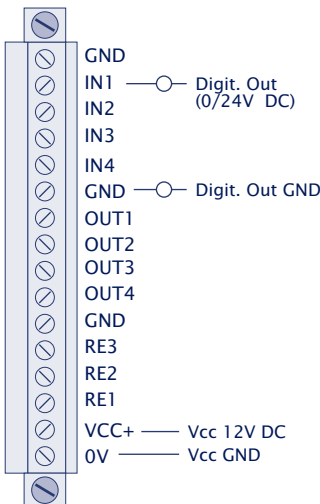
#### Prinzipschaltbild



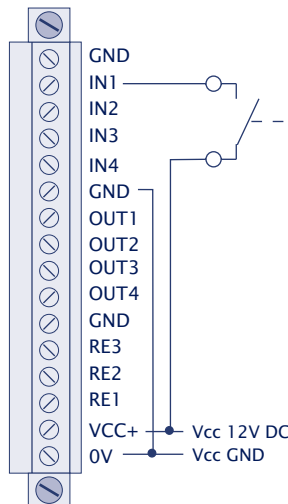
Bei einer Eingangsspannung >4V wird der Eingang netzwerkseitig auf den Status ON gesetzt. Eine Spannung < 2V entspricht dem Status OFF.

#### Beschaltungsbeispiel

Anschlussbeispiel für spannungsliefernde Ausgänge



Anschlussbeispiel für potentialfreie Kontakte

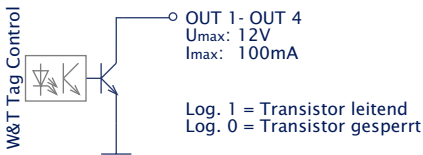


### 4.3.2 Digitale Ausgänge

Zur Ansteuerung externer Relais, Anzeigen usw. stellt der RFID-Server vier digitale Ausgänge in Open-Collector-Schaltung mit folgenden Eckdaten zur Verfügung.

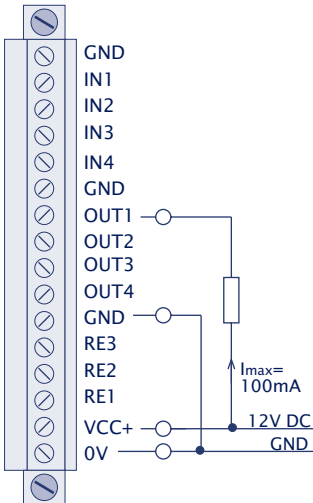
- Spannungsbereich: 0-12VDC
- max. Schaltstrom: 100mA
- Innenwiderstand: <math>< 17\Omega</math>

#### Prinzipschaltbild

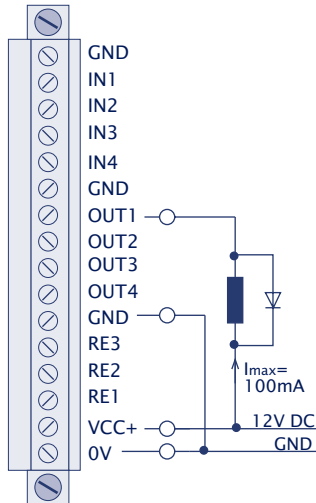


#### Beschaltungsbeispiel

Anschlussbeispiel mit ohmscher Last (z.B. Halbleiterrelais)



Anschlussbeispiel mit induktiver Last (z.B. Relaisspule)



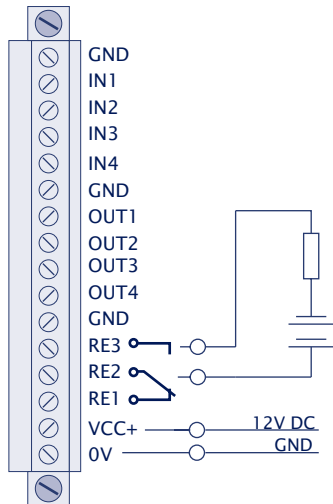
### 4.3.3 Relaisausgang

Für das potentialfreie Schalten externer Verbraucher verfügt der RFID-Server neben den Open-Collector-Ausgängen über ein Relais mit einem Umschaltkontakt.

- max. zulässige Schaltspannung: 48V DC
- max. Schaltstrom: 2A
- max. Schaltfrequenz: 1.800/hour  
(1s=ON 1s=OFF)

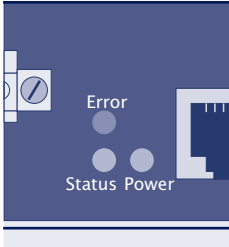
### Beschaltungsbeispiel

Anschlussbeispiel Relaiskontakt



## 4.4 LED-Anzeigen

### 4.4.1 Power und Netzwerkstatus

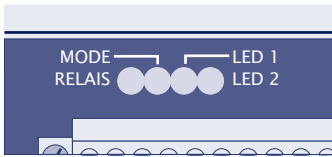


- **Power**  
Signalisiert das Anliegen der Versorgungsspannung. Sollte die LED nicht leuchten, überprüfen Sie bitte den korrekten Anschluss der Versorgungsspannung.
- **Status**  
Diese blitzt bei jeglicher Netzwerkaktivität des RFID-Servers auf. Periodisches Blinken signalisiert, dass Verbindung zu einem Teilnehmer im Netzwerk besteht.
- **Error**  
Die Error-LED signalisiert den Link-Status der Ethernet-Schnittstelle. Hat sich der RFID-Server ordnungsgemäß mit einem Hub/Switch verbunden, ist die Error-LED konstant aus. Empfängt der RFID-Server keine gültigen Link-Signale wird dieses durch periodisches Blinken angezeigt. Mögliche Ursachen hierfür sind ...
  - ... falsch verdrahtete Patchkabel oder RJ45-Dosen
  - ... fehlende Konnektierung der RJ45-Dose am Switch
  - ... Kabelbrüche
  - ... ein ausgeschalteter Switch/Hub

Konstantes Leuchten der Error-LED signalisiert einen nicht korrekt beendeten Selbsttest des TCP/IP-Stacks. Der RFID-Server ist in diesem Zustand nicht mehr betriebsfähig.

Tritt der Fehler als Folge eines vorzeitig abgebrochenen Firmware-Updates auf, so starten Sie diesen unter Verwendung der alten IP-Adresse erneut. Sollte sich das Problem nicht beheben lassen oder unabhängig von einem vorangegangenen Firmware-Update auftreten, schicken Sie das Gerät bitte zwecks Überprüfung ein.

#### 4.4.2 RFID-Status



##### ■ **MODE**

Die Mode-LED signalisiert die aktuelle Betriebsart des RFID-Servers sowie den Status der für die Erfassung von Tags zuständigen HF-Moduls.

##### **MODE-LED = ON**

Der RFID-Server befindet sich in der Betriebsart *W&T Tag-Control* und ist unter Berücksichtigung der im Setup hinterlegten Filterregeln bereit für die Erfassung von Tags.

##### **MODE-LED = Blinken**

Der RFID-Server befindet sich in der Betriebsart *W&T Tag-Control*, das HF-Modul wurde jedoch aufgrund von Über-temperatur automatisch abgeschaltet. In diesem Zustand können keine Tags erfasst werden. Mögliche Ursachen hierfür sind ...

- ... längerer Betrieb ohne einen vorherigen Abgleich der internen Antenne
- ... längerer Betrieb bei einer zu hohen Umgebungstemperatur (> 50°C)
- ... gravierende Änderung der elektromagnetischen Umgebung nach Abgleich der internen Antenne



**MODE-LED = OFF**

Ein Internet-Browser hat sich in die WBM-Konfiguration eingeloggt. Es können keine Tags verarbeitet werden. Die TCP-Dienste *W&T Tag-Control* wie auch *Protocol-Mode* sind gestoppt.

**■ RELAIS**

Die Relais-LED signalisiert den aktuellen Status des internen Relais. Leuchtet die LED nicht, ist das Relais im Ruhezustand. Bei konstantem Leuchten ist das Relais angezogen. Die Zuordnung, welcher Kontakt im jeweiligen Zustand geschlossen ist, kann der Gehäusebedruckung entnommen werden.

**■ LED1 und LED2**

Die Funktionen der LED1 und LED2 können durch den Anwender über *Aktionen* der Filterregeln im Modus W&T Tag-Control frei konfiguriert werden. Ab Werk haben beide LEDs keine Funktion.



## **5 Web-Based-Management - Grundlagen**

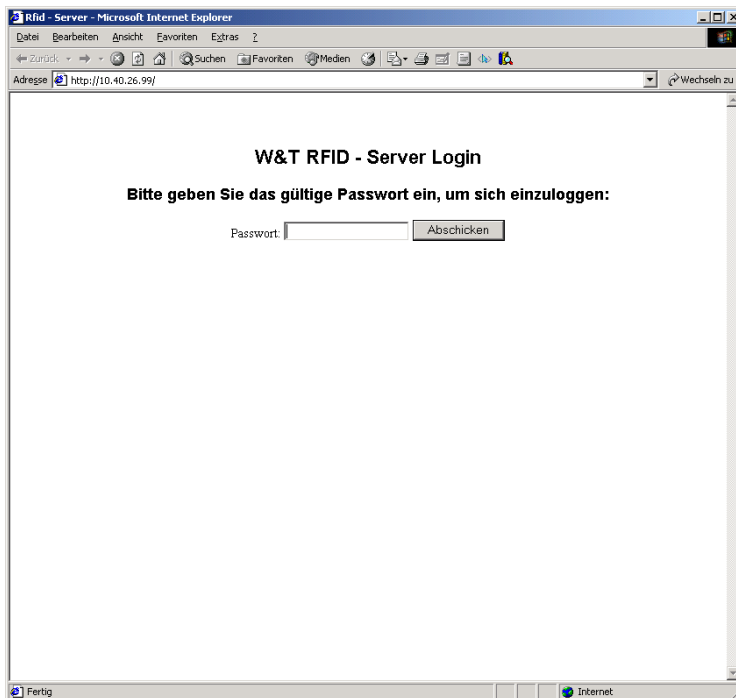
Nach Anschluss der Hardware und Vergabe der IP-Adresse, erfolgt die gesamte weitere Konfiguration der RFID-Servers über das Netzwerk mit Hilfe des geräteinternen Web-Servers und einem Standard Internet-Browser.

- Die Navigation auf den Web-Seiten
- Struktur der Web-Seiten
- Übernahme und Aktivierung der Einstellungen

## 5.1 Start des Web Based Management

Die gesamte Konfiguration des RFID-Servers erfolgt über den integrierten Web-Server des RFID-Servers. Dieses **Web-Based-Management** erlaubt alle Einstellungen mit Hilfe eines Standard Internet-Browsers durchzuführen - unabhängig vom Betriebssystem des verwendeten Rechners.

Durch Eingabe der IP-Adresse bzw. der URL des RFID-Servers in die Adressleiste des Browsers gelangen Sie auf die WBM-Startseite. Alternativ kann zu diesem Zweck auch der Button *Browser* in WuTility betätigt werden.



Nach einem erfolgreichen Login in das WBM des RFID-Servers, sind alle weiteren Webseiten zweigeteilt. Auf der linken Seite befindet sich immer der Navigationsframe, den man mit dem Inhaltsverzeichnis eines Buches vergleichen kann. Rechts ist der Anzeige- und Konfigurationsframe platziert.

## 5.2 Web Based Management - Login und Navigation

Der WBM-Zugang arbeitet sessionorientiert und ist über das Systempasswort geschützt, welches auf der Startseite eingegeben werden muss. Ab Werk ist kein Systempasswort vergeben und das entsprechende Eingabefeld kann leer bleiben. Wurde im Zuge der Konfiguration ein Systempasswort eingestellt, muss dieses auf der Startseite eingegeben werden bevor der Button *Abschicken* betätigt wird.



*Der Start einer WBM-Session hat zur Folge, dass TCP-Verbindungen zu Anwendungen, die Tags verarbeiten, geschlossen werden. Eine Neuverbindung zu den Diensten W&T Tag-Control und Protocol-Mode ist erst nach dem Beenden der WBM-Session wieder möglich.*



*Der gleichzeitige Zugriff auf das WBM des RFID-Servers von mehreren Rechnern aus ist nicht möglich. Ist eine WBM-Session aktiv, wird der Versuch eines Verbindungsaufbaus von einem zweiten Rechner abgewiesen.*

### Login Timeout

Wird für mehr als 40 Sekunden keine Eingabe gemacht, beendet der RFID-Server selbstständig die aktuelle WBM-Session und es muss ein erneuter Login durchgeführt werden. Alle auf der aktuellen Konfigurationsseite gemachten Eingaben und Änderungen werden damit verworfen.

