TÜV
PRODUCT SERVICE

RAPPORT TECHNIQUE SUR LA SECURITE CONTRE MANIPULATION DES DONNEES

Famille des enregistreurs sans papier
LOGOSCREEN

Fabricant

M.K.Juchheim
Moltkestraße 13-31
36039 Fulda

Rapport n°: MF58870
Révision 1.0 du 11 février 2000

Organisme de certification et d'essai:

TÜV Product Service GmbH
Automation and Software - IQSE
Ridlerstraße 31
80339 München

TÜV
PRODUCT SERVICE

Rapport technique sur la sécurité contre manipulation des données de la famille des enregistreurs sans papier LOGOSCREEN

Sommaire Page

1 Objet du contrôle

Le rapport technique décrit la méthodologie et le résultat des différents tests réalisés sur les enregistreurs de type LOGOSCREEN concernant la sécurité contre manipulation des données.

Le contrôle a été effectué en Novembre 1999 sur commande de la société M.K.Juchheim.

2 Champ d'application du contrôle

2.1 Objet testé

La famille des enregistreurs LOGOSCREEN comprend les types LOGOSCREEN et LOGOSCREEN 500. Ce sont des enregistreurs électroniques X-t pour l'acquisition, la visualisation, la mémorisation et l'exploitation de données de mesure analogiques et numériques. Les appareils gérés par microprocesseur peuvent être configurés grâce à différentes interfaces. Ces enregistreurs sont destinés à remplacer les enregistreurs à tracé continu et à pointés classiques. Leur forme est adaptée pour le montage dans des armoires de commande. Les données sont archivées sur disquette au lieu de l'être sur papier. Une interface sérielle permet également de lire les données, puis de les archiver sur PC. En plus des disquettes, les données peuvent être stockées sur CD-ROM, lecteur optique, etc. Les mesures sont connectées par des bornes à visser embrochables situées à l'arrière de l'enregistreur, puis elles sont numérisées et mémorisées à intervalles programmables. Le traitement ultérieur dépend de la configuration. Il est possible, par ex. de choisir entre la mémorisation continue, la mémorisation pendant un intervalle de temps et la mémorisation commandée par les événements.

2.2 Champ d'application de l'objet testé

Le contrôle s'applique à:

- L'enregistreur LOGOSCREEN
- La documentation destinée à l'utilisateur

2.3 Contrôles

Le contrôle s'applique à:

- Sécurité des données
  - Définition des objectifs de sécurité
  - Analyse de risque
  - Test de violation
- Contrôle des mesures préventives
- Remarques concernant la sécurité des données dans la documentation

3 Bases des tests

Etant donné le domaine d'application de la famille des enregistreurs LOGOSCREEN et le fait que le contrôle porte essentiellement sur la « Sécurité contre manipulation des données », le contrôle a été effectué d'après les directives suivantes:

GSH98	IT Grundschutzhandbuch 1998 (Manuel de sécurité de base 1998)

3.1 Management de la qualité lors du contrôle

QSH (Version 2)	Manuel de qualité de TÜV Product Service GmbH
QSH IQSE (Version 1.4)	Manuel de qualité de IQSE
EN 45001 (05.90)	Allgemeine Kriterien zum Betreiben von Prüflaboratorien. (Critères communs aux laboratoires d'essai.)

4 Documents ayant servis au contrôle

Le contrôle a été basé sur les documents et échantillons suivants:

[U1]	Enregistreur, type LOGOSCREEN : 955010 (6 canaux) article n° # 0040528301099450008
[U2]	Logiciel d'exploitation pour PC (PCA version 108.02.04,Ver. Pgm 3.02) sur CD-Rom
[U3]	Notice de mise en service B95.5010.0.2
[U4]	Notice de mise en service B95.5010.2.2
[U5]	Diagrammes du flux des données High-Level et récapitulatif des fonctions
[U6]	Différents plans et protocoles de contrôle se rapportant au LOGOSCREEN et au logiciel d'exploitation

5 Documentation de contrôle

Les documents ci-après contiennent différents résultats de contrôle et ont été rédigées par l'organisme de contrôle:

[P1]	Compte rendu de l'entretien du 8.12.1999 avec la sté. M.K.Juchheim
[P2]	Analyse de risque / Système FMEA de l'enregistreur sans papier LOGOSCREEN, version 0.2 du 3.1.2000
[P3]	Tests de violation au niveau de l'enregistreur sans papier LOGOSCREEN, version 1.0 du 25.1.2000

6 Méthodologie et résultats des tests

6.1 Sécurité des données

6.1.1 Définition des objectifs de sécurité

Les objectifs de sécurité pour la famille des enregistreurs sans papier LOGOSCREEN ont été définis en commun avec la société M. K. Juchheim (voir également [P1]). Ils sont décrits dans le tableau suivant.

