

STM4000/STM6000 – Systèmes de mesure numériques pour l'essai de métrologie et le contrôle de la communication de données



STM4000

STM6000

Informations sur les compteurs intelligents

07 30 3F 89 **B1B** 1B 1B

Analyse de la communication

Test de fonctionnement

Interface

Gestion des clés

Protocole

Concentrateur de données

Généralités



Le monde énergétique de l'avenir est un monde numérique. Les réseaux et les compteurs électriques doivent toujours répondre à de nouvelles exigences. Les fluctuations, l'utilisation et les changements de canaux de distribution doivent être commandés de manière fiable et efficace. Cependant, avec chaque nouveau participant au réseau, comme les voitures électriques ou les installations photovoltaïques, le nombre d'interfaces, de voies de communication et d'états de fonctionnement nécessaires augmente. La technologie numérique est indispensable pour gérer toutes ces exigences. Les nouvelles technologies permettent aux différents participants du réseau de communiquer entre eux et, si nécessaire, de réagir en conséquence.

Compteur intelligent ou compteur électronique – Quelle est la différence ?



Compteur intelligent

Le compteur numérique (également appelé compteur intelligent) remplace progressivement le simple compteur électronique. Alors que le compteur électronique, par exemple, utilise l'interface infrarouge pour être lu sur place, des processus complexes se déroulent dans le compteur intelligent qui vont bien au-delà de l'essai de métrologie. La principale différence entre les deux types de compteurs est la transmission des données, qui s'effectue via l'interface locale dans le cas du compteur électronique et via un réseau dans le cas du compteur intelligent.



Compteur électronique

Depuis longtemps, les relevés de compteurs intelligents ne sont plus effectués par l'opérateur du point de mesure sur place, mais sont transmis par internet. Ce faisant, les sujets tels que la sécurité des données, le cryptage et l'interopérabilité revêtent une grande importance.

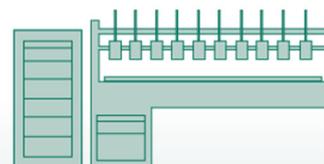


Le terme compteur intelligent est interprété et défini différemment dans le monde. Cependant, toutes les définitions ont en commun qu'un compteur intelligent, par rapport à un compteur électronique, possède une interface de communication et est connecté à un réseau. Cette interface peut avoir différentes caractéristiques et utiliser une grande variété de technologies et de protocoles.

Les objectifs de ces interfaces sont en grande partie identiques : il s'agit de transmettre des informations provenant du compteur. Certaines de ces informations sont généralement affichées (sans demande) sur l'écran ou envoyées via l'interface de communication (p. ex., le relevé du compteur), d'autres doivent être demandées spécifiquement au compteur. L'avenir promet avec grande certitude que cette communication sera exclusivement cryptée. Cela permet de répondre aux exigences croissantes en matière de protection des données et d'adapter la communication à l'état actuel de la technique.

Contrôles automatiques d'un compteur intelligent

- Essai de métrologie d'un compteur intelligent avec ou sans cryptage
- Test de fonctionnement
- Analyse de la communication



Essai de métrologie

Les essais de métrologie d'un compteur intelligent et d'un compteur électronique diffèrent principalement dans l'utilisation de l'interface de communication. Cette interface d'automatisation du processus d'essai peut être utilisée, par exemple, pour interroger des données qui auraient normalement été lues manuellement. La tâche principale reste l'acquisition de valeurs de mesure avec la précision correspondante.

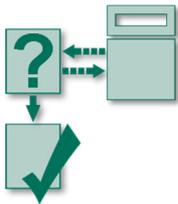


Lors de l'utilisation de compteurs intelligents, des mots de passe (p. ex., DLMS LLS¹) ou des matériels cryptographiques clés (p. ex., DLMS HLS²) peuvent être nécessaires. Même si seules les valeurs de mesure doivent être récupérées automatiquement à partir de votre compteur intelligent, vous avez également besoin des informations sur le matériel clé de votre compteur pour ce processus. Les fonctions de sécurité de ce type ne peuvent jamais être désactivées ou contournées, même pour des essais de métrologie.

