Zertifizierungsbericht

Zertifizierungs-Vorgang:	**TUVIT-DSZ-ITSEC-9150**
Produkt / System:	MAWIS Version 2.0
Hersteller:	MOBA Mobile Automation AG Freiberger Straße 69-71 01159 Dresden
Auftraggeber:	s. o.
Prüfstelle:	Prüfstelle für IT-Sicherheit der TÜViT GmbH
Evaluierungsbericht:	*Version 1.0 vom 03.01.2005* Dokument-Nummer: *20569941_TÜV_037.01* Verfasser/in: Volker Nies
Formaler Ablauf:	vollständig / ordnungsgemäß durchgeführt
Ergebnis:	E1 / niedrig
Evaluierungsauflagen:	eine (siehe Abschnitt 1.5.1)
Prüfbegleiter:	Dr. Silke Keller
Zertifizierungsauflagen:	eine (siehe Abschnitt 1.6.1)

Essen, den 31.01.2005

Dr. Christoph Sutter Dr. Silke Keller

Inhaltsverzeichnis

1 Grundlage und Gegenstand der Zertifizierung

Die Zertifizierung wurde auf Grundlage der Zertifizierungsbedingungen der Zertifizierungsstelle der TÜViT und des mit dem Bundesamt für Sicherheit in der Informationstechnik[1] abgestimmten Zertifizierungsschemas durchgeführt.

1.1 Evaluationsgegenstand (EVG) und Prüfkriterien

Die Zertifizierung hat das Mülltonnen-Identifikationssystem MAWIS, Version 2.0[2] der Firma MOBA Mobile Automation AG, Freiberger Straße 69-71, 01159 Dresden als Gegenstand und bescheinigt, dass dieses auf Grundlage der *"Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik Version 1.2 (1991)"*[3] und des „*Handbuch für die Bewertung der Sicherheit von Systemen der Informationstechnik Version 1.0 (1993)"*[4], gegen die produktspezifischen Sicherheitsvorgaben von der Prüfstelle für IT-Sicherheit der TÜV Informationstechnik GmbH[5] evaluiert wurde.

Ein Auszug aus ITSEC und ITSEM findet sich in Kapitel 4.

1.2 Durchführung der Evaluierung und Evaluierungsendbericht

Die Evaluierung wurde in der Zeit vom 24.01.2003 bis zum 03.01.2005 von Volker Nies durchgeführt. Die Leitung der Evaluierung wurde von Dr. Patrick Bödeker wahrgenommen und der Evaluierungsendbericht Version 1.0 vom 03.01.2005 (Nummer: 20569941_TÜV_037.01) wurde von Volker Nies erstellt.

1.3 Prüfergebnis der Evaluierung

Die Evaluierung wurde erfolgreich durchgeführt. Die Sicherheitsfunktionen werden gemäß den Sicherheitsvorgaben geleistet, was von den Prüfergebnissen bestätigt wird. Im Sinne von ITSEC handelt es sich bei dem Evaluationsgegenstand[6] um ein Produkt.

Bei dem EVG handelt es sich um das Mülltonnen-Identifikationssystem, das im Bereich der Müllentsorgung eingesetzt wird, wo Abrechnungssysteme gefordert werden, die eine verursacher- und mengengerechte Gebührenabrechnung ermöglichen. Der EVG weist folgende Sicherheitsfunktionalität auf:

- Identifizierung

[1] Im folgenden kurz BSI genannt

[2] Im folgenden kurz MAWIS genannt

[3] Im folgenden kurz ITSEC genannt

[4] Im folgenden kurz ITSEM genannt

[5] Im folgenden kurz Prüfstelle für IT-Sicherheit der TÜViT GmbH genannt

a) Verwendung von Transpondern, die mit einmaligen, unverwechselbaren Identifikationsnummern programmiert sind.

b) Automatische Identifizierung der Mülltonne

- Unverfälschtheit

a) Verwendung von manipulationssicheren Transpondern.

b) Prüfung der im Transponder gespeicherten CRC-Prüfsumme nach dem Auslesen der Transponder- Identifikationsnummer.

c) Sicherung der Übertragung der Transponder-ID vom Ident-Control an den Fahrzeugrechner.

d) Sicherung der Entleerungsdaten in der Memory-Card durch CRC-Prüfsumme. Die Prüfsumme wird im Board-Control berechnet, auf der Memory-Card gespeichert.

e) Die CRC-Prüfsumme wird beim Einlesen der Daten von der Memory-Card in den Entsorger PC geprüft. Nach Konvertierung der Entleerungsdaten erfolgt die Sicherung der Entleerungsdatensätze in der Entleerungsdatei durch:

- CRC-Prüfsumme für jeden einzelnen Datensatz, Nummerierung der Datensätze und
- CRC-Prüfsumme für die gesamte Entleerungsdatei.

Die Prüfsummen und die Datensatznummerierung werden bei der Generierung der Entleerungsdatei am Entsorger PC gebildet.

f) Integritätsprüfung der Entleerungsdateien nach der Datenübertragung.

- Zuverlässigkeit der Dienstleistung

a) Redundante Speicherung der Entleerungsdaten in verschiedenen, voneinander unabhängigen, physikalischen Speichern im Fahrzeugrechner.

b) Verlust einer Memory-Card (bzw. der Daten von einer Memory-Card) kann anhand der Protokolldatei festgestellt werden. In der Protokolldatei auf dem PC des Entsorgers werden alle Bedienvorgänge an den für Entleerungstouren vorbereiteten und an den zurückerhaltenen/eingelesenen Memory-Cards dokumentiert.

Die angestrebte Evaluationsstufe **E1** wurde erreicht und die untersuchten Mechanismen besitzen die Mindeststärke **niedrig**.

1.4 Erweiterung der Ergebnisse auf andere Konfigurationen

Der EVG ist durch die Versionsnummer (Version 2.0) eindeutig gekennzeichnet. Eine Erweiterung der Ergebnisse auf andere Konfigurationen des EVG ist nicht möglich.

Jede Änderung der Hardware oder Firmware seitens des EVG-Herstellers ist der Prüfstelle und der Zertifizierungsstelle anzuzeigen und zieht ggf. eine Re-Evaluation bzw. Re-Zertifizierung nach sich.

[6] Im folgenden kurz EVG genannt

1.5 Auflagen, Hinweise und Empfehlungen aus der Evaluation

1.5.1 Auflagen, Hinweise und Empfehlungen für den Hersteller

Der Evaluierungsendbericht enthält die folgende Auflage an den Hersteller.

- **Der Auftraggeber muss dafür Sorge tragen, dass auch in Zukunft alle notwendigen Testgegenstände und –werkzeuge, die in Abschnitt 1.3.2 des Einzelprüfberichts „Tests der Prüfstelle, Version 1.0 vom 17.09.2004“ [EPT] aufgeführt werden, zur Verfügung stehen, um die Tests jederzeit unter gleichen Bedingungen wiederholen zu können.**

1.5.2 Auflagen, Hinweise und Empfehlungen für den Anwender

Der Evaluierungsendbericht enthält keine Auflagen, Hinweise oder Empfehlungen für den Anwender.

1.6 Zertifizierungsauflagen und Hinweise

1.6.1 Zertifizierungsauflagen

Die Auflage aus dem Evaluierungsendbericht ist einzuhalten (siehe Abschnitt 1.5.1). Aus der Zertifizierung ergeben sich keine weiteren Auflagen.

1.6.2 Zertifizierungshinweise für den Anwender

Es existieren keine Hinweise für den Anwender.

1.7 Unabhängigkeit des Prüfbegleiters

Der Prüfbegleiter hat innerhalb der letzten 2 Jahre für das die Zertifizierung beauftragende Unternehmen keine Beratungen oder sonstige Dienstleistungen erbracht und mit diesem Unternehmen auch keine Beziehungen gepflegt, die seine Beurteilung beeinflussen könnten.

Der Prüfbegleiter ist zu keiner Zeit an Prüfverfahren für das dem Zertifizierungsvorgang zugrunde liegende Produkt beteiligt gewesen.

2 Zusammenfassung der Sicherheitsvorgaben

2.1 Definition des EVG und Art der Nutzung

2.1.1 Definition des EVG

Gegenstand der Evaluierung ist das Mülltonnen-Identifikationssystem mit der Bezeichnung *MAWIS (Moba Automatic Waste Identification System) Rev. 2.0*. Der EVG wird im Bereich der Müllentsorgung eingesetzt, wo Abrechnungssysteme gefordert werden, die eine verursacher- und mengengerechte Gebührenabrechnung ermöglichen. Zur Umsetzung dieser Anforderung sind organisatorische wie auch technische Lösungen geeignet, mit

deren Hilfe die erforderlichen Daten für eine aufwandsabhängige Abrechnung erfasst und der Gebührenabrechnung zur Verfügung gestellt werden können. Der EVG ist ein Automatisierungssystem, mit dessen Hilfe im Rahmen der regelmäßigen Mülltonnenleerung der Entleerungsvorgang einer Mülltonne erfasst wird. Dazu ist jede Mülltonne mit einer eindeutigen Identifikationsnummer versehen, die wiederum einem Verursacher zugeordnet ist. Die Identifikationsnummer wird beim Entleeren der Mülltonne automatisch erfasst, gespeichert und für die Gebührenabrechnung zur Verfügung gestellt. So wird eine auf Menge und Verursacher ausgerichtete Gebührenabrechnung ermöglicht und dabei höchste Kostentransparenz und permanente Auskunftsfähigkeit gewährleistet. Das eigentliche Abrechnungssystem und die von diesem durchgeführte Auswertung der erfassten Daten sind **nicht** Bestandteil des EVG.

