





Version 1.9.1 - 13.06.2014



## Inhalt

1.	LIZE	NZVERTRAG	2
2.	PRO	DUKTHAFTUNG	
3.	Über	sicht	4
4.	WLA	N Konfiguration mit dem Client	5
	4.1.	Auswahl der Betriebsarten "Managed" oder "Ad-hoc"	6
	4.2.	Konfigurieren der Netzwerk ESSID	7
	4.3.	Konfigurieren des Authentifizierungs-Verfahren	
	4.4.	Verbindungs-Schlüssel Typen	9
	4.5.	Schlüssel und Schlüssellänge	9
	4.6.	Schlüsseleingabe	
	4.7.	DHCP Modus	
	4.8.	Einstellungen zum blue PiraT2 übertragen	
5.	Weite	erführende Informationen und Konfiguration am Laptop	
6.	Verb	indung mit dem Datenlogger über WLAN	
7.	Abbi	ldungsverzeichnis	
8.	Kont	akt	

# 1. LIZENZVERTRAG

Lesen Sie bitte die Lizenzvereinbarung dieses Lizenzvertrages sorgfältig, bevor Sie die Software installieren. Durch das Installieren der Software stimmen Sie den Bedingungen dieses Lizenzvertrages zu.

Diese Software-Lizenzvereinbarung, nachfolgend als "Lizenz" bezeichnet, enthält alle Rechte und Beschränkungen für Endanwender, die den Gebrauch der begleitenden Software,

Bedienungsanleitung und sonstigen Unterlagen, nachfolgend als "Software" bezeichnet, regeln.

- 1. Dieser Lizenzvertrag ist eine Vereinbarung zwischen dem Lizenzgeber und Lizenznehmer, der die Lizenz erhält, um die genannte Software zu verwenden.
- 2. Dem Lizenznehmer ist bekannt, dass dies nur eine beschränkte nichtexklusive Lizenz ist. Dies bedeutet das der Lizenznehmer keinerlei Recht auf Unter-lizenzvergabe hat. der Lizenzgeber ist und bleibt der Eigentümer aller Titel, Rechte und Interessen an der Software.
- 3. Die Software ist urheberrechtlich geschütztes Eigentum der Telemotive AG. Das Programm oder Teile davon dürfen nicht an Dritte vermietet, verkauft, weiterlizenziert oder sonst in irgendeiner Form ohne ausdrückliche, schriftliche Genehmigung der Telemotive AG weitervermarktet werden. Der Anwender darf die Software und deren Bestandteile weder verändern, modifizieren noch sonst in jeglicher Form rückentwickeln oder dekompilieren.
- 4. Diese Software unterliegt keiner Garantie. Die Software wurde verkauft wie sie ist, ohne jegliche Garantie. Falls irgendwann ein Benutzer sein System ändert, trägt der Lizenzgeber keine Verantwortung dafür, die Software zu ändern, damit sie wieder funktioniert.
- 5. Diese Lizenz erlaubt dem Lizenznehmer, die Software auf mehr als einem Computersystem zu installieren, solange die Software nicht gleichzeitig auf mehr als einem Computersystem verwendet wird. Der Lizenznehmer darf keine Kopien der Software machen oder Kopien der Software erlauben, wenn keine Autorisierung dafür besteht. Der Lizenznehmer darf lediglich zu Aushilfszwecken Kopien der Software machen. Der Lizenznehmer ist nicht berechtigt, die Software oder Ihre Rechte aus dieser Lizenzvereinbarung weiterzugeben oder zu übertragen.
- Der Lizenzgeber ist gegenüber dem Lizenznehmer weder für Schäden, einschliesslich kompensatorischer, spezieller, beiläufiger, exemplarischer, strafender oder folgenreicher Schäden, verantwortlich, die sich aus dem Gebrauch dieser Software durch den Lizenznehmer ergeben.
- 7. Der Lizenznehmer ist bereit, den Lizenzgeber zu schützen und zu entschädigen und fern zu halten von allen Ansprüchen, Verlusten, Schäden, Beschwerden, oder Ausgaben, die mit den Geschäftsoperationen des Lizenznehmers verbunden sind oder sich aus diesen ergeben.
- Der Lizenzgeber hat das Recht, diesen Lizenzvertrag sofort zu kündigen und das Softwarebenutzungsrecht des Lizenznehmers zu begrenzen, falls es zu einem Vertragsbruch seitens des Lizenznehmers kommt. Die Laufdauer des Lizenzvertrags ist auf unbestimmte Zeit festgelegt.
- 9. Der Lizenznehmer ist bereit, dem Lizenzgeber alle Kopien der Software bei Kündigung des Lizenzvertrags zurückzugeben oder zu zerstören.
- 10. Dieser Lizenzvertrag beendet und ersetzt alle vorherigen Verhandlungen, Vereinbarungen und Abmachungen zwischen dem Lizenzgeber und Lizenznehmer bezüglich dieser Software.
- 11. Dieser Lizenzvertrag unterliegt deutschem Recht.
- 12. Wenn eine Bestimmung dieses Lizenzvertrags nichtig ist, wird dadurch die Gültigkeit der verbleibenden Bestimmungen dieses Lizenzvertrags nicht berührt. Diese nichtige Bestimmung wird durch eine gültige, in Übereinstimmung mit den gesetzlichen Vorschriften stehende Bestimmung mit ähnlicher Absicht und ähnlichen wirtschaftlichen Auswirkungen ersetzt.
- 13. Der Lizenzvertrag kommt durch Übergabe der Software von dem Lizenzgeber an den Lizenznehmer und/oder durch den Gebrauch der Software durch den Lizenznehmer wirksam zustande. Dieser Lizenzvertrag ist auch ohne die Unterschrift des Lizenzgebers gültig.
- 14. Die Lizenz erlischt automatisch, wenn der Lizenznehmer den hier beschriebenen Lizenzbestimmungen nicht zustimmen oder gegen die Lizenzbestimmungen dieses Lizenzvertrags verstoßen. Bei Beendigung ist der Lizenznehmer verpflichtet, sowohl die Software, als auch sämtliche Kopien der Software in bereits installierter Form oder gespeichert auf einem Datenträger zu löschen, zu vernichten oder der Telemotive AG zurück zugeben.
- 15. Der Lizenznehmer haftet für alle Schäden, welche dem Lizenzgeber durch die Verletzung dieses Lizenzvertrags entstehen.