### 5.2.2 Die Navigation

Der Navigationsframe beinhaltet einen Verzeichnisbaum, in dem alle verfügbaren Menüpunkte des RFID-Servers nach Kategorien geordnet aufgelistet sind. Durch Mausklick auf die einzelnen Elemente werden entweder weitere Menüpunkte einer Kategorie angezeigt und/oder ein neuer Inhalt im Konfigurationsframe aufgebaut.



*Vermeiden Sie die Benutzung der Schaltflächen Vor und Zurück Ihres Browsers. Verwenden Sie zur Navigation ausschließlich den Navigationsbaum bzw. die Buttons und*

*Links des WBM. Anderenfalls können im Hintergrund zwischengespeicherte Parameter beim Weiterspringen verloren gehen.*

Die Icons im Menübaum haben dabei folgende Bedeutung:



Haupt- oder Unterkategorie mit Verzweigungen zu weiteren Inhalten. Ein Mausklick auf dieses Symbol erweitert den Menübaum.



Haupt- oder Unterkategorie mit Verzweigungen zu weiteren Inhalten. Ein Mausklick auf dieses Symbol erweitert den Menübaum und zeigt einen neuen Inhalt im Konfigurationsframe.



Zeigt an, dass weitere Unterkategorien oder Inhalte vorhanden sind. Ein Mausklick auf dieses Symbol erweitert den Menübaum, ändert aber nicht den Inhalt des Konfigurationsframes.



Durch Mausklick auf dieses Icon wird der erweiterte Verzeichnisbaum wieder geschlossen.



Kennzeichnet eine Konfigurationsseite, die durch Mausklick im Konfigurationsframe angezeigt wird.

### 5.2.3 Speicherung und Aktivierung der Einstellungen

Alle Eingaben und Änderungen auf einer Webseite, werden zunächst vom Browser lediglich zwischengespeichert.

Für das Speichern der Einstellungen im RFID-Server, das Zurücksetzen von Änderungen sowie das Beenden einer WBM-Session verfügen die Konfigurationsseiten über drei Buttons.

Speichern

Die auf der jeweiligen Seite vorgenommenen Einstellungen werden an den RFID-Server übertragen und dort in den nicht-flüchtigen Speicher übernommen. Bei Änderungen der netzwerkseitigen Basisparameter führt der RFID-Server anschließend automatisch einen Neustart durch und für weitere Einstellungen muss eine neue WBM-Session aufgebaut werden.

Rücksetzen

Alle seit Aufruf der jeweiligen Webseite vorgenommenen Änderungen werden rückgängig gemacht und auf ihre ursprünglichen Werte zurückgesetzt. Es erfolgt keine Übertragung der Parameter an den RFID-Server.

Logout

Die WBM-Session zum RFID-Server wird beendet. Eventuell auf der jeweiligen Webseite vorgenommene Einstellungen müssen *vorher* mit Hilfe des Buttons *Speichern* gesichert werden. Mit Beendigung der WBM-Session wird automatisch der eingestellte Kommunikationsmodus *W&T Tag-Control* oder *Protocol-Mode* gestartet, so dass sich Tag-verarbeitende Client-Anwendungen wieder mit dem RFID-Server verbinden können.





## **6 WBM - Allgemeine Konfiguration**

Dieses Kapitel beschreibt neben der Konfiguration aller Basisparameter auch die Diagnose-Möglichkeiten.

- Session Control
  - Einstellen der Passwörter
  - Gerätereset / Werkseinstellungen
- Device
  - Einstellen der Netzwerkparameter
  - Einstellen der Systemuhr
  - Einstellen des Betriebsmodus
- Gesamtkonfiguration Sichern / Wiederherstellen
- Diagnose

## 6.1 Session Control

Neben der Möglichkeit einen Reset des RFID-Servers zu veranlassen, beinhaltet der Menüweig *Session Control* auch die Konfigurationsseite der Passwörter.

### 6.1.1 Session Control >> Reset ...



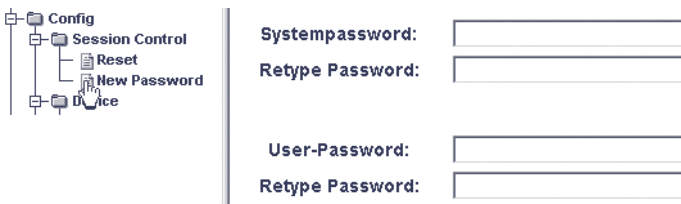
#### ... Hardware Reset

Die Betätigung des Button *Hardware Reset* hat die gleiche Funktion, wie ein Aus-/Einschalten des RFID-Servers. Nach dem Reset startet der RFID-Server die konfigurierte Betriebsart *W&T Tag-Control* oder *Protocol-Mode*.

#### ... Restore Factory Defaults

Die gesamte Konfiguration des RFID-Servers inklusive der IP-Adresse wird durch Betätigen des Buttons *Restore Factory Defaults* auf die Werkseinstellungen zurückgesetzt. Die IP-Adresse lautet anschließend 0.0.0.0 und muss neu vergeben werden (siehe Kapitel *Vergabe der IP-Adresse*).

### 6.1.2 Session Control >> New Password ...



Der Zugänge zum Web Based Management sowie zu den Datendiensten für die Tag-Kommunikation können über zwei separate Kennwörter geschützt werden. Die Kennwörter dürfen nicht

gleich sein und müssen sich in mindestens einem Zeichen unterscheiden.

Ab Werk ist weder ein Systempasswort noch ein User Passwort vergeben. Das Eingabefeld beim Start des WBM kann leer bleiben. Nach Aufbau der TCP-Verbindung zur *W&T Tag-Control* muss kein User Passwort gesendet werden.

Nach Vergabe der neuen Passwörter und Betätigen des Buttons *Speichern* führt der RFID-Server automatisch einen Reset durch.

### **... Systempasswort**

Das Systempasswort schützt die nachfolgend aufgeführten Konfigurations- und Steuerzugänge des RFID-Servers. Es ist auf eine Länge von maximal 31 Zeichen begrenzt.

- WBM-Port (konfigurierbar, ab Werk = 80)
- Reset-Port (nicht konfigurierbar, 8888)

Beim Zugriff auf das WBM des RFID-Servers muss das Systempasswort auf der Web-Seite eingegeben werden. Bei Nutzung des Reset-Ports muss das Systempasswort nullterminiert ([password] + 0x00) bis spätestens 2s nach dem Öffnen der TCP-Verbindung an den RFID-Server gesendet werden (siehe Kapitel *Reset des RFID-Server über das Netzwerk*).

### **... User Password**

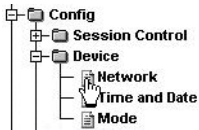
Das User Passwort schützt die Netzwerk-Kommunikation mit dem Modus *W&T Tag-Control* und dem *Protocol-Port* vor unautorisiertem Zugriff. Das Kennwort ist auf 31 Zeichen begrenzt.

Wurden alle Eingaben gemacht, klicken Sie auf den *Speichern*-Button. Damit werden die Parameter in den RFID-Server übertragen und es wird automatisch ein Neustart durchgeführt.

## 6.2 Device

Der Menüzeitweig *Device* enthält die Konfigurationsseiten zur Einstellung der netzwerkseitigen Basisparameter, der integrierten Echtzeituhr sowie der Betriebsart zur Erfassung von Tags.

### 6.2.1 Device >> Network



#### Config >> Device >> Network

IP-Address :

Subnetmask :

Gateway :

**Wichtig :**  
Im Zweifelsfall 'BOOTP' und 'DHCP' abschalten!

IP allocation:  Static (BOOTP & DHCP **disabled**)

BOOTP Client :  BOOTP **enable**

DHCP Client :  DHCP **enable**

Leasetime : 0 Minuten

HTTP-Config Port :

W&T Tag-Control Port :

Protocol Port:

Systemname:

DNS1 :

DNS2 :

Wurden alle Eingaben gemacht, klicken Sie auf den *Speichern*-Button. Die Parameter werden an den RFID-Server übertragen und es wird automatisch ein Neustart durchgeführt.

### IP Adresse

Die IP-Adresse kann an dieser Stelle geändert werden. Sollte sich die neue IP-Adresse nicht im gleichen Subnet wie der für die Konfiguration verwendete Rechner befinden, ist der RFID-Server nach dem Speichern unter Umständen nicht mehr erreichbar.



*Jede IP-Adresse muss immer netzwerkweit eindeutig sein.*



*Bei Fehleingaben ist - unabhängig von der aktuellen Adresse des RFID-Servers - das Ändern der IP-Adresse jederzeit über das Inventarisierungstool Wutility möglich (siehe Kapitel Vergabe der IP-Adresse)*

### Subnet Mask / Gateway

In gerouteten Netzwerkumgebungen müssen die passende Subnet Mask sowie die IP-Adresse des Gateway eingetragen werden. Beide Parameter erhalten Sie von dem zuständigen Netzwerkadministrator.

### BOOTP-/DHCP Client

Zur Vermeidung ungewollter Adressvergaben oder Adressänderungen, empfehlen wir die Protokolle BOOTP und DHCP zu deaktivieren, sofern diese nicht explizit in der jeweiligen Netzwerkumgebung verwendet werden.

Erhält der RFID-Server seine Netzwerkparameter von einem DHCP-Server, wird die verbleibende Lease-Time angezeigt (siehe Kapitel *IP-Vergabe per DHCP-Protokol*)

### WBM-Port

Die Portnummer für das Web Based Management kann hier verändert werden. Ab Werk ist der HTTP-Standardport 80 konfiguriert. Wird hier eine andere Portnummer eingestellt, muss diese beim Aufruf des WBM in der Adresszeile des Browsers angegeben werden (z.B. `http://10.10.10.20:8080`)

### W&T Tag-Control Port

Über den hier konfigurierten TCP-Port kann ein Client auf den Modus *W&T Tag Control* zugreifen. Ab Werk ist der Port 2683 voreingestellt.

### Protocol Port

Über den hier konfigurierten TCP-Port kann ein Client auf den *Protocol Mode* zugreifen. Ab Werk ist der Port 2684 voreingestellt.



*WBM-Port, W&T Tag-Control-Port und Protokoll-Port müssen sich voneinander unterscheiden. Es dürfen keine gleichen Portnummern für unterschiedliche Dienste verwendet werden.*

### Systemname

Bei mehreren RFID-Servern in einem Netzwerk erlaubt der Systemname die Unterscheidung der Geräte innerhalb der Anzeige des Inventarisierungstools *WuTility*. Darüberhinaus wird der Systemname auch zur Identifizierung gegenüber einem DHCP-Server verwendet.

Zur Erzeugung eines einzigartigen Systemnamens kann mit dem Button *MAC-Adresse anhängen* ein spezielles Schlüsselwort (<wut1>) eingefügt werden. Dieses wird bei der Ausgabe an *WuTility* und bei Verwendung des DHCP-Protokolls vom RFID-Server durch die letzten sechs Stellen (3-Byte) der weltweit eindeutigen Ethernet-Adresse ersetzt.

### DNS

Bei einigen Netzteilnehmern, wie z.B. Timeserver, ist es sinnvoll, diese nicht über Ihre IP-Adresse sondern über einen Namen zu adressieren. Dazu muss ein DNS-Server angegeben werden.

## 6.2.2 Device >> Time and Date

### Config >> Device >> Date and Time

Time :	<input type="text" value="10"/> : <input type="text" value="37"/>
Offset :	<input type="text" value="1"/>
Day :	<input type="text" value="25"/> Mittwoch
Month :	<input type="text" value="07"/>
Year :	<input type="text" value="2007"/>
NTP enable :	<input type="checkbox"/> Apply TimeServer
Timeserver1 :	<input type="text"/> <input type="button" value="Abfragen"/>
Timeserver2 :	<input type="text"/> <input type="button" value="Abfragen"/>
Synchronisation at :	<input type="text" value="00"/> : <input type="text" value="00"/>
<input type="button" value="Speichern"/> <input type="button" value="Rücksetzen"/> <input type="button" value="Logout"/>	

Der RFID-Server verfügt über eine Echtzeituhr mit Datumsfunktion. Uhrzeit und Datum sind werksseitig voreingestellt und können auf dieser Konfigurationsseite umgestellt werden. Die Uhr ist durch eine interne Batterie gestützt, so dass die eingestellte Zeit auch ohne Anschluss der Spannungsversorgung erhalten bleibt.

