TÜV
PRODUCT SERVICE

TECHNISCHER BERICHT ZUR DATENMANIPULATIONSSICHERHEIT

Bildschirmschreiberfamilie
LOGOSCREEN

Hersteller

M.K.Juchheim
Moltkestraße 13-31
36039 Fulda

Bericht-Nr.: MF58870
Revision 1.0 vom 11. Februar 2000

Prüf- und Zertifizierungsstelle:

TÜV Product Service GmbH
Automation, Software and Electronics - IQSE
Ridlerstraße 65
80339 München

TÜV
PRODUCT SERVICE

Technischer Bericht zur Datenmanipulationssicherheit der Bildschirmschreiberfamilie LOGOSCREEN

Inhalt Seite

1 Gegenstand der Prüfung 3
2 Umfang der Prüfung 3
2.1 Prüfobjekt 3
2.2 Umfang des Prüfobjekts 3
2.3 Prüfungen 3
3 Prüfungsgrundlagen 4
3.1 Qualitätsmanagement bei der Prüfung 4
4 Prüfungsunterlagen 4
5 Prüfungsdokumentation 4
6 Durchführung und Ergebnis der Prüfungen 5
6.1 Datensicherheit 5
6.1.1 Definition der Sicherheitsziele 5
6.1.2 Bedrohungsanalyse 5
6.1.3 Penetrationstests 6
6.2 Prüfung der fehlervermeidenden Maßnahmen 6
6.3 Hinweisende Datensicherheit in der Produktdokumentation 6
7 Zusammenfassung 7

1 Gegenstand der Prüfung

Der vorliegende Technische Bericht stellt die Durchführung und die einzelnen Ergebnisse der Prüfung des Bildschirmschreiberfamilie LOGOSCREEN unter dem Aspekt der Datenmanipulationssicherheit dar.

Die Prüfung wurde im November 1999 durch die Fa. M.K.Juchheim beauftragt.

2 Umfang der Prüfung

2.1 Prüfobjekt

Die Bildschirmschreiberfamilie LOGOSCREEN umfasst die Typen LOGOSCREEN und LOGOSCREEN 500. Dieses sind elektronische X-t-Meßschreiber zur Erfassung, Visualisierung, Speicherung und Auswertung von analogen und digitalen Meßdaten. Die mit einem Microcontroller gesteuerten Geräte sind über verschiedene Schnittstellen konfigurierbar. Die Geräte sind für den Austausch von herkömmlichen Linienschreibern und Punktschreibern vorgesehen. Ihre Bauform ist für den Schaltschrankeinbau geeignet. Die Archivierung der Daten erfolgt auf Disketten an Stelle von Papierrollen. Alternativ können die Daten über eine serielle Schnittstelle ausgelesen und auf PCs archiviert werden. Als Medium stehen hier neben Disketten dann CDROM, magneto-optische Platten u.a. zur Verfügung. Die Meßdaten werden über auf der Rückseite befindliche steckbare Schraubklemmen aufgeschaltet und in einstellbaren Abständen digitalisiert und abgespeichert. Die weitere Verarbeitung kann durch Konfiguration beeinflußt werden. So ist z.B. zwischen fortlaufender Speicherung, Speicherung in einem Zeitfenster und ereignisgesteuerter Speicherung zu wählen.

2.2 Umfang des Prüfobjekts

Das Prüfobjekt umfaßt die nachfolgend gelisteten Komponenten:

- LOGOSCREEN Gerät
- Anwenderdokumentation

2.3 Prüfungen

Das Produkt wurde hinsichtlich nachfolgender Prüfschritte untersucht:

- Datensicherheit
  - Definition der Sicherheitsziele
  - Bedrohungsanalyse
  - Penetrationstests
- Prüfung der fehlervermeidenden Maßnahmen
- Hinweise zur Datensicherheit in der Produktdokumentation

3 Prüfungsgrundlagen

Auf Grund der Anwendung der Bildschirmschreiberfamilie LOGOSCREEN und des Prüfungsschwerpunktes Datenmanipulationssicherheit wurde die Prüfung in Anlehnung an folgende Richtlinien durchgeführt:

GSH98	IT Grundschutzhandbuch 1998

3.1 Qualitätsmanagement bei der Prüfung

QSH (Version 2)	Qualitätssicherungshandbuch der TÜV Product Service GmbH
QSH IQSE (Version 1.4)	Qualitätssicherungshandbuch des IQSE
EN 45001 (05.90)	Allgemeine Kriterien zum Betreiben von Prüflaboratorien

4 Prüfungsunterlagen

Folgende Unterlagen und Prüfmuster lagen der Prüfung zugrunde:

[U1]	LOGOSCREEN Gerät Typ: 955010 (6Kanal) SN# 0040528301099450008
[U2]	PC Auswerteprogramm (PCA Version 108.02.04, Prg.Ver. 3.02) auf CD-Rom
[U3]	Betriebsanleitung B95.5010.0.1
[U4]	Betriebsanleitung B95.5010.2.2
[U5]	High-Level Datenflußdiagramme und Funktionsübersichten
[U6]	verschiedene Prüfpläne und Prüfprotokolle zum LOGOSCREEN und zur Auswertesoftware

5 Prüfungsdokumentation

Folgende Dokumente enthalten einzelne Prüfergebnisse und wurden von der Prüfstelle verfaßt:

[P1]	Bericht zur Besprechung mit Fa. M.K.Juchheim am 8.12.1999
[P2]	Bedrohungsanalyse / System FMEA des Bildschirmschreibers LOGOSCREEN, Version 0.2 vom 3.1.2000
[P3]	Penetrationstests am Bildschirmschreiber LOGOSCREEN, Version 1.0 vom 25.1.2000

6 Durchführung und Ergebnis der Prüfungen

6.1 Datensicherheit

6.1.1 Definition der Sicherheitsziele

Für die Bildschirmschreiberfamilie LOGOSCREEN wurden gemeinsam mit Fa. M. K. Juchheim Sicherheitsziele festgelegt (s. auch [P1]). Diese sind in der nachfolgenden Tabelle aufgeführt.

6.1.2 Bedrohungsanalyse

An Hand der vorgelegten Systemstruktur wurde für die definierten Sicherheitsziele eine Bedrohungsanalyse durchgeführt. Die identifizierten Sicherheitsmaßnahmen gliedern sich in technische und organisatorische Maßnahmen sowie Maßnahmen zur Fehlervermeidung in der Entwicklung.

	Sicherheitsziel	**Bedrohung**	**Maßnahme**
1	Korrekte, der vom Anwender definierten Konfiguration entsprechende und reproduzierbare Aufzeichnung der aufgeschalteten Meßwerte.	Daten werden fehlerhaft aufgezeichnet (z.B. falsch skaliert, falsche Abtastungsrate, etc.)	Definierte, angewandte und nachgewiesene systematische Softwareentwicklungsverfahren mit festgelegten Verifikations- und Validationsschritten zum Erreichen einer korrekten Implementation.
2	Erkennen von Aufzeichnungslücken bzw. Erkenen, daß Daten gelöscht worden sind	Entnehmen des Speichermediums, Ausschalten des Schreibers, gelöschte Daten	Alle Aufzeichnungen werden mit einer jeweils aktuellen Datums- und Zeitmarke verknüpft. Die Auswertesoftware erlaubt die Darstellung aller gespeicherten Daten. Der Anwender kann mit dieser SW nach Aufzeichnungslücken suchen. Hierbei helfen ihm aufgezeichnete Ereignissen wie z.B. Netz ein/aus.
3	Erkennen, daß Daten unauthorisiert modifiziert worden sind	Datenaufzeichnungen werden nachträglich in Teilen oder im Ganzen manipuliert	Daten werden in einem nicht offen gelegtem Binärformat gespeichert. Gezieltes Ändern ist daher nicht möglich. Eine Signatur sichert blockweise alle gespeicherten Daten.
4	Schutz der Gerätekonfiguration vor unbemerkter Veränderung	Protokollparameter oder auch das Datum werden unbefugt verändert.	Ein 5-stelliges Passwort schützt den Zugang zum Konfigurationsmenu. Die Geräte werden mit voreingestelltem, d.h. aktiviertem Zugangsschutz ausgeliefert. Alle Konfigurationsänderungen werden protokolliert.