# 2. PRODUKTHAFTUNG

Für alle Angebote, Verkäufe und Lieferungen gelten ausschließlich die nachstehenden Bedingungen und zwar auch dann, wenn der Käufer, Besteller und dergleichen andere Bedingungen vorschreibt. Abänderungen sind nur gültig, wenn sie schriftlich vereinbart werden.

- Die Technische Dokumentation ist Bestandteil des Produktes. Werden die Inhalte und insbesondere die Sicherheitshinweise und Handlungsanleitungen der Dokumentation nicht beachtet, kann dies den Ausschluss der Produkthaftung und der Produktgewährleistung zur Folge haben.
- 2. Die Produkte gehören zur Gruppe der Testtools. Bei Einsatz des Gerätes kann eine Störung des zu testenden Systems nicht 100% ausgeschlossen werden. Damit kann die Garantie eines einwandfrei funktionierenden Systems nicht vom Hersteller übernommen werden. Der Einsatz des Produktes erfolgt auf eigene Gefahr.
- Die Haftung f
  ür den Ersatz von Sch
  äden gem
  ä
  ß
  §
  1 des Produkthaftungsgesetzes, wird, im Rahmen des
  §
  9 PHG ausdr
  ücklich ausgeschlossen, soweit zwingende gesetzliche Bestimmungen nichts anderes vorsehen.
- 4. Der Hersteller lehnt in jedem Fall die Verantwortung für indirekte, beiläufige, spezielle oder folgenreiche Schäden, einschließlich dem Verlust von Gewinn, von Einnahmen, von Daten, des Gebrauchs, jedem anderem wirtschaftlichen Vorteils oder Schäden aus Ansprüchen Dritter gegen den Kunden, ab, die aus dieser Abmachung, ob in einer Handlung im Vertrag, strenger Verbindlichkeit, klagbares Delikt (einschließlich der Nachlässigkeit) oder anderen gesetzlichen oder gerechten Theorien entsteht. Die Beweispflicht liegt beim Käufer.
- 5. Die Telemotive AG gewährleistet die gesetzliche Garantie gemäß deutschen Rechts.
- 6. Außer den Garantien, die ausdrücklich in dieser Vereinbarung festgelegt worden sind, werden alle Produkte "geliefert, wie vertraglich vereinbart, soweit der Kunde vom Hersteller nicht ausdrücklich zusätzliche oder implizierten Garantien empfängt. Der Hersteller dementiert hiermit ausdrücklich irgendwelche und alle weiteren Garantien irgendeiner Art oder Natur bezüglich der Produkte, ob ausdrücklich oder stillschweigend, einschließlich unbeschränkt, jede Garantie des Titels, der Marktfähigkeit, der Qualität, der Genauigkeit oder Eignung zu einem bestimmten Zweck oder zum Zweck des Kunden. Der Hersteller streitet ausdrücklich irgendwelche Garantien ab, die vom Handelsbrauch, der Handelssitte oder der Leistung einbezogen werden können. Abgesehen von den festgesetzten ausdrücklichen Garantien in dieser Abmachung, sind die Produkte mit allen Fehlern und der vollständigen Gefahr einer nicht befriedigenden Qualität, Leistung, Genauigkeit bereitgestellt. Der mögliche Aufwand wird vom Kunden getragen. Der Hersteller übernimmt keine Garantie, dass die Produkte fehlerfrei arbeiten.