#### Time

Geben Sie die neue Uhrzeit im Format *hh:mm* an.

#### Offset

Offset der lokalen Uhrzeit zur UTC-Zeit. Für die deutsche Winterzeit lautet der Offset +1 (= UTC+1). Bei Sommerzeit entsprechend +2 (= UTC+2).

#### Day

Tag der Datumsanzeige im Format *dd*.

**Month**

Monat der Datumsanzeige im Format *mm*.

**Year**

Jahr im Format *yy*.

**NTP enable**

Automatischer Zeitabgleich am NTP-Server einschalten

**Timeserver**

Adresse des Timeservers (maximal 2), über den Button *Abfragen* wird ein Verbindungstest durchgeführt und auf das Ergebnis angezeigt.

**Synchronisation at**

Die Uhrzeit, zu der der RFID-Server eine Synchronisation mit dem Timeserver vornehmen soll.

**6.2.3 Device >> Mode**

**Config >> Device >> Mode**

**Mode:**

- W&T Tag Control Mode
- Iso Protocol Mode

Speichern    Rücksetzen    Logout

Für den produktiven Einsatz und die Verarbeitung von Tags stellt der RFID-Server zwei Betriebsarten zur Verfügung. Nach einem Neustart des Gerätes sowie nach Beendigung einer WBM-Session wird der hier eingestellte Modus automatisch aktiviert.

**W&T Tag-Control Mode**

Die aufwändige Abarbeitung der HF-Kommunikation nach ISO15693 wird hierbei vollkommen selbstständig vom RFID-Server übernommen. Erfassung und Verlust von Tags stellen Ereignisse dar, welche vom Anwender festlegbare Filterregeln durchlaufen. Wurde eine Filterregel durchlaufen, wird als deren Ergebnis eine Aktion ausgeführt. Diese kann zum Beispiel aus dem Schalten eines Ausganges oder auch der netzwerkseitigen



Übertragung des Ereignisses an einen Client bestehen (siehe Kapitel *W&T Tag Control - Konfiguration*).

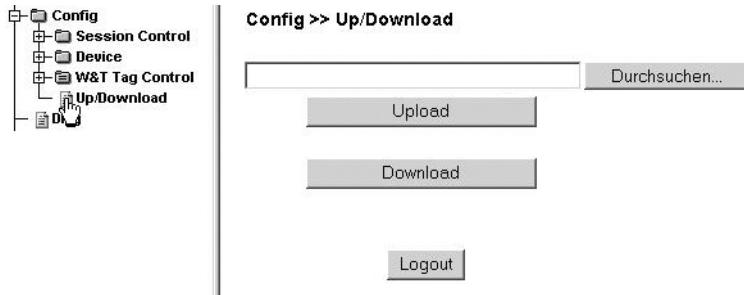
### **Protocol Mode**

In diesem Modus arbeitet der RFID-Server quasi als Gateway zwischen dem Netzwerk und der HF-Schnittstelle. Alle Kommandos des Standards ISO15693-3 können über das Netzwerk an den RFID-Server gesendet werden, welcher diese dann auf der HF-Schnittstelle ausführt. Die Netzwerkanwendung muss hierbei alle Aufgaben wie zum Beispiel Tag-Inventarisierung, Kollisionsbehandlung usw. übernehmen (siehe Kapitel *Protocol Mode*).



*Mit dem Start einer WBM-Session wird der eingestellte Betriebsmodus unterbrochen. Es werden keine Tags mehr erfasst und eventuell bestehende TCP-Verbindungen zu Netzwerk-Clients werden unterbrochen. Der eingestellte Betriebsmodus wird wieder gestartet, sobald die WBM-Session beendet wird.*

## 6.3 Up-/Download - Konfigurationsprofile



Der RFID-Server bietet dem Anwender die Möglichkeit, alle im Web-Based-Management vorgenommenen Einstellungen als Binärdatei vom Gerät herunterzuladen oder gespeicherte Einstellungen wieder einzuspielen.

### Download

Die gesamte Konfiguration des RFID-Server wird als Binärdatei abgerufen. So kann der Anwender bei Projekten mit mehreren gleich konfigurierten RFID-Servern an einem Gerät die Grundkonfiguration vornehmen, diese auslesen und später in die anderen Geräte einspielen.

Betätigen Sie für den Abruf der Konfigurationsdatei den Button *Download* und speichern Sie die Datei unter dem gewünschten Namen ab.

### Upload

Um eine gespeicherte Konfiguration in den RFID-Server einzuspielen wählen Sie über den Dialog *Durchsuchen...* die gewünschte Datei aus. Mit Betätigung des Buttons *Upload* wird die Übertragung gestartet und das Gerät führt anschließend automatisch einen Neustart durch.



*Bei der Übertragung von Binärdateien an einen RFID-Server werden alle darin enthaltenen Einstellungen außer der IP-Adresse übernommen.*

## 6.4 Diagnose und Abgleich

**Config >> Diag**

Browser: MS Internet Explorer

Endstufentemperatur: 39°C

Pegel 1: 1139

Pegel 2: 942

Pegel 3: 252

Spannung 1: 4.97 V

Spannung 2: 4.94 V

Spannung 3: 11.67 V

Abgleich 1: 0708

Abgleich 2: 151

Abgleich 3: 96

Status: 0x0000

abgleichen

Logout

Auf der Diagnosesseite des WBM besteht die Möglichkeit einen manuellen Abgleich der integrierten Antenne des RFID-Servers durchzuführen. Ein solcher Abgleich ist zum Beispiel notwendig, wenn sich der Einsatzort des RFID-Servers oder dessen magnetisches Umfeld ändert.

Für den Modus *W&T Tag-Control* besteht neben dem hier beschriebenen manuellen Antennenabgleich auch die Möglichkeit einen zyklischen automatischen Abgleich durchführen zu lassen.

Bei den ausgegebenen Messwerten handelt es sich um interne Schaltungsparameter, welche für den Anwender im Normalfall keine Bedeutung haben.



*Während eines Abgleichs dürfen sich keine Tags in der Erfassungsreichweite des RFID-Servers befinden. Ggf. ist der Abgleich nach Entfernen des/der Tags zu wiederholen.*



# 7 W&T Tag-Control - Konfiguration

In diesem Kapitel wird die Funktionsweise und Konfiguration des Modus W&T Tag-Control beschrieben.

- Aufbau
- Filter
- Tag-Listen
- Time Condition
- Input Condition
- Aktion
- Master (Filterset)

## 7.1 Aufbau des W&T Tag Control

Im Modus *W&T Tag-Control* scannt der RFID-Server ständig seinen Erfassungsbereich ab. Neuerkennung sowie auch der Verlust von Tags stellen Ereignisse dar, welche zusammen mit der individuellen Tag-ID, den vom Anwender konfigurierbaren *Filtersets* zugeführt werden.

Wenn die *Action* eines Filtersets gesetzt ist, werden die Bedingungen - sofern gesetzt - nacheinander wie folgt geprüft, wobei das Ergebnis entweder *Wahr* oder *Falsch* lautet.

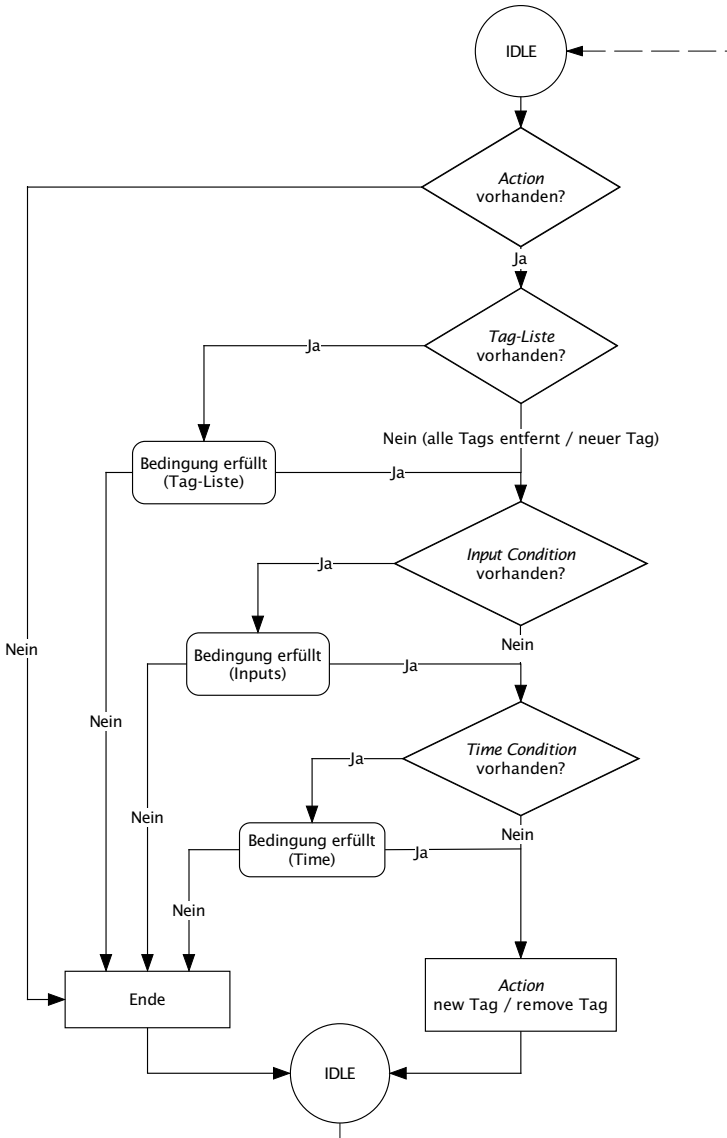
- Tag-Listen  
Ist die erkannte Tag-ID Bestandteil der Tag-Liste?
- Time Condition  
Ist die aktuelle Zeit innerhalb des konfigurierten Zeitfensters?
- Input Condition  
Entspricht der aktuelle Status der digitalen Eingänge dem konfigurierten Status?

Ist das Resultat einer dieser Prüfungen *Falsch*, wird das Filterset ohne weitere Aktion verlassen.

Haben alle Prüfungen innerhalb eines Filtersets das Ergebnis *Wahr*, wird die vom Anwender konfigurierte *Action* durchgeführt. Folgende Möglichkeiten bestehen:

- Schalten digitaler Ausgänge
- Schalten des Relais
- Akustisches Signal des integrierten Summers
- Speichern der Ereignisse
- Senden der Tag-ID mit Zeitstempel an eine verbundene TCP-Client-Anwendung

Der detaillierte Entscheidungsablauf, wie er bei jedem Tag-Ereignis durchgeführt wird, kann dem folgenden Flussdiagramm entnommen werden.



### Beispiel

Mit der Werkseinstellung ist das *Filterset 1* so konfiguriert, dass die Erfassung und der Verlust *jedes* Tag mit einem langen bzw. kurzen Signalton quittiert werden. Hierfür befinden sich auf der Konfigurationsseite des Filtersets folgende Einstellungen:

## Config &gt;&gt; W&amp;T Tag Control &gt;&gt; MASTER &gt;&gt; Filterset 1

		beachten ignorieren		
TAG-List:	Liste 1	<input type="checkbox"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
	Liste 2	<input type="checkbox"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
	Liste 3	<input type="checkbox"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
	Liste 4	<input type="checkbox"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
	Liste 5	<input type="checkbox"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
	Liste 6	<input type="checkbox"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
	Liste 7	<input type="checkbox"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
	Liste 8	<input type="checkbox"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>

**Input Condition:**

**Time Condition:**

**Action:**

<input type="text" value="action 1"/>	TAG kommt
<input type="text" value="action 2"/>	TAG geht

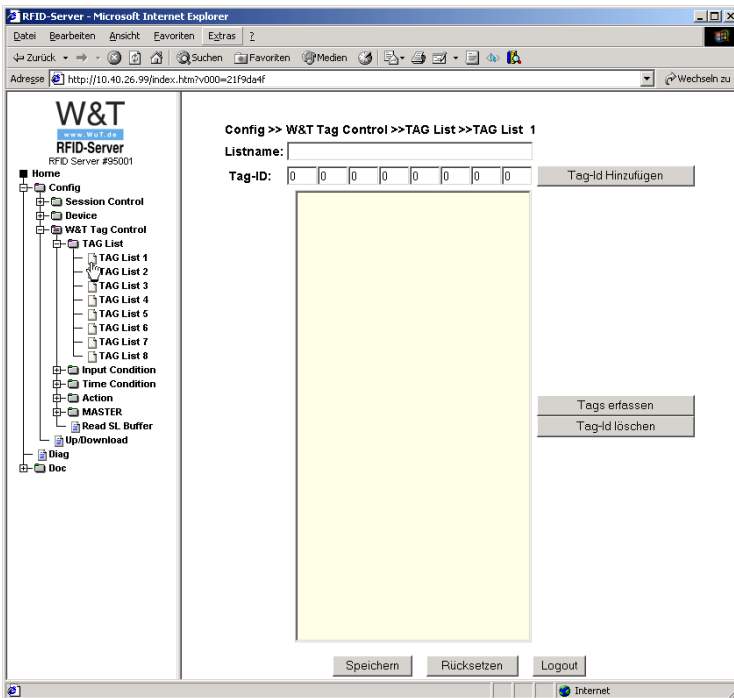
Die Bedingungen *Tag-List*, *Input Condition* und *Time Condition* sind leer. Unter *Action* ist bei der Neuerfassung eines Tags die *Action 1* (langer Ton) und bei Verlust die *Action 2* (kurzer Ton) konfiguriert.