Prüfergebnis:

Die Bedrohungsanalyse hat ergeben, daß gegen alle Bedrohungen der definierten Sicherheitsziele Maßnahmen identifiziert sind und daß diese zur Sicherung der Korrektheit der Implementation und der Wirksamkeit der Manipulationssicherheit ausreichend sind. Das Ergebnis ist im Dokument [P2] festgehalten.

6.1.3 Penetrationstests

Die technischen Maßnahmen wurden an einem funktionsfähigen Seriengerät ([U1], [U2]) mit Penetrationstests auf Schwachstellen hin untersucht. Die von Fa. M. K. Juchheim vorgelegten, umfangreichen Rahmenprüfpläne und Testprotokolle wurden inspiziert.

Prüfergebnis:

Die durchgeführten Penetrationstests haben keine Schwachstellen im Datenformat und den zuständigen Fehlererkennungsroutinen aufgedeckt und sind im Dokument [P3] festgehalten. Die von Fa. M. K. Juchheim durchgeführten und dokumentierten Tests haben ebenfalls keine Hinweise auf Mängel ergeben.

6.2 Prüfung der fehlervermeidenden Maßnahmen

Die europäischen Vorgehensweisen für Konformitätsnachweise (93/465/EWG "Beschluß des Rates vom 22. Juli 1993 über die in den technischen Harmonisierungsrichtlinien zu verwendenden Module für die verschiedenen Phasen der Konformitätsbewertungsverfahren und die Regeln für die Anbringung und Verwendung der CE-Konformitätskennzeichnung") messen der der Qualitätssicherung des Herstellers in der Produktion und Produktpflege hohe Bedeutung zu. Die Fa. M. K. Juchheim erfüllt diese Anforderungen durch ein zertifiziertes und überwachtes Qualitätsmanagement-System nach DIN ISO 9001. Außerdem betreibt Fa. M. K. Juchheim ein akkreditiertes Kalibrierlaboratorium.

Die vorgelegte Dokumentation [U6] belegt, daß die durch das Qualitätsmanagement-System definierten Maßnahmen auf LOGOSCREEN angewandt werden und die für das erste Sicherheitsziel benötigten Maßnahmen einschließen.

6.3 Hinweisende Datensicherheit in der Produktdokumentation

Die Prüfung der technischen Dokumentation wurde anhand der Betriebsanleitung [U3] und der Schnittstellenbeschreibung [U4] durchgeführt. Hierbei wurde nur der Aspekt Datensicherheit berücksichtigt. Die Dokumentation enthält keine expliziten Hinweise zu Datensicherheit. Die Verwendung des Passwortschutzes für die Konfiguration ist beschrieben. Angaben über die Bedeutung der Diskettenseigenschaften und der Diskettenlagerung auf die Datenintegrität gibt es nicht.

7 Zusammenfassung

Die Bildschirmschreiberfamilie LOGOSCREEN stellt auf Grund Ihres Konzepts und ihrer Eigenschaften eine elektronische Ersatzmöglichkeit für Linienschreiber oder Punktschreiber mit zusätzlichen Mechanismen zur Gewährung der Datenintegrität und -manipulationssicheit dar. Die Wirksamkeit der implementierten Mechanismen sichert den vorgesehenen Einsatz zuverlässig, wenn die Lagerbedingungen und Archivierungsdauer von Disketten bzw. des gewählten Backupmediums berücksichtigt werden. Der Anwender muß für die Bereithaltung der Auswertesoftware zum Lesen der Meßdaten und der erforderlichen Betriebssystemsoftware über den geforderten Archivierungszeitraum seiner Meßdaten Sorge tragen.

TÜV PRODUCT SERVICE GMBH
Automation, Software and Electronics - IQSE
Projektleiter

i.A.

Reiner Heilmann