- 7. Die Telemotive AG ist berechtigt, mangelhafte Waren gegen gleichartige einwandfreie Waren innerhalb einer angemessenen Frist einzutauschen oder den Mangel innerhalb einer angemessenen Frist zu beheben. Bei diesem Fall erlischt ein Anspruch auf Wandlung oder Preisminderung. Gewährleistungsrechte setzen eine rechtzeitige Mängelrüge voraus.
- 8. Der Weiterverkauf, die Weitergabe, Schenkung, Tauschgeschäfte oder der Verleih der angebotenen Produkte an Dritte, ist ohne Freigabe von Telemotive nicht gestattet.
- 9. Als Rechtsgrundlage ist deutsches Recht anzuwenden.

© by Telemotive AG, 2014



## 3. Übersicht

Mit der \*WLAN\* Erweiterung des blue PiraT2 können folgende Funktionen realisiert werden:

- Drahtlose Verbindung mit dem Logger aufbauen
- Konfigurieren des Datenloggers über die WLAN Verbindung
- Herunterladen der Daten über die WLAN Verbindung
- Auslesen der aktuellen Konfiguration über die WLAN Verbindung

# Um die WLAN ("Wireless Lan") Funktionen des blue PiraT2 nutzen zu können ist eine Lizenz notwendig. Alle folgenden Schritte können nur mit einer gültigen Lizenz vorgenommen werden.

Dieses Dokument bezieht sich auf die blue PiraT2 Firmware Version 1.9.1 und blue PiraT2 Client-Version 1.9.1. Einige Eigenschaften und Funktionen variieren je nach Modell und Feature-Lizenz oder stehen in älteren Versionen nicht zur Verfügung.

Software-Updates und Anleitungen für andere, optional erhältliche, Lizenzen stehen im blue PiraT Service Center der Telemotive AG zur Verfügung (Adresse siehe unter Kontakt)

Bitte stellen Sie sicher, dass Sie eine aktuelle Firmware und Software verwenden.

Es gibt zwei verschiedene Möglichkeiten die WLAN Funktion des blue PiraT2 zu verwenden. Der Standard ist die Verwendung des Wireless LAN im "Managed Modus" ("Infrastruktur Modus" oder "Modus A").In diesem Modus wird der Datenlogger blue PiraT2 in die bestehende Netzwerk-Infrastruktur integriert.



Abbildung 1: Infrastruktur-Modus



Der zweite Modus (Modus B) ist die "Ad-hoc" Konfiguration (siehe Abbildung 2). Diese Konfiguration kann verwendet werden, wenn der PC direkt mit dem Datenlogger verbunden werden soll, ohne einen Access Point dazwischen zu schalten.

Hinweis: Der Laptop ist bei Verwendung von "ad-hoc" auch entsprechend zu konfigurieren. Hierfür sind Administratorrechte auf dem Laptop notwendig.



Abbildung 2: Ad-hoc-Modus

# 4. WLAN Konfiguration mit dem Client

Um die WLAN Verbindung (Managed/Ad-hoc) konfigurieren zu können, ist eine Verbindung des Datenloggers mit dem Client auf dem PC notwendig. Bitte verbinden Sie den Datenlogger mit dem PC und starten Sie den Client.