Details zur Definition der Filtersets sowie deren Bedingungen und Aktionen enthalten die folgenden Kapitel.



## 7.2 Filter TAG- Listen

Jedes Tag hat eine individuelle ID die aus 8 Bytes besteht und das Tag eindeutig identifiziert. Diese ID kann in einer Liste hinterlegt werden und so eine Gruppierung der vorhandenen Tags erreicht werden (z.B. Gruppe Administratoren). Die Listen können durch einen 20 stelligen Namen beschrieben werden, um jeder Gruppe einen individuellen Namen zu geben.



## 7.3 Filter Time Condition

Die Zeitbegrenzung ist sehr flexibel einstellbar, sie reicht von einem klar begrenzten Bereich (z.B. 12.12.2005 7.00 Uhr bis 13.12.2005 17.00 Uhr) bis zu einer sich zyklisch wiederholenden Periode (z.B. jeden Mittwoch ganztägig).

The screenshot shows the configuration page for 'Time Condition 1'. The table below summarizes the visible settings:

Parameter	Von	Bis	möglicher Zahlenbereich
Minute:	00	00	0-59
Hour:	00	00	0-23 (0 ist Mitternacht)
Day:	00	00	1-31
Month:	00	00	1-12
Year:	00	00	00-99

**Weekday:**

- Sonntag
- Montag
- Dienstag
- Mittwoch
- Donnerstag
- Freitag
- Samstag

Der Filter setzt sich aus folgender Struktur zusammen:

Start und Stop

Jahr  
 Monat  
 Tag  
 Stunde  
 Minute

optional Wochentag

### Wochentag

Die Einträge Start und Stop geben jeweils die Anfangs- bzw. Endzeitpunkte eines Zeitraums vor. Optional können für diese Periode auch Wochentage festgelegt werden.

Wenn in einem der Elemente Jahr, Monat oder Tag des Zeitraums nichts definiert wird, ist es ab bzw. von diesem Zeitpunkt an immer aktiv! Ist also der Startmonat 05 und als Stopmonat nichts festgelegt, gilt der Zeitraum von 05 (Mai) bis zum Ende des Jahres (Dezember).

Beispiel:

Die Regel ist jedes Jahr zwischen dem 05.07. 08.00 Uhr und dem 06.07. 18.00 Uhr erfüllt.

	Jahr	Monat	Tag	Stunde	Minute
Start	Leer	07	05	08	00
Stop	Leer	07	06	18	00
Wochentag	Leer				

Die Regel ist jeden Samstag und Sonntag zwischen 08.00 Uhr und 18.00 Uhr erfüllt.

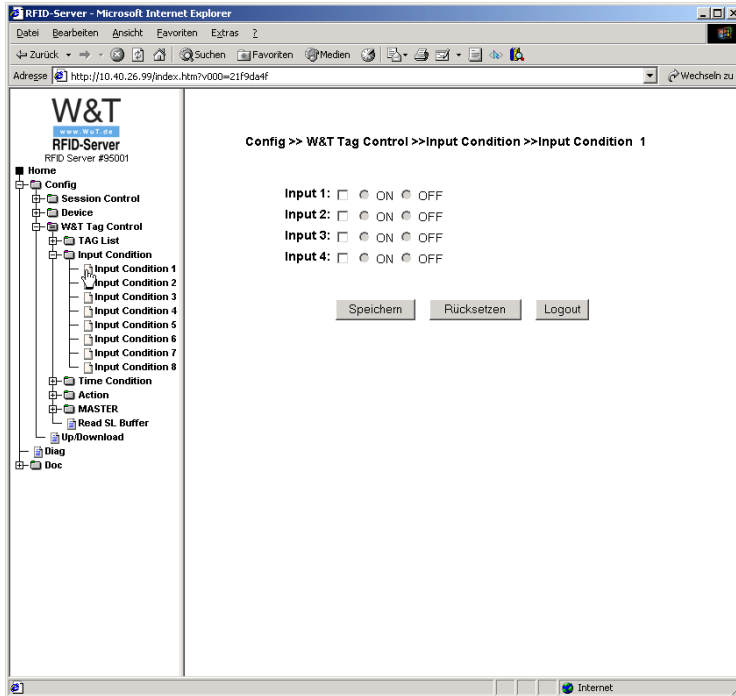
	Jahr	Monat	Tag	Stunde	Minute
Start	Leer	Leer	Leer	08	00
Stop	Leer	Leer	Leer	18	00
Wochentag	Samstag Sonntag				

Die Regel ist jedes Jahr ab Juli an jedem Samstag und Sonntag zwischen 08.00 Uhr und 18.00 Uhr erfüllt.

	Jahr	Monat	Tag	Stunde	Minute
Start	Leer	07	05	08	00
Stop	Leer	Leer	Leer	18	00
Wochentag	Samstag Sonntag				

## 7.4 Filter Input Condition

Der logische Zustand an einem Eingang kann als Filter genutzt werden.

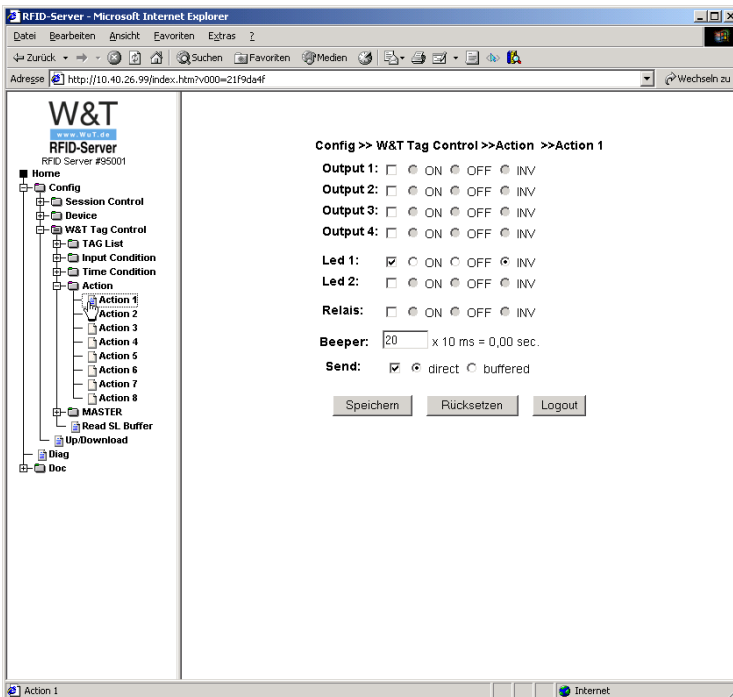


Jeder der vier Eingänge kann mit dem Zustand „Ein“ oder „Aus“ als Filter genutzt werden, falls der Eingang beschaltet ist.

## 7.5 Aktionen

Nachdem ein TAG die Filter durchlaufen hat und nicht aussortiert wurde, können verschiedene Aktionen durchgeführt werden.

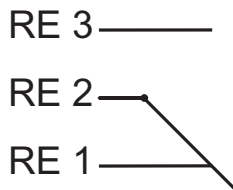
- Setzen der digitale Ausgänge
- Setzen der LEDs 1 und 2
- Schalten des Relais
- akustisches Signal (Summer)
- Meldung an Clientanwendung



Die Aktionen können jeweils beim Erkennen und / oder beim Verlassen eines neuen Tags im Erkennungsbereich des RFID-Servers ausgeführt werden (siehe 4.4 Filterset). Es können 8 frei konfigurierbare Aktionslisten definiert werden.

Wird mit Hilfe eines Tags eine Aktion ausgeführt, so können die digitalen Ausgänge und LEDs jeweils an, aus oder invertierend geschaltet werden.

Als weitere Aktion kann das Relais geöffnet oder geschlossen werden.



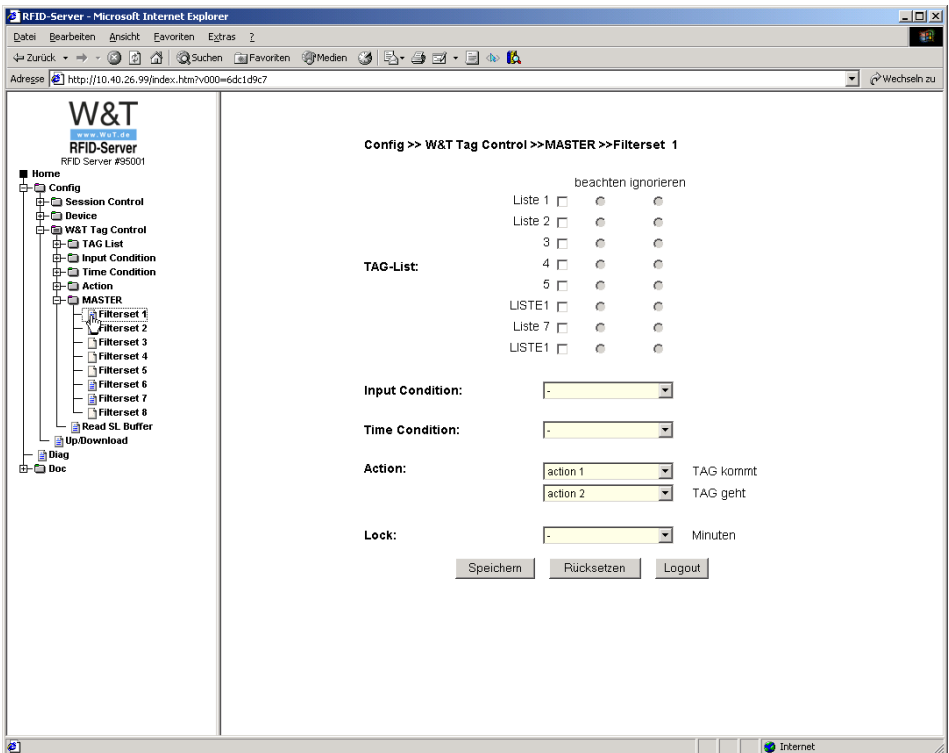
Zusätzlich kann ein akustisches Signal über den Summer von 0,01 Sek. bis 2,55 Sek. erzeugen werden.

Die Option TAG-Daten senden verschickt die aktuelle TAG-ID inklusive des Status und eines Zeitstempels sowie die vom TAG ausgelöste Filtersetnummer.

Die TAG-Daten können direkt versendet werden, d.h. sie werden sofort nach Auslösen der Aktion an den Client versendet. Steht zu diesem Zeitpunkt keine Netzwerkverbindung zur Verfügung, ist die Meldung verloren. Als sicherere Option können die TAG-Daten im Gerät zwischengespeichert werden. Die Daten werden dann in einen Ringbuffer geschrieben und müssen explizit per Befehl aus dem Buffer gelesen werden. Mittels einer Quittung, die von der Clientanwendung gesendet werden muss, wird dann die Meldung aus dem Ringbuffer gelöscht. Soll keine Meldung erfolgen, muss die Option „keine Daten senden“ aktiviert werden. Mit dieser Option wird dann keine Protokollierung der kommenden und gehenden Tags erzeugt.

## 7.6 Master (Filterset)

In einem Filterset werden Filter und Aktionen festgelegt. Die Filter dienen zur Sortierung, der in den Erfassungsbereich ein- und austretenden Tags. Aktionen werden nur dann ausgeführt, wenn das Tag nicht durch die Filter aussortiert wurde. Filtersets verknüpfen die einzelnen Filter-Elemente des W&T Tag Control zu einer Funktionseinheit. Ein Filterset muss **mindestens eine Aktion** beinhalten, entweder bei kommendem oder gehendem TAG.