6.1.2 Analyse du risque

Une analyse de risque a été effectuée pour les objectifs de sécurité définis en s'appuyant sur la structure soumise du système. Les mesures de sécurité identifiées se répartissent en mesures techniques et d'organisation ainsi qu'en mesures de prévention lors du développement.

	Objectif de sécurité	Risque	Mesure
1	Enregistrement correct et reproductible des mesures suivant la configuration définie par l'utilisateur.	Enregistrement erronées de données (par ex. graduation erronée, cadence erronée de scrutation, etc.)	Procédure de développement définie, éprouvée et systématique du logiciel avec étapes de vérification et de validation définies pour obtenir une implémentation correcte
2	Détection de pertes d'enregistrement.	Extraction du support d'enregistrement, mise hors tension de l'enregistreur.	Le logiciel d'exploitation permet de représenter toutes les données mémorisées. Ce logiciel permet à l'utilisateur de rechercher des enregistrements manquants. L'enregistrement d'événements lui facilite la tâche, par ex. mise sous tension/hors tension.
3	Détection de modifications de données sans autorisation.	Les données enregistrées manipulées ultérieurement en partie ou en totalité.	Les données sont enregistrées dans un format binaire penvent être inaccessible. Une signature protège en bloc toutes les données mémorisées.
4	Détection d'effacement de données.	Effacement de données.	Tous les enregistrements sont reliés par une date et un repère de temps.
5	Protection de la configuration de l'appareil contre des modifications non décelées.	Les paramètres de protocole ou la date sont modifiés sans autorisation.	Un mot de passe à 5 caractères protège l'accès au menu de configuration. Les appareils sont livrés avec un code d'accès activé. Toutes les modifications de configuration sont enregistrées sous forme de protocole.

Résultat des tests:

L'analyse du risque montre, que des dispositions ont été identifiées contre tous les risques existants pour les objectifs de sécurité définis et qu'elles sont suffisantes pour assurer l'implémentation correcte ainsi que l'efficacité de la sécurité contre la manipulation. Le résultat est établi dans le document [P2].

6.1.3 Tests de violation

Les mesures techniques ont été examinées sur un appareil de série en état de fonctionnement ([U1], [U2]) avec tests de violation réalisés sur des points faibles. De nombreux schémas- cadres de contrôle et protocoles d'essai présentés par la sté M. K. Juchheim ont été vérifiés.

Résultat des tests:

Les différents tests de violation n'ont décelé aucun point faible ni au niveau du format des données ni de la détection d'erreurs ; ces tests sont relatés dans le document [P3]. Les tests effectués et documentés par la société M. K. Juchheim ne donnent pas lieu à relever une quelconque déficience.

6.2 Tests concernant les mesures pour prévenir les erreurs

Les procédures européennes des certificats de conformité (93/465/CEE "Décret du Conseil du 22 juillet 1993 sur les modules à appliquer dans les directives d'harmonisation techniques pour les différentes phases des procédures d'évaluation des conformités ainsi que les règles d'application du sigle CE") attribuent une grande importance à l'assurance qualité du fabricant quant à la production et à l'entretien du produit. La société. M. K. Juchheim remplit ces exigences grâce au système d'assurance qualité suivant DIN ISO 9001. De plus, la société M. K. Juchheim possède un laboratoire d'étalonnage accrédité.

La documentation présentée [U6] justifie que les mesures définies par le système d'assurance qualité est appliqué au LOGOSCREEN et qu'il englobe les mesures nécessaires pour le premier objectif de sécurité.

6.3 Sécurité des données dans la documentation du produit

Le contrôle de la documentation technique a été effectué sur la base de la notice de mise en service [U3] et de la description des interfaces [U4], en prenant uniquement en compte l'aspect sécurité des données. La documentation ne contient pas de remarques explicites concernant la sécurité des données. L'utilisation du mot de passe pour la configuration est décrite. Il n'existe aucune information sur l'influence des propriétés et du stockage des disquettes sur l'intégrité des données.

7 Résumé

En raison de son concept et de ses propriétés, la famille des enregistreurs sans papier LOGOSCREEN représente une solution de remplacement électronique pour des enregistreurs à tracé continu ou à pointés avec des mécanismes supplémentaires pour garantir l'intégrité et la sécurité contre toute manipulation des données. L'efficacité des mécanismes implémentés assure la fiabilité de l'application pourvue que les conditions de stockage et la durée d'archivage des disquettes ou des fichiers backup (copies) soient respectées. L'utilisateur doit veiller à ce que le logiciel d'exploitation des données et le logiciel du système soient valables pour la durée d'archivage de ses données requise.

TÜV PRODUCT SERVICE GMBH
Automation, Software and Electronics - IQSE
Directeur de projet

i.A. R Heilmann

Reiner Heilmann