TÜV
PRODUCT SERVICE

TECHNICAL REPORT
ON
DATA-MANIPULATION SECURITY

Paperless recorder series
LOGOSCREEN

Manufacturer

M.K.Juchheim
Moltkestraße 13-31
D-36039 Fulda

Report-No.: MF58870
Revision 1.0 of 11th February 2000

Test and Certification Body:

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

TÜV
PRODUCT SERVICE

Technical report on the data-manipulation security of the LOGOSCREEN series of paperless recorders

Contents Page

1 Subject of Testing

This technical report describes the performance and the individual results of the test of the LOGOSCREEN series of paperless recorders with regard to data-manipulation security.

The test was instigated by the company M. K. Juchheim in November 1999.

2 Scope of Testing

2.1 Test specimen

The LOGOSCREEN series of paperless recorders includes the types LOGOSCREEN and LOGOSCREEN 500. These 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, 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. The further processing can be determined by configuration. For instance, a selection may be made between continuous storage, storage in a time-slot (window) and event-controlled storage.

2.2 Scope of test specimen

The test specimen comprised the following listed components:

- LOGOSCREEN 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 LOGOSCREEN series of paperless recorders 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]	LOGOSCREEN instrument type: 955010 (6-channel) SN# 0040528301099450008
[U2]	PC evaluation program (PCA Version 108.02.04, Prg.Ver. 3.02) on CD-ROM
[U3]	Operating Manual B95.5010.0.1
[U4]	Operating Manual B95.5010.2.2
[U5]	high-level data flowcharts and functional overviews
[U6]	various test plans and test records for LOGOSCREEN and the evaluation software

5 Test documentation

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

[P1]	Report of the meeting with the company M. K. Juchheim on 8th December 1999
[P2]	Threat analysis / System-FMEA for the paperless recorder LOGOSCREEN, Version 0.2 on 3.1.2000
[P3]	Penetration tests on the paperless recorder LOGOSCREEN, Version 1.0 on 25th January 2000

6 Performance and result of test

6.1 Data security

6.1.1 Definition of the security objectives

Security objectives for the LOGOSCREEN series of paperless recorders were laid down jointly with M. K. Juchheim, (see also document [P1]). These have been listed in the following table.

6.1.2 Threat analysis

A threat analysis was carried out for the defined securityobjectives, on the basis of the system structure as presented. The safety measures that were identified are divided into technical and organizational 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 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 5-character password protects access to the configuration menu. The instruments are delivered with a preset active access protection. All changes to the configuration are recorded.

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 [P2].

6.1.3 Penetration tests

The technical measures were investigated for vulnerabilities by penetration tests on an series instrument in working condition, see [U1]. The extensive master test plans and test records provided by M. K. Juchheim were inspected.

Test result:

The performed penetration tests revealed no vulnerabilities in the data format and the corresponding error-detection routines. These results are recorded in document [P3]. The tests that were carried out and documented by M. K. Juchheim also failed to show any indication of a 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 M. K. Juchheim fulfils these requirements through a certified and monitored quality management system according to (DIN) ISO 9001. Furthermore, the company operates an accredited calibration laboratory.

The documentation [P3] that has been presented testifies that the quality management system is applied to the LOGOSCREEN and includes the measures required for the first security objective.

6.3 Security instructions in the product documentation

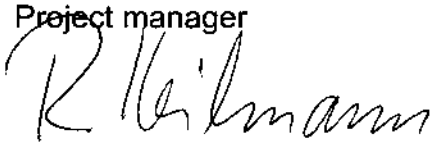
The inspection of the technical documentation was made on the Operating Manual (see document [U3]) and the Interface Description (see document [U4]). Only the data security aspect was considered. The documentation does not include explicit notes on data security. The use of the password protection for the configuration 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 LOGOSCREEN series of paperless recorders 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