Der EVG gewährt Schutz vor Datenverlust und versehentlicher Datenverfälschung (insb. durch Übertragungsfehler), bietet aber **keinen** Schutz gegen eine gezielte Manipulation der Entleerungsinformationen, insbesondere im Rahmen der Übertragung zwischen

- Ident-Control und Fahrzeugrechner (*Board-Control*),
- Fahrzeugrechner und Entsorger-PC,
- Entsorger-PC und PC in der Gebührenabrechnungsstelle.

Mittels einer sog. „Schwarze Liste“ lassen sich Behälter identifizieren, für die kein Rechnungsadressat verfügbar ist. Durch Führen der „Schwarzen Liste“ kann das Kippen von bestimmten Behältern registriert und bei Bedarf verhindert werden. Diese Funktionalität liegt jedoch **außerhalb** des Fokus dieser Zertifizierung.

Optional kann zur massebezogenen Gebührenabrechnung eine Schüttungswaage an den EVG angeschlossen werden, der dazu über eine Waageschnittstelle verfügt. Über diese Schnittstelle ist es möglich, der Identifikationsnummer die Masse des aus dem Behälter entsorgten Abfalls zuzuordnen. Die Schüttungswaage ist **nicht** Bestandteil des EVG und die Erfassung des korrekten Gewichts des entsorgten Abfalls liegt **außerhalb** des Fokus dieser Zertifizierung.

Der EVG setzt sich aus folgenden Komponenten zusammen:

Bezeich-nung	Komponente	Beschreibung
K1	Fahrzeugrechner (Board-Control), bestehend aus Hardware, Firmware und den Komponenten - Tastatur, - LC-Display, - Memory-Card-Interface, - Übertragungsschnittstelle (Verbindung Ident-Control), - Übertragungsschnittstelle	Der Fahrzeugrechner befindet sich im Führerhaus der Müllsammelfahrzeuge und empfängt die Entleerungsdaten über die Übertragungsschnittstelle vom Ident-Control. Die empfangenen Daten werden auf eine Memory-Card übertragen und als Redundanz zusätzlich in zwei nichtflüchtigen Speichern innerhalb des Fahrzeugrechners gespeichert.

Bezeich-nung	Komponente	Beschreibung
	(Verbindung Waage).	Falls das Fahrzeug optional mit einer dynamischen Schüttungswaage ausgestattet ist, empfängt der Fahrzeugrechner zusätzlich die Masse des aus dem identifizierten Behälters entsorgten Mülls. Die Masse wird den Entleerungsdaten vor dem Speichern in o.g. Datenträgern zugeordnet. **Die Erfassung des korrekten Gewichts des entsorgten Abfalls liegt außerhalb des Fokus dieser Evaluation.**
K2	Memory-Card (auf der sich die Entleerungsinformationen befinden)	Die Memory-Card wird in den Fahrzeugrechner eingesteckt und dient zur - Übertragung der „Schwarze Liste“ an die Fahrzeugrechentechnik **(diese Funktionalität liegt jedoch außerhalb des Fokus dieser Evaluation)**; - Übertragung der Tourenvorgabe an die Fahrzeugrechentechnik; - Ablage der erfassten Entleerungsdatensätze. Zur Auswertung der erfassten Daten wird sie aus dem Fahrzeugrechner entnommen und an die Einsatzleitung bzw. die Abrechnungsstelle weitergegeben.
K3	Folgende Hard- u. Software für Personal Computer (beim Entsorger): - Memory-Card-Interface; - MAWIS-Memory-Card-Software zum o Vorbereiten der Memory-Card, o Auslesen der Memory-Card, und zur o Ablage der Entleerungsdatei.	Am Personal-Computer (PC) beim Entsorger wird mit Hilfe der entsprechenden PC-Software die Memory-Card mit den Tagesdienst-Informationen sowie ggf. mit der „Schwarzen Liste“ und der Tourenvorgabe programmiert. Nach Schichtende werden die Entleerungsdaten aus der Memory-Card ausgelesen und in einer Entleerungsdatei gesichert[7]. Die Entleerungsdateien können an die Gebührenabrechnungsstelle übertragen werden. Die Konfiguration der MAWIS-Memory-Card-Software wird vor versehentlicher Modifikation geschützt.

[7] Das Abrechnungssystem und die von ihm durchgeführte Auswertung der erfassten Daten ist **nicht Teil des EVG**.

Bezeich-nung	Komponente	Beschreibung
K4	Folgende Software für Personal Computer (in der Gebührenab-rechnungsstelle) - PC-Software zur Übertragung der Entleerungsdateien vom Entsorger in die Gebühren-abrechnungsstelle, - Modul zur Prüfung der Datenintegrität im Anschluss an die Datenübertragung.	Die Entleerungsdateien können vom PC des Entsorgers auf den PC der Gebühren-abrechnungsstelle übertragen werden. Im Anschluss an die Übertragung wird die Integrität der empfangenen Daten überprüft.
K5	Transponder	Identifikationsträger an jeder Mülltonne. Die im Transponder einprogrammierte Identifikationsnummer kann bei der Entleerung der Tonne berührungslos (elektromagnetisch) ausgelesen werden.
K6	Ident-Control mit - Sende-/Empfangsantenne, - Kippsensor, - Übertragungsschnittstelle (Verbindung: Fahrzeugrechner).	Das Ident-Control führt bei der Mülltonnen-entleerung über eine Sende-/Empfangsantenne die berührungslose Kommunikation mit dem Transponder durch, liest das Signal des Kippsensors ein und überträgt die Identifikationsnummer des Transponders über die Übertragungsschnittstelle an den Fahrzeugrechner. Je nach Anzahl der am Müllfahrzeug vorhandenen Schütten können ein bis drei Ident-Control in einer Fahrzeugausrüstung integriert werden. Ggf. wird durch eines der Ident-Control die Funktionalität „Schwarze Liste“ realisiert. Es liefert ein digitales Signal, wenn an einer Schüttung ein in der „Schwarzen Liste“ enthaltener Behälter identifiziert wurde. **Diese Funktionalität liegt jedoch außerhalb des Fokus dieser Evaluation.**
K7	Dokumentation	Handbuch für Benutzer und Einsatzleiter.

Tabelle 1: Komponenten des EVG

Die Auslieferung des EVG erfolgt durch persönliche Übergabe. Zum Lieferumfang gehört:

	Bezeichnung
Hard- und Software	• Transponder, Versionen RI-TRP-RRHP oder RI-TRP-RR2B • Memory-Card 128 KByte, Artikelnummer 03-05-02010 • Ident-Control Hardware: IDC 20-1, Artikelnummer 04-55-00680 (IDC 20 mit 1 RF und 4 Durchführungen) IDC 20-2, Artikelnummer 04-55-00685 (IDC 20 mit 2 RF und 6 Durchführungen) IDC 20-1 I5, Artikelnummer 04-55-00720 (IDC 20 mit 1 RF und 5 digitalen Eingängen) IDC 20-0 I5, Artikelnummer 04-55-00725 (IDC 20 ohne RF und 5 digitalen Eingängen) • Ident-Control Firmware, Version 8.24S1 • Antenne, Neigungssensor • Board-Control Hardware, Platinen-Version 2.3 • Board-Control Firmware, Version 663FAD, 663SD und 663W7D) • PC-Software: RwfMawis.exe, Version 3.0.1.0 MAWIS_Check.exe, Version 1.0.0.1 Reg-files, die für jeden Kunden separat erzeugt werden Chipk.ini, die für jede Installation von RwfMawis neu generiert wird • Hardware USB-Memory-Card Interface, Platinen- Version 3.20 Firmware USB- Memory-Card- Interface, Version 3.20 MemCard32.DLL, Version 2.2.2.43 Hlgapi32.DLL, Version 1.5.1.71
Doku-mentation	• Bedienungsanleitung Fahrzeugausrüstung, MAWIS MOBA Automatic Waste Identification System, Version 5.1, 10.10.2003 • Ident System-Check Routineüberprüfung, Version 2.0, 04.07.2003 • MAWIS - Gefährdung der Datensicherheit und Gegenmaßnahmen im MAWIS, Version 1.4, 23.08.2004 • MAWIS Rev. 2.0 - RWFMawis Softwaredokumentation, Version 1.3, 23.08.2004 • MAWIS - Beschreibung der Anwendung MAWIS_CHECK.exe, Version 4, 23.08.2004 • Bedienungsanleitung - Wartung des Monitors für die Behälteridentifikation, Version 4.32, 10.10.2003

Tabelle 2: Auslieferungsbestandteile von MAWIS 2.0

2.1.2 Art der Nutzung

Der EVG ist ein Hard- und Software Produkt, das für die Installation in vielen Entsorgungsunternehmen entwickelt wurde und damit im Sinne der ITSEC ein Produkt.

