Weisungen

zur Verordnung des EJPD über Messmittel für Geschwindigkeitskontrollen und Rotlichtüberwachungen im Strassenverkehr (Geschwindigkeitsmessmittelverordnung; SR 941.261)

(Weisungen über Geschwindigkeitsmessmittel)

vom 12. Januar 2009

Das Bundesamt für Metrologie (METAS),

gestützt auf Artikel 17 des Bundesgesetzes vom 9. Juni 1977[1] über das Messwesen sowie auf Artikel 1, Artikel 2, Artikel 4 Absatz 2, Artikel 4 Absatz 3 und Artikel 4 Absatz 4 der Verordnung des EJPD vom 31. März 2009[2] über Messmittel für Geschwindigkeitskontrollen und Rotlichtüberwachungen im Strassenverkehr (Geschwindigkeitsmessmittelverordnung),

erlässt folgende Weisungen:

1. Gegenstand

Die Weisungen regeln insbesondere:

- die Mindestanforderung über die Zugriffssicherheit auf Datenverarbeitungskomponenten von Messmitteln für Geschwindigkeitskontrollen und Rotlichtüberwachungen im Strassenverkehr;
- die Mindestanforderung an den Umgang mit von Messmitteln und Messverfahren mit digitaler Datenübertragung in der Verkehrsüberwachung generierten Daten;
- die Mindestanforderungen an elektromagnetische Störfestigkeit;
- die Mindestanforderung an den Einsatz von Blitzleuchten bei Rotlichtüberwachungsanlagen und Geschwindigkeitsmessungen im Strassenverkehr.

---

[1] SR **941.20**
[2] SR **941.261**

2. Geltungsbereich

Die Weisungen gelten für Messmittel, welche unter Artikel 2 der Geschwindigkeitsmessmittelverordnung fallen.

3. Aufhebung bisheriger Vorschriften

Alle vorhergehenden Weisungen betreffend Messmittel, welche unter Artikel 2 der Geschwindigkeitsmessmittelverordnung fallen, werden aufgehoben.

4. Inkrafttreten

Diese Weisungen treten am 31. März 2009 in Kraft.

Bundesamt für Metrologie

Der Direktor

Dr. Christian Bock

I. Mindestanforderung über die Zugriffssicherheit auf Datenverarbeitungskomponenten von Messmitteln für Geschwindigkeitskontrollen und Rotlichtüberwachungen im Strassenverkehr

Zweck und Geltungsbereich

Die vorliegenden Weisungen legen die minimalen Sicherheitsanforderungen an den Zugriff auf Daten und an die Konfiguration von Verkehrsüberwachungssystemen (nachfolgend System genannt) – mit Verweisen auf die entsprechenden Standards – fest.

A. Systeme mit Verbindung an eine Zentrale [802.1x], [EAP]

1. Authentifizierung

Es muss sichergestellt sein, dass nur berechtigte (d.h. authentifizierte Benutzer) Zugriff auf das System haben:

Die Benutzer des Systems müssen sich daher beim Betreiber des Systems bzw. in der Zentrale authentifizieren lassen. Die Authentifizierung erfolgt mindestens nach dem Standard IEEE 802.1x.

Der heutige Mindeststandard zur Authentifizierung in Rechnernetzen ist IEEE 802.1x. Er stellt eine generelle Methode für die Authentifizierung und Autorisierung in IEEE 802-Netzen zur Verfügung.

Am Netzwerkzugang erfolgt die Authentifizierung eines Teilnehmers (Client) durch den Authenticator. Dieser gibt die Authentifizierungsnachricht an den Authentifizierungsserver weiter, welcher die übermittelten Informationen prüft und gegebenenfalls den Zugriff auf die durch den Authenticator angebotenen Dienste zulässt oder abweist. Für diesen Authentifizierungsablauf können mehrere Mechanismen verwendet werden: die Mitteilungsformate sind mindestens mit dem Extensible Authentication Protocol (EAP) zu definieren.

2. Protokollierung des Netzwerkzugangs

Jeder Netzwerkzugang bzw. jeder versuchte Zugriff auf das System muss auf dem zentralen Authentifizierungsserver (RADIUS-Server) protokolliert werden. Die entsprechenden Aufzeichnungen sind gemäss den jeweiligen (kantonalen) Datenschutz- bzw. Archivierungsrichtlinien aufzubewahren.