Ein Filterset besteht aus 6 Elementen, die beliebig kombiniert werden können. Es setzt sich zusammen aus vier Filtern und einer Aktion beim Erfassen eines Tags und einer weiteren Aktion beim Verlassen des Erfassungsbereichs eines Tags.

- TAG-Listen-Filter
- Zeitbegrenzungs-Filter
- Zustand der digitalen Eingänge
- Wiedererkennungs-Filter

Der Filter „TAG-Listen“ ist in zwei Bereiche unterteilt. Hier können die in Gruppen (siehe Kap. 2.3) zusammengefassten TAG-IDs zur Verarbeitung in dem W&T Tag Control zugelassen oder ignoriert werden. Die Gruppen können in beliebigen Kombinationen zugelassen oder ignoriert werden. Ist in der Zugelassen-Liste keine Gruppe eingetragen, werden **alle TAG-IDs zugelassen!**

*Enthält die TAG-Liste keinen Eintrag, werden alle RFID-TAGs (beliebige TAG-ID) zur Weiterverarbeitung genutzt!*

Beispiel:

Liste 1: Administratoren

Liste 2: Kunden

Liste 3: Mitarbeiter

In dem Filter *Time Condition* werden Zeiträume festgelegt, zu denen das Filterset aktiv ist. Ist kein Zeitraum eingetragen, ist dieses Filterset immer aktiv.

Als weitere Filterbedingung können die logischen Zustände der vier digitalen Inputs genutzt werden. Diese können beliebig kombiniert werden.

Die Wiedererfassungszeit eines TAGs ist in der Grundeinstellung auf Null gesetzt. Das heißt, wenn ein TAG den Erfassungsbereich verlässt und sofort wieder eintritt, wird das TAG erneut verarbeitet. Wird eine Zeit grösser Null eingestellt, so



wird diese TAG-ID für die eingestellte Zeit gesperrt. Es können Sperrzeiten von 0 bis 255 min. eingestellt werden.

Aktionen können jeweils beim Eintreten oder Verlassen eines TAGs in den Erfassungsbereich des RFID-Servers, ausgeführt werden. Jedes Filterelement besteht aus einer der 8 Listen, die zuvor konfiguriert wurden.



# 8 W&T Tag-Control - Netzwerkprotokoll

Im Modus W&T Tag-Control stellt der RFID-Server einen TCP-Server-Dienst zur Verfügung, über welchen mit Hilfe eines einfachen Binärprotokolls Tag-Ereignisse gelesen werden können. Darüberhinaus besteht auch direkter Zugriff auf die digitalen Ein- und Ausgänge des RFID-Servers. Für die Implementierung in eigene Anwendungen beschreibt das folgende Kapitel den Aufbau und die einzelnen Befehle dieses Protokolls.

- Aufbau der Datenstrukturen
- Erfassung/Verlust von Tags
- Lesen/Schreiben der User-Daten von Tags
- Lesen/Schreiben der digitalen Ein-/Ausgänge
- Fehlerbehandlung

## 8.1 Kommunikationsgrundlagen

Um den RFID-Server aus Anwendungsprogrammen anzusprechen und an die Daten zu kommen, ist ein Zugriff über TCP-Sockets möglich. Wie bereits mehrfach angesprochen, bietet der RFID-Server die Möglichkeit, den Zugang durch die Anwendung mit einem Password zu schützen.

Der RFID-Server bietet einen Serversocket auf dem TCP/IP-Datenport (TCP-Port 2683), über den sich ein Client verbinden kann. Die Kommunikation findet nur mit **einem** aktiven Client pro Port statt. Wird eine aktive Verbindung gestört, so beendet der RFID-Server die Verbindung und wartet auf einen neuen Verbindungsaufbau.

Die Kommunikation zwischen dem RFID-Server und dem Client (PC) erfolgt über ein TPC/IP Socket.

Das Kommunikationsprotokoll setzt sich aus einer Übertragungsschicht und einer Applikationsschicht zusammen. Dabei definiert die Übertragungsschicht die Form eines Datenaustausches zwischen beiden Kommunikationspartnern und durch die Applikationsschicht wird die Befehlsstruktur festgelegt.

## 8.2 Verbindungsaufbau

Um eine TCP-Socket Verbindung zum RFID-Server aufzubauen wird die IP-Adresse, der entsprechende TCP Port des Gerätes und ein eventuell vergebenes Userpasswort benötigt.

Falls ein Passwort vergeben ist, muss dieses binnen 3 Sekunden nach Öffnen der Verbindung gesendet werden, sonst wird die Verbindung sofort wieder geschlossen. Dieses Kennwort muss null-terminiert sein, d.h. es muss mit einem null Byte (00) abgeschlossen werden. Die IP-Adresse und der Datenport werden in den Netzwerkeinstellungen im Web-Based-Management konfiguriert.

Der RFID-Server sendet „PASSWD?“ zurück falls das Datenpasswort falsch ist und beendet sofort die Verbindung.

Der Datenaustausch zwischen PC und dem RFID-Server geschieht dabei durch einfache Befehle, die auf den nächsten Seiten ausführlich beschrieben werden.

### 8.3 Definition der Protokoll-Strukturen

Um den Inhalt eines Paketes eindeutig identifizieren und auswerten zu können, müssen alle Daten in Form von Protokollstrukturen an den RFID-Server gesendet werden.

Alle Strukturen beginnen mit dem gleichen Header, der aus zwei Words (*send\_sequence* und *req\_sequence*) besteht. Die beiden Werte sind immer 0 (00 00). Dann folgt der Befehl („*Command*“) der vom RFID-Server ausgeführt werden soll und die **Gesamtlänge** („*length*“) der Struktur inklusive der ersten 4 Bytes. Der Header einer Struktur besteht also immer aus vier Words. Die Funktionsparameter eines Befehls werden nach der Längenangabe („*length*“) an das Datenpaket angehängt. Sie haben eine variable Länge (siehe Kapitel Befehle) und müssen der Gesamtlänge des Paketes hinzugerechnet werden.

Für die Übertragung der Daten ergibt sich folgende Datenstruktur:

	0		2		4		6		8		∞		
Struktur	send_seq.		rec_seq.		command		length		parameter				
Inhalt	00	00	00	00	00	03	19	00	00	00	.....	00	00
Bytefolge	Low	High	Low	High	Low	High	w	gh	Low				High
Variablentyp	Word		Word		Word		Word		Variabel				

- BYTE: vorzeichenlose Zahl mit einer Länge von 8 Bit 00
- WORD: vorzeichenlose Zahl mit einer Länge von 16 Bit 00 00
- LONG: vorzeichenlose Zahl mit einer Länge von 32 Bit 00 00 00 00



Beim Senden und Empfangen gilt für alle Struktur-Variablen: **Low-Byte first**

Beispiel:

Ausgabestring des RFID-Servers:

00 00 00 00 00 03 00 19 00 E0 04 01 00 0F 1E 41 F9 07 05 08 02 0B 1C 20 01

Struktur-Head:

	2		4		6		8	
Struktur	send_seq.		rec_seq.		command		length	
Inhalt	00	00	00	00	00	03	19	00
Bytefolge	Low	High	Low	High	Low	High	Low	High
Variblenotyp	Word		Word		Word		Word	

Struktur-Parameter:

	8	10	18				25	26										
	Action	Tag-ID						Timestamp	Filterset	Struktur								
	00	E9	3F	0F	1E	E9	1E	00	04	20	1C	0B	02	08	05	07	01	Inhalt
		Low							High									Bytefolge
	Byte	8 Byte						7 Byte				Byte	Variblenotyp					

Struktur:

Daraus ergibt sich der Befehl 03 00 und die Länge der gesamten Struktur von 00 19 Bytes.

Nutzdaten:

Ein Tag wurde erfasst (*Action* 00), mit der Tag ID E00401000F1E41F9.

Der Zeitstempel (Timestamp) setzt sich aus 7 Bytes zusammen.

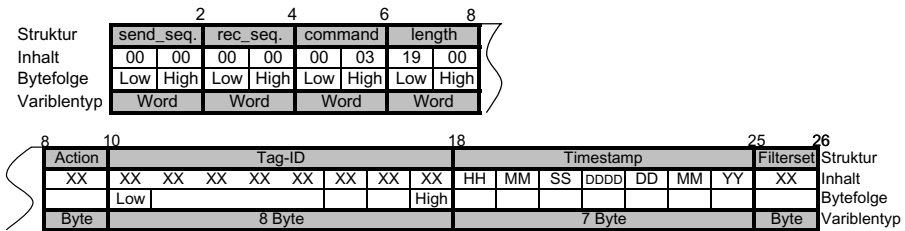
Byte	Description	Beispiel	
1	Year	07	2007
1	Month	05	Mai
1	Day	08	8
1	Weekday	02	Dienstag
1	Hour	0B	11 Std.
1	Minute	1C	28 Min.
1	Second	20	32 Sek.

Es ergibt sich eine Zeit (11:28:32), ein Wochentag (Dienstag) und ein Datum (08.05.07). Gültige Werte für das Jahr sind im Bereich von 0x00 (2000) bis 0x63 (2099). Der Wochentag beginnt mit 0x00 (Sonntag) und endet mit 0x06 (Samstag).

Auslöser des Paketes war das Filterset 01.

### 8.3.1 Filtermatch (0300)

Der RFID-Server gibt diese Struktur aus, wenn ein Tag in seinen Erfassungsbereich eintritt oder ihn verlässt und in der Gerätekonfiguration die Aktion direktes Senden eingeschaltet ist.



Die Struktur besteht aus einem allgemeinen Teil, der sich aus einer Initialisierung, dem ausführenden Befehl und der Gesamtlänge der Struktur zusammensetzt. Danach kommen die eigentlichen Nutzdaten. Diese bestehen aus:

- *Action*: Ein Tag ist im Erfassungsbereich erkannt worden (*Action 01*) oder hat ihn verlassen (*Action 00*).
- *Tag ID*: Die achtstellige Kennung des Tags
- *Timestamp*: Ein mit Datum versehener, sekundengenaue Zeitstempel. Dieser setzt sich zusammen aus:

Byte	Description
1	Year
1	Month
1	Day
1	Weekday
1	Hour
1	Minute
1	Second

- *Filterset*: Die Nummer des, durch das Tag-Event ausgelöste Filterset.





- *Timestamp*: Ein mit Datum versehener, sekundengenauer Zeitstempel. Dieser setzt sich zusammen aus:

Byte	Description
1	Year
1	Month
1	Day
1	Weekday
1	Hour
1	Minute
1	Second

- *Filterset*: Die Nummer des, durch das Tag-Event ausgelöste Filterset.

### 8.3.3 Clear Buffer (0302)

Diese Struktur dient zum Löschen des Ereignisspeichers.

	2		4		6		8	
Struktur	send_seq.		rec_seq.		command		length	
Inhalt	00	00	00	00	02	03	08	00
Bytefolge	Low	High	Low	High	Low	High	Low	High
Variablentyp	Word		Word		Word		Word	

Bestätigt wird das Löschen vom RFDI-Server mit der gleichen Struktur.

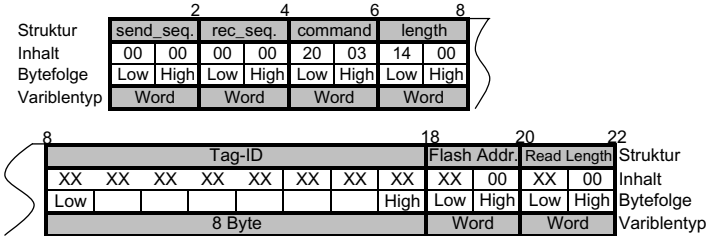
### 8.3.4 Buffer out of memory (030F)

Der RFID-Server übermittelt folgende Struktur nur, wenn sein Ereignisspeicher übergelaufen ist (> 2990 Ereignisse) und Ereignisse verloren gegangen sind.