2.2 Angenommene Einsatzumgebung

2.2.1 Technische Einsatzumgebung

Als technische Einsatzumgebung wird benötigt:

- ein geeignetes Fahrzeug für die Installation des EVG
  - 24 V Versorgungsspannung (Klemme 15) für Fahrzeugrechner und Ident-Control,
  - Platz im Führerhaus für die Installation des Fahrzeugrechners
  - Platz an der Rückseite des Fahrzeugs für die Anbringung von Ident-Control mit Antenne
  - Kippsensor und Tonnensensor
  - Wird die Waageschnittstelle benutzt, muss das Fahrzeug mit einer dynamischen Schüttungswaage je Schüttung ausgerüstet sein.
- geeignete Müllbehälter zur Befestigung der Transponder,
- Rechnersystem beim Entsorger:
  - PC mit einem Windows- Betriebssystem ab Windows 95
  - freie Festplattenkapazität min. 150 MB
  - freier ISA- Slot oder RS232- Schnittstelle oder USB- Schnittstelle zum Anschluss des Memory-Card Interface
- weitere für den Betrieb des EVG erforderlichen Komponenten, die vom Hersteller zur Verfügung gestellt werden, die aber **nicht** Bestandteil des EVG sind:
  - Equipment zur Transpondermontage an die Müllbehälter
  - Handlesegerät zur Unterstützung der Erstausrüstung
  - Behälterverwaltungssoftware in der Gebührenabrechnungsstelle
  - Software für den Änderungsdienst (Auftragsbearbeitung) in der Gebührenabrechnungsstelle und beim Entsorger
  - Abrechnungssoftware zur Gebührenbescheiderstellung

2.2.2 Administrative Einsatzumgebung

Auf Seiten des Entsorgungsunternehmens ggf. in Verbindung mit der Gebührenabrechnungsstelle[8] muss ein System-Verwalter bzw. Projektleiter für den Einsatz des EVG verantwortlich sein für:

- die Systempflege, welche die Installation der Software zum Auslesen der Memory-Card auf dem Entsorger PC; die Rechteverwaltung zur Sicherstellung, dass nur befugte Personen Zugriff auf Memory-Card-Software und die Entleerungsdaten haben sowie die Sicherstellung, dass keine für MAWIS schädliche Software installiert wird beinhaltet;
- das Anbringen der Transponder an die Müllbehälter;
- die Verwaltung und Konfiguration der Memory-Cards;
- das Auslesen der Entleerungsdaten aus der Memory-Card mit der Erstellung der Entleerungsdateien für jede ausgelesene Memory-Card;
- die Generierung der Daten für die Gebührenabrechnung, aus den Entleerungsdateien der ausgelesenen Memory-Cards;
- die Bereitstellung der Entleerungsdateien für die Datenübertragung an die Gebührenabrechnungsstelle;
- die Datensicherung und Einleitung geeigneter Maßnahmen bei Störungen.

Während der Betriebsphase ist ein Wartungs- und Servicedienst zu organisieren, wobei auf die Dienstleistung der Firma MOBA zurückgegriffen werden kann.

Vorausgesetzt wird, dass das Personal des Entsorgungsunternehmens und der Gebührenabrechnungsstelle in den Umgang mit dem EVG eingewiesen wird und die für es relevanten Teile richtig bedienen kann sowie loyal ist und keinen absichtlichen Versuch unternimmt, die erfassten Daten zu manipulieren.

Der Einsatzleiter muss möglichst täglich eine Datensicherung vornehmen, mindestens aber in dem Zeitraum in dem die Daten auf dem Fahrzeugrechner noch zur Verfügung stehen. Dabei ist der gesamte Pfad der MAWIS-Memory-Card Software zu sichern (enthält Programme und Daten in Unterverzeichnissen).

[8] Im Allgemeinen wird in kleineren Gemeinden die Gebührenabrechnung durch das Landratsamt bzw. die Kommune, in größeren Gemeinden bzw. Städten direkt beim Entsorger, durchgeführt. Erfolgt eine Übertragung der Entleerungsdaten zur gebührenabrechnenden Stelle, ist dort ebenfalls ein dafür Verantwortlicher einzusetzen.

2.3 Subjekte, Objekte und Zugriffsarten / Aktionen

2.3.1 Schützenswerte Objekte

O1 Entleerungsinformation bestehend aus der Transponder-ID der geleerten Mülltonne. Diese wird von der Komponente Ident-Control gelesen. Sie wird nach dem Kippen des Müllbehälters an den Fahrzeugrechner übertragen.

O2 Entleerungsdaten, die belegen, dass eine bestimmte Mülltonne zu einem bestimmten Zeitpunkt geleert wurde. Sie bestehen aus

- Transponder-ID (Entleerungsinformation O1), die durch den Fahrzeugrechner von einem Ident-Control empfangen wurde, wobei das Objekt O1 nach dem Empfang im Board-Control in Objekt O2 übergeht,
- Datum und Uhrzeit,

und zusätzlich falls optional eine Waage an das System angeschlossen ist

- Masse des entsorgten Mülls oder eine Fehlerinformation, wobei an der Fehlerinformation erkennbar ist, aus welchem Grund keine Masse in der Entleerungsinformation enthalten ist.

2.3.2 Subjekte

S1 Personen, die Zugang bzw. Zugriff auf die Mülltonne besitzen (Mülltonnenbesitzer, Nachbarn, Fremde).

S2 Teil der Fahrzeugbesatzung, der die Tonnen zur Entleerung in die Schüttung einführt.

S3 Teil der Fahrzeugbesatzung, der Zugriff auf Fahrzeugrechner und Memory-Card hat.

S4 Büropersonal beim Entsorgungsunternehmen, das mit der Memory-Card umgeht und auf die Datei für die Gebührenabrechnung zugreifen kann:

- Eingewiesenes Personal, das die Memory-Cards vorbereiten und lesen darf.
- Der Einsatzleiter und seine Vertreter als Systemverwalter, die zusätzlich Service- und Backupkarten erstellen dürfen.

S5 Technisches System (K1, K6), das die Datensätze im Fahrzeug generiert, überträgt und speichert.

S6 Personal-Computer (K3) beim Entsorger, an dem die Datensätze aus der Memory-Card gelesen und als Entleerungsdateien gespeichert werden.

S7 Personal-Computer (K4) in der Gebührenabrechnungsstelle, an dem die Entleerungsdateien empfangen und verarbeitet werden.

S8 Personal bei der Gebührenabrechnungsstelle, das die Entleerungsdateien empfängt und verwaltet.

2.3.3 Zugriffsarten / Aktionen

Folgende Aktionen der Subjekte im Bezug auf die Objekte sind definiert:

A1 Bearbeiten der Transponder, einschließlich Austausch, Entfernen und Verändern, durch Mülltonnenbesitzer, Nachbarn, Fremde (S1).

A2 Anhängen der Tonne an die Schüttung des Fahrzeugs durch Fahrzeugbesatzung (S2), zwecks Entleerung der Mülltonne, Erfassung der Mülltonnen-Identifikationsnummer und ggf. Wägung des enthaltenen Mülls.

A3 Einstecken der Memory-Card in den Fahrzeugrechner, Entnehmen und Abliefern durch Fahrzeugbesatzung (S3).

A4 Erneutes Übertragen der im Fahrzeugrechner gespeicherten Daten in eine Backup- oder Service-Card durch Fahrzeugpersonal (S3) im Fall einer verlorenen oder fehlerhaften Memory-Card.

A5 Auslesen der Datensätze aus der Memory-Card und als "abgerechnet" markieren durch Büropersonal beim Entsorger (S4).

A6 Generieren, Übertragen und Speichern der Datensätze durch Technisches System am Fahrzeug (S5), beim Entsorger (S6) oder Gebührenabrechnungsstelle (S7), mit der Möglichkeit Übertragungsstörungen.

A7 Manuelle Übertragung der Entleerungsdateien bei Übertragungsstörungen durch Büropersonal beim Entsorger (S4) und der Gebührenabrechnungsstelle (S8).

Die folgende Tabelle gibt die erlaubten Zugriffsarten der Subjekte auf die Objekte wieder:

	O1	**O2**
S1	A1	
S2	A2	
S3		A3, A4
S4		A5, A7
S5		A6
S6		A6
S7		A6
S8		A7

Tabelle 3: Zugriffsarten Subjekte/Objekte

2.4 Bedrohungen und Sicherheitsziele

2.4.1 Bedrohungen

Für den angenommenen Einsatz werden die folgenden fünf Bedrohungen angenommen:

B1: Absichtliche oder unabsichtliche Unterdrückung oder Verfälschung der Transponder-Identifikationsnummer (O1) durch Mülltonnenbesitzer, Nachbarn, Fremde (S1) mittels Manipulation am Transponder der Mülltonnen.

