TÜV
PRODUCT SERVICE

TECHNICAL REPORT ON DATA-MANIPULATION SECURITY

Paperless Recorders
Memo-Graph / Eco-Graph

Manufacturer

Endress+Hauser Wetzer GmbH + Co KG
Obere Wank 1
D-87484 Nesselwang

Report-No.: EN59580
Revision 1.1 of 13. Juni 2000

Test and Certification Body:

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

PRODUCT SERVICE

Technical report on the data-manipulation security of the paperless recorders Memo-Graph / Eco-Graph

Contents Page

1 Subject of Testing

This technical report describes the performance and the individual results of the test of the paperless recorders Memo-Graph / Eco-Graph with regard to data-manipulation security.

The test was instigated by the company Endress+Hauser in May 2000.

2 Scope of Testing

2.1 Test specimen

The paperless recorders Memo-Graph / Eco-Graph are electronic X-t recorders for the acquisition, visualization, storage and evaluation of analog and digital measurement data. The instruments are controlled by microprocessors, and can be configured through various interfaces. The instruments are intended to replace the usual pen and dot-matrix chart recorders. The design is suitable for mounting in equipment cabinets. Data are archived on diskettes or flash memory cards, instead of on paper chart rolls. As an alternative, the data can be read out via a serial interface and archived on PCs. In this case, available media include not only diskettes, but also CDROM, magneto-optical disks etc. The measurement signals are applied to plug-in screw terminals on the back panel of the instrument, and are digitalized and stored at adjustable intervals. Scaling, real time clock, visualisation modes, and further options can be set by configuration.

2.2 Scope of test specimen

The test specimen comprised the following listed components:

- Memo-Graph / Eco-Graph instrument
- user documentation

2.3 Tests

The product was investigated in the following test stages:

- Data security
  - Definition of the security objectives
  - Threat analysis
  - Penetration tests
- Test of fault avoidance measures
- Security instructions in the product documentation

3 Testing principles

In view of the area of application of the paperless recorders Memo-Graph / Eco-Graph and the main theme of the test – data-manipulation security – the tests performed were derived from the following guidelines:

GSH98	IT Basic Security Manual 1998 („Grundschutzhandbuch")

3.1 Quality management during the test

QSH (Version 2)	Quality Assurance Manual of TÜV Product Service GmbH
QSH IQSE (Version 1.4)	Quality Assurance Manual of IQSE
EN 45001 (05.90)	General Criteria for the Operation of Test Laboratories

4 Test material

The following documents and test samples were used as material for the test:

[U1]	Eco-Graph, SW Ver. ELV000A V1.00.04 (6 channel) SN# 46543807
[U2]	PC evaluation program (ReadWin Version 2.28c) on CD-Rom
[U3]	Operating Manual BA 097R/09/a3/11.99, No.:510 00987 (Eco-Graph)
[U4]	Operating Manual BA 078R/09/a3/09.99, No.:510 00227 (Memo-Graph)
[U5]	EasyCase architecture diagrams and description for Eco-Graph, of 9.6.1996
[U6]	EasyCase architecture diagrams and description for Memo-Graph, of 7.6.1999
[U7]	Quality instruction MP001 - Development standards 01, of 22.10. 1998
[U8]	Quality instruction MP007 - Software development and -documentation, of 4.8.1999
[U9]	various test plans and test records for Memo-Graph

5 Test documentation

The following documents containing the individual test results have been prepared by the test agency:

[P1]	Threat analysis / System FMEA for the paperless recorders Memo-Graph / Eco-Graph, Version 1.0 of 16.5.2000
[P2]	Technical Report MF58870 of 11.2.2000 by TÜV Product Service, Munich
[P3]	Analysis of portability of the results from [P2] on the paperless recorders Memo-Graph / Eco-Graph (Endress+Hauser), Version 1.0 of 16.5.2000
[P4]	Penetration Tests, Version 1.0 of 25.1.2000 (s. [P2])

6 Performance and result of test

6.1 Data security

6.1.1 Definition of the security objectives

Regarding the aspect data manipulation security the test agency defined a set of security objectives for the paperless recorders Memo-Graph / Eco-Graph. These objectives are derived from application relevant scenarios and are listed in the following table.

6.1.2 Threat analysis

On the basis of the presented system structure a threat analysis was carried out for the defined security objectives. The safety measures that were identified are divided into technical and organisational measures, as well as measures for the avoidance of errors during development.