	2		4		6		8	
Struktur	send_seq.		rec_seq.		command		length	
Inhalt	00	00	00	00	0F	03	08	00
Bytefolge	Low	High	Low	High	Low	High	Low	High
Variablentyp	Word		Word		Word		Word	

### 8.3.5 Readflash (0320)

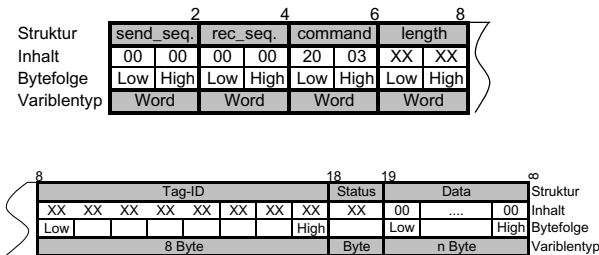
Folgende Struktur dient zum Lesen des Flashinhalts eines Tags.



- *Tag ID*: Die achtstellige Kennung des Tags
- *Flash Address*: Die Startadresse ab der gelesen werden soll.
- *Read Length*: Die Anzahl der Bytes die gelesen werden sollen.

Die beiden mitgelieferten Tags haben jeweils 128 Bytes Speicher, davon sind 112 Bytes zur freien Verfügung und 16 Bytes fest für die Tag-ID reserviert.

Der RFID-Server antwortet mit der gleichen Struktur, die einen Status der Leseanfrage und den Inhalt des Flashs enthält.



- *Tag ID*: Die achtstellige Kennung des Tags
- *Status*: Ergebniss des Lesevorgangs:

Byte	Description
00	OK
01	no Answer
02	read Error
04	Busy

- *Data*: Die Nutzdaten die ausgelesen wurden.

Zum Auslesen wird die vollständige ID des zu lesenden Tags benötigt, die Startadresse (der Adressraum wird linear abgebildet und beginnt bei 0) und die Anzahl der Bytes die gelesen werden sollen (max. 128 Bytes).



*Der TAG Datenzugriff muss in der Konfiguration passend zum Hersteller des Tags eingestellt sein!*

Beispiel:

*Send: 00 00 00 00 20 03 14 00 E9 3F 1E 0F 00 01 04 E0 00 00 09 00*

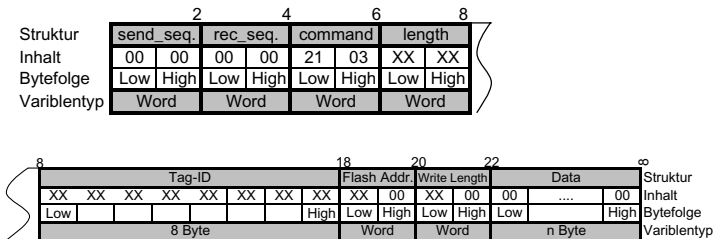
Diese Struktur fragt den Speicherinhalt des Tags mit der ID E0 04 01 00 0F 1E 3F an. Ab der Speicherstelle 0 (00 00) sollen 9 Bytes (00 09) aus dem Speicher ausgelesen werden.

*Rec.: 00 00 00 00 20 03 1A 00 E9 3F 1E 0F 00 01 04 E0 00 31 32 33 34 35 36 37 38 39*

Der RFID-Server gibt daraufhin diese Struktur aus. Die, wie die Anfrage auch aus dem Befehl (03 20), der Gesamtlänge (00 1A) und der Tag ID (E0 04 01 00 0F 1E 3F E9) besteht. Dann folgt der Status des Lesevorgangs (0) und die ausgelesenen Daten (31 32 33 34 35 36 37 38 39).

### 8.3.6 Writeflash (0321)

Folgende Struktur dient zum Schreiben des Tag-Flashinhalts.



- *Tag ID*: Die achtstellige Kennung des Tags

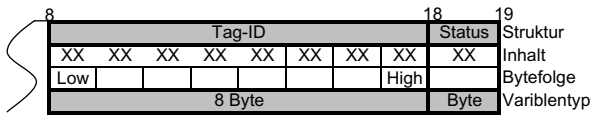
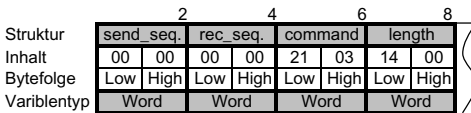
- *Flash Adresse*: Die Startadresse ab der geschrieben werden soll.

- *Write Length*: Die Anzahl der Bytes die geschrieben werden sollen.

- *Data*: Die Nutzdaten die ausgeschrieben werden sollen.

Die beiden mitgelieferten Tags haben jeweils 128 Bytes Speicher, davon sind 112 Bytes zur freien Verfügung und 16 Bytes fest für die Tag-ID reserviert.

Der RFID-Server antwortet mit der gleichen Struktur, die einen Status der Schreibanfrage enthält.



- *Tag ID*: Die achtstellige Kennung des Tags

- *Status*: Ergebnis des Schreibvorgangs:

Byte	Description
00	OK
01	no Answer
03	write Error
04	Busy

Zum Schreiben wird die vollständige ID des zu schreibenden Tags benötigt. Die Startadresse (der Adressraum wird linear abgebildet und beginnt bei 0), die Anzahl der Bytes die geschrieben werden sollen (max. 128 Bytes) und die zu schreibenden Daten.



*Der TAG Datenzugriff muss in der Konfiguration passend zum Hersteller des Tags eingestellt sein!*

Beispiel:

### 8.3.7 Get IO (0322)

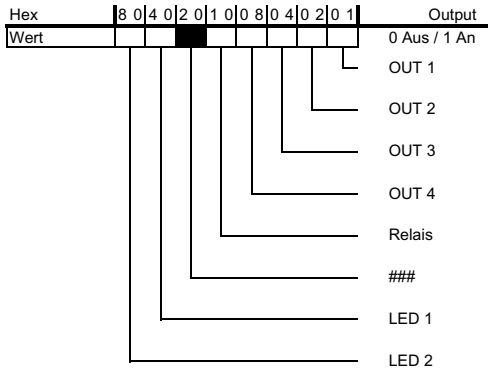
Um den Zustand der IOs abzufragen wird folgende Struktur benutzt.

	2		4		6		8	
Struktur	send_seq.		rec_seq.		command		length	
Inhalt	00	00	00	00	22	03	08	00
Bytefolge	Low	High	Low	High	Low	High	Low	High
Variablentyp	Word		Word		Word		Word	

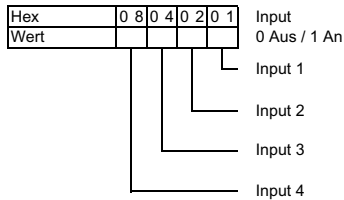
Der RFID-Server liefert den Zustand der Inputs und der Outputs in dieser Struktur zurück.

Name	Type	Hex
Struct_Init	1 Long	00 00 00 00
Struct_Cmd	1 Word	03 22
Struct_length	1 Word	00 0A
Outputs	1 Byte	40
Inputs	1 Byte	09

- Ouputs: Über diesen Hexwert sind alle digitalen Ausgänge und die beiden Led's kodiert. Wird der Wert binär umgerechnet, kann er mit Hilfe der folgende Tabelle übersetzt werden.



- Inputs: Über diesen Hexwert sind alle digitalen Eingänge kodiert. Wird der Wert binär umgerechnet, kann er mit Hilfe der folgende Tabelle übersetzt werden.



Beispiel:

Outputs :            9    A  
 Binär umgerechnet: 1001 1010  
 Geschaltet :        LED 2, Relais, Out 4, Out2

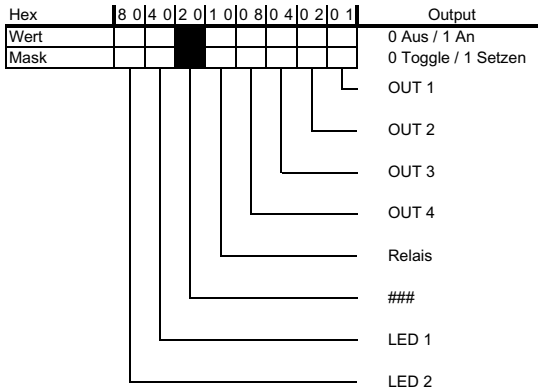
Inputs :             0    C  
 Binär umgerechnet: 0000 1100  
 Geschaltet:         Input 3, Input 4

### 8.3.8 Set Output (0323)

Das Setzen der Outputs am RFID-Server wird mit Hilfe von dieser Struktur übermittelt.

	2		4		6		8		9	10
Struktur	send_seq.		rec_seq.		command		length		Output	Mask
Inhalt	00	00	00	00	23	03	0A	00	XX	XX
Bytefolge	Low	High	Low	High	Low	High	Low	High		
Variablentyp	Word		Word		Word		Word		Byte	Byte

Über den Wert von *Mask* wird festgelegt, ob ein Ausgang auf einen festen Wert gesetzt wird (*Mask* = 1) oder der Wert getog- get (hin- und hergeschaltet) werden soll (*Mask* = 0).



Zum Setzen der Outputs wird entweder der Wert, den der Output annehmen soll, gesetzt (*Mask* = 1) oder der Output auf Toggle (*Mask* = 0) gesetzt.



Beispiel:

Outputs :           9     A  
Binär umgerechnet: 1001 1010  
Benutzen :           LED 2, Relais, Out 4, Out2

Maske :             9     0  
Binär umgerechnet: 1001 0000  
Einschalten:        LED 2, Relais  
Toggeln:            Out 4, Out2

## 8.4 Fehlerbehandlung

Auftretende Fehler werden mit Hilfe von zwei Error-Funktionen signalisiert.

### 8.4.1 Syntaxfehler (FF00)

Syntaxfehler in der Kommunikation werden mit der Funktion „*Syntax\_Error (0xFF00)*“ dargestellt.

	2		4		6		8		9	
Struktur	send_seq.		rec_seq.		command		length		Syntax_Err.	
Inhalt	00	00	00	00	FF	00	0A	00	XX	00
Bytefolge	Low	High	Low	High	Low	High	Low	High	Low	High
Variablentyp	Word		Word		Word		Word		Word	

Der *Syntax\_Error*-Code hat dabei folgende Bedeutung:

Syntax_Error	Description
00 00	Cmd unknown
00 01	Parameter length
00 02	Parameter wrong
00 03	Cmd forbidden

*Cmd unknown* bedeutet, dass der Befehl, der übermittelt wurde, nicht bekannt ist. Alle im W&T Tag Control Modus nutzbaren Befehle sind in Kapitel 11.3 beschrieben.

Sollte die Strukturlänge nicht stimmen, wird der Fehler *Parameter length* ausgegeben. Die Strukturlänge muss immer über die gesamte Struktur berechnet werden.

*Parameter wrong* wird immer dann zurück gegeben, wenn ein falscher Parameter zu einem Befehl an den RFID-Server übermittelt wurde.

Befehle die zu diesem Zeitpunkt nicht erlaubt sind, werden mit dem Fehler *Cmd forbidden* ausgegeben.

### 8.4.2 Funktionale Fehler (FF02)

Funktionale Fehler, die geräteintern auftreten, werden durch die Funktion RFID\_Error (0xFF02) dargestellt.

Struktur	2		4		6		8		9	
Inhalt	send_seq.	rec_seq.	command		length		RFID_Err.			
Bytefolge	00	00	00	00	F2	00	0A	00	XX	00
Variblentyp	Low	High	Low	High	Low	High	Low	High	Low	High
	Word		Word		Word		Word		Word	

Der *RFID\_Error*-Code hat dabei folgende Bedeutung:

RFID Error	Description
03 02	Out of Buffermemory
03 03	temporarily stop of HW
03 04	parameter wrong

*Out of Buffermemory* wird vom RFID-Server ausgegeben, wenn in den W&T Tag Control Aktionen gepuffertes Senden aktiviert wurde und mehr als 2990 Events im Buffer aufgelaufen sind. Der Ringbuffer überschreibt dann die ersten Events und speichert somit immer die aktuellsten 2990 Ereignisse.

*Temporarily stop of HW* bedeutet, dass die Hardware einen zeitweisen Ausfall gemeldet hat. Dies kann z.B. durch eine überhitzte Endstufe verursacht werden.

*Parameter wrong*, nachdem der RFID-Server den Befehl empfangen hat, stimmen die dazugehörigen Parameter nicht mit den erwarteten Werten überein. Der angegebene Parameter wurde vom Gerät nicht verstanden.



## 9 Kommunikation per OPC

OPC bietet die Möglichkeit, über eine standardisierte Softwareschnittstelle die Erfassung und den Verlust von Tags zu verarbeiten. Anwendungen, die als OPC-Client agieren, können sich mit dem W&T OPC-Server verbinden, welcher die Kommunikation mit dem RFID-Server abwickelt und die Ereignisse dann in entsprechenden OPC-Variablen zur Verfügung stellt.