B2: Verfälschung oder Unterdrückung der Entleerungsinformation (O1) aufgrund eines Übertragungsfehlers zwischen Transponder und Fahrzeugrechner.

B3: Versehentliche Verfälschung oder Unterdrückung der Entleerungsdaten (O2) zwischen Fahrzeugrechner und Entsorger PC (S6) oder zwischen Entsorger PC und PC in der Gebührenabrechnungsstelle (S7).

B4: Verlust aller Entleerungsdaten (O2) einer Tour durch Verlust oder Beschädigung der Memory-Card, auf der diese Daten abgelegt sind.

B5: Versehentliche Verfälschung oder Verlust einer Entleerungsdatei, die die Entleerungsdaten (O2) einer Tour beinhaltet, beim Entsorger (S4) oder in der Gebührenabrechnungsstelle (S8).

2.4.2 Sicherheitsziele und Sicherheitseigenschaften

SZ1: Die Entleerungsinformation (O1) korrekt zu erfassen und dem Fahrzeugrechner zur Verfügung zu stellen.

SZ2: Eine Verfälschung der Entleerungsinformation (O1) durch Übertragungsstörungen zwischen Ident-Control und Board-Control (S5) zu erkennen.

SZ3: Eine zufällige Verfälschung der Entleerungsinformation (O2) durch Übertragungsstörungen auf der gesamten Strecke zwischen Fahrzeugrechner (S5) und dem Personal Computer in der Gebührenabrechnungsstelle (S8) zu erkennen.

SZ4: Eine Manipulation der Transponder-ID (O1) durch Mülltonnenbesitzer, Nachbarn, Fremde (S1) zu verhindern oder zu erkennen.

SZ5: Verlorene Entleerungsinformationen (O2) auf der Memory-Card, mit Unterstützung des Fahrzeug- oder Büropersonals (S3, S4) aus den in dem Board-Control (K1) vorhandenen Sicherheitskopien auf verschiedenen Speichermedien wieder zu erhalten.

SZ6: Das Aufdecken einer versehentlichen Veränderung von Entleerungsinformationen (O2), innerhalb der Entleerungsdatei zu unterstützen.

2.5 Sicherheitsfunktionen

Zur Erreichung des Sicherheitsziels und zur Abwehr der Bedrohungen enthält der EVG die folgenden drei sicherheitsspezifischen Funktionen:

Bezeichnung	Sicherheitsfunktion	Beschreibung
SF1	Identifizierung	a) Verwendung von Transpondern, die mit einmaligen, unverwechselbaren Identifikationsnummern programmiert sind. b) Automatische Identifizierung der Mülltonne.
SF2	Unverfälschtheit	a) Verwendung von manipulationssicheren Transpondern. b) Prüfung der im Transponder gespeicherten CRC-Prüfsumme nach dem Auslesen der Transponder-Identifikationsnummer. c) Sicherung der Übertragung der Transponder-ID vom Ident-Control an den Fahrzeugrechner. d) Sicherung der Entleerungsdaten in der Memory-Card durch CRC-Prüfsumme. Die Prüfsumme wird im Board-Control berechnet, auf der Memory-Card gespeichert. e) Die CRC-Prüfsumme wird beim Einlesen der Daten von der Memory-Card in den Entsorger PC geprüft. Nach Konvertierung der Entleerungsdaten erfolgt die Sicherung der Entleerungsdatensätze in der Entleerungsdatei durch: • CRC-Prüfsumme für jeden einzelnen Datensatz, • Nummerierung der Datensätze und • CRC-Prüfsumme für die gesamte Entleerungsdatei. Die Prüfsummen und die Datensatznummerierung werden bei der Generierung der Entleerungsdatei am Entsorger PC gebildet. f) Integritätsprüfung der Entleerungsdateien nach der Datenübertragung.

Bezeich-nung	Sicherheitsfunktion	Beschreibung
SF3	Zuverlässigkeit der Dienstleistung	a) Redundante Speicherung der Entleerungsdaten in verschiedenen, voneinander unabhängigen, physikalischen Speichern im Fahrzeugrechner. b) Verlust einer Memory-Card (bzw. der Daten von einer Memory-Card) kann anhand der Protokolldatei festgestellt werden. In der Protokolldatei auf dem PC des Entsorgers werden alle Bedienvorgänge an den für Entleerungstouren vorbereiteten und an den zurückerhaltenen/eingelesenen Memory-Cards dokumentiert.

2.6 Korrelation Sicherheitsfunktionen / Bedrohungen / Sicherheitsziele

Die folgende Tabelle zeigt welche Sicherheitsfunktionen den jeweiligen Bedrohungen entgegenwirken:

	SF1	SF2	SF3
B1	X	X	
B2		X	
B3		X	
B4			X
B5		X	

Tabelle 4: Korrelation Sicherheitsfunktionen/Bedrohungen

Die Sicherheitsfunktionen sind für die vorgesehene Art der Nutzung des MAWIS sowohl geeignet als auch zweckmäßig.

Aus der Tabelle ist erkennbar, dass es zu jeder Bedrohung mindestens eine Sicherheitsfunktion gibt, die dieser Bedrohung entgegenwirkt und jede Sicherheitsfunktion zur Abwehr mindestens einer Bedrohung beiträgt.

Der Bedrohung B1 der Unterdrückung oder Verfälschung der Transponder-Identifikationsnummer mittels Manipulation wird durch die Verwendung von Transpondern mit einmaliger unverwechselbarer Identifikationsnummer und durch die automatische Identifizierung der Mülltonne (SF1) und der Verwendung durch manipulationssichere Transponder (SF2) entgegengewirkt.

Der Bedrohung der Verfälschung oder Unterdrückung der Entleerungsinformationen durch einen Übertragungsfehler zwischen Transponder und Fahrzeugrechner (B2) wird durch SF2 mit der Prüfung der im Transponder gespeicherten CRC Prüfsumme und der Sicherung der Übertragung der Transponder-ID vom Ident-Control an den Fahrzeugrechner entgegengewirkt.

Der Bedrohung der versehentlichen Verfälschung oder Unterdrückung der Entleerungsdaten zwischen Fahrzeugrechner und Entsorger PC oder zwischen Entsorger PC und PC in der Gebührenabrechnungsstelle (B3) wird durch SF2 mit der Sicherung der Entleerungsdaten in der Memory-Card durch CRC-Prüfsumme, der Prüfung der CRC-Prüfsumme beim Entsorger und der Integritätsprüfung der Entleerungsdateien nach der Datenübertragung entgegengewirkt.

Der Bedrohung (B4) des Verlustes der Entleerungsdaten einer Tour durch Verlust oder Beschädigung der Memory-Card, auf der diese Daten abgelegt sind, wird durch SF3 entgegengewirkt, da die Entleerungsdaten redundant in verschiedenen physikalischen Speichern im Fahrzeugrechner gespeichert werden und der Verlust einer Memory-Card anhand der Protokolldatei auf dem PC des Entsorgers festgestellt werden kann.

Einer versehentliche Verfälschung oder Verlust einer Entleerungsdatei, die die Entleerungsdaten einer Tour beinhaltet (B5) wird durch SF2 mit der Sicherung der Entleerungdaten in der Memory-Card durch CRC-Prüfsumme und Integritätsprüfung der Entleerungsdaten nach der Datenübertragung entgegengewirkt.

2.7 Evaluationsstufe und Mechanismenstärke

Die vom Antragsteller angestrebte Evaluationsstufe ist **E1**.

Die vom Antragsteller angestrebte Mindeststärke der Mechanismen ist **niedrig**.

3 Ergebnisse der Evaluierung

3.1 Wirksamkeit – Konstruktion

3.1.1 Aspekt 1: Eignung der Funktionalität

ITSEC 3.14 *Die Analyse der Eignung muss die sicherheitsspezifischen Funktionen und Mechanismen den in den Sicherheitsvorgaben identifizierten Bedrohungen zuordnen, denen sie entgegenwirken müssen.*

ITSEC 3.15 *Die Analyse der Eignung muss zeigen, wie die sicherheitsspezifischen Funktionen und Mechanismen den identifizierten Bedrohungen entgegenwirken. Sie muss zeigen, dass es keine identifizierten Bedrohungen gibt, denen nicht eine oder mehrere der aufgeführten sicherheitsspezifischen Funktionen angemessen entgegenwirken.*

ITSEC 3.16 *Es ist zu überprüfen, ob die Analyse der Eignung alle Anforderungen hinsichtlich Inhalt, Form und Nachweis erfüllt. Es ist zu überprüfen, ob die Analyse alle Informationen verwendet hat, die in Abbildung 4 [3] für die angestrebte Evaluationsstufe angegeben sind.*

Feststellung der Zertifizierungsstelle: Die Prüfstelle hat überprüft und festgestellt, dass die Analyse der Eignung alle Anforderungen an Inhalt, Form und Nachweise (ITSEC 3.14, 3.15) erfüllt sowie alle relevanten Informationen verwendet hat. Die Zuordnungen der Sicherheitsfunktionen zu den Bedrohungen sind in Abschnitt 2.6 dargestellt.