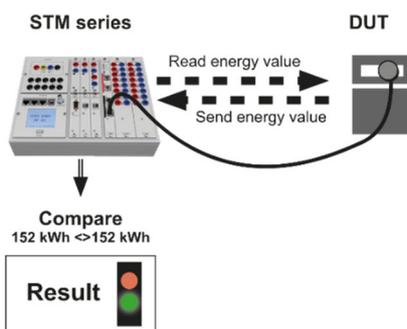
1 LLS = Low Level Security (niveau de sécurité bas)

2 HLS = High Level Security (niveau de sécurité élevé)

Test de fonctionnement



Les objectifs des tests de fonctionnement et des analyses de communication diffèrent principalement en termes de contenu. D'une part, il y a l'évaluation d'un résultat (bon/mauvais). D'autre part, il y a l'examen détaillé de la communication (timing, séquence, etc.).



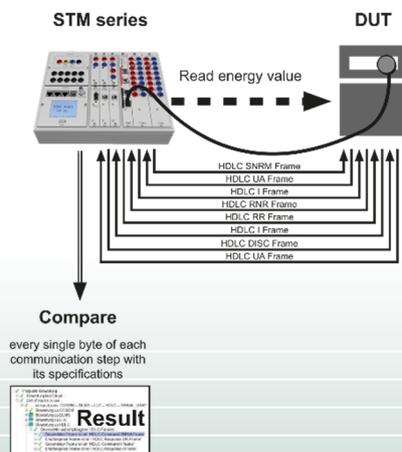
L'objectif d'un test de fonctionnement est de garantir l'exécution correcte d'une fonction ou d'un processus de communication. Par exemple, une valeur prédéfinie est interrogée, la réponse correspondante est comparée à la valeur attendue, puis évaluée (bonne ou mauvaise).

Les tests de fonctionnement qui ont donné de bons résultats en laboratoire ne fournissent toutefois que des informations limitées sur la capacité de l'objet testé à communiquer correctement avec d'autres participants à la communication sur le terrain.

La raison pour cela est qu'un essai fonctionnel évalue le *résultat* et non la *façon* par laquelle la communication entre le système de contrôle et l'objet testé a lieu.

Les objets testés d'un test de fonctionnement ne sont pas évalués sur la base de leur comportement de communication, mais sur le résultat obtenu.

Analyse de la communication



L'objectif d'une analyse de communication est d'examiner en détail la communication de l'objet testé et de s'assurer que chaque octet transmis est conforme aux spécifications. Contrairement au test de fonctionnement, ce contrôle n'est pas axé sur l'évaluation du contenu à transmettre, mais sur la *conformité au processus systématique de communication*.

Un objet testé échoue avec la mention « Non réussi » dès qu'un détail de la transmission n'a pas été respecté (séquence, contenu spécifique au protocole, timing, etc.). Un tel contrôle peut être appliqué à la communication de l'objet testé s'il est spécifié de manière suffisamment claire. La charge utile (payload) à transmettre n'est pas le point central de l'analyse de la communication.

Dans notre illustration, nous montrons schématiquement une analyse de communication en nous concentrant sur le protocole HDLC et les télégrammes associés. Outre l'interrogation de la valeur du compteur et de la réponse du compteur dans l'iframe, 6 autres frames de communication sont échangés. Pour assurer une communication correcte entre deux appareils, chaque composant de ces frames doit être mis en œuvre conformément à la spécification.

Les deux sont importants.

Le test de fonctionnement est important, mais il ne permet pas à lui seul de tirer des conclusions sur les raisons pour lesquelles un objet testé est défectueux. Il est complété par l'analyse de communication, qui compare tous les paramètres et informations spécifiques au protocole avec la spécification et les évalue en conséquence. Vous recevez un résultat complet sur la qualité de votre objet testé.

Pour des informations détaillées sur le sujet, veuillez consulter notre site web :

<https://www.zera.de/news/communication-testing/communication-testing-editorial/>

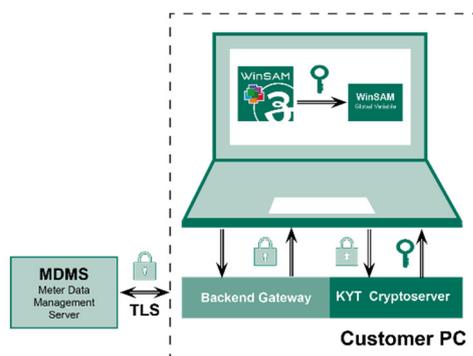


Gestion des clés



La gestion des clés est un élément central de la sécurité des informations. Il est important d'assurer cette sécurité dans la communication entre le dispositif de test de compteurs et l'objet testé. La meilleure solution pour cela est une connexion protégée à un système de gestion des données de compteurs (MDMS) ou à une infrastructure similaire. Un MDMS désigne le système de gestion des données de compteurs. Il veille, entre autres, à ce que les données nécessaires au contrôle soient mises à disposition.