	Security objective	Threat	Measures
1	Correct and reproducible recording of the measurement signals that are applied, in accordance with the user-defined configuration.	Data may be incorrectly recorded (e.g incorrect scaling, wrong sampling rate etc.)	A defined, practised and proven systematic software development procedure, with verification and validation steps laid down to achieve a correct implementation.
2	Recognition of gaps in the recording and/or recognition that data have been deleted.	Removal of the storage media, switch-off of the recorder, deletion of data	All recordings have a corresponding current date and time mark attached. The evaluation software ReadWin permits the display of all stored data. The operator can use this software to search for gaps in the recordings. Assistance is provided by recorded events, such as power on/off.
3	Recognition that data have been altered without authorization	Data recordings may be wholy or partly manipulated at a later date.	Data are stored in an unpublished binary format. Intentional alteration is therefore not possible. A blockwise signature secures all stored data.
4	Protection of the instrument configuration from unobserved changes.	Unauthorized changes to protocol parameters or the date.	A 4-character password inhibits unauthorised configuration modification. The password must explicitly be activated. All changes to the configuration are recorded. Modification protection can also be implemented by use of a digital input (e.g. key switch).

Test result:

The threat analysis showed that measures are identified to protect against each of the threats to the defined security objectives and that the measures are sufficient to secure the correctness of the implementation and provide effective security against manipulation of data. The results are recorded in the document [P1].

6.1.3 Penetration tests

The technical measures were investigated for vulnerabilities by penetration tests on a series instrument. Design properties of this instrument as well as the instruments Memo-Graph / Eco-Graph were analysed. The test plans and test records provided by Endress+Hauser were inspected.

Test result

The above mentioned analysis of the design properties ([P3]) demonstrated, that the test results of the above mentioned penetration tests can be applied to the paperless recorders Memo-Graph / Eco-Graph. The performed penetration tests revealed no vulnerabilities in the data format and the corresponding error-detection routines. These results are recorded in document [P4]. The tests that were carried out and documented by Endress+Hauser also did not indicate any deficiency.

6.2 Testing of fault avoidance measures

The European methodology for certificates of conformity (93/465/EEC „Decision of the Council on 22nd July 1993 on the modules to be applied in the technical harmonization guidelines for the various phases of the conformity evaluation procedure, and the rules for application and use of the CE-conformity mark") attach importance to the manufactuer's quality ensurance in production and maintenance. The company Endress+Hauser fulfils these requirements through a certified and monitored quality management system according to DIN ISO 9001.

The documentation [U7] up to [U9] that has been presented testifies that the quality management system is applied to the paperless recorders Memo-Graph / Eco-Graph and includes the measures required for the first security objective.

6.3 Security instructions in the product documentation

The inspection of the technical documentation was made on the Operating Manuals (see document [U3] and [U4]). Only the data security aspect was considered. The documentation does not include explicit notes on data security. The use of the password and of the digital input for the configuration protection is described. Details on the significance of diskette characteristics and diskette storage for data integrity are not provided.

7 Summary

The concept and properties of the paperless recorders Memo-Graph / Eco-Graph make them into a possible electronic replacement for pen or dot-matrix chart recorders, with additional mechanisms to ensure the integrity of the data and security against manipulation. The effectiveness of the implemented mechanisms secures the envisaged application reliably, provided that the storage conditions and archive duration for diskettes or the selected backup media are respected. The user must take care that the evaluation software to read the measurement data and the operating system that is required are available for the required duration of the archiving of his measurement data.

on behalf of

TÜV PRODUCT SERVICE GMBH
Automation, Software and Electronics - IQSE
Project manager

Reiner Heilmann

TÜV
PRODUCT SERVICE

TECHNISCHER BERICHT ZUR DATENMANIPULATIONSSICHERHEIT

Bildschirmschreiber
Memo-Graph / Eco-Graph

Hersteller

Endress+Hauser Wetzer GmbH + Co KG
Obere Wank 1
D-87484 Nesselwang

Bericht-Nr.: EN59580
Revision 1.1 vom 13. Juni 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 Bildschirmschreiber Memo-Graph / Eco-Graph

Inhalt Seite

1 Gegenstand der Prüfung

Der vorliegende Technische Bericht stellt die Durchführung und die einzelnen Ergebnisse der Prüfung der Bildschirmschreiber Memo-Graph / Eco-Graph unter dem Aspekt der Datenmanipulationssicherheit dar.

Die Prüfung wurde Anfang Mai 2000 durch die Fa. Endress+Hauser beauftragt.

2 Umfang der Prüfung

2.1 Prüfobjekt

Die Bildschirmschreiber Memo-Graph / Eco-Graph 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 oder Flash-Speicherkarten 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. Skalierung, Echtzeituhr, Anzeigearten, und weitere Optionen können durch Konfiguration beeinflußt werden.