3.1.2 Aspekt 2: Zusammenwirken der Funktionalität

ITSEC 3.18 *Die Analyse des Zusammenwirkens muss eine Analyse aller möglichen Beziehungen zwischen den sicherheitsspezifischen Funktionen und Mechanismen zur Verfügung stellen.*

ITSEC 3.19 *Die Analyse des Zusammenwirkens muss zeigen, dass es nicht möglich ist, eine sicherheitsspezifische Funktion oder einen Mechanismus dazu zu veranlassen, mit den Aufgaben anderer sicherheitsspezifischer Funktionen oder Mechanismen in Konflikt zu geraten oder ihnen entgegenzuwirken. Diese Analyse muss unter Verwendung zumindest jener Informationen durchgeführt werden, die in Abbildung 4 [3] für die angestrebte Evaluationsstufe angegeben sind.*

ITSEC 3.20 *Es ist zu überprüfen, ob die Analyse des Zusammenwirkens alle Anforderungen hinsichtlich Inhalt, Form und Nachweis erfüllt. Es ist zu überprüfen, ob die Analyse alle Informationen verwendet hat, die in Abbildung 4 [3] für die angestrebte Evaluationsstufe angegeben sind.*

Feststellung der Zertifizierungsstelle: Die Prüfstelle hat überprüft und festgestellt, dass die Analyse des Zusammenwirkens alle Anforderungen an Inhalt, Form und Nachweise (ITSEC 3.18, 3.19) erfüllt sowie alle relevanten Informationen verwendet hat.

3.1.3 Aspekt 3: Stärke der Mechanismen

ITSEC 3.22 *Die Analyse der Stärke der Mechanismen muss alle sicherheitsspezifischen Mechanismen auflisten, die innerhalb des EVG als kritisch festgestellt wurden. Sie muss Analysen über die Algorithmen, Prinzipien und Eigenschaften enthalten, die diesen Mechanismen zugrundeliegen oder sie muss auf solche Analysen verweisen.*

ITSEC 3.23 *Die Analyse der Stärke der Mechanismen muss aufzeigen, dass alle kritischen Mechanismen die Definition der beanspruchten Einstufung der Mindeststärke, wie in den Paragraphen 3.6 bis 3.8 beschrieben, erfüllen: im Fall von kryptographischen Mechanismen muss dies durch eine Aussage der zuständigen nationalen Behörde erfolgen. Andere Analysen müssen unter Verwendung zumindest jener Informationen durchgeführt werden, die in Abbildung 4 [3] für die angestrebte Evaluationsstufe angegeben sind.*

ITSEC 3.24 *Es ist zu überprüfen, ob alle Mechanismen, die kritisch sind, als solche identifiziert wurden. Es ist zu überprüfen, ob die vorgelegte Analyse der Stärke der Mechanismen alle Anforderungen bezüglich Inhalt, Form und Nachweis erfüllt. Es ist zu überprüfen, ob die Analyse alle Informationen verwendet hat, die in Abbildung 4 [3] für die angestrebte Evaluationsstufe angegeben sind. Es ist zu überprüfen, ob die Spezifikationen/Definitionen aller kritischen Mechanismen die beanspruchte Mindeststärke gewährleisten. Wo erforderlich, sind* ***Penetrationstests*** *durchzuführen, um die Mindeststärke der Mechanismen zu bestätigen oder zu verwerfen.*

Feststellung der Zertifizierungsstelle: Im Prüfobjekt werden alle vorhandenen Mechanismen als kritisch eingestuft und in Typ A und B Mechanismen unterschieden. Die Prüfstelle hat überprüft und festgestellt, dass alle Mechanismen, die kritisch sind, als solche identifiziert wurden. Die vorgelegte Analyse der Stärke der Mechanismen erfüllt alle Anforderungen an Inhalt, Form und Nachweise (ITSEC 3.22, 3.23) und verwendet alle relevanten Informationen. Die Spezifikationen/Definitionen aller kritischen Mechanismen gewährleisten

die geforderte Mindeststärke niedrig. Von der Prüfstelle sind Penetrationstests durchgeführt worden, die die Mindeststärke der Mechanismen bestätigen.

3.1.4 Aspekt 4: Bewertung der Konstruktionsschwachstellen

ITSEC 3.26 *Die Liste der Schwachstellen, die durch den Antragsteller vorgelegt werden muss, muss alle ihm bekannten Schwachstellen in der Konstruktion des EVG aufführen. Sie muss jede Schwachstelle ansprechen, eine Analyse ihrer möglichen Auswirkungen beinhalten und die Maßnahmen aufzeigen, die zur Abhilfe vorgeschlagen oder zur Verfügung gestellt werden.*

ITSEC 3.27 *Die Analyse der möglichen Auswirkungen jeder bekannten Schwachstelle muss aufzeigen, dass die betreffende Schwachstelle in der beabsichtigten Einsatzumgebung des EVG nicht ausgenutzt werden kann, weil entweder*

- *die Schwachstelle angemessen durch andere, nicht beeinträchtigte Sicherheitsmechanismen geschützt ist oder*
- *gezeigt werden kann, dass die Schwachstelle in Bezug zu den Sicherheitsvorgaben ohne Bedeutung ist, in der Praxis nicht existieren wird oder dass ihr angemessen durch dokumentierte technische, personelle, organisatorische oder materielle Sicherheitsmaßnahmen außerhalb des EVG entgegengewirkt werden kann. Diese externen Sicherheitsmaßnahmen müssen in der entsprechenden Dokumentation beschrieben (oder hinzugefügt worden) sein.*

Die Analyse muss unter Verwendung zumindest jener Informationen durchgeführt werden, die in Abbildung 4 [3] für die angestrebte Evaluationsstufe angegeben sind.

ITSEC 3.28 *Es ist zu überprüfen, ob die Liste der bekannten Schwachstellen in der Konstruktion alle Forderungen bezüglich Inhalt, Form und Nachweis, so wie oben beschrieben, erfüllt. Es ist zu überprüfen, ob die Analyse alle Informationen verwendet hat, die in Abbildung 4 [3] für die angestrebte Evaluationsstufe angegeben sind. Es ist eine eigene Schwachstellenanalyse unter Berücksichtigung der aufgelisteten und der während der Evaluation gefundenen Schwachstellen durchzuführen. Es ist zu überprüfen, ob alle Kombinationen von bekannten Schwachstellen untersucht wurden. Es ist zu überprüfen, ob die Analysen der möglichen Auswirkungen der Schwachstellen keine undokumentierten oder unvernünftigen Annahmen über die vorgesehene Einsatzumgebung enthalten. Es ist zu überprüfen, ob alle Annahmen und Anforderungen bezüglich externer Sicherheitsmaßnahmen ausreichend dokumentiert wurden. Es sind Penetrationstests durchzuführen, um zu bestätigen oder zu widerlegen, ob die bekannten Schwachstellen in der Praxis wirklich ausgenutzt werden können.*

Feststellung der Zertifizierungsstelle: Die Prüfstelle hat überprüft und festgestellt, dass die Liste der bekannten Schwachstellen in der Konstruktion alle Forderungen bezüglich Inhalt, Form und Nachweise (ITSEC 3.26, 3.27), so wie oben beschrieben, erfüllt. Sie hat überprüft und festgestellt, dass die Analyse alle relevanten Informationen verwendet hat.

Es wurde fünf Schwachstellen vom Hersteller angegeben, die von der Prüfstelle bewertet wurden. Die bekannten Konstruktionsschwachstellen können in der beabsichtigten Einsatzumgebung nicht ausgenutzt werden, da sie durch organisatorische und technische Maßnahmen geeignet geschützt sind. Die Prüfstelle hat eine eigene Schwachstellenanalyse durchgeführt und keine weitere Schwachstellen in der Konstruktion gefunden. Die Prüfstelle

hat alle Kombinationen der bekannten Schwachstellen untersucht. Die Prüfstelle hat überprüft und festgestellt, dass die Analysen der möglichen Auswirkungen der Schwachstellen keine undokumentierten oder unvernünftigen Annahmen über die vorgesehene Einsatzumgebung enthalten. Sie hat überprüft und festgestellt, dass alle Annahmen und Anforderungen bezüglich externer Sicherheitsmaßnahmen ausreichend dokumentiert sind.

Die Prüfstelle hat Penetrationstests durchgeführt und bestätigt, dass die bekannten Schwachstellen in der Praxis wirklich nicht ausgenutzt werden können.