Signification



La gestion des clés a pour tâche de gérer les clés nécessaires aux processus de cryptage (également : procédures cryptographiques¹).

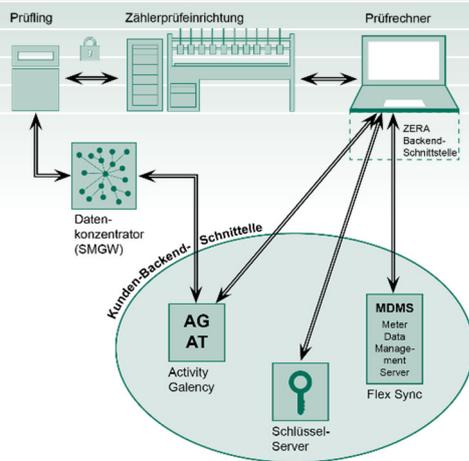
La sécurité des communications cryptées ou des données cryptées dépend directement de la gestion des clés. Elle garantit le secret des clés et en vérifie l'authenticité.

Ses tâches comprennent la génération, le stockage, l'échange et la protection des clés. Les termes alternatifs sont *Encryption Keymanagement* ou *Keymanagement*.²

¹ Cryptologie : La cryptologie (du grec κρυπτός kryptós « caché, dissimulé, secret » et -logie) est une science qui traite du cryptage et du décryptage des informations et donc de la sécurité de l'information.
Source : Wikipedia

² Source : www.security-insider.de

Système de gestion des données de compteurs – MDMS



Une connexion réussie à l'objet testé protégé³ est nécessaire pour la communication entre le dispositif de test de compteurs et le compteur. Les informations sur les clés et les mots de passe doivent être fournis au moment du contrôle. Dans ce cas, le traitement manuel par l'examineur est inapproprié.

En fournissant une connexion protégée au système de contrôle via un MDMS ou une infrastructure similaire, les clés et les mots de passe peuvent être fournis sous forme cryptée. Les données sont décryptées et mises à disposition pour être utilisées uniquement directement dans le système de contrôle. Le contrôle peut interpréter un décryptage réussi, mais ne peut pas le voir comme du texte en clair.

3 protégé signifie ici que, par exemple, des mots de passe sont utilisés pour vérifier l'autorisation de l'utilisateur et que des procédures de cryptage sont utilisées pour garantir que les données ne peuvent pas être lues ou modifiées pendant la transmission.

Pour des informations détaillées sur le sujet, veuillez consulter notre site web :