3. Passwörter

Die Passwörter haben aus mindestens acht Zeichen zu bestehen und müssen mindestens zwei Zahlen oder Sonderzeichen enthalten. Sie sind geheim zu halten und dürfen nicht weitergegeben werden. Beim Verdacht, dass Unberechtigte sie kennen, sind sie unverzüglich zu ändern.

B. Systeme ohne Netzanbindung an die Zentrale [TOKEN]

1. Authentifizierung

Bei einem System ohne Netzanbindung an die Zentrale muss die Authentifizierung eines Teilnehmers durch einen dem Stand der Technik entsprechenden Security-Token erfolgen. Die Security-Token sind von der Zentrale zu verwalten.

Beispiele sicherer Security-Token:

SecurID token von RSA Security:

eToken tokens von Aladdin Knowledge Systems:

Als Security-Token wird eine Hardwarekomponente bezeichnet, die in der Regel eine Chipkarte enthält, aus der Daten weder herauskopiert noch manipuliert werden können.

2. Protokollierung des Netzwerkzuganges

Jeder Netzwerkzugang bzw. jeder versuchte Zugriff auf das System muss protokolliert werden. Die entsprechenden Aufzeichnungen sind gemäss den jeweiligen (kantonalen) Datenschutz- bzw. Archivierungsrichtlinien aufzubewahren.

3. Passwörter

Die Passwörter haben aus mindestens acht Zeichen zu bestehen und müssen mindestens zwei Zahlen oder Sonderzeichen enthalten. Sie sind geheim zu halten und dürfen nicht weitergegeben werden. Beim Verdacht, dass Unberechtigte sie kennen, sind sie unverzüglich zu ändern.

C. Systeme mit WLAN / wireless network

Für den Fall, dass ein System Daten drahtlos übermittelt, ist zusätzlich Folgendes zu beachten:

1. Datenverschlüsselung

Alle Daten müssen mindestes nach dem IEEE-Standard 802.11i verschlüsselt werden (der IEEE-Standard 802.11i, auch bekannt als WPA2, ist ein im Juni 2004 ratifiziertes Sicherheitsprotokoll für WLAN und umfasst die Regeln für die Verwendung von Advanced Encryption Standard [AES] zur Verschlüsselung von Daten).

2. Sendeleistung WLAN

Zur Erhöhung der Sicherheit sollte zusätzlich die Reichweite der drahtlosen Verbindung durch Einstellen der maximalen Leistung des Wireless-Access-points auf die notwendige Distanz begrenzt werden.

D. Systeme mit Anschluss ans Internet

Aus Sicherheitsgründen ist es untersagt, Systeme direkt mit dem Internet zu verbinden.

E. Systeme mit mehreren Zugriffsmöglichkeiten

Können die Daten auf verschiedene Arten (z.B. Funk und Kabel) übertragen werden, soll grundsätzlich diejenige Methode verwendet werden, welche die höchste Daten- und Zugriffssicherheit gewährleistet.

II. Anforderungen in Zusammenhang mit der digitaler Datenübertragung in der Verkehrsüberwachung

Zweck und Geltungsbereich

Diese Weisungen legt die Anforderungen an Messmittel und Messverfahren für physikalische Grössen (Bild- und Messdaten) fest, bei welchen eine digitale Bilddokumentation erstellt und zusammen mit den Messdaten mit einem digitalen Datenübertragungssystem in die Auswertezentrale übertragen wird. Das Datenübertragungssystem ist Bestandteil des Messverfahrens, bei dem der (rechtlich verbindliche) Wert der Messgrösse am Ende der Datenübertragung mit Hilfe einer Auswertesoftware entsteht.

1. Datenschutz

Die von den Messmitteln erfassten bzw. von den Messverfahren ermittelten Daten sind grundsätzlich Personendaten. Die entsprechenden (kantonalen) Datenschutzbestimmungen – insbesondere über deren Verwendung, Weitergabe und (zeitliche) Aufbewahrung – sind einzuhalten.