Wenn Sie den Datenlogger zum ersten Mal für WLAN konfigurieren ist eine Verbindung über ein LAN Kabel notwendig. Später können dann Änderungen über eine bestehende WLAN Verbindung gemacht werden.

Ist der Client mit dem Datenlogger verbunden, können Sie die Konfigurations- Applikation starten. Im Logger Konfigurations-Menü im Auswahlbaum findet sich unter dem Eintrag **[Allgemein]** => **[WLAN]** alle Einstellungen für eine WLAN Verbindung.

Um das WLAN Interface zu verwenden, muss dieses aktiviert werden. Hierfür bitte die Checkbox **[WLAN aktivieren]** auswählen.



Konfiguration (10.64.76.61) 8		
Kanäle * Trigger * 🛛 * 👼 *		
Image: Sprachaufzeichnung         Image: Sprachaufzeichnung	Managed       •         SSID)       bpngWLAN         -Modus       WPA-PSK (WPA oder WPA2)         /p       passphrase         /p       •         interview       •         viert       •         satenloggers       192         192       . 168       . 2       . 1         (Default: 192.168.2.1)       . 155       . 255         ss Datenloggers       255       . 255       . 0	Schlüssel anzeigen

Abbildung 3: WLAN Konfiguration

## 4.1. Auswahl der Betriebsarten "Managed" oder "Ad-hoc"

Wählen Sie aus dem Drop Down Menü den Modus aus (siehe Abbildung 4):

## Managed:

Wählen Sie **[Managed]**, um den Datenlogger in einem bestehenden Infrastruktur LAN Netzwerk mit WLAN Access Point zu verwenden.

## Ad-hoc:

Direkte Verbindung von PC/Laptop (bluePiraT2 Client) mit dem Datenlogger.

🗐 🖓 🔁 Allgemein	WLAN	
	WLAN aktiv	
···· 🦉 Netzwerkeinstellungen		
Puffer	Betriebsart	Managed 🗸
···· 🦉 Komprimierung		Managed
🖉 Ruhezustand	Netzwerk Name (ESSID)	Ad-hoc by
🤌 Sprachaufzeichnung	Authentifizierungs-Modus	WPA-PSK (WPA oder WPA2)
🤌 Kaskadierung		
🥭 Zeitzone	Verschlusselungstyp	passphrase 🗸 🗸
🖉 GPS	Schlüssel	•••••
MLAN CAN	DHCP-Modus	





bP2_WLAI	Anleitung	_V1.9.1.doc
----------	-----------	-------------

## 4.2. Konfigurieren der Netzwerk ESSID

Der Netzwerkname kann individuell vom Benutzer gesetzt werden (siehe Abbildung 5).

## Managed:

Für den "Infrastruktur Modus" (Managed) muss die ESSID (Netzwerk Name) des Funknetzwerkes eingegeben werden, mit dem der Logger verbunden werden soll.

## AD-hoc:

Hier kann der Benutzer die ESSID frei konfigurieren, um sich später mit dem Datenlogger zu verbinden.

Kanāle * Trigger *	条 Konfiguration (10.64.76.61) 🛛 🛚 🛛			
Image: Allgemein     WLAN       Image: Allgemein     Image: Allgemein	Kanäle 🔹 Trigger 👻 🔜 👻 👻			
Ruhezustand   Sprachaufzeichnung   Kaskadierung   Kaskadierung   Zeitzone   GPS   WLAN     Hersen   WLAN     Hersen   CAN   Hersen   Serial   Hersen   Hersen <tr< td=""><td>Allgemein     Allgemein     Netzwerkeinstellungen     Puffer     Puffer     Puffer     Puffer     Putfer     Potfer     Synachaufzeichnung     Putfer     Zeitzone     PoS     PutAn     PoS     PoS     PutAn     PoS     PoS</td><td>WLAN WLAN aktiv Betriebsart Netzwerk Name (ESSID) Authentifizierungs-Modus Verschlüsselungstyp Schlüssel DHCP-Modus O DHCP-Client DHCP-Client DHCP deaktiviert IP-Adresse des Datenlogs Subnetzmaske des Daten</td><td>Managed       •         bpngWLAN       •         wPA-PSK (WPA oder WPA2)       •         passphrase       •         gers       192       •         168       2       •         (Default: 192.168.2.1)       •         loggers       255       •         255       •       0         (Default: 255.255.255.0)       •</td><td>Schlüssel anzeigen</td></tr<>	Allgemein     Allgemein     Netzwerkeinstellungen     Puffer     Puffer     Puffer     Puffer     Putfer     Potfer     Synachaufzeichnung     Putfer     Zeitzone     PoS     PutAn     PoS     PoS     PutAn     PoS     PoS	WLAN WLAN aktiv Betriebsart Netzwerk Name (ESSID) Authentifizierungs-Modus Verschlüsselungstyp Schlüssel DHCP-Modus O DHCP-Client DHCP-Client DHCP deaktiviert IP-Adresse des Datenlogs Subnetzmaske des Daten	Managed       •         bpngWLAN       •         wPA-PSK (WPA oder WPA2)       •         passphrase       •         gers       192       •         168       2       •         (Default: 192.168.2.1)       •         loggers       255       •         255       •       0         (Default: 255.255.255.0)       •	Schlüssel anzeigen