**Vorläufig/Preliminary  
(in Vorbereitung)**



## **10 Datenbankintegration per ODBC**

Das W&T-Tool sammelt Daten vom W&T RFID-Server und schreibt sie über die Universalschnittstelle ODBC in eine beliebige Datenbank. Außerdem bietet das Programm den Export als Excel-Tabelle an, was vor allem eine grafische Darstellung ermöglichen soll.

**Vorläufig/Preliminary  
(in Vorbereitung)**

## 10.1 ODBC-Grundlagen

Ein zentraler Begriff in der ODBC-Welt ist die „Datenquelle“. Darunter versteht man einen benannten Parametersatz, der auf eine Datenbank verweist. Die von Sensobase verwendete Datenquelle heißt standardmäßig „W&T Sensor Database“. Alle auf einem Rechner installierten Datenquellen lassen sich mit dem Windows-Dienstprogramm „Datenquellen (ODBC)“ verwalten. Sensobase wird Sie durch alle notwendigen Schritte zum Anlegen und Konfigurieren Ihrer Datenquelle führen.

Der wichtigste Parameter jeder Datenquelle ist der verwendete ODBC-Treiber, der vor allem bestimmt, in welchem Format die Daten gespeichert werden und welche Datenbank-Operationen überhaupt zur Verfügung stehen. Weitere Parameter legen fest, *wo* die Daten gespeichert werden, sowie die Optionen, die mit dem speziellen Datenbankformat zu tun haben. Da der Konfigurationsdialog zur Eingabe dieser Parameter vom jeweiligen Treiberhersteller mitgeliefert wird, können diese Optionen sehr unterschiedlich ausfallen.

**Vorläufig/Preliminary  
(in Vorbereitung)**



## **11 Protocol Mode**

Dieser Modus ist die transparente Umsetzung des ISO 15693-3 Standards. Nach dem Aktivieren der Betriebsart Protocol Mode, kann sich eine netzwerkseitige Anwendung über den eingestellten Protocol Port (Default TCP-Port 2684) mit dem RFID-Server verbinden.

**Vorläufig/Preliminary  
(in Vorbereitung)**

## 11.1 Funktionsbeschreibung

(in Vorbereitung)

**Vorläufig/Preliminary  
(in Vorbereitung)**

## **Anhang**

- Firmware-Update
- Reset des RFID-Servers über das Netzwerk (TCP-Port 8888)
- Verwendete Port-/Socketnummern und Netzwerksicherheit
- Hardware-Reset auf Werkseinstellungen
- Zahlensysteme / Programmiergrundlagen
- Technische Daten

## Firmware-Update

Die Gerätesoftware des RFID-Servers wird ständig weiterentwickelt. Der folgende Abschnitt beschreibt, wie ein eventueller Update der Firmware durchzuführen ist.

### Wo ist die aktuelle Firmware erhältlich?

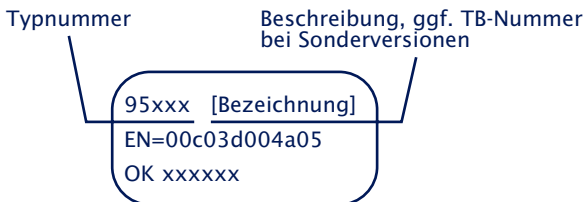
Die jeweils aktuellste Firmware inkl. der verfügbaren Updatetools und einer Revisionsliste ist auf unseren Webseiten unter folgender Adresse veröffentlicht:

<http://www.wut.de>

Sie navigieren von dort aus am einfachsten mit Hilfe der auf der linken Seite befindlichen Suchfunktion. Geben Sie in das Eingabefeld zunächst die Typnummer Ihres Gerätes ein. Markieren Sie in der zugehörigen Auswahlbox den Punkt *Firmware* und betätigen den Button *Los*.

Sie gelangen direkt auf die Seite mit der aktuellsten Firmware für ihren RFID-Server.

Sollten Sie die Typnummer nicht kennen, können Sie diese dem auf der Frontseite befindlichen Aufkleber entnehmen, der auch die Ethernet-Adresse aufweist.



*Insbesondere wenn der Aufkleber als Bezeichnung eine TB-Nummer ausweist, ist es möglich, dass der RFID-Server über eine spezielle, kundenspezifische Firmware oder Konfiguration verfügt. Diese würde durch einen Upload der*

*Standard-Firmware überschrieben. Bitte kontaktieren Sie in solchen Fällen vor dem Update unbedingt den verantwortlichen Administrator.*

### **Firmware-Update per Netzwerk unter Windows**

Voraussetzung ist ein PC unter Windows 9x/NT/2000/XP/2003/Vista mit einem Netzwerkanschluss und aktiviertem TCP/IP-Stack. Für den Update-Prozess benötigen Sie zwei Files, die wie bereits beschrieben auf der Website <http://www.wut.de> zum Download bereitstehen.

- Das ausführbare Update-Tool *WuTility* für die Übertragung der Firmware in den RFID-Server.
- Die Datei mit der neuen Firmware die in den RFID-Server übertragen werden soll.

Eine spezielle Vorbereitung des RFID-Servers für den Firmware-Update ist nicht erforderlich.

Das Update-Tool ist weitestgehend selbsterklärend. Sollten doch Fragen oder Unklarheiten bestehen, nutzen Sie bitte die zugehörige Dokumentation oder Online-Hilfe.



*Unterbrechen Sie nie selbstständig den Update-Prozess durch Ziehen des Netzsteckers. Nach einem unvollständigen Update besteht die Gefahr, dass der RFID-Server betriebsunfähig ist. Sollte die Übertragung z.B. aufgrund eines Stromausfalls doch unterbrochen worden sein, versuchen Sie einen Neustart des Updates unter der bisherigen IP-Adresse des Gerätes.*

## Reset des RFID-Server über das Netzwerk

Für den Fall, dass der RFID-Server über das Netzwerk einem Reset unterzogen werden soll, wurde der TCP-Port 8888 eingerichtet. Wird zu diesem Port eine TCP-Verbindung aufgebaut, akzeptiert der RFID-Server diese zunächst, schließt sie dann sofort wieder und führt einen Neustart seiner Firmware durch.

### Verwendung des Systempasswortes

Wurde ein Systempasswort konfiguriert (siehe Kapitel *Session Control*), muss dieses nullterminiert (= `[password] + 0x00`) und innerhalb von 2s nach erfolgreichem Verbindungsaufbau an den RFID-Server gesendet werden. Empfängt der RFID-Server ein falsches oder gar kein Systempasswort innerhalb dieser Zeit, sendet er die Meldung `PASSWD?` gefolgt von einem Nullbyte (0x00) an den Client und beendet die TCP-Verbindung.

Ist kein Systempasswort konfiguriert, wird der RFID-Server, wie im Beispiel beschrieben, nach Aufbau der TCP-Verbindung diese sofort wieder schließen und einen Reset durchführen.



*Durch diesen Reset werden Bufferinhalte und alle eventuell aktiven Verbindungen gelöscht. Der Reset kann von jeder beliebigen Station mit Kenntnis des Systempasswortes ausgelöst werden.*

## Verwendete Ports und Netzwerksicherheit

Mit seiner Standardwerkseinstellung verwendet der RFID-Server die in nachstehender Tabelle aufgeführten TCP- und UDP-Portnummern.

Portnummer	Protokoll	Anwendung	veränderbar	abschaltbar
69	TCP	Update über TFTP <sup>2</sup>	nein	nein
80	TCP	Listenport TCP/http	ja	nein
2683	TCP	W&T Tag Control	ja	ja
2684	TCP	Protokoll	ja	ja
8513	UDP	Inventarisierung <sup>1</sup>	nein	nein
8888	TCP	Reset <sup>2</sup>	nein	nein

<sup>1</sup> kein schreibender Zugriff auf das RFID-Server möglich

<sup>2</sup> passwortgeschützt



*Jede Portnummer darf im RFID-Server nur für einen Dienst verwendet werden. Sollen bei den veränderbaren Ports abweichende Nummern zum Einsatz kommen, ist darauf zu achten, dass keine Portnummer doppelt verwendet wird.*

### Der W&T RFID-Server und die Netzwerksicherheit

Die Sicherheit in Netzwerken wird heute zu Recht zunehmend beachtet. Alle Experten sind sich darüber einig, dass es eine absolute Sicherheit beim heutigen Stand der Technik nicht geben kann. Jeder Kunde muss daher für seine konkreten Voraussetzungen ein angemessenes Verhältnis zwischen Sicherheit, Funktionsfähigkeit und Kosten festlegen.

Um hier dem Kunden eine größtmögliche Flexibilität zu ermöglichen, die sich an wechselnden Sicherheitsanforderungen von einer reinen Test- und Installationsumgebung bis hin zu kritischen Produktionsanwendungen orientiert, sind die Sicherheitsmaßnahmen in hohem Maße durch den Kunden konfigurierbar. Dieses Kapitel gibt einen Überblick über die Sicherheitsmaßnahmen, die auf dem W&T RFID-Server implementiert sind bzw. genutzt werden können. Es wird hierbei vorausgesetzt, dass die Original-Firmware von W&T (ohne kundenspezifische Anpassungen) eingesetzt wird. Weitere Details sind den jeweiligen Abschnitten der Bedienungsanleitung zu entnehmen.

### **Das Berechtigungskonzept des RFID-Servers**

Wie bereits im Kapitel Web-Based Management beschrieben, kennt der RFID-Server zwei Stufen von Berechtigungen:

- Administrator (Systempasswort)
- User (User-Passwort)

Die Steuer- und Konfigurationszugänge des RFID-Servers werden über das Systempasswort geschützt. Ab Werk ist *kein* System-Passwort voreingestellt, so dass nach einem Login jeder über Vollzugriff auf die entsprechenden Einstellungen und Funktionen verfügt.

Der Zugriff auf die HF-Ereignisse wie zum Beispiel Erfassung und Verlust von Tags sowie die digitalen E/As ist durch das User-Passwort geschützt. Ab Werk ist dieses nicht vergeben, so dass sich jeder auf die entsprechenden TCP-Dienste des RFID-Servers konnektieren kann.

Zur Vermeidung unbefugter Zugriffe empfiehlt sich daher grundsätzlich sowohl ein Systempasswort wie auch User-Passwort zu verwenden. Diesbezügliche weitere Maßnahmen, wie z.B. dessen Zusammensetzung und regelmäßiger Wechsel, sind bei Bedarf durch den Kunden organisatorisch sicherzustellen.

Die Übertragung der Passwörter an den RFID-Server erfolgt ohne Verschlüsselung. Es ist also ggf. zu gewährleisten, dass passwort-geschützte Zugriffe nur über ein vom Kunden als sicher betrachtetes Intranet erfolgen. Bei Zugriffen über das öffentliche Internet sind zusätzliche Maßnahmen wie Aufbau eines VPN-Tunnels (Virtual Private Network) zu treffen. Dies ist jedoch eine generelle Problematik der Netzwerksicherheit, für die jeder Kunde entsprechende Lösungen finden muss.

### **Ports mit Sonderfunktion**

Neben dem Zugriff über die Web-Oberfläche sind einige Funktionen auch über verschiedene TCP- bzw. UDP-Ports aktivierbar. Diese sind in der Tabelle auf der vorherigen Seite dargestellt. Teilweise sind die Funktionen über das WBM ein- und ausschaltbar. Grundsätzlich ist zu empfehlen, alle nicht benötigten Funktionen abzuschalten.



- **Port für Inventarisierung mit WuTility**

Wie alle „intelligenten“ Komponenten von W&T kann der RFID-Server über das Tool *WuTility* angesprochen werden. Hierbei kann das Tool über den UDP-Port 8513 Informationen wie Hard- und Firmware-Version, IP-Adresse etc. auslesen. Dieser Zugriff ist grundsätzlich nicht abschaltbar. Ein schreibender Eingriff in das Gerät ist auf diesem Wege jedoch nicht möglich.

- **Firmware-Update**

Der Firmware-Update erfolgt ebenfalls mit Hilfe des Inventarisierungstools *WuTility*. Nach einer speziellen Initialisierung des Updates über den TCP-Port 80 und unter Verwendung des Systempasswortes, wird die eigentliche Firmware dann per TFTP über den UDP-Port 69 an das Gerät übertragen.