<https://www.zera.de/news/key-management-editorial/>

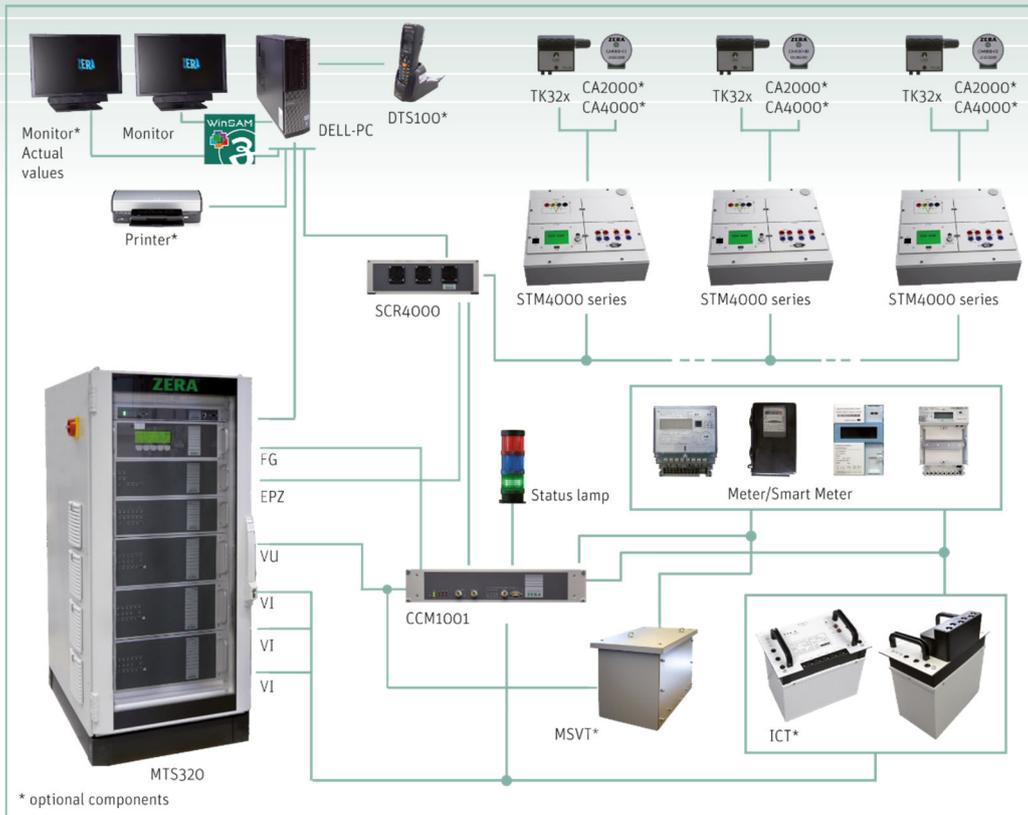


Solutions matérielles – STM4000 et STM6000

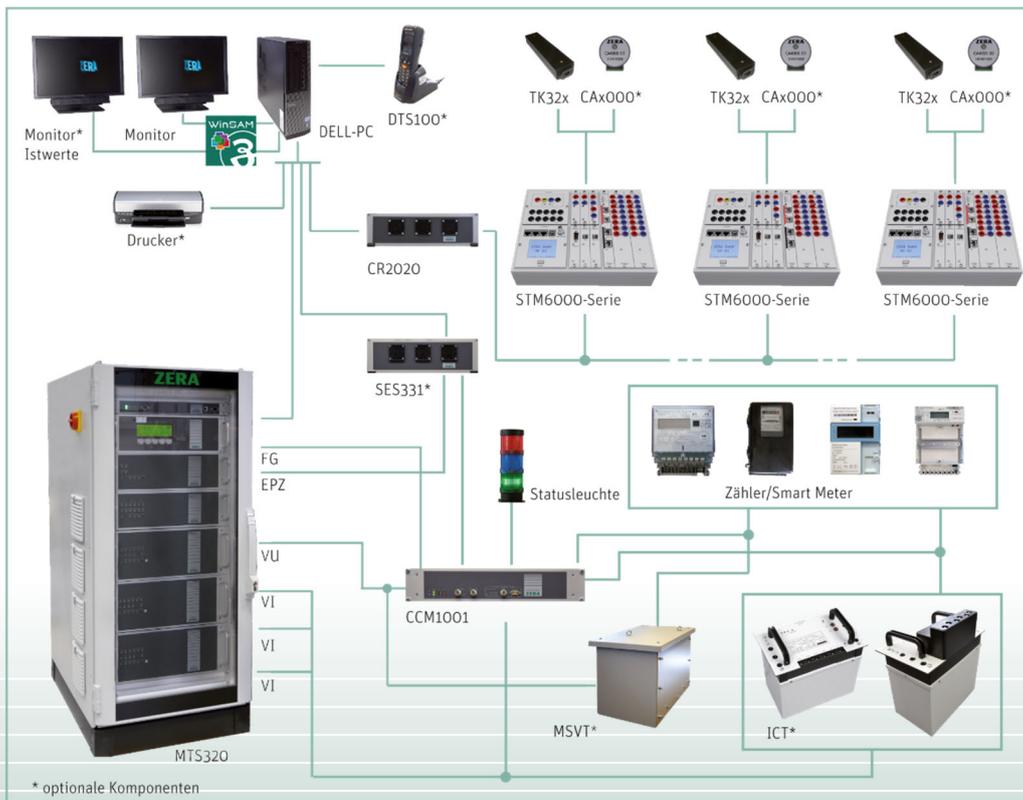
Avec nos systèmes de mesure numériques STM4000 et STM6000, vous avez la possibilité d'examiner en détail votre compteur également en termes de communication de données. Au plus tard, lorsque l'interopérabilité, c'est-à-dire la communication de plusieurs appareils, éventuellement de différents fabricants et avec la même norme, joue un rôle, cette analyse est indispensable pour identifier les écarts.

Fonction de base	Module(s) STM4000	Module(s) STM6000
Écran TFT couleur 2,8 po.	STM4000	STM6000
Bouton de réinitialisation	STM4000	STM6000
Mesure impulsionnelle de métrologie via BNC (y compris diviseur 1, 10, 100, 1000)	STM4000	STM6000
Essai de métrologie via LED (puissance active/réactive)	STM4000	STM6000
Essai de métrologie via LED (tête de lecture externe/adaptateur de communication supplémentaire)	-	STM6000
Circuit de tension individuel par phase et N	STM4120	STM6000, STM6110, STM6120
Circuits auxiliaires	en option	en option
Communication via interface optique (IR), max. 57 600 bauds, IEC 62056-21/IEC 61107 (EN1107), IEC 62056/-42/-46/-53 DLMS/COSEM (HDLC, LLC, DLMS (autor. par LLS, HLS), COSEM), ABB (Elster) Vision	STM4000	STM6220
Communication via Ethernet	-	STM6000
Mesure et réglage de l'intensité lumineuse	STM4000, CA4000	STM6000, CA6000

Série STM4000



Série STM6000



Tout dans un logiciel

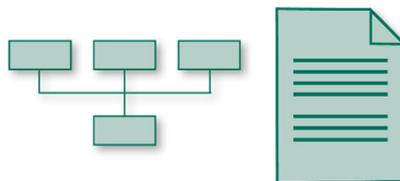


La commande complète et **entièrement automatique** de l'essai de métrologie et de l'analyse de la communication est mise en œuvre par notre logiciel de contrôle et de commande WinSAM.

En option, diverses licences permettent la réalisation d'extensions fonctionnelles :

- Cas de test selon des spécifications FNN (DE)
- Contrôle de réception (DE)
- Backend Gateway (DE)
- Licence DLMS
- Visionneuse de journaux

Interfaces et protocoles



Type	STM4000	STM6000
RS485 (2/4 câbles), max. 115,2 kbauds <ul style="list-style-type: none"> - Modbus* - ANSI12.22 (compteur Echelon) par le logiciel du fabricant du compteur 	STM4200	STM6230
Essai de métrologie via transmetteur SO (EN62053-31)	1x (24V)	4x, 8x, 12x (5 ... 27 V)
Essai de métrologie via récepteur SO (EN62053-31)	-	4x, 8x, 12x
RS232, max. 115,2 kbauds	STM4200	STM6240
Mbus, max. 38,4 kbauds	Esclave	STM621x Maître/ Esclave
Mesure du temps maximum tm/te	-	Au niveau de toutes les entrées
CL, 20 mA	-	STM6200
Communication via interface optique (IR), 9,6 kbauds, SML : TRO3109-1	-	STM6220
Communication via interface LMN (câblée, à l'arrière, interface optique, 921,6 kbauds), bluebook, IEC13239, RFC5246, TRO3109-1 : COSEM (HDLC, TLS, SML, COSEM)	-	STM6290
EDL (info/interface MSB), SML : TRO3109-1	-	STM6250
SyM ² , TRO3109-1, IPv4	-	STM6260

* en option

Solutions spécifiques aux clients

En plus de nos produits standard, nous proposons également des adaptations personnalisées pour PLC, RF ou NFC. Nous serons heureux de vous conseiller à ce sujet. Contactez-nous ou écrivez-nous à sales@zera.de.



Logiciel

Grâce au logiciel de contrôle et de commande WinSAM, l'ensemble du contrôle de vos systèmes stationnaires peut être réalisé de manière entièrement automatique, les résultats de mesure enregistrés et les données des clients gérées. WinSAM combine toutes les fonctionnalités dont vous avez besoin pour notre série STM.



Fiche d'informations STM4000

Dans notre fiche d'informations, vous trouverez de plus amples informations, des explications et des données clés sur notre système de mesure numérique de la série STM4000 – notre solution flexible et rentable pour le contrôle moderne de compteurs.

<https://www.zera.de/products/meter-test-systems/stationary-meter-test-systems/>



Fiche d'informations STM6000

Vous trouverez un aperçu des différents modules et de leurs fonctionnalités dans notre fiche d'informations STM6000. Ce système de mesure numérique présente le plus haut niveau d'expansion de nos solutions de contrôle modernes. La structure est développée de manière modulaire jusque dans les moindres détails, ce qui est parfait pour des solutions personnalisées.

<https://www.zera.de/products/meter-test-systems/stationary-meter-test-systems/>