3.2 Wirksamkeit – Betrieb

3.2.1 Aspekt 1: Benutzerfreundlichkeit

ITSEC 3.31 *Die Analyse der Benutzerfreundlichkeit muss mögliche Betriebsarten des EVG beschreiben, einschließlich des Betriebes nach Bedien- oder Betriebsfehlern, und ihre Konsequenzen und Folgerungen für die Aufrechterhaltung eines sicheren Betriebes.*

ITSEC 3.32 *Die Analyse der Benutzerfreundlichkeit muss aufzeigen, dass jeder menschliche oder andere Fehler, der sicherheitsspezifischen Funktionen oder Mechanismen ausschaltet oder unbrauchbar macht, leicht festzustellen ist. Sie muss zeigen, dass es erkennbar ist, wenn ein EVG in einer Weise konfiguriert oder benutzt werden kann, die unsicher ist (d.h. die sicherheitsspezifischen Funktionen und Mechanismen des EVG erfüllen die Sicherheitsvorgaben nicht), obwohl ein Endnutzer oder Administrator vernünftigerweise von einem sicheren Zustand ausgehen kann. Die Analyse muss unter Verwendung zumindest jener Informationen durchgeführt werden, die in Abbildung 4 [3] für die angestrebte Evaluationsstufe angegeben sind.*

ITSEC 3.33 *Es ist zu überprüfen, ob die vorgelegte Analyse der Benutzerfreundlichkeit alle Anforderungen hinsichtlich Inhalt, Form und Nachweis erfüllt. Es ist zu überprüfen, ob die Analyse alle Informationen verwendet hat, die in Abbildung 4 [3] für die angestrebte Evaluationsstufe angegeben sind. Die Analyse ist nach undokumentierten oder unvernünftigen Annahmen über die vorgesehene Betriebsumgebung zu überprüfen. Es ist zu überprüfen, ob alle Annahmen und Forderungen zu externen Sicherheitsmaßnahmen (wie z. B. externe prozedurale, materielle und personelle Kontrollmaßnahmen) ordnungsgemäß dokumentiert wurden. Jede Konfigurations- und Installationsprozedur ist nachzuvollziehen, um zu überprüfen, ob der EVG sicher konfiguriert und benutzt werden kann. Dabei ist lediglich die Dokumentation für den Nutzer und für den Administrator als Grundlage zu benutzen. Wo erforderlich, sind zusätzliche Tests durchzuführen, um die Analyse der Benutzerfreundlichkeit zu bestätigen oder zu widerlegen.*

Feststellung der Zertifizierungsstelle: Die Prüfstelle hat überprüft und festgestellt, dass die vorgelegte Analyse der Benutzerfreundlichkeit alle Anforderungen hinsichtlich Inhalt, Form und Nachweisen (ITSEC 3.31, 3.32) erfüllt sowie die Analyse alle relevanten Informationen verwendet hat. Sie hat ferner überprüft und festgestellt, dass die Analyse keine undokumentierten oder unvernünftigen Annahmen über die vorgesehene Betriebsumgebung enthält. Die Prüfstelle hat überprüft und festgestellt, dass alle Annahmen und Forderungen zu externen Sicherheitsmaßnahmen ordnungsgemäß

dokumentiert wurden. Jede Konfigurations- und Installationsprozedur ist von der Prüfstelle nachvollzogen worden und es wurde festgestellt, dass der EVG sicher konfiguriert und benutzt werden kann, wenn lediglich die Dokumentation für den Nutzer und Administrator zu Grunde gelegt wird. Zusätzliche Tests der Prüfstelle bestätigen die Analyse der Benutzerfreundlichkeit.

3.2.2 Aspekt 2: Bewertung der operationellen Schwachstellen

ITSEC 3.35 *Die Liste der Schwachstellen, die durch den Auftraggeber vorgelegt werden muss, muss alle ihm bekannten operationellen Schwachstellen des EVG aufführen. Sie muss jede Schwachstelle ansprechen, eine Analyse ihrer möglichen Auswirkungen beinhalten und die Maßnahmen aufzeigen, die zur Abhilfe vorgeschlagen oder zur Verfügung gestellt werden.*

ITSEC 3.36 *Die Analyse der möglichen Auswirkungen jeder bekannten Schwachstelle muss aufzeigen, dass die betreffende Schwachstelle in der beabsichtigten Einsatzumgebung des EVG nicht ausgenutzt werden kann, weil entweder*

- *die Schwachstelle angemessen durch andere, nicht beeinträchtigte externe Sicherheitsmaßnahmen geschützt ist oder*
- *gezeigt werden kann, dass die Schwachstelle bezüglich der Sicherheitsvorgaben ohne Bedeutung ist oder in der Praxis nicht ausgenützt werden kann.*

Die Analyse muss unter Verwendung zumindest jener Informationen durchgeführt werden, die in Abbildung 4 [3] für die angestrebte Evaluationsstufe angegeben sind. Alle geforderten externen Sicherheitsmaßnahmen müssen in der entsprechenden Dokumentation beschrieben (oder hinzugefügt worden) sein.

ITSEC 3.37 *Es ist zu überprüfen, ob die Liste der bekannten operationellen Schwachstellen alle Anforderungen bezüglich Inhalt, Form und Nachweis, so wie oben beschrieben, erfüllt. Es ist zu überprüfen, ob die Analyse alle Informationen verwendet hat, die in Abbildung 4 [3] für die angestrebte Evaluationsstufe angegeben sind. Es ist eine eigene Schwachstellenanalyse unter Berücksichtigung der aufgelisteten und der während der Evaluation gefundenen Schwachstellen durchzuführen. Es ist zu überprüfen, ob alle Kombinationen von bekannten Schwachstellen untersucht wurden. Es ist zu überprüfen, ob die Analysen der möglichen Auswirkungen keine undokumentierten oder unvernünftigen Annahmen über die vorgesehene Einsatzumgebung enthalten. Es ist zu überprüfen, ob alle Annahmen und Forderungen zu externen Sicherheitsmaßnahmen ausreichend dokumentiert wurden. Es sind Penetrationstests durchzuführen, um zu bestätigen oder zu widerlegen, ob die bekannten Schwachstellen in der Praxis wirklich ausgenutzt werden können.*

Feststellung der Zertifizierungsstelle: Die Prüfstelle hat überprüft und festgestellt, dass die Liste der bekannten operationellen Schwachstellen alle Forderungen bezüglich Inhalt, Form und Nachweise (ITSEC 3.35, 3.36), so wie oben beschrieben, erfüllt. Sie hat überprüft und festgestellt, dass die Analyse alle relevanten Informationen verwendet hat.

Es wurde zehn Schwachstellen vom Hersteller angegeben. Die Prüfstelle bewertet die operationellen Schwachstellen als nicht ausnutzbar, da ihnen durch die administrative Einsatzumgebung in ausreichender Weise entgegengewirkt wird. Die Prüfstelle hat eine eigene Schwachstellenanalyse durchgeführt und keine weitere operationelle

Schwachstellen gefunden. Die Prüfstelle hat alle Kombinationen der bekannten Schwachstellen untersucht. Die Prüfstelle hat überprüft und festgestellt, dass die Analysen der möglichen Auswirkungen der Schwachstellen keine undokumentierten oder unvernünftigen Annahmen über die vorgesehene Einsatzumgebung enthalten. Sie hat überprüft und festgestellt, dass alle Annahmen und Anforderungen bezüglich externer Sicherheitsmaßnahmen ausreichend dokumentiert sind.

Die Prüfstelle hat Penetrationstests durchgeführt und bestätigt, dass die bekannten Schwachstellen in der Praxis wirklich nicht ausgenutzt werden können.

3.3 Korrektheit – Konstruktion – Entwicklungsprozess

3.3.1 Phase 1: Anforderungen (Sicherheitsvorgaben)

ITSEC E1.2 *Die Sicherheitsvorgaben müssen die sicherheitsspezifischen Funktionen darlegen, die vom EVG zur Verfügung gestellt werden. Im Falle eines Systems müssen die Sicherheitsvorgaben zusätzlich eine System-Sicherheitspolitik (SSP) enthalten, die die Sicherheitsziele und Bedrohungen des Systems identifiziert. Für ein Produkt müssen die Sicherheitsvorgaben zusätzliche Aussagen enthalten, die die Art des Produkteinsatzes, die vorgesehene Einsatzumgebung und die für diese Einsatzumgebung angenommenen Bedrohungen identifizieren. Die in den Sicherheitsvorgaben aufgeführten sicherheitsspezifischen Funktionen müssen in informeller Notation (siehe ITSEC Kapitel 2) spezifiziert werden.*

ITSEC E1.3 *Im Falle eines Systems müssen die Sicherheitsvorgaben darlegen, auf welche Weise die vorgeschlagene Funktionalität die Sicherheitsziele erfüllt und wie sie den definierten Bedrohungen angemessen entgegenwirkt. Im Fall eines Produktes müssen die Sicherheitsvorgaben darlegen, warum die Funktionalität für diese Art des Einsatzes zweckmäßig ist und wie sie den angenommenen Bedrohungen entgegenwirkt.*

ITSEC E1.4 *Es ist zu überprüfen, ob die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis erfüllen. Es ist zu überprüfen, ob es Inkonsistenzen innerhalb der Sicherheitsvorgaben gibt.*

Feststellung der Zertifizierungsstelle: In den Sicherheitsvorgaben wird der EVG als Produkt im Sinne von ITSEC definiert. Die Prüfstelle hat überprüft und festgestellt, dass die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweise (ITSEC E1.2, E1.3) für ein Produkt erfüllen. Sie hat überprüft und festgestellt, dass es keine Inkonsistenzen innerhalb der Sicherheitsvorgaben[9] gibt.