2.2 Umfang des Prüfobjekts

Das Prüfobjekt umfaßt die nachfolgend gelisteten Komponenten:

- Memo-Graph / Eco-Graph 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 Bildschirmschreiber Memo-Graph / Eco-Graph 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]	Eco-Graph, SW Ver. ELV000A V1.00.04 (6Kanal) SN# 46543807
[U2]	PC Auswerteprogramm (ReadWin Version 2.28c) auf CD-Rom
[U3]	Betriebsanleitung BA 097R/09/a3/11.99, No.:510 00987 (Eco-Graph)
[U4]	Betriebsanleitung BA 078R/09/a3/09.99, No.:510 00227 (Memo-Graph)
[U5]	EasyCase Architektur Diagramme und Beschreibung für Eco-Graph, vom 9.6.1996
[U6]	EasyCase Architektur Diagramme und Beschreibung für Memo-Graph, vom 7.6.1999
[U7]	Verfahrensanweisung MP001 - Entwicklungsstandards 01, vom 22.10. 1998
[U8]	Verfahrensanweisung MP007 - Softwareerstellung und -dokumentation, vom 4.8.1999
[U9]	verschiedene Testpläne und Testprotokolle zum Memo-Graph

5 Prüfungsdokumentation

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

[P1]	Bedrohungsanalyse / System FMEA der Bildschirmschreiber Eco-Graph, Memo-Graph, Version 1.0 vom 16.5.2000
[P2]	Technischer Bericht MF58870 vom 11.2.2000 der TÜV Product Service, München
[P3]	Analyse der Übertragbarkeit der Ergebnisse aus [P2] auf die papierlosen Schreiber Memo-Graph / Eco-Graph (Fa. Endress+Hauser), Version 1.0 vom 16.5.2000
[P4]	Penetrationstests, Version 1.0 vom 25.1.2000 (s. [P2])

6 Durchführung und Ergebnis der Prüfungen

6.1 Datensicherheit

6.1.1 Definition der Sicherheitsziele

Unter dem Aspekt der Datenmanipulationssicherheit wurden von der Prüfstelle anhand von Szenarien eine Reihe von einsatzrelevanten Sicherheitszielen für die Bildschirmschreiber Memo-Graph / Eco-Graph festgelegt. Diese sind in der nachfolgenden Tabelle aufgeführt sind.

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. Erkennen, 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 ReadWin erlaubt die Darstellung aller gespeicherten Daten. Der Anwender kann mit dieser SW nach Aufzeichnungslücken suchen. Hierbei helfen ihm aufgezeichnete Ereignisse 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 4-stelliges Passwort verhindert die unbefugte Modifikation der Konfiguration. Dass Passwort muß explizit aktiviert werden. Konfigurationsänderungen werden protokolliert. Der Änderungsschutz kann auch über einen Digitaleingang (z.B. Schlüsselschalter) realisiert werden.

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 [P1] festgehalten.

6.1.3 Penetrationstests

Die technischen Maßnahmen wurden an einem Seriengerät mit Penetrationstests auf Schwachstellen hin untersucht. Die Konstruktionseigenschaften dieses Gerätes sowie der Geräte Memo-Graph / Eco-Graph wurden analysiert. Die von Fa. Endress+Hauser vorgelegten Testpläne und Testprotokolle wurden inspiziert.

Prüfergebnis:

Durch die o.g. Analyse der Konstruktionseigenschaften ([P3]) wurde nachgewiesen, daß die Testergebnisse der o.g. Penetrationstests auf die Bildschirmschreiber Memo-Graph / Eco-Graph übertragbar sind. Die durchgeführten Penetrationstests haben keine Schwachstellen im Datenformat und den zuständigen Fehlererkennungsroutinen aufgedeckt und sind im Dokument [P4] festgehalten. Die von Fa. Endress+Hauser 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. Endress+Hauser erfüllt diese Anforderungen durch ein zertifiziertes und überwachtes Qualitätsmanagement-System nach DIN ISO 9001.

Die vorgelegte Dokumentation [U7] bis [U9] belegt, daß die durch das Qualitätsmanagement-System definierten Maßnahmen auf die Bildschirmschreiber Memo-Graph / Eco-Graph 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 Betriebsanleitungen [U3] und [U4] durchgeführt. Hierbei wurde nur der Aspekt Datensicherheit berücksichtigt. Die Dokumentation enthält keine expliziten Hinweise zu Datensicherheit. Die Möglichkeit der Bediensperre für Konfigurationsänderungen mittels Freigabecode und mittels Digitaleingang ist beschrieben. Angaben über die Bedeutung der Diskettenlagerung auf die Datenintegrität gibt es nicht.

7 Zusammenfassung

Die Bildschirmschreiber Memo-Graph / Eco-Graph stellen 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