- **Reset über Port 8888**

Durch den Aufbau einer Verbindung (z.B. mit Telnet) auf den TCP-Port 8888 kann ein Reset des Gerätes ausgelöst werden. Hierzu ist sofort nach dem Verbindungsaufbau das Systempasswort (falls gesetzt) anzugeben. Diese sofortige Übergabe des Passwortes ist praktisch nicht manuell, sondern nur durch ein Programm möglich. Die Folgen eines Resets sind die gleichen, wie die einer kurzzeitigen Unterbrechung der Stromversorgung.

### **Wiederherstellung der Factory Defaults**

Durch Wiederherstellen der Werkseinstellungen (Factory Defaults) über das WBM, können alle vom Kunden vorgenommene Einstellungen wieder rückgängig gemacht werden. Unter anderem werden auch das System- und User-Passwort gelöscht.

## Hardware-Reset auf Werkseinstellungen

Neben der Möglichkeit den RFID-Server über das Web-Based-Management auf seine Werkseinstellungen (Factory Defaults) zurückzusetzen, kann dieses auch hardwaremäßig erfolgen. Das Gerät verfügt zu diesem Zweck über einen auf der Platine befindlichen Jumper, welcher im Normalbetrieb geöffnet sein muss. Um die Werkseinstellungen abzurufen, gehen Sie wie folgt vor:

- Machen Sie den RFID-Server spannungslos und öffnen Sie das Gehäuse durch Lösen der beiden Schrauben auf der Geräterückseite.
- Schließen Sie den Jumper und schließen dann die Spannungsversorgung wieder an.
- Nach ca. 3s ist die aktuelle Konfiguration gelöscht und die Werkseinstellungen sind reaktiviert.
- Machen Sie den RFID-Server spannungslos, öffnen den Jumper und schließen dann das Gehäuse wieder.



*Das Zurücksetzen des nichtflüchtigen Speichers führt zum Verlust aller von den Defaultwerten abweichenden Einstellungen, einschließlich der IP-Adresse. Das Einstellungsprofil der Factory-Defaults kann u.U. durch ein kundenspezifisches Profil ersetzt worden sein. In diesem Fall sind nach dem Zurücksetzen die kundenspezifischen Einstellungen aktiviert.*

**Zahlensysteme/Programmiergrundlagen**

Binär				Hex
0	0	0	0	0
0	0	0	1	1
0	0	1	0	2
0	0	1	1	3
0	1	0	0	4
0	1	0	1	5
0	1	1	0	6
0	1	1	1	7
1	0	0	0	8
1	0	0	1	9
1	0	1	0	A
1	0	1	1	B
1	1	0	0	C
1	1	0	1	D
1	1	1	0	E
1	1	1	1	F

- BYTE: vorzeichenlose Zahl mit einer Länge von 8 Bit 00
- WORD: vorzeichenlose Zahl mit einer Länge von 16 Bit 00 00
- LONG: vorzeichenlose Zahl mit einer Länge von 32 Bit 00 00 00 00

**Eine kleine Auffrischung der Zahlensysteme**

In der Computertechnik arbeitet man mit Bits und Bytes, also eigentlich im dualen oder auch binären Zahlensystem.

Duale Zahlen sind für den Menschen leider sehr unübersichtlich. Wer erkennt schon auf Anhieb, dass dual 110001110101 = dezimal 3189 ergibt?

Da man jeden Input bzw. Output des RFID-Servers als eine Stelle einer 12-stelligen Binärzahl sehen muss, ist es unausweichlich, sich noch einmal mit dieser Materie zu beschäftigen.

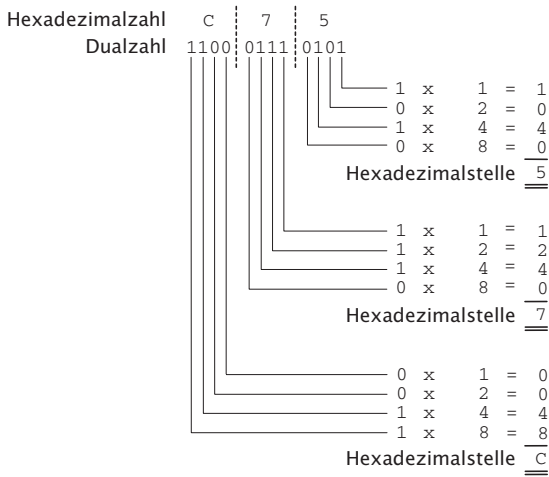
	Dualzahl	110001110101			
Bit 0	=	2 <sup>0</sup>	=	1	
Bit 1	=	2 <sup>1</sup>	=	2	
Bit 2	=	2 <sup>2</sup>	=	4	
Bit 3	=	2 <sup>3</sup>	=	8	
Bit 4	=	2 <sup>4</sup>	=	16	
Bit 5	=	2 <sup>5</sup>	=	32	
Bit 6	=	2 <sup>6</sup>	=	64	
Bit 7	=	2 <sup>7</sup>	=	128	
Bit 8	=	2 <sup>8</sup>	=	256	
Bit 9	=	2 <sup>9</sup>	=	512	
Bit 10	=	2 <sup>10</sup>	=	1024	
Bit 11	=	2 <sup>11</sup>	=	2048	

			1	x	1	=	1
			0	x	2	=	0
			1	x	4	=	4
			0	x	8	=	0
			1	x	16	=	16
			1	x	32	=	32
			1	x	64	=	64
			0	x	128	=	0
			0	x	256	=	0
			0	x	512	=	0
			1	x	1024	=	1024
			1	x	2048	=	2048
							<u>3819</u>
						Dezimalzahl	

Das Umrechnen von Dual- in Dezimal-Zahlen ist nicht schwierig. Dennoch fehlt die spontane Zuordnung zwischen gesetz-





Mit etwas Übung lässt sich das bequem im Kopf rechnen.

## Technische Daten

<b>Spannungsversorgung ...</b> ... DC	12V (+/-5%)
<b>Stromaufnahme</b>	typ. 700mA max. 950mA
<b>Zulässige Umgebungstemperatur ...</b> ... Lagerung ... Betrieb	-40 ... +70°C 0 ... +50°C
<b>Zulässige rel. Luftfeuchtigkeit</b>	0 - 95% (nicht kondensierend)
<b>Netzwerk</b>	10/100BaseT, RJ45 für STP-Verk.
<b>Galvanische Trennung</b>	Ethernet-Anschluss: min. 500V
<b>Abmessungen</b>	200 x 280 x 41 mm
<b>Gewicht</b>	ca. 950g
<b>Betriebsfrequenz</b>	13,56 MHz
<b>HF-Sendeleistung</b>	ca. 1W
<b>Unterstützte Transponder</b>	ISO 15693-3 (weitere auf Anfrage)
<b>Schreib-/Lesereichweite</b>	typ. 35cm
<b>Digitale Eingänge</b>	4 x stromziehend 3-4mA 0-24V, Schaltschwelle 4V +/-1V
<b>Digitale Ausgänge ...</b> ... Relais ... Open Collector	1 x Umschalter, max. 48V DC max. 5A, Schaltfrequenz 1800/h 4 x Open Collector, 0-12V, max. 100mA, Ri ca. 170hm

**Konformitätserklärung**



www.WuT.de

W&T Interfaces für: TCP/IP, Ethernet, RS-232, RS-485, USB, 20mA, Glas-und Kunststoff-LWL, http, SNMP, OPC, I/O digital, I/O analog, ISA, PCI, ...

**EG-Konformitätserklärung zur CE-Kennzeichnung**

Die Wiesemann & Theis GmbH, Wuppertal erklärt hiermit, daß das Produkt

**RFID-Server, Typ 95001**


den wesentlichen Schutzanforderungen entspricht, die in den Richtlinien des Rates über elektrische und elektronische Produkte festgelegt sind:


- 1. 89/336/EWG (2004/108) EMV-Richtlinie
- 2. 73/23/EWG, bzw. 93/68/EWG Niederspannungsrichtlinie
- 3. 99/5/EWG RTTE-Richtlinie-Sendefunkgeräte / Telekommunikations-Endgeräte

Zur Beurteilung wurden folgende Normen herangezogen:

- zu 1.) Stör-Emission gemäß ETS EN301489-3 (V.1.4.1):
  - 1.1. EN 55022 K1.B Störspannung/Störfeld
  - 1.2. EN 61000-3-2 Stromoberwellen
  - 1.3. EN 61000-3-3 Flicker
- Störfestigkeit gemäß ETS EN301489-3 (V.1.4.1):
  - 1.4. EN 61000-4-2/2001 ESD
  - 1.5. EN 61000-4-3/2002 +A1 Einstrahlung E-Feld
  - 1.6. EN 61000-4-4/2005 Burst
  - 1.7. EN 61000-4-5/2001 Surge
  - 1.8. EN 61000-4-6/2001 Einströmung
  - 1.9. EN 61000-4-11/2005 Spannungsunterbrechung
- zu 2.) 2.1. EN 60950-1 (2003) Elektrische Sicherheit, ITE
- zu 3.) 3.1. EN 50371 (2002) Sicherheit von Personen in elektromagnetischen Feldern
- 3.2. EN 50364 (2001) Begrenzung der Exposition von Personen durch Sendefunkgeräte
- 3.2. EN 300330-2 (V.1.3.1) EMV und Spektrumangelegenheiten

Wuppertal, den 11.06.2007

  
 Klaus Meyer, EMV-Beauftragter

  
 Dipl.-Ing. Rüdiger Theis, Geschäftsführer

Wiesemann & Theis GmbH  
 Porschestraße 12  
 42279 Wuppertal  
 GF: Dipl.-Ing. Rüdiger Theis

Tel.: 0202/2680-0  
 Fax: 0202/2680-265  
 info@WuT.de  
 www.WuT.de

Handelsregister:  
 Amtsgericht Wuppertal HRB6377  
 UStID Nr.: DE121008340  
 Steuer Nr.: 131/5937/014

Bankverbindung:  
 Postbank Essen  
 Konto: 289397436  
 BLZ: 36010043

## Index

### A

Abgleich Antenne 58  
 Antennenabgleich 30  
 Auto Negotiation 33

### B

Basisparameter 52  
 Berechtigungskonzept 102  
 Beschaltungsbeispiel 36, 37, 38  
 Binärdatei 57  
 BOOTP 23, 53  
 BOOTP Client 53

### D

DHCP 19, 53  
 Digitale Ausgänge 37  
 Digitale Ein-/Ausgänge 35  
 Digitale Eingänge 36  
 DNS 54  
 Download Konfiguration 57

### E

Echtzeituhr 55  
 Error 39  
 Error-LED 39  
 Ethernet-Adresse 54

### F

Factory Defaults 50, 104  
 Ferrite 32  
 Firmware-Update 98, 99

### G

Gateway 53

### H

Halb-Duplex 33  
 Hardware-Reset 104

### I

Icons 46  
 IP Adresse 13, 53  
 IP-Vergabe 13

### K

Konfigurationsframe 46  
 Konfigurationsprofile 57  
 Konformitätserklärung 109

### L

Lease-Time 20  
 LED-Anzeigen 39  
 Link-Status 33  
 Login 45  
 Login Timeout 45

### M

MAC-Adresse 17, 54  
 Menübaum 46  
 MODE 40  
 Mode 56  
 Montage 28

### N

Navigation 45  
 Navigationsframe 45  
 Network 52  
 Netzwerkanschluss 33  
 Netzwerksicherheit 101  
 New Password 50

### O

ODBC 93  
 OPC 91  
 Open-Collector 37

### P

Port 8888 103  
 Power 39  
 Programmiergrundlagen 105  
 Protocol Mode 56, 95  
 Protocol Port 54

### Q

Quickstart 8

### R

RARP 25  
 Relaisausgang 38  
 Reset 50, 100  
 Restore Factory Defaults 50  
 RFID-Status 40  
 RJ45 33

### S

Session Control 50  
 Sonderfunktion 102  
 Spannungsversorgung 32  
 Status 39  
 Status-LED 39  
 Steckernetzteil 32  
 Subnet Mask 53



System Name 20  
Systemname 54  
Systempasswort 51  
Systemübersicht 10

**T**

Tag-Control Mode 56  
Tag-Control Port 54  
Technische Daten 108  
Time and Date 55

**U**

Uhr 55  
Unterkategorie 46  
Upload Konfiguration 57  
User Password 51

**V**

Vergabe der IP-Adresse 13

**W**

W&T Tag-Control 59  
W&T Tag-Control Mode 56  
WBM-Port 53  
Web-Based Management 44, 102  
Werkseinstellungen 12, 50, 104  
Wiederherstellung der Factory  
Defaults 103  
WuTility 14, 19

**Z**

Zahlensysteme 105