3.3.2 Phase 2: Architekturentwurf

ITSEC E1.5 *Diese Beschreibung muss die grundsätzliche Struktur sowie alle externen Schnittstellen des EVG darlegen. Sie muss die Hard- und Firmware darlegen, die der EVG benötigt, und die Funktionalität der unterstützenden Schutzmechanismen angeben, die in dieser Hard- oder Firmware implementiert sind.*

[9] Für eine Zusammenfassung der Sicherheitsvorgaben siehe Kapitel 2.

ITSEC E1.6 *Die Beschreibung der Architektur muss darlegen, wie die sicherheitsspezifischen Funktionen der Sicherheitsvorgaben zur Verfügung gestellt werden.*

ITSEC E1.7 *Es ist zu überprüfen, ob die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis erfüllen.*

Feststellung der Zertifizierungsstelle: Die Prüfstelle hat überprüft und festgestellt, dass die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweise (ITSEC E1.5, E1.6) erfüllen.

3.3.3 Phase 3: Feinentwurf

ITSEC E1.8 *Keine Anforderungen.*

ITSEC E1.9 *Keine Anforderungen.*

ITSEC E1.10 *Keine Aufgaben.*

Feststellung der Zertifizierungsstelle: Entfällt bei ITSEC E1.

3.3.4 Phase 4: Implementierung

ITSEC E1.11 *Falls die Testdokumentation zur Verfügung gestellt wird, muss sie Testpläne, Testziele, Testverfahren und Testergebnisse enthalten. Falls eine Bibliothek von Testprogrammen zur Verfügung gestellt wird, muss sie Testprogramme und -werkzeuge enthalten, mit denen alle Tests, die in der Testdokumentation beschrieben sind, wiederholt werden können.*

ITSEC E1.12 *Falls die Testdokumentation zur Verfügung gestellt wird, muss sie die Übereinstimmung zwischen den Tests und den sicherheitsspezifischen Funktionen in den Sicherheitsvorgaben darlegen.*

ITSEC E1.13 *Es sind für alle in den Sicherheitsvorgaben identifizierten sicherheitsspezifischen Funktionen Tests durchzuführen, mit denen geprüft wird, ob der EVG die Sicherheitsvorgaben erfüllt. Zusätzlich sind Tests zur Fehlersuche durchzuführen. Falls auf angemessene Weise nachgewiesen wird, dass solche Tests bereits durch den oder im Auftrag des Antragsteller(s) durchgeführt wurden, ist eine Wiederholung der Tests durch den Evaluator nicht erforderlich. Die Testergebnisse müssen aber von ihm stichprobenhaft überprüft werden.*

Feststellung der Zertifizierungsstelle: Die Prüfstelle hat für alle in den Sicherheitsvorgaben identifizierten sicherheitsspezifischen Funktionen Tests durchgeführt und festgestellt, dass der EVG die Sicherheitsvorgaben erfüllt. Dabei wurden keine Fehler gefunden.

3.4 Korrektheit – Konstruktion – Entwicklungsumgebung

3.4.1 Aspekt1: Konfigurationskontrolle

ITSEC E1.15 *Die Konfigurationsliste muss darlegen, wodurch der EVG eindeutig identifiziert ist (Versionsnummer).*

ITSEC E1.16 *Die Konfigurationsliste muss darlegen, wie der EVG eindeutig identifiziert wird.*

ITSEC E1.17 *Es ist zu überprüfen, ob die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis erfüllen.*

Feststellung der Zertifizierungsstelle: Die Prüfstelle hat überprüft und festgestellt, dass die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweise erfüllen (ITSEC E1.15, E1.16).

3.4.2 Aspekt2: Programmiersprachen und Compiler

ITSEC E1.18 Keine Anforderungen.

ITSEC E1.19 Keine Anforderungen.

ITSEC E1.20 Keine Aufgaben.

Feststellung der Zertifizierungsstelle: Entfällt bei ITSEC E1.

3.4.3 Aspekt3: Sicherheit beim Entwickler

ITSEC E1.21 Keine Anforderungen.

ITSEC E1.22 Keine Anforderungen.

ITSEC E1.23 Keine Aufgaben.

Feststellung der Zertifizierungsstelle: Entfällt bei ITSEC E1.

3.5 Korrektheit – Betrieb – Betriebsdokumentation

3.5.1 Aspekt1: Benutzerdokumentation

ITSEC E1.25 Die Benutzerdokumentation muss die sicherheitsspezifischen Funktionen, die für den Endnutzer von Bedeutung sind, darlegen. Daneben muss sie auch Richtlinien für ihre sichere Anwendung enthalten. Die Benutzerdokumentation, zu welcher beispielsweise Referenz-Manuale, Benutzeranleitungen etc. gehören, muss strukturiert aufgebaut, in sich konsistent und mit allen anderen für diese Stufe gelieferten Dokumenten ebenfalls konsistent sein.

ITSEC E1.26 Die Benutzerdokumentation muss darlegen, wie ein Endnutzer den EVG in einer sicheren Art und Weise nutzt.

ITSEC E1.27 Es ist zu überprüfen, ob die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis erfüllen.

Feststellung der Zertifizierungsstelle: Vom Hersteller wurden folgende Dokumentationen zur Verfügung gestellt:

Ref.	Titel	Version	Datum
[BD_FZA]	Bedienungsanleitung Fahrzeugausrüstung MAWIS MOBA Automatic Waste Identification System	5.1	10.10.2003
[BDSD_Chck]	MAWIS - Beschreibung der Anwendung MAWIS_CHECK.exe	4	23.08.2004
[BDSD_DS]	MAWIS - Gefährdung der Datensicherheit und Gegenmaßnahmen im MAWIS	1.4	23.08.2004

Ref.	Titel	Version	Datum
[BDSD_ISC]	Ident System-Check Routineüberprüfung	2.0	04.07.2003
[BDSD_RWF]	MAWIS Rev. 2.0 - RWFMawis Softwaredokumentation	1.3	23.08.2004
[SD_Wart]	Bedienungsanleitung - Wartung des Monitors für die Behälteridentifikation	4.32	10.10.2003

Die Prüfstelle hat überprüft und festgestellt, dass die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweise (ITSEC E1.25, E1.26) erfüllen.

3.5.2 Aspekt2: Systemverwalterdokumentation

ITSEC E1.28 *Die Systemverwalter-Dokumentation muss die sicherheitsspezifischen Funktionen darlegen, die für den Systemverwalter von Bedeutung sind. Sie muss zwei Funktionsarten unterscheiden: solche, mit denen der Systemverwalter die Sicherheitsparameter kontrollieren kann, und solche, mit denen er lediglich Informationen abfragen kann. Wenn ein Systemverwalter notwendig ist, muss sie alle Sicherheitsparameter darlegen, die er kontrollieren kann. Sie muss jeden Typ eines sicherheitsrelevanten Ereignisses darlegen, der für die Systemverwaltungsfunktionen von Bedeutung ist. Sie muss Details zu den Verfahren, die für die Sicherheitsadministration relevant sind, in einer Form darlegen, die für die Handhabung ausreichend ist. Sie muss Richtlinien zu der konsistenten und wirksamen Nutzung der Sicherheitseigenschaften des EVG enthalten und darlegen, wie solche Eigenschaften zusammenwirken. Sie muss die Anweisungen darlegen, wie das System/Produkt installiert wird und wie es, wenn erforderlich, konfiguriert wird. Die Systemverwalter-Dokumentation, z.B. Referenz-Manuale, Systemverwalter-Anleitungen etc., muss strukturiert aufgebaut, in sich konsistent und mit allen anderen für diese Stufe gelieferten Dokumenten ebenfalls konsistent sein.*

ITSEC E1.29 *Die Systemverwalter-Dokumentation muss darlegen, wie der EVG sicher verwaltet wird.*

ITSEC E1.30 *Es ist zu überprüfen, ob die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis erfüllen.*

Feststellung der Zertifizierungsstelle: Die Prüfstelle hat überprüft und festgestellt, dass die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweise (ITSEC E1.28, E1.29) erfüllen.

3.6 Korrektheit – Betrieb – Betriebsumgebung

3.6.1 Aspekt1: Auslieferung und Konfiguration

ITSEC E1.32 *Wenn unterschiedliche Konfigurationen möglich sind, muss die Auswirkung der einzelnen Konfigurationen auf die Sicherheit dargelegt werden. Die Verfahren der Auslieferung und Systemgenerierung sind darzulegen.*

ITSEC E1.33 Die vorgelegten Informationen müssen darlegen, wie die genannten Verfahren die Sicherheit aufrechterhalten.

