Data management system for protection systems

No strategy without secure data

Protection systems are crucial assets of critical infrastructures. Therefore, regular tests as well as systematic maintenance and documentation are urgently required. Special data management systems such as OMICRON's ADMO can provide meaningful support for these processes. In this way, not only the requirements of the standards regarding cyber security are met. Utilities thus create the basis for efficient and secure maintenance management.

Electric utilities worldwide are affected by the rapid advance of digital technology. The smart grid, digital substations, IEDs, the IEC 61850 standard and IT-OT convergence (information technology and operational technology systems) all create not only a seamless connection for the integration of protection, control, and communication equipment, but also new complexity.

Although the wide variety of data produced every day can make it considerably more difficult to gain an overview, it can also lead to better decision-making, provided the analyses are meaningfully and correctly performed. Modern analysis tools are better at managing and presenting comprehensive data, meaning that better use can be made of the data, and their true meaning revealed. In this new environment, utilties face various challenges, especially with regard to data management while installing, operating, and maintaining protection systems.

Operators of critical infrastructures

The digital revolution fundamentally changes the working environment for the technicians, engineers, and managers working in the electric utilities, particularly when it comes to maintaining protection systems.

In the past, a variety of different technical and IT solutions were used side-by-side without integration. Today, digitization provides reliable ways to greatly improve data management for maintaining protection systems. But this also produces new problems, such as data security (cyber security), that have to be resolved.

According to the new standards (IEC ISO 27001/271019), utilities are classified as "operators of critical in-