Abbildung 5: Netzwerknamen eingeben



## 4.3. Konfigurieren des Authentifizierungs-Verfahren

Folgende Authentifizierungs-Verfahren können verwendet werden (siehe Abbildung 6):

## WEP (Wired Equivalent Privacy):

WEP ist ein Verschlüsselungsverfahren für Drahtlosnetzwerke nach dem IEEE 802.11Standard. Ein bestimmter Schlüssel wird in den einzelnen Clients abgespeichert.

## WEP-Open:

Der Client Schlüssel muss mit dem Schlüssel des Access-Points (AP) übereinstimmen.

## WEP-Shared Key:

Arbeitet mit einer "Challenge Response" Prozedur. Der Client sendet eine Anfrage an den AP. Der AP sendet einen zufälligen Text zurück zum Client. Der Client verschlüsselt den Text mit seinem Schlüssel und sendet den an den AP zurück. Anschließend entschlüsselt der AP den eingehenden Text mit seinem Schlüssel und beide Texte müssen dann übereinstimmen.

## WEP-Open (ohne Authentifizierung):

Bei diesem Verfahren muss kein Schlüssel eingegeben werden. Somit kann sich jeder mit diesem Netzwerk verbinden.

## WPA-PSK (Pre Shared Key):

Der Schlüssel des Benutzers ist im Voraus bekannt. Die Schlüssel werden vor der Kommunikation ausgetauscht. Die gesicherten und übertragenden Schlüssel müssen übereinstimmen.

## Hinweis: Dieser Schlüssel kann nicht im Ad-hoc Modus verwendet werden.

Konfiguration (10.64.76.61) - Verbindung getrennt	1			
Kanäle 🛪 Trigger 🛪 🔤 🔹				
Image: Second	WLAN WLAN aktiv Betriebsart Netzwerk Name (ESSID) Authentifizierungs-Modus Verschlüsselungstyp Schlüssel DHCP-Modus  OHCP-Client DHCP deaktiviert IP-Adresse des Datenlog Subnetzmaske des Dater	Managed bpngWLAN WPA-PSK (WPA oder WPA2) WEP-Open (ohne Authentifizierung) WEP-Share Key WPA-PSK (WPA oder WPA2) gers 192 · 168 · 2 · 1 iloggers 255 · 255 · 255 · 0	(Default: 192.168.2.1) (Default: 255.255.255.0)	Schlüssel anzeigen

## Abbildung 6: Auswahl des Authentifizierungs-Verfahrens

Für den Managed Modus wählen Sie bitte den [Authentifizierungs-Modus] welcher von Ihrem Access Point (AP) eingestellt und verwendet wird.

Für Ad-hoc und Master Modus wählen Sie bitte den [Authentifizierungs-Modus], welcher für die Verbindung zwischen Logger und Endgerät verwendet werden soll. Auf beiden Seiten muss das gleiche Authentifizierungs-Verfahren verwendet werden.



## 4.4. Verbindungs-Schlüssel Typen

Bitte wählen Sie den Verbindungs-Schlüssel Typ (siehe Abbildung 7):

## Passphrase:

Sicherheitsschlüssel wird aus einem Passwort generiert.

## ASCII:

Sicherheitsschlüssel muss gesetzt werden und wird im ASCII-Code angezeigt.

#### Hexadezimal:

Sicherheitsschlüssel muss eingestellt werden und wird in Hexadezimal Zeichen angegeben.

📫 Konfiguration (10.64.76.61) - Verbindung getrennt 👘	8			
Kanäle 🔹 Trigger 👻 🔜 👻				
Kanale * Trigger *       *         Allgemein         Allgemein         Puffer         Puffer         Strachaufzeichnung         Strachaufzeichnung         Zeitzone         PS         WLAN         E- Serial         E- Serial<	WLAN VULAN aktiv Betriebsart Netzwerk Name (ESSID) Authentifizierungs-Modus Verschlüsselungstyp Schlüssel DHCP-Modus OHCP-Client DHCP-Client DHCP deaktiviert IP-Adresse des Datenlogg Subnetzmaske des Datenl	Managed bpngWLAN WEP-Open passphrase hexadecimal passphrase ASCII gers 192 · 168 · 2 oggers 255 · 255 · 2	(Default: 192.168.2     (Default: 255.255	1) 1) 1)

Abbildung 7: Auswahl des Verschlüsselungstyps

## 4.5. Schlüssel und Schlüssellänge

## Wählen Sie die Schlüssellänge für WEP:

64 bit:	40 bit + Initialisierungs Vec Hexadezimal ASCII passphrase	tor 24 bit: → 10 Zeichen → 5 Zeichen → individuelle Länge
128 bit:	104 bit + Initialisierungs Ve Hexadezimal ASCII passphrase	ector 24 bit: → 26 Zeichen → 13 Zeichen → individuelle Länge

## Für WPA ist die Verschlüsselung mit 256 Bit definiert:

Hexadezimal	→ 64 Zeichen
ASCII	→ nicht verfügbar
passphrase	→ 8 bis 63 Zeichen



Konfiguration (10.64.76.61) - Verbindung getrennt 🛛 🕸				
Kanäle 🔹 Trigger 👻 🔯 🔹 🐺				
Kahale + Higger • Imp + Imp •         Image: Aligemein         Image: Aligem	WLAN  WLAN aktiv  Betriebsart Netzwerk Name (ESSID) Authentifizierungs-Modus Verschlüssellungstyp Schlüssel DHCP-Modus  OHCP-Client DHCP-Client DHCP deaktiviert IP-Adresse des Datenlogg Subnetzmaske des Datenlog	Managed   bpngWLAN  WEP-Open  passphrase  128  64  ers  192  168  2  1  oggers  255  255  255  0	(Default: 192.168.2.1) (Default: 255.255.255.0)	Schlüssel anzeigen

Abbildung 8: Auswahl der Schlüssellänge

## 4.6. Schlüsseleingabe

Der Schlüssel wird durch den Benutzer gesetzt. Die Schlüssel-Länge hängt vom eingestellten Authentifizierungs-Modus und der gewählten Schlüssellänge ab (siehe Abschnitt 4.5).

Ist der eingegebene Schlüssel nicht kompatibel zu den Einstellungen, erscheint ein Fehler und eine Anzeige im Infobereich (siehe Abbildung 9).

🛟 Konfiguration (10.64.76.61) 🛛 🛛 🖉			
Kanäle 🔹 Trigger 👻 🌄 🔹 🌄			
🗐 📄 Allgemein	WLAN		
Name	WLAN aktiv		
Netzwerkeinstellungen			
Komprimierung	Betriebsart	Managed 👻	
P Ruhezustand	Netzwerk Name (ESSID)	bpngWLAN	
	Authentifizierungs-Modus	WEP-Open 👻	
Kaskadierung	Verschlüsselungstyp	ASCII	
	Schlüssellänge	128	
WLAN	Schlüssel		Schlüssel anzeigen
	DUCD Madua		
	DHCP-Modus		
🗈 🖻 FlexRay	DHCP doaktiviort		
MOST		102 100 2 (Default: 192 168 2 1)	
Humen Analog	IP-Adresse des Datenlogg		
🗊 🔚 Digitaler Eingang	Subnetzmaske des Dateni	oggers 255 . 255 . 255 . 0 (Detault: 255.255.255.0)	
🖶 🗁 🛅 Digitaler Ausgang			
🖶 🔚 Kamera			
Online Streaming			
🗄 🛅 Datenbasen	🕖 Die Zeichenlänge des Schlü	issels muss genau 13 betragen. Aktuell: 26	
	Defaultkonfigura	tion Von Datei laden Als Datei speichern Vom Log	gger lesen Zum Logger senden

Abbildung 9: Fehler bei der Schlüsseleingabe

# Telemotive AG

## 4.7. DHCP Modus

Zuletzt muss nun der DHCP Modus (Dynamic Host Configuration Protocol) konfiguriert werden. DHCP erlaubt die Zuordnung der IP-Adresse des Loggers über einen Server.

## **DHCP Server:**

Die zu verbindenden Endgeräte beziehen die IP-Adresse/Subnetzmaske vom Datenlogger. Diese Einstellung wird nur vom Master Modus unterstützt.



Abbildung 10: Einstellung "DHCP Server"

## **DHCP Client:**

Die Zuordnung der IP-Adresse/Subnetzmaske gegenüber dem Logger wird vom Server durchgeführt.



## Abbildung 11: Einstellung "DHCP-Client"

## **DHCP deaktiviert:**

Wenn DHCP deaktiviert ist muss die IP Adresse und Subnetzmaske bekannt sein und manuell konfiguriert werden.



Abbildung 12: Einstellung "DHCP-Deaktiviert"

#### Hinweis:

Die Gegenstelle muss zusätzlich manuell konfiguriert werden. Hierfür werden Administrationsrechte auf dem Rechner benötigt. Für den Ad-hoc-Modus ist es ratsam, die IP-Adresse/Subnetzmaske manuell auf beiden Seiten zu konfigurieren.





## 4.8. Einstellungen zum blue PiraT2 übertragen

Wenn alles konfiguriert ist, kann die Konfiguration mit der Schaltfläche **[Zum Logger senden]** (rechts unten) zum Datenlogger übertragen werden.

## Hinweis:

Die Konfiguration auf dem Datenlogger wird erst nach einem Neustart des Datenloggers aktiv.



## 5. Weiterführende Informationen und Konfiguration am Laptop

Wenn für den Ad-hoc Modus die IP Adresse/Subnetzmaske manuell gesetzt werden muss, dann ist kein DHCP Service möglich. Es kann auch sein das DHCP im Infrastruktur Netzwerk nicht möglich ist. Auch dann müssen IP Adresse und Subnetzmaske manuell gesetzt werden.

Hierfür öffnen Sie bitte den [Status] der WLAN-Netzwerkkarte.

Die Einstellungen der WLAN Karte können dann über [Eigenschaften] erreicht werden.

#### Hinweis: Administrations-Rechte sind notwendig

ff]] Status von Drahtlosnetzwerkve	erbindung 🛛 🔍
Allgemein	
Verbindung	
IPv4-Konnektivität:	Kein Internetzugriff
IPv6-Konnektivität:	Kein Internetzugriff
Medienstatus:	Aktiviert
Kennung (SSID):	TMW
Dauer:	00:33:38
Übertragungsrate:	54,0 MBit/s
Signalqualität:	atl.
Details Drahtloseig	enschaften
Aktivität	
Gesendet —	Empfangen
Bytes: 0	adddi   180
👻 Eigenschaften 🛛 🛞 Dea	ktivieren Diagnose
L	Schließen

#### Abbildung 13: Status der Drahtlosnetzwerkverbindung

Jetzt können Sie Ihr TCP / IP-Protokoll wählen (siehe Abbildung 14). Bitte stellen Sie sicher, dass Sie das richtige Kommunikationsprotokoll verwenden. Hierfür kontaktieren Sie bei Bedarf bitte Ihren Netzwerk Administrator.

Klicken Sie auf den Namen Ihres verwendeten WLAN-Protokolls und dann auf [Eigenschaften].



Eigenschaften von Drahtlosnetzwe	rkverbindung 🔀
Verbindung herstellen über:	
Intel(R) Centrino(R) Advanced-N	6230
	Konfigurieren
Client für Microsoft-Netzwerke     Gos-Paketplaner     Gos-Pa	Microsoft-Netzwerke (P/IPv6) (P/IPv4) hicht-Topologieerkennun t-Topologieerkennung
Installieren Deinstallieren Eigenschaften Beschreibung TCP/IP, das Standardprotokoll für WAN-Netzwerke, das den Datenaustausch über verschiedene, miteinander verbundene Netzwerke ermöglicht.	
[	OK Abbrechen

## Abbildung 14: Eigenschaften der Drahtlosnetzwerkverbindung

Wählen Sie **[Folgende IP Adresse verwenden]** und geben Sie IP Adresse und Subnetzmaske ein (siehe Abbildung 15). Verwenden Sie für Ihren PC eine IP Adresse im Subnetz des Datenloggers. Als Standardgateway wird die IP Adresse des Loggers eingegeben.

Wählen Sie **[Folgende DNS Server Adressen verwenden:]** und geben Sie hier ebenfalls die IP Adresse des blue PiraT2 ein.

#### Hinweis:

Die manuelle Einstellung der IP Adresse/Subnetzmaske darf nur erfolgen, wenn kein DHCP-Server im Netz vorhanden ist.

Allgemein IP-Einstellungen können automatisc Netzwerk diese Funktion unterstütz den Netzwerkadministrator, um die heziehen	h zugewiesen werden, wenn das t. Wenden Sie sich andernfalls an geeigneten IP-Einstellungen zu
<ul> <li>IP-Adresse automatisch bezieh</li> </ul>	nen
<ul> <li>Folgende IP-Adresse verwend</li> </ul>	en:
IP-Adresse:	192.168.2.2
Subnetzmaske:	255 . 255 . 255 . 0
Standardgateway:	192.168.2.1
DNS-Serveradresse automatis	ch beziehen
— Folgende DNS-Serveradressen	n verwenden:
Bevorzugter DNS-Server:	192.168.2.1
Alternativer DNS-Server:	· · ·
Einstellungen beim Beenden ü	iberprüfen
	Erweitert
	OK Abbrechen

## Abbildung 15: Eigenschaften des Internetprotokolls

# Telemotive AG

# 6. Verbindung mit dem Datenlogger über WLAN

## Schritt 1:

Verbinden Sie den PC/Laptop mit dem vorher konfigurierten Netz.

## Schritt 2:

Öffnen Sie den Client und schauen sie in die Netzwerklogger Liste. Bei erfolgreicher Verbindung vom blue PiraT2 via WLAN erscheint der Logger (siehe Abbildung 16) in der Liste mit WLAN Symbol (🛜).

Netzwerk-Logger 88			-
Name	IP	Verbunden mit	
ੂ DUT_114	192.168.0.233 192.168.2.1		
+ IP-Direkteingabe			

Abbildung 16: Liste der Logger im Netzwerk



# 7. Abbildungsverzeichnis

Abbildung 1: Infrastruktur-Modus	4
Abbildung 2: Ad-hoc-Modus	5
Abbildung 3: WLAN Konfiguration	6
Abbildung 4: WLAN Betriebsart einstellen	6
Abbildung 5: Netzwerknamen eingeben	7
Abbildung 6: Auswahl des Authentifizierungs-Verfahrens	8
Abbildung 7: Auswahl des Verschlüsselungstyps	9
Abbildung 8: Auswahl der Schlüssellänge	. 10
Abbildung 9: Fehler bei der Schlüsseleingabe	. 10
Abbildung 10: Einstellung "DHCP Server"	. 11
Abbildung 11: Einstellung "DHCP-Client"	. 11
Abbildung 12: Einstellung "DHCP-Deaktiviert"	. 11
Abbildung 13: Status der Drahtlosnetzwerkverbindung	. 13
Abbildung 14: Eigenschaften der Drahtlosnetzwerkverbindung	. 14
Abbildung 15: Eigenschaften des Internetprotokolls	. 14
Abbildung 16: Liste der Logger im Netzwerk	. 15



#### 8. Kontakt



## **Telemotive AG**

Büro München Frankfurter Ring 115a 80807 München

Tel.:	+49 89 357 186-0
Fax.:	+49 89 357 186-520
E-Mail:	info@telemotive.de
Web:	www.telemotive.de

Vertrieb	
Tel.:	+49 89 357 186-550
Fax.:	+49 89 357 186-520
E-Mail:	sales@telemotive.de

Support +49 89 357 186-518 E-Mail: produktsupport@telemotive.de https://sc.telemotive.de/bluepirat ServiceCenter:



Tel.:

