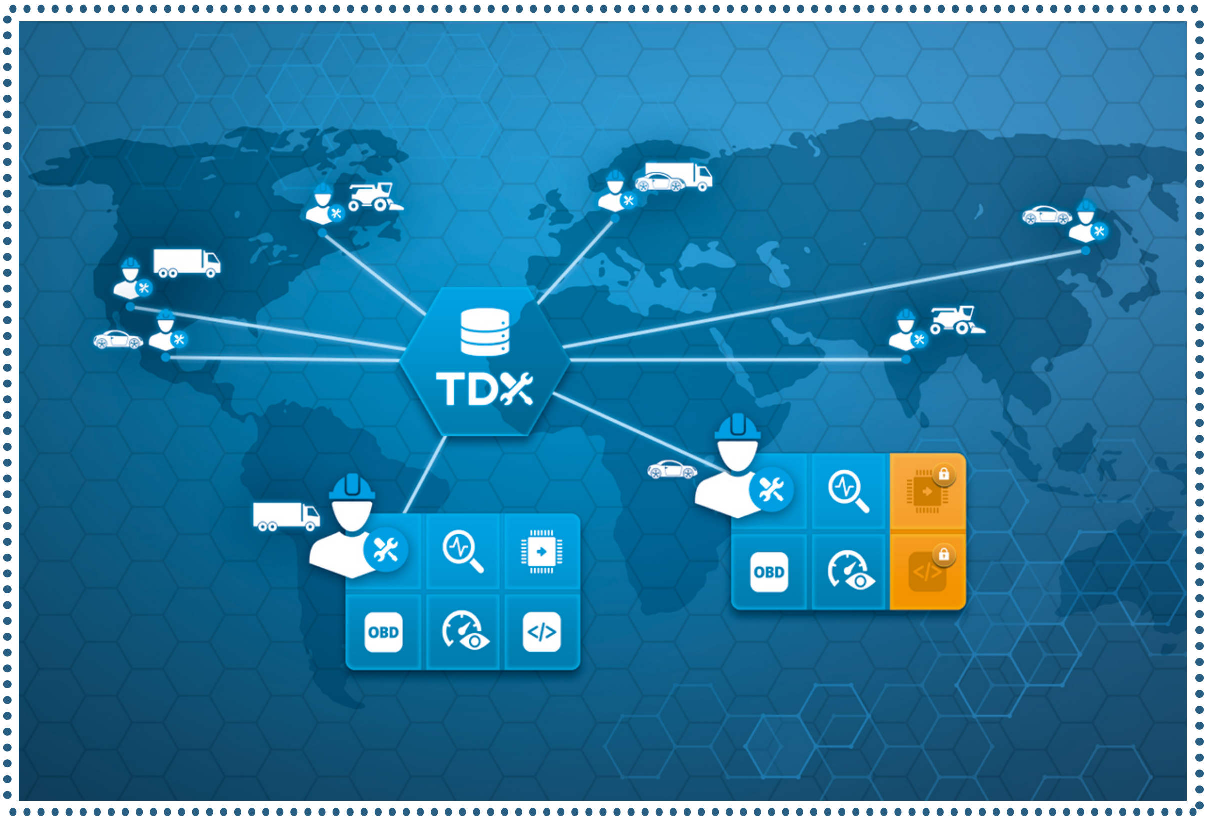


Non-Identical Twins: Repair Shop Diagnostics and Authorization Management

There are tens of thousands of individual repair shop testers in the field today. On top of that, they are deployed all over the world by different users with different requirements and authorizations. Improper handling can lead to serious damage. This multi-user scenario can only be mastered with an appropriate allocation of tester functions and central administration. Integrated authorization management fits into the core processes and, furthermore, offers additional security.

Most OEMs and system suppliers maintain a large number of service repair shops worldwide or send out mobile service technicians to offer their customers both fast and targeted maintenance and repair services. This requires the provision of an efficient repair shop tester. However, due to the enormous number of service testers in the field, usage and access are very difficult to keep in check. Especially in the case of external access, control units on vehicles, for example, can be incorrectly programmed, which can affect traffic safety and, in a worst case scenario, lead to an accident with personal injury.

The repair shop tester requires a robust authorization system to avoid serious consequences due to the lack of protection of sensitive data as well as critical functions. This helps both to protect against unauthorized access and to enable authorized users rights-based access. The allocation of individual authorizations has proven to be too complex, especially with a large number of users. In short, there is one question that has to be answered: Who can access which data and functions and how?

Roles as the Key to Central Authorization Management

Originally published in German in the section "Measurement - Test - Diagnosis" of the technical magazine HANSER automotive 07/2020, published by Carl Hanser, Munich, Germany

A rights- and role-based access control system is much more efficient for implementing and especially maintaining authorizations. With Role Based Access Control (RBAC), authorizations are assigned to the respective employees based on roles, which in turn contain tester functions (e.g. ECU update). Often, roles within companies are already defined by the organizational structure and can be reused. The advantages of RBAC in contrast to other approaches are the simpler administration as well as the more flexible adjustment possibilities without the specification of rigid rules.

For the responsible administrators, the focus is on central management and control of the roles as well as the corresponding role model. The complete administration up to the publication in the tester must run in the background. A central role and user database (RUDB) forms the basis and is an absolute requirement without which authorization management cannot be implemented. For the administration itself, certain requirements must be met. An administrator must be able to create new roles relatively easily: In turn, these roles are stored with intended tester functions. This is usually only time-consuming at the beginning because, once defined, role models should remain the same in their basic features and rarely be changed. The assignment of employees to their respective roles is also an integral part of administration and forms the basis for the rights-based use of diagnostic functions in the service tester. Here, it is important that an automated update process helps ensure the currently valid roles and rights are always effective in the tester. The assigned rights should not only be available when the tester is online. Especially for mobile service technicians, who often work at locations without Internet access, the local availability of user-specific authorizations is absolutely necessary.

To assign users to the intended roles, they must also be usable in the RUDB. Administrators must familiarize themselves with the working of the administration tool as quickly as possible so they can not only create roles but also users with unique credentials, the user name and a password, and communicate these to the employees. Many companies already maintain such employee and/or user databases so that the necessary credentials are already available. Active Directory, for example, is a common service that controls identity access across a specific enterprise. The manual transmission of this information is particularly complex which means it is sensible for it to be exported directly into the RUDB.

Even if the role model does not normally have to be changed over a longer period of time, it may still be necessary to make adjustments at short notice. These could be due to changing project affiliations, vacation replacements, a change in department or a higher experience level. For example, the necessary functions can be activated by providing proof of special, certified training. The entire system of authorization management must be flexible enough to allow ad hoc adjustments to be made. Especially the possibility to limit the time of such short-term changes offers additional degrees of freedom. It is not only adjustments to the role assignment that should be easy but also subsequent adjustments to the role itself.

MANAGING Autorizations

An authorization management system that is obligatory for the after-sales tester must therefore be implemented as quickly as possible and, above all, be able to be maintained and kept up to date in a centralized form. To make this possible, Softing TDX offers the ideal tool support along the dedicated DESIGN-MANAGE-WORK workflow.

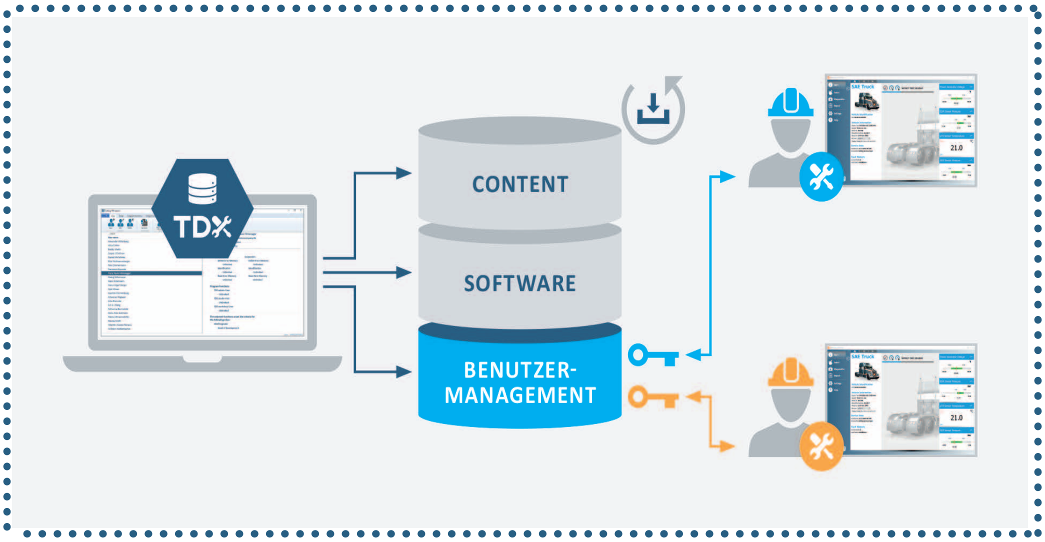
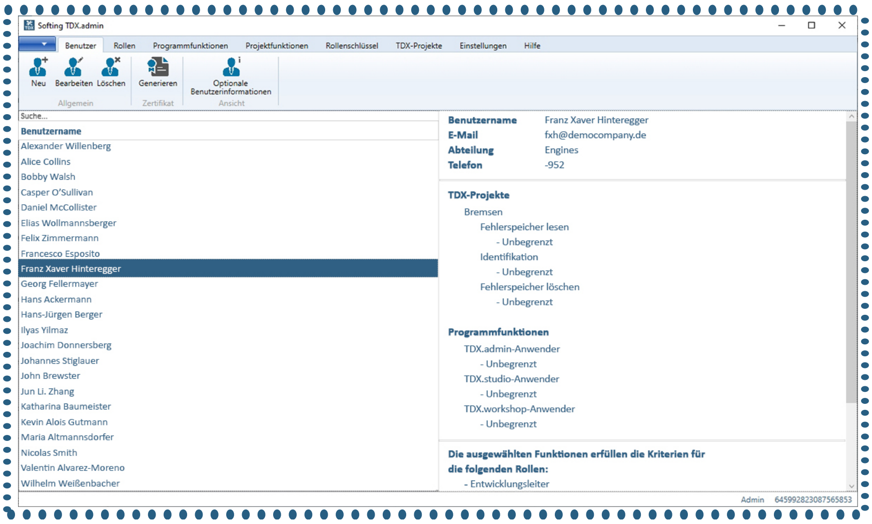


Figure 1: Concept for implementing a role-based user management © Softing Automotive

Originally published in German in the section “Measurement-Test-Diagnosis” of the technical magazine HANSERautomotive 07/2020, published by Carl Hanser, Munich, Germany



Benutzername

Alexander Willenberg
Alice Collins
Bobby Walsh
Casper O'Sullivan
Daniel McCollister
Elias Wollmannsberger
Felix Zimmermann
Francesco Esposito
Franz Xaver Hinteregger
Georg Fellermayer
Hans Ackermann
Hans-Jürgen Berger
Ilyas Yilmaz
Joachim Donnersberg
Johannes Stiglauer
John Brewster
Jun Li. Zhang
Katharina Baumeister
Kevin Alois Gutmann
Maria Altmannsdorfer
Nicolas Smith
Valentin Alvarez-Moreno
Wilhelm Weißenbacher

Benutzername	Franz Xaver Hinteregger
E-Mail	fxh@democompany.de
Abteilung	Engines
Telefon	-952

TDX-Projekte

- Bremsen
  - Fehlerspeicher lesen
    - Unbegrenzt
  - Identifikation
    - Unbegrenzt
  - Fehlerspeicher löschen
    - Unbegrenzt

Programmfunktionen

- TDX.admin-Anwender
  - Unbegrenzt
- TDX.studio-Anwender
  - Unbegrenzt
- TDX.workshop-Anwender
  - Unbegrenzt

Die ausgewählten Funktionen erfüllen die Kriterien für die folgenden Rollen:

- Entwicklungsleiter

Admin 645992823087565853

Figure 2: Editing of users with TDX.admin © Softing Automotive

Alongside the DESIGN component for creating a tester, the Softing TDX toolbox contains the independent MANAGEMENT component Softing TDX.admin for creating and managing user roles and corresponding user authorizations. The intuitive interface ensures minimal training and familiarization are needed. Clear icons, a workflow-optimized display and improved tool tips make the tool easier to use. Softing thus offers a consistent and integrative tool suite for holistic use in the after-sales area.

With Softing TDX.admin, new users are very easy to create and also edit in the RUDB. It is often the case that individual users are added, e.g. new employees join the company. A user name, e-mail contact and password, as a minimum, are defined and sent to the user when it comes to creating users from TDX.admin. The individual user information can be extended with further attributes, such as an ID or department affiliation. But it is not only the creation of users from TDX.admin that plays an important role. New users must also be able to register themselves from the tester software and the corresponding data transferred to the RUDB. This is done automatically with a notification to the administrator responsible that a previously unknown user from the field has now registered.

In the next step of the MANAGE workflow, defined roles are created alongside users with Softing TDX.admin. In this way, an already existing role model of a company can be optimally mapped to the tester software or supplemented. The design is completely flexible so that the models can be optimally integrated into existing company processes. The roles can also be easily adapted as required and applied to individual users or user groups.

The created roles are then stored with defined properties which control the usable functionality in the tester in a user-specific way. For example, the diagnostic function ECU update is active for one "repair shop foreman" and inactive for the "mechatronics engineer". Administratively, this is controlled intuitively via the assignment to the corresponding functions of a TDX project previously imported into Softing TDX.admin. A distinction is made between program functions and project functions for the available functions.

This has the advantage that not only diagnostic functions are provided with access rights, but also certain settings of the tester itself, such as access to server paths or other detailed settings that only an expert should operate. Another major advantage is that defined functions can also be delegated to specific users for a limited time.

Once the users, roles and functions are assigned, the model must be activated. This is done via user-specific certificates, which are automatically applied in the service tester and thus enable functionality. These certificates are always updated automatically for online testers. But they are also available offline which means that even testers that never go online or travel can be provided with certificates.

Authorization Management - a Necessity

The sometimes enormous number of repair shop testers in the field facilitates access to data and functions, both by authorized and unauthorized persons. And this can result in considerable damage – whether intentional or unintentional. To avoid this, a functioning and easily maintainable authorization management system is an absolute prerequisite nowadays for a complete after-sales solution. Softing TDX.admin is a tool which is simple to use and which makes it possible to implement a consistent diagnostic concept for an after-sales tester which can be used for years to come.

www.automotive.softing.com

Processed according to documents of
Softing Automotive, 85540 Haar

Originally published in German in the section "Measurement-Test-Diagnosis" of the technical magazine HANSERautomotive 07/2020, published by Carl Hanser, Munich, Germany