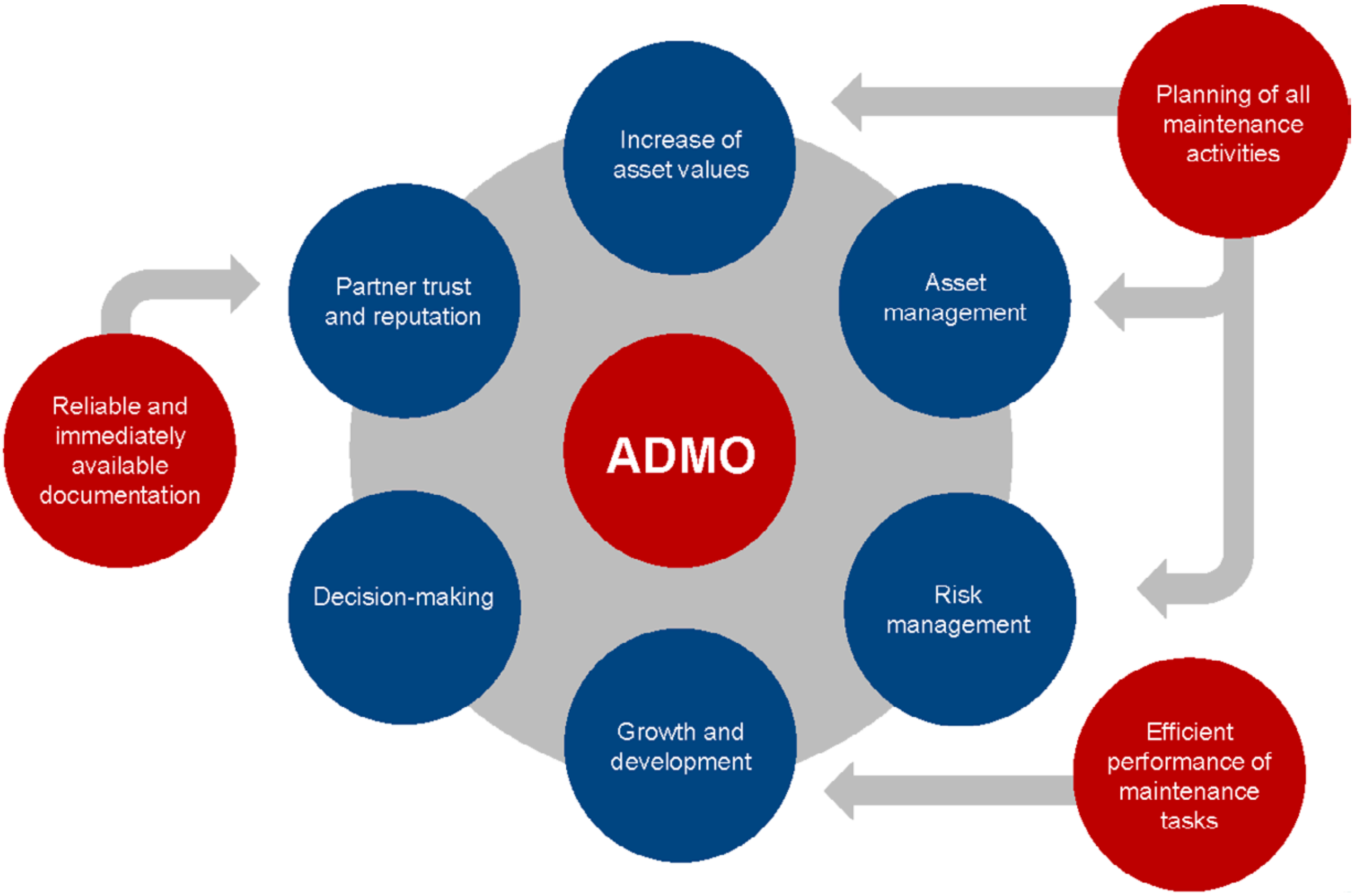

Planning of all maintenance activities
Increase of asset values
Partner trust and reputation
Asset management
Reliable and immediately available documentation
ADMO
Decision-making
Risk management
Growth and development
Efficient performance of maintenance tasks

Figure 1. *The advantages of an integrated data management system for the technical requirements of an electric utility - such as OMICRON's ADMO - are above all the better, faster, more secure and rule-compliant data management.*

frastructures". As a result they have to comply with special rules for their protection systems, as well as completing good, systematic, and traceable maintenance work and documentation.
Maintenance data therefore not only have to be stored, but also analyzed, and used for enhancements of the protection system. The data contain a wealth of information which can be used by managers to better assess and understand the condition of the systems, and which is also important the planning of the future infrastructure. It is then possible to derive more effective procedures for the necessary work and investment, as well as greatly simplifying decision-making processes at management level **(Figure 1)**.

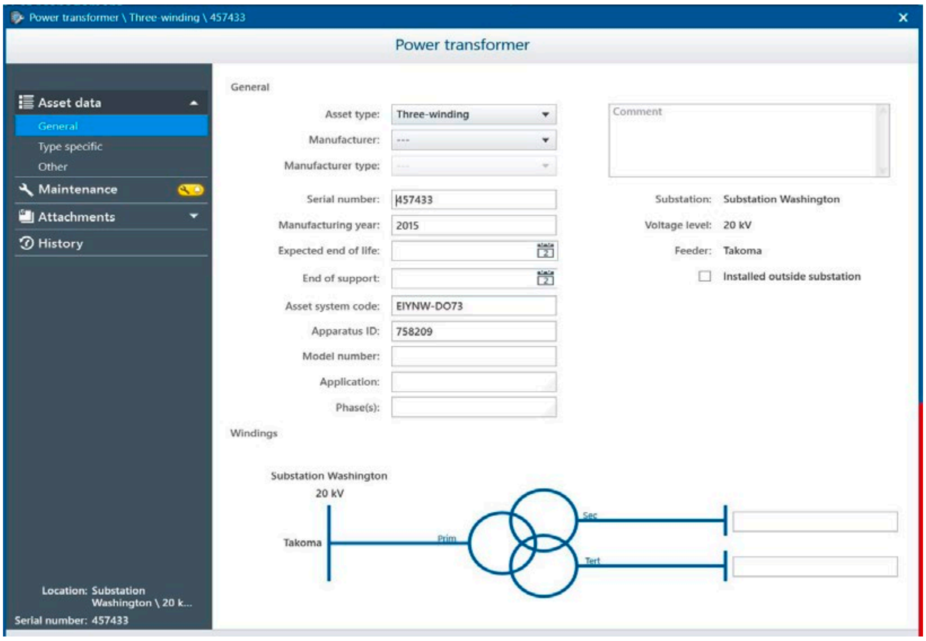
The data of the protection system

The role of the protection system is crucial for ensuring a secure energy supply. Regular testing and systematic maintenance and documentation are therefore absolutely essential. It also requires a secure and ergonomic management of large amounts of information or data, as illustrated by the typical selection below:

- Operating parameters
- Relay settings
- Test data
- Test sets
- Maintenance plans
- Network disturbance data
- Tripping schedules
- Manuals
- Wiring diagrams
- Building plans
- Documentation
- Data analysis

However, it is evident that despite all the efforts to go digital worldwide, many utilities still work with spreadsheet programs, paper lists, and the simplest of uncoordinated databases for the maintenance management of their protection systems. This makes it far more difficult to manage the diversity of data, and is actually no longer in compliance with the latest standards.

In contrast, a modern solution for maintenance and repair work in protection systems all these data are stored, along with the entire network architecture and the accompanying assets, on a central server (Figure 2). These data are then available to authorized team members. This centralized information can be analyzed and organized in every conceivable way, to provide an excellent insight into the different aspects of the protection system. Such data therefore are the foundation for condition-based and targeted maintenance planning, as well as for strategic investment decisions.



Power transformer \ Three-winding \ 457433

Power transformer

General

Asset type: Three-winding
Manufacturer: ---
Manufacturer type: ---
Serial number: 457433
Manufacturing year: 2015
Expected end of life:
End of support:
Asset system code: EIYNW-DO73
Apparatus ID: 758209
Model number:
Application:
Phase(s):

Comment

Substation: Substation Washington
Voltage level: 20 kV
Feeder: Takoma
☐ Installed outside substation

Location: Substation Washington \ 20 k...
Serial number: 457433

Figure 2. *A modern data management system not only manages the original data of the individual assets, but also the associated technical data and the entire network structure on a central server.*

Why isn't the ERP system enough?

The question that keeps arising is "why is specialized software necessary for the maintenance management of protection systems when one of the largest known ERP systems is already installed?"

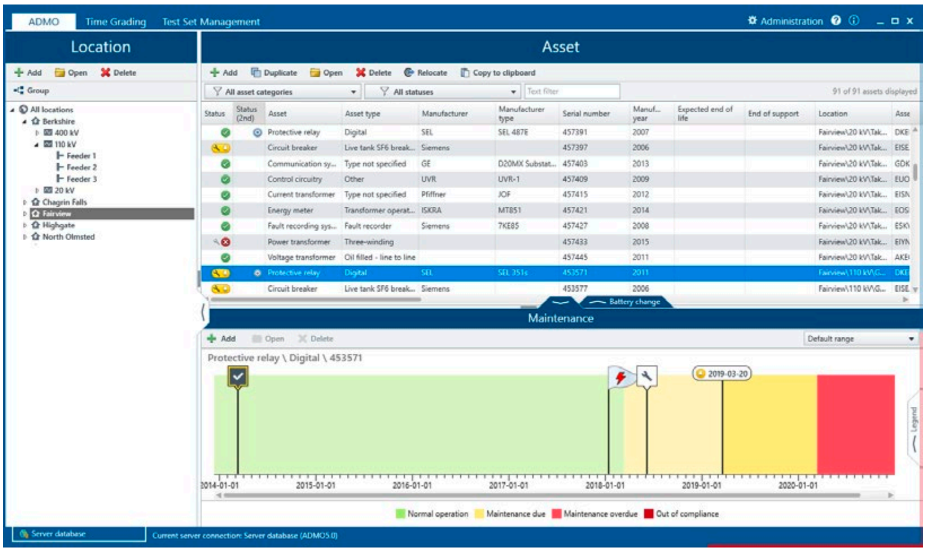
The necessary business, operational, and organizational data about the assets and the network are available in a conventional ERP system, of course, as the relevant processes have been created. But to work with protection systems, the technicians and engineers need specialized technical data, which the large systems are not designed to manage. In addition to this, on-site testing and maintenance tasks are performed with laptops, and standard ERP systems do not have the requisite functionality for this.

It is certainly true that larger utilities frequently use modules from their ERP system (such as SAP or Maximo). However, these modules typically only allow the management of basic plant data and do not offer adaptable solutions for protection systems. From the network technology aspect, the ERP system is also located in the office IT area, the technical applications for the infrastructure of a utility on the other hand should be in a separate and secure area, in order to meet cyber security requirements. All this makes the day-to-day work of the technicians and engineers responsible for the protection system more difficult. It is therefore not possible to devise an integrated and adaptable software solution for the technical requirements of a utility in this way, and even if it were possible, it would not be practicable.

To work meaningfully with the data of a protection system, it is important to first group them into main categories, something that is not offered by ERP systems. The following categories are useful:

- Plant data
- Test data
- Relay settings
- Maintenance data
- Test equipment data

A good solution for data management should recognize these categories, be user-friendly yet powerful,



Status	Status (2nd)	Asset	Asset type	Manufacturer	Manufacturer type	Serial number	Manuf... year	Expected end of life	End of support	Location	Asse
✓	◉	Protective relay	Digital	SEL	SEL 487E	457391	2007			Fairview\20 kV\Tak...	DKE
🔧		Circuit breaker	Live tank SF6 break...	Siemens		457397	2006			Fairview\20 kV\Tak...	EISE
✓		Communication sy...	Type not specified	GE	D20MX Substat...	457403	2013			Fairview\20 kV\Tak...	GDK
✓		Control circuitry	Other	UVR	UVR-1	457409	2009			Fairview\20 kV\Tak...	EUO
✓		Current transformer	Type not specified	Pfiffner	JOF	457415	2012			Fairview\20 kV\Tak...	EISN
✓		Energy meter	Transformer operat...	ISKRA	MT851	457421	2014			Fairview\20 kV\Tak...	EOS
✓		Fault recording sys...	Fault recorder	Siemens	7KE85	457427	2008			Fairview\20 kV\Tak...	ESK
✗		Power transformer	Three-winding			457433	2015			Fairview\20 kV\Tak...	EIYN
✓		Voltage transformer	Oil filled - line to line			457445	2011			Fairview\20 kV\Tak...	AKE
🔧	◉	Protective relay	Digital	SEL	SEL 351s	453571	2011			Fairview\110 kV\G...	DKE
🔧		Circuit breaker	Live tank SF6 break...	Siemens		453577	2006			Fairview\110 kV\G...	EISE

Figure 3. *The meaningful organization and clear presentation of the data stored in the data management system is an important basis for the efficient planning of maintenance tasks.*

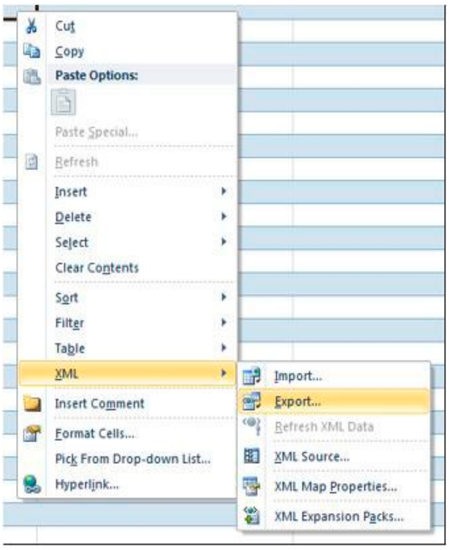


Figure 5. *An export function for different standard formats is available, so that data can also be used outside the system.*

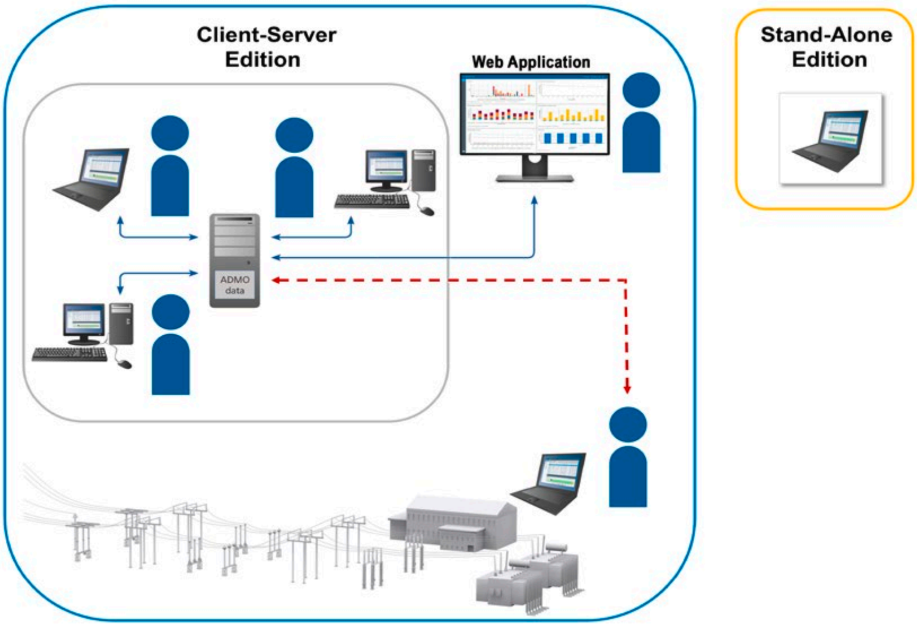


Figure 4. *Different options are available for different areas of application and requirements: a stand-alone solution or a client-server version that allows offline access to the data and data analysis via a web application.*

but also meet the specific requirements of operating and maintaining protection systems.

Protected data exchange with the ERP system then ensures that the plant data present in these categories are always up to date. A specialized database like this provides the user with the following functionalities, for example:

- On-site testing both online an offline
- Management of the test data
- Management of the relay settings
- Asset history and comparison
- Maintenance management
- Protection system analysis

System for maintaining protection systems

A simple design and simple and intuitive operation are the basic requirements for a data management system that is used to maintain protection systems. Its structure should reflect the requirements for performing test and maintenance tasks.

Three primary data areas are necessary to organize the system data of a protection system:

Location

This reflects the hierarchical structure of the network. The substations are grouped according to their geographical location, the voltage levels are defined together with their feeders. There is also an overview of all the associated assets at this location.

Asset

All the assets are described here with their technical data. Beside the relays, the protection system contains a multitude of additional assets. Each individual asset belongs to a predefined category and contains quite specific data for the particular asset type. As highly specialized assets are used in the substations, it makes sense to work with different categories. A user-defined category also provides the opportunity to describe the entire system as detailed as possible.

Maintenance

Timetables and the timeline associated with each asset are shown at this level. In this area, the dates for commissioning, maintenance, as well as for other events and necessary work are documented. Assets with pending maintenance tasks are highlighted. This area also answers questions such as:

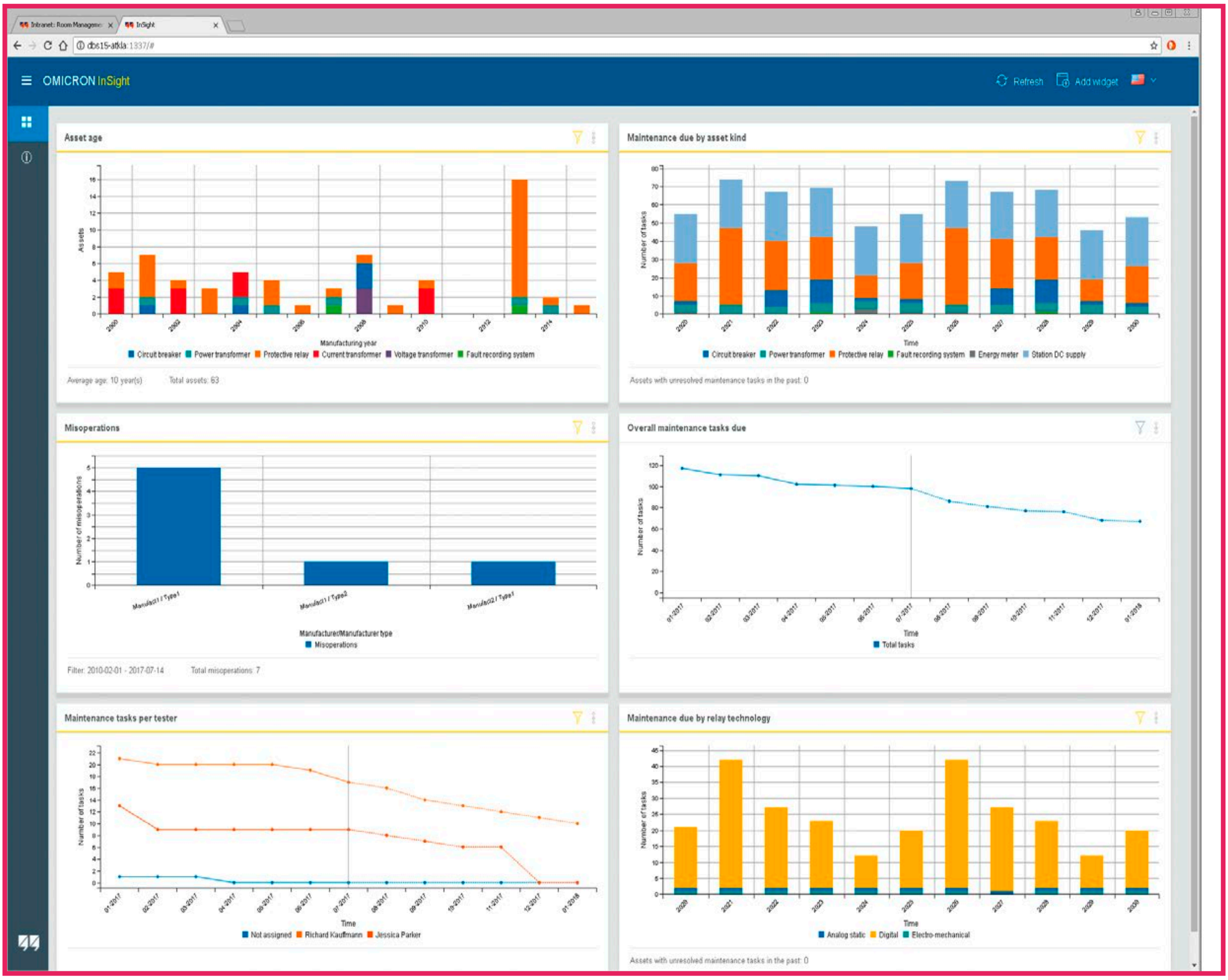


Figure 6. *Using filters, the asset data can be extracted, processed, analyzed and visualized according to various criteria.*

- When was the last time maintenance was performed?
- When is the next maintenance scheduled?
- Where are the test reports for the individual assets?
- What is the current test and maintenance status of the whole system?
- Are all the requisite test item plates and test plans available on site?