ITSEC E1.34 Es ist zu überprüfen, ob die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis erfüllen.

Feststellung der Zertifizierungsstelle: Die Prüfstelle hat überprüft und festgestellt, dass die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweise (ITSEC E1.32, E1.31) erfüllen.

3.6.2 Aspekt2: Anlauf und Betrieb

ITSEC E1.35 Die Prozeduren für einen sicheren Anlauf und Betrieb müssen dargelegt werden.

ITSEC E1.36 Die vorgelegten Informationen müssen darlegen, wie die Prozeduren die Sicherheit aufrechterhalten.

ITSEC E1.37 Es ist zu überprüfen, ob die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweis erfüllen.

Feststellung der Zertifizierungsstelle: Die Prüfstelle hat überprüft und festgestellt, dass die zur Verfügung gestellten Informationen alle Anforderungen an Inhalt, Form und Nachweise (ITSEC E1.35, E1.36) erfüllen.

4 Auszug aus ITSEC und ITSEM

4.1 Vertrauenswürdigkeit - Wirksamkeit

ITSEC 3.2:

Die Bewertung der Wirksamkeit erfordert die Betrachtung der folgenden Aspekte des EVG:

a) die Eignung der sicherheitsspezifischen Funktionen des EVG, den in den Sicherheitsvorgaben aufgezählten Bedrohungen zu widerstehen;

b) die Fähigkeit der sicherheitsspezifischen Funktionen und Mechanismen des EVG, in einer Weise zusammenzuwirken, dass sie sich gegenseitig unterstützen und ein integriertes, wirksames Ganzes bilden;

c) die Fähigkeit der Sicherheitsmechanismen des EVG, einem direkten Angriff zu widerstehen;

d) ob bekannte Sicherheitsschwachstellen in der *Konstruktion* des EVG in der Praxis die Sicherheit des EVG kompromittieren können;

e) dass der EVG nicht in einer Weise konfiguriert werden kann, die unsicher ist, aber von der ein Systemverwalter oder ein Endnutzer vernünftigerweise glauben könnte, dass sie sicher ist;

f) ob bekannte Sicherheitsschwachstellen beim *Betrieb* des EVG in der Praxis die Sicherheit des EVG kompromittieren können.

4.2 Vertrauenswürdigkeit – Korrektheit

ITSEC 4.2-4.10:

Sieben Evaluationsstufen werden bezüglich des Vertrauens in die Korrektheit eines EVG definiert. E0 bezeichnet die niedrigste, E6 die höchste dieser Stufen. Die sieben Evaluationsstufen können wie folgt *charakterisiert* werden:

Stufe E0

Diese Stufe repräsentiert unzureichende Vertrauenswürdigkeit.

Stufe E1

Auf dieser Stufe müssen für den EVG die Sicherheitsvorgaben und eine informelle Beschreibung des Architekturentwurfs vorliegen. Durch funktionale Tests muss nachgewiesen werden, dass der EVG die Anforderungen der Sicherheitsvorgaben erfüllt.

Stufe E2

Zusätzlich zu den Anforderungen für die Stufe E1 muss hier eine informelle Beschreibung des Feinentwurfs vorliegen. Die Aussagekraft der funktionalen Tests muss bewertet

werden. Ein Konfigurationskontrollsystem und ein genehmigtes Distributionsverfahren müssen vorhanden sein.

Stufe E3

Zusätzlich zu den Anforderungen für die Stufe E2 müssen der Quellcode bzw. die Hardware-Konstruktionszeichnungen, die den Sicherheitsmechanismen entsprechen, bewertet werden. Die Aussagekraft der Tests dieser Mechanismen muss bewertet werden.

Stufe E4

Zusätzlich zu den Anforderungen für die Stufe E3 muss ein formales Sicherheitsmodell Teil der Sicherheitsvorgaben sein. Die sicherheitsspezifischen Funktionen, der Architekturentwurf und der Feinentwurf müssen in semiformaler Notation vorliegen.

Stufe E5

Zusätzlich zu den Anforderungen für die Stufe E4 muss ein enger Zusammenhang zwischen dem Feinentwurf und dem Quellcode bzw. den Hardware-Konstruktionszeichnungen bestehen.

Stufe E6

Zusätzlich zu den Anforderungen für die Stufe E5 müssen die sicherheitsspezifischen Funktionen und der Architekturentwurf in einer formalen Notation vorliegen, die konsistent mit dem zugrundeliegenden formalen Sicherheitsmodell ist.

4.3 Klassifizierung von Sicherheitsmechanismen

ITSEM 6.C.4-6.C.7

Ein Mechanismus vom **Typ A** ist ein Sicherheitsmechanismus mit einer potentiellen Schwachstelle in seinem Algorithmus, seinen Prinzipien oder seinen Eigenschaften, aufgrund derer er durch Einsatz ausreichender Ressourcen, Fachkenntnisse und entsprechender Gelegenheiten mit einem direkten Angriff überwunden werden kann. Ein Beispiel für einen Mechanismus vom Typ A ist ein Authentisierungsprogramm, bei dem ein Passwort verwendet wird; wenn das Passwort erraten werden kann, indem nacheinander alle möglichen Passwörter ausprobiert werden, handelt es sich um einen Authentisierungsmechanismus vom Typ A. Mechanismen vom Typ A bedienen sich häufig eines "Geheimnisses" wie etwa eines Passworts oder eines kryptographischen Schlüssels.

Alle Mechanismen vom Typ A eines EVG haben eine Stärke, die dem Aufwand an Ressourcen, Fachkenntnissen und Gelegenheiten, zur Gefährdung der Sicherheit durch einen direkten Angriff auf den Mechanismus entspricht.

Bei der Bewertung der Stärke eines Mechanismus soll der Kontext, in dem der Mechanismus eingesetzt wird, mit berücksichtigt werden. Siehe den Unterabschnitt *Beispiele* weiter unten.

Ein Mechanismus vom **Typ B** ist ein Sicherheitsmechanismus, der bei perfekter Konzipierung und Implementierung keine Schwächen aufweist. Ein Mechanismus vom Typ B kann als nicht durch einen direkten Angriff überwindbar betrachtet werden, gleichgültig, wie groß der Aufwand an Ressourcen, Fachkenntnissen und entsprechenden Gelegenheiten ist. Ein mögliches Beispiel für einen Mechanismus vom Typ B wäre die Zugangskontrolle auf der Basis von Zugangskontrolllisten: Bei perfekter Konzipierung und Implementierung kann dieser Mechanismus vom Typ B nicht durch einen direkten Angriff überwunden werden. Mechanismen vom Typ B können jedoch durch indirekte Angriffe überwunden werden, mit denen sich andere Wirksamkeitsanalysen befassen.

4.4 Mindeststärke der Sicherheitsmechanismen

ITSEC 3.5-3.8

Alle kritischen Sicherheitsmechanismen (d.h. diejenigen, deren Versagen eine Sicherheitslücke hervorrufen würde), werden hinsichtlich ihrer Fähigkeit bewertet, einem direkten Angriff zu widerstehen. Die Mindeststärke jedes kritischen Mechanismus wird entweder als *niedrig, mittel* oder *hoch* bewertet.

Damit die Mindeststärke eines kritischen Mechanismus als **niedrig** eingestuft werden kann, muss erkennbar sein, dass er Schutz gegen zufälliges unbeabsichtigtes Eindringen bietet, während er durch sachkundige Angreifer überwunden werden kann.

Damit die Mindeststärke eines kritischen Mechanismus als **mittel** eingestuft werden kann, muss erkennbar sein, dass er Schutz gegen Angreifer mit beschränkten Gelegenheiten oder Betriebsmitteln bietet.

Damit die Mindeststärke eines kritischen Mechanismus als **hoch** eingestuft werden kann, muss erkennbar sein, dass er nur von Angreifern überwunden werden kann, die über sehr gute Fachkenntnisse, Gelegenheiten und Betriebsmittel verfügen, wobei ein solcher erfolgreicher Angriff als normalerweise nicht durchführbar beurteilt wird.

5 Literaturreferenzen

[1] ITSEC: *Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik,* Version 1.2 (1991)

[2] ITSEM: *Handbuch für die Bewertung der Sicherheit von Systemen der Informationstechnik,* Version 1.0 (1993)

[3] Laut Abbildung 4 der ITSEC-Kriterien sind für die Stufe E1 mindestens folgende Informationen bzw. Unterlagen für die Durchführung der Schwachstellenanalyse zu verwenden:

a) die Sicherheitsvorgaben,
b) eine informelle Beschreibung der Funktionen,
c) eine informelle Beschreibung des Architektur-Entwurfs und
d) die vollständige Betriebsdokumentation.

6 Abkürzungen

AIS	Anwendungshinweise und Interpretationen zum Schema
BSI	Bundesamt für Sicherheit in der Informationstechnik
CRC	Cyclic Redundancy Code
EVG	Evaluationsgegenstand