2. Technische Anforderungen an die Daten

2.1 Datenintegrität

Die Integrität und Vertraulichkeit der Daten müssen garantiert sein. Die Authentizität der Daten muss sowohl nachvollziehbar sein: das mit einer digitalen Signatur versehene Datenfile darf nach seiner Aufzeichnung nicht verändert werden.

Eine Veränderung der aufgezeichneten Daten hat grundsätzlich die Ungültigkeit der Daten zur Folge.

2.2 Daten als Beweismittel

Als Beweismittel taugen grundsätzlich nur Daten, welche bei der Auswertung mit Hilfe der digitalen Signatur als korrekt übermittelt erkannt wurden. Der Beweisdatensatz ist daher zusammen mit dem Signaturschlüssel im Original sicher aufzubewahren. Datensätze, welche nachträglich weiterverarbeitet und in anderer Form gespeichert werden, gelten als Kopie.

2.3 Aufbewahrungszeit

Die zeitliche Verfügbarkeit der Daten ist – insbesondere mit Blick auf länger dauernde (Gerichts-)Verfahren – zu gewährleisten. METAS empfiehlt eine Aufbewahrungszeit von mindestens 5 Jahren.

2.4 Zusätzliche Vorschriften

Zusätzlich ist insbesondere zu beachten:

2.4.1 Veränderung von Daten

Jede Veränderung von Daten und der zugehörigen Bilddokumentation muss feststellbar sein.

2.4.2 Verschlüsselung von Daten

Zur Wahrung der Vertraulichkeit müssen die Daten auf ungeschützten Übertragungskanälen verschlüsselt übertragen werden.

2.4.3 Verfahren zur Sicherstellung

Die angewandten Verfahren zur Sicherstellung dieser Anforderungen müssen transparent und nachvollziehbar sein.

2.4.4 Zeitstempel

Die Datensätze (Bild- und Messdatensatz) sind einzeln mit einem Zeitstempel (Datum und Uhrzeit) zu versehen.

2.4.5 Übertragung

Bild- und Messdatensatz müssen nachweisbar zusammengehören und sind integral als Beweisdatensatz zu übertragen. Die Datenübertragung erfolgt nur auf dem unidirektionalen Weg vom Messsystem zur Datenauswertung.

2.4.6 Datenformate und Übertragungsraten

Proprietäre Datenformate und Übertragungsraten sind gestattet.

2.4.7 Komprimierung von Daten

Werden die Daten vor der Übertragung mit einem irreversiblen Verfahren komprimiert, muss mindestens 80-% Bildqualität gewährleistet bleiben.

2.4.8 Identität des Absenders

Die Identität des Absenders muss im Beweisdatensatz enthalten und feststellbar sein.

2.4.9 Nachträgliche Veränderung

Eine nachträgliche Veränderung des Beweisdatensatzes muss feststellbar sein.

2.4.10 Digitale Signatur

Der Beweisdatensatz muss vor der Übertragung mit einer dem Stand der Technik entsprechenden und anerkannten digitalen Signatur versehen werden.

2.4.11 Verschlüsselung

Die Daten sind vor der Übertragung auf ungeschützten Übertragungswegen nach dem Stand der Technik zu verschlüsseln. Werden die Daten auf einem geschützten Übertragungsweg (nur autorisierte Personen haben Zugriff) übermittelt, so ist eine Verschlüsselung nicht zwingend notwendig.

2.4.12 Schutz der Messanlage

Die Messanlage vor Ort ist physisch so zu schützen, dass ein Zugriff auf funktionale Komponenten durch Unberechtigte ohne Gewaltanwendung nicht möglich ist. Jeder Zugriff auf Daten oder Programme der Messanlage (Kamera und Messmittel) muss im Messsystem durch Zugriffsrechte geregelt sein. Der Zugriff auf das Messsystem ist nur vor Ort mit “Administrator-Rechten“ via Terminal gestattet. Die Zugriffsrechte sind METAS mitzuteilen.

2.4.13 Programmtransfers

Ein “Programmtransfer“ (Software-Updates, usw.), ausgenommen der Datentransfer, ist über den geschützten oder ungeschützten Übertragungsweg nicht gestattet.

2.4.14 Passwörter

Der Zugang zum Programmteil jeder Messanlage ist durch ein individuelles Passwort abzusichern.

III. Anforderungen an elektromagnetische Störfestigkeit

Zweck und Geltungsbereich

Elektromagnetische Umgebungsbedingungen müssen sowohl grundsätzlich allgemeine Anforderungen bzw. die Kriterien der Klasse E2 (vgl. unten, Ziffer 1) als auch zusätzlich weitere Anforderungen (vgl. unten, Ziffer 2) erfüllen.

Für Messmittel mit Stromversorgung durch die Fahrzeugbatterie gelten die oben erwähnten allgemeinen Anforderungen, die zusätzlichen Anforderungen sowie – darüber hinaus – weitere (vgl. unten, Ziffer 3) spezielle Anforderungen erfüllen:

1. Allgemeine Kriterien

Die allgemeinen Mindestkriterien der Klasse E2 lauten (vgl. Anhang 1, Ziffer 1.3.3 der Messmittelverordnung; SR 941.210) sind wie folgt zu interpretieren:

2.1 Kriterium A:

Das Messmittel soll während und nach dem Test ungestört arbeiten. Weder Effizienzverschlechterung noch Funktionsverlust sind erlaubt. Die verlangten Fehlergrenzen bleiben gehalten.

2.2 Kriterium B:

Das Messmittel soll nach dem Test ungestört arbeiten. Weder Effizienzverschlechterung noch Funktionsverlust sind erlaubt. Die verlangten Fehlergrenzen bleiben gehalten. Während dem Test ist eine Effizienzverschlechterung oder ein Funktionsverlust erlaubt, unter der Annahme dass keine fehlerbehafteten Daten verarbeitet werden. Keine Zustandsänderung und keine Datenänderung sind erlaubt.

2.3 Kriterium C:

Funktionsverlust ist erlaubt unter der Voraussetzung dass die Funktion vom Messmittel selbständig wieder herstellt wird oder dass sie bei manuellem Eingriff auf die Steuerung wieder hergestellt werden kann. Für automatische Messmittel muss dieses Prozess voll automatisch laufen.

Einflussgrösse	**Bewertungskriterium**
Spannungsunterbrechungen	C
Kurzzeitige Spannungsabfälle (für Spannungsabfälle auf 0 % während eines Zyklus) Kurzzeitige Spannungsabfälle (in übrigen Fällen)	B C
Spannungstransienten in Versorgungs- und/oder Signalleitungen	B

Entladung statischer Elektrizität	B
Elektromagnetische Hochfrequenzfelder	A
Leitungsgeführte elektromagnetische HF-Felder in Versorgungs- und/oder Signalleitungen	A
Stossspannungen in Versorgungs- und/oder Signalleitungen	B
Netzfrequente magnetische Felder	A

2. Zusätzlichen Anforderungen

Neben den Kriterien der Klasse E2 (vgl. oben, Ziffer 1) müssen, die folgenden Mindestanforderungen zusätzlich erfüllt sein:

Einflussgrösse	**Prüfschärfegrad**	**Bewertungskriterium**
Elektromagnetische HF-Felder	Von 80 MHz bis 1 GHz: 20 V/m, 80 % AM (1 kHz) Von 1,4 GHz bis 2,0 GHz: 20 V/m, 80 % AM (1 kHz) Von 2,0 GHz bis 2,7 GHz: 10 V/m, 80 % AM (1 kHz) Der spezifizierte Prüfschärfegrad ist das quadratische Mittel vom unmodulierten Signal.	A
Leitungsgeführte elektromagnetische HF-Felder in Versorgungs- und/oder Signalleitungen	Von 150 kHz bis 80 MHz: 20 V, 80 % AM (1 kHz) Der spezifizierte Prüfschärfegrad ist das quadratische Mittel vom unmodulierten Signal.	A

3. Spezielle Anforderungen (nur bei Verwendung von Messmitteln mit Stromversorgung durch die Fahrzeugbatterie)

Für Messmittel mit Stromversorgung durch die Fahrzeugbatterie gelten die oben erwähnten allgemeinen Anforderungen (vgl. oben Ziffer 1), die zusätzlichen Anforderungen (vgl. oben 2) sowie – darüber hinaus – folgende, untenstehende Mindestanforderungen:

Einflussgrösse	**Prüfschärfegrad für 12 V Systeme**	**Prüfschärfegrad für 24 V Systeme**	**Bewertungskriterium**
Spannungstransienten in Versorgungsleitungen, die durch induktive Lasten erzeugt werden.	–100 V	600 V	C
Spannungstransienten in Versorgungsleitungen, die durch die abrupte Unterbrechung von Strömen in	+50 V	+50 V	B

Einflussgrösse	**Prüfschärfegrad für 12 V Systeme**	**Prüfschärfegrad für 24 V Systeme**	**Bewertungskriterium**
parallel geschalteten Geräten erzeugt werden.			
Spannungstransienten in Versorgungsleitungen, die von DC Motoren erzeugt werden wenn sie als Generator wirken nachdem die Zündung ausgeschaltet wird.	+10 V	+20 V	C
Spannungstransienten in Versorgungsleitungen, die durch Schaltvorgänge erzeugt werden.	Negative Transienten 150 V Positive Transienten 100 V	Negative Transienten 200 V Positive Transienten 200 V	A
Spannungsabfälle, die durch das Einschalten der Starter-Motor-Stromkreise von Verbrennungsmotoren verursacht werden.	7 V	16 V	B
Spannungstransienten in Signalleitungen, die durch Schaltvorgänge erzeugt werden.	Negative Transienten 60 V Positive Transienten 40 V	Negative Transienten 80 V Positive Transienten 80 V	A

IV. Anforderungen an den Einsatz von Blitzleuchten bei Rotlicht-Überwachungsanlagen und Geschwindigkeitsmessungen im Strassenverkehr

Zweck und Geltungsbereich

Beim Einsatz von Rotlichtüberwachungs- und Geschwindigkeitsmessanlagen bei Dunkelheit werden beim Fotografieren in der Regel Blitzleuchten verwendet, damit ein erfasstes Fahrzeug eindeutig identifiziert werden kann. Die Aufnahme wird dabei häufig frontal gemacht, damit gleichzeitig mit dem Fahrzeug auch der Fahrer erkannt werden kann.

Fotoblitze sind für den Fahrzeuglenker ein unvorhergesehenes, nicht einkalkulierbares Einzelereignis. Verschiedene Untersuchungen (Lichttechnisches Institut Karlsruhe, Augenklinik Tübingen) haben gezeigt, dass intensive Blitze – vor allem Weissblitze – die Sehfähigkeit des Fahrzeuglenkers für kurze Zeit stark beeinträchtigen können.

1. Anforderungen beim Einsatz von Blitzleuchten bei Heckfotografien

Für Heckfotografien dürfen grundsätzlich alle zugelassenen Arten von Blitzleuchten eingesetzt werden. Es wird empfohlen, wenn möglich wenig intensive Weissblitze oder rotfarbige Blitze einzusetzen.

2. Anforderungen beim Einsatz von Blitzleuchten bei Frontfotografien

2.1 Unbeleuchtete Strassen

Frontblitzleuchten, welche im Bereich der Augenhöhe des Fahrzeuglenkers aufgestellt werden, dürfen bei unbeleuchteter Strasse nur rotfarbiges Blitzlicht mit einer maximalen effektiven Lichtstärke von 1000 Candela ausstrahlen. Bei beleuchteter Strasse ist eine angemessene Erhöhung der Lichtstärke zulässig.

2.2 Weissblitze

Der Einsatz von Weissblitzen ist ausnahmsweise erlaubt, wenn die folgenden Mindestanforderungen erfüllt sind:

2.2.1 Strassenbeleuchtung

Die Strasse muss gut beleuchtet sein.

2.2.2 Installation der Blitzleuchte

Die Installation der Blitzleuchte sollte seitlich und in einer Höhe von mindestens 3 m über der Fahrbahn erfolgen, damit gewährleistet wird, dass die Verbindungslinie von der Blitzleuchte zum Fahrer ausserhalb der normalen Blickrichtung des Fahrzeuglenkers liegt.

3. Fragen betreffende den konkreten Einsatz bzw. den Standort von Blitzleuchten

Bei Zweifelsfällen (besonderer Einsatzorte, Einsatz von Weissblitzen in dunkler Umgebung, exponierte Lagen) sollten zusätzliche Abklärungen durch geeignete Experten vor Ort durchgeführt werden.