© Softing Automotive

DIAGNOSEKONZEPT FÜR AFTERSALES-TESTER

Ungleiche Zwillinge: Werkstattdiagnose und **Berechtigungsmanagement**

Die Anzahl einzelner Werkstatttester im Feld geht heute in die Zehntausende. Zusätzlich sind diese weltweit bei unterschiedlichen Anwendern mit unterschiedlichen Voraussetzungen und Berechtigungen im Einsatz. Unsachgemäße Handhabung kann dabei zu großen Schäden führen. Dieses Multi-User Szenario lässt sich nur mit einer bedarfsgerechten Zuordnung von Tester-Funktionen sowie durch eine zentrale Administration beherrschen.

Die meisten OEMs und Systemlieferanten unterhalten weltweit eine Vielzahl an Service-Werkstätten oder entsenden mobile Service-Techniker, um ihren Kunden sowohl schnelle als auch zielgerichtete Wartungs- und Reparaturleistungen anzubieten. Dies setzt die Bereitstellung eines effizienten Werkstatttesters voraus. Aufgrund der enormen Anzahl an Service-Testern im Feld, lassen sich jedoch die Verwendung und der Zugriff kaum kontrollieren. Insbesondere bei Fremdzugriff können beispielsweise Steuergeräte an Fahrzeugen falsch programmiert werden, was die Verkehrssicherheit beeinflussen und im schlimmsten Fall zu einem Unfall mit Personenschaden führen kann. Um schwerwiegende Folgen durch den mangelnden Schutz von sensiblen Daten sowie kritischen Funktionen zu vermeiden, bedarf es einer robusten Autorisierung am Werkstatttester. Dies hilft sowohl vor unbefugtem Zugriff zu schützen als auch befugten Nutzern, rechtebasierte Zugriffe zu ermöglichen. Die Vergabe einzelner Berechtigungen hat sich insbesondere bei einer großen Anzahl von Nutzern als zu komplex erwiesen. Kurz zu-

sammengefasst muss die Frage beantwortet werden: Wer darf wie auf welche Daten und Funktionen zugreifen?

Rollen als Schlüssel zum zentralen Berechtigungsmanagement

Wesentlich effizienter für die Umsetzung und vor allem die Pflege von Berechtigungen gestaltet sich eine rechte- und rollenbasierte Zugriffskontrolle. Beim sogenannten Role Based Acces Control (RBAC) werden den jeweiligen Mitarbeitern basierend auf Rollen, hinter denen wiederum Tester-Funktionen (z. B. Steuergeräte-Update) stecken, Berechtigungen zugewiesen. Oft sind Rollen in Unternehmen bereits durch die Aufbauorganisation definiert und können wiederverwendet werden. Die Vorteile von RBAC im Gegensatz zu anderen Ansätzen liegen in der einfacheren Verwaltung sowie den flexibleren Anpassungsmöglichkeiten ohne die Vorgabe von starren Regeln.

füllt sein. So muss ein Administrator möglichst einfach neue Rollen erstellen können, die wiederum mit intendierten Testerfunktionen hinterlegt sind. Meist ist dies ein initialer Aufwand, da einmal definierte Rollenmodelle in ihren Grundzügen gleichbleiben und selten geändert werden sollten. Die Zuordnung der Mitarbeiter zu den jeweiligen Rollen ist ebenfalls fester Bestandteil der Administration und bildet die Grundlage für die rechtebasierte Nutzung von Diagnosefunktionen im Service-Tester. Dabei ist es wichtig, dass mithilfe eines automatisierten Updateprozesses immer die aktuell gültigen Rollen und Rechte im Tester wirksam werden. Dabei sollten die zugewiesenen Rechte nicht nur verfügbar sein, wenn der Tester online ist. Insbesondere für mobile Service-Techniker, die oft an Orten ohne Internet-Zugriff arbeiten, ist die lokale Verfügbarkeit der nutzerspezifischen Berechtigungen absolut notwendig. Für eine Zuordnung der Nutzer zu den vorgesehenen Rollen, ger Dienst, der die Identitätszugriffe unternehmensweit steuert. Die manuelle Übertragung dieser Informationen ist mit großem Aufwand verbunden, was einen direkten Export in die RUDB sinnvoll macht.

Auch wenn das Rollenmodell sich über einen längeren Zeitraum nicht ändern sollte, kann es doch vorkommen, dass kurzfristig Anpassungen notwendig werden. Sei es durch wechselnde Projektzugehörigkeiten, Urlaubsvertretungen, einen Wechsel in der Abteilung oder eine höhere Erfahrungsstufe. Beispielsweise können durch den Nachweis spezieller, zertifizierter Schulungen die dafür notwendigen Funktionen freigeschaltet werden. Das gesamte Berechtigungsmanagement muss so flexibel sein, dass sich ad hoc auf Anpassungen reagieren lässt. Besonders die Möglichkeit einer zeitlichen Limitierung solcher kurzfristigen Änderungen bietet zusätzliche Freiheitsgrade. Nicht nur Anpassungen in der Rollenzuordnung müs-

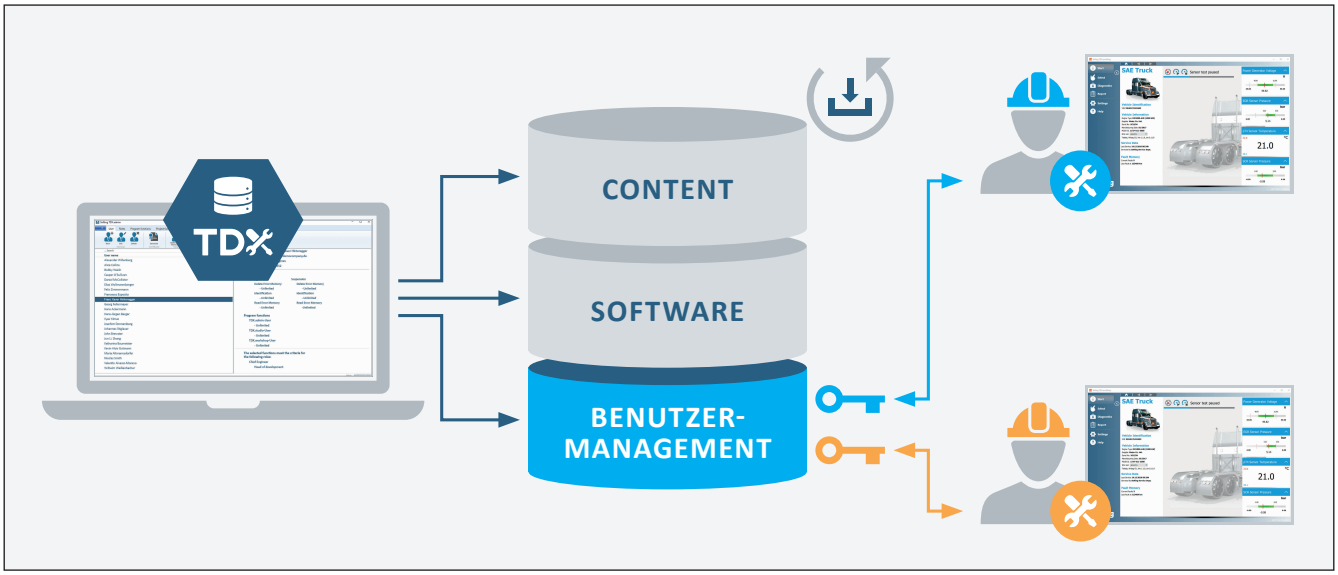

Bild 1: Konzept zur Umsetzung eines rollenbasierten Benutzermanagements. © Softing Automotive

Für die verantwortlichen Administratoren stehen dabei die zentrale Verwaltung und Steuerung der Rollen sowie des dazugehörigen Rollenmodells im Vordergrund. Die komplette Administration bis hin zur Veröffentlichung im Tester muss dabei im Hintergrund laufen. Eine zentrale Rollen- und Nutzerdatenbank (RUDB) bildet die Grundlage und ist absolute Voraussetzung, ohne die ein Berechtigungsmanagement nicht umsetzbar ist. Für die Administration selbst müssen bestimmte Anforderungen erfüllt sein. So muss ein Administrator möglichst einfach neue Rollen erstellen können, die wiederum mit intendierten Testerfunktionen hinterlegt sind. Meist ist dies ein initialer Aufwand, da einmal definierte Rollenmodelle in ihren Grundzügen gleichbleiben und selten geändert werden sollten. Die Zuordnung der Mitarbeiter zu den jeweiligen Rollen ist ebenfalls fester Bestandteil der Administration und bildet die Grundlage für die rechtebasierte Nutzung von Diagnosefunktionen im Service-Tester. Dabei ist es wichtig, dass mithilfe eines automatisierten Updateprozesses immer die aktuell gültigen Rollen und Rechte im Tester wirksam werden. Dabei sollten die zugewiesenen Rechte nicht nur verfügbar sein, wenn der Tester online ist. Insbesondere für mobile Service-Techniker, die oft an Orten ohne Internet-Zugriff arbeiten, ist die lokale Verfügbarkeit der nutzerspezifischen Berechtigungen absolut notwendig. Für eine Zuordnung der Nutzer zu den vorgesehenen Rollen, müssen diese auch in der RUDB nutzbar sein. Der Administrator muss mit dem Administrations-Tool möglichst schnell in der Lage sein, neben den Rollen auch die Nutzer mit eindeutigen Credentials, dem Benutzernamen und einem Passwort, anzulegen und diese den Mitarbeitern zu übermitteln. In vielen Unternehmen werden bereits entsprechende Mitarbeiter- bzw. Nutzerdatenbanken gepflegt, sodass die notwendigen Credentials bereits verfügbar sind. Active Directory ist beispielsweise ein gängiger Dienst, der die Identitätszugriffe unternehmensweit steuert. Die manuelle Übertragung dieser Informationen ist mit großem Aufwand verbunden, was einen direkten Export in die RUDB sinnvoll macht.

Auch wenn das Rollenmodell sich über einen längeren Zeitraum nicht ändern sollte, kann es doch vorkommen, dass kurzfristig Anpassungen notwendig werden. Sei es durch wechselnde Projektzugehörigkeiten, Urlaubsvertretungen, einen Wechsel in der Abteilung oder eine höhere Erfahrungsstufe. Beispielsweise können durch den Nachweis spezieller, zertifizierter Schulungen die dafür notwendigen Funktionen freigeschaltet werden. Das gesamte Berechtigungsmanagement muss so flexibel sein, dass sich ad hoc auf Anpassungen reagieren lässt. Besonders die Möglichkeit einer zeitlichen Limitierung solcher kurzfristigen Änderungen bietet zusätzliche Freiheitsgrade. Nicht nur Anpassungen in der Rollenzuordnung müssen einfach möglich sein, sondern auch nachträgliche Anpassungen der Rolle selbst.

Berechtigungen managen

Ein für den Aftersales-Tester obligatorisches Berechtigungsmanagement ist also möglichst schnell zu implementieren und vor allem einfach und zentral zu pflegen und aktuell zu halten. Um dies zu ermöglichen bietet Softing TDX entlang des dezidierten Workflows *DE-*

SIGN-MANAGE-WORK die ideale Toolunterstützung. Neben der *DESIGN*-Komponente zur Erstellung eines Testers beinhaltet der Softing TDX Werkzeugkasten die eigenständige *MANAGEMENT*-Komponente Softing TDX.admin zur Erstellung und Verwaltung von Benutzerrollen und entsprechenden Anwender-Berechtigungen. Die intuitive Oberfläche sorgt dabei für minimalen Einarbeitungsaufwand. Deutliche Icons, eine workflowoptimierte Darstellung sowie verbesserte Tool-Tipps erleichtern die Bedienung des Werkszeugs. Softing bietet damit eine konsistente und integrative Toolkette für die ganzheitliche Nutzung im Service-Bereich.

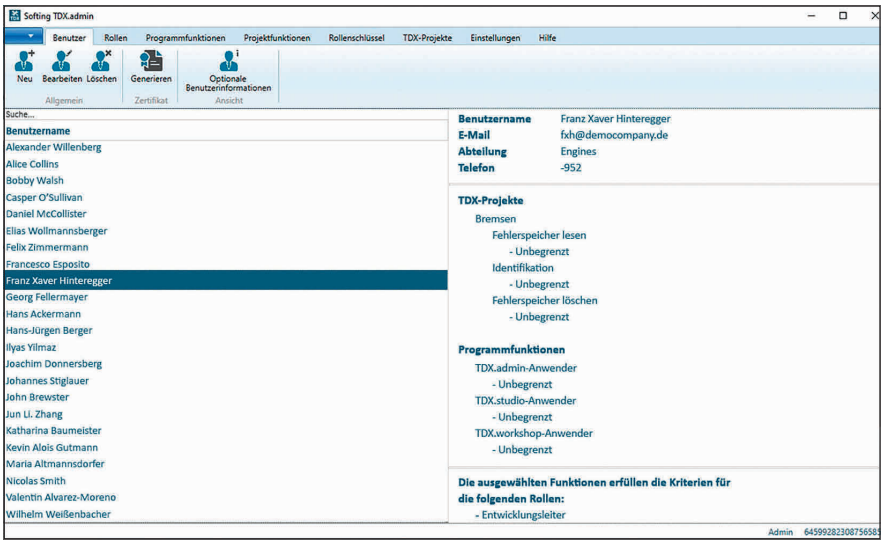

Bild 2: Editieren von Benutzern mit Softing TDX.admin. © Softing Automotive

Mit Softing TDX.admin lassen sich ganz einfach neue Nutzer in der RUDB anlegen und auch bearbeiten. Meist ist es so, dass einzelne Nutzer ergänzt werden, da z. B. neue Mitarbeiter dem Unternehmen beitreten. Für das Anlegen der Nutzer aus dem TDX.admin heraus werden mindestens Benutzernamen, E-Mail-Kontakt sowie das Passwort festgelegt und an den Nutzer versendet. Die individuelle Nutzerinformation ist um weitere Attribute wie einer ID oder der Abteilungszughörigkeit erweiterbar.

Aber nicht nur das Anlegen der Nutzer aus dem TDX.admin spielt eine wichtige Rolle. Ebenso müssen sich auch neue Nutzer aus der Tester-Software heraus registrieren können und die entsprechenden Daten in die RUDB übernommen werden. Dies erfolgt automatisiert mit einer Benachrichtigung des zuständigen Administrators, dass sich ein vorher nicht bekannter Nutzer aus dem Feld neu registriert hat.

Im nächsten Schritt des *MANAGE*-Workflows werden mit Softing TDX.admin neben den Nutzern auch definierte Rollen erstellt. Somit lässt sich ein bereits vorhandenes Rollenmodell eines Unternehmens optimal auf die Tester-Software abbilden oder ergänzen. Dabei ist man in der Gestaltung völlig flexibel, sodass sich die Modelle optimal in bestehende Unternehmensprozesse einfügen. Auch die Rollen lassen sich bei Bedarf einfach anpassen und auf einzelne Nutzer oder Nutzer-Gruppen anwenden. Die erstellten Rollen werden im Weiteren mit definierten Eigenschaften hinterlegt, welche die verwendbare Funktionalität im Tester nutzerspezifisch steuern. So ist z. B. die Diagnose-Funktion Steuergeräte-Update für den einen „Werkstattmeister" aktiv und für den „Mechatroniker" inaktiv. Administrativ wird dies intuitiv über die Zuordnung zu den entsprechenden Funktionen eines zuvor in Softing TDX.admin importierten TDX-Projektes gesteuert.

Bei den verfügbaren Funktionen wird zwischen Programmfunktionen und Projektfunktionen unterschieden. Das hat den Vorteil, dass nicht nur Diagnosefunktionen mit Zugriffsrechten versehen werden, sondern auch bestimmte Einstellungen des Testers selbst, wie z. B. der Zugriff auf Server-Pfade oder weitere Detaileinstellungen, die nur ein Experte bedienen sollte. Ein weiterer großer Vorteil ist, dass definierte Funktionen auch zeitlich limitiert an bestimmte Nutzer übertragen werden können.

Sind die Nutzer, Rollen und Funktionen zugeordnet, dann gilt es, das Modell aktiv zu schalten. Dies erfolgt über User-spezifische Zertifikate, die im Service-Tester automatisch angezogen werden und somit Funktionalität freischalten. Diese Zertifikate werden bei Online-Testern immer automatisch aktualisiert. Sie sind aber auch offline verfügbar, sodass auch Tester, die nie ans Netz gehen oder auf Reisen sind, mit Zertifikaten versorgt werden können.

Fazit

Die teils enorme Anzahl an Werkstatttestern im Feld erleichtert den Zugriff auf Daten und Funktionen, sowohl von berechtigten als auch von unberechtigten Personen. Hieraus können – gewollt oder ungewollt – enorme Schäden entstehen. Um dies zu vermeiden, gehört heutzutage ein funktionierendes und einfach wartbares Berechtigungsmanagement zur absoluten Voraussetzung für eine in sich vollständige Aftersales-Lösung. Mit Softing TDX.admin steht dafür ein komfortabel bedienbares Tool zur Verfügung, das es ermöglicht, ein konsistentes Diagnosekonzept für einen Aftersales-Tester umzusetzen und über Jahre hinweg zu verwenden. ■ (oe)

www.automotive.softing.com

Bearbeitet nach Unterlagen der Softing Automotive, 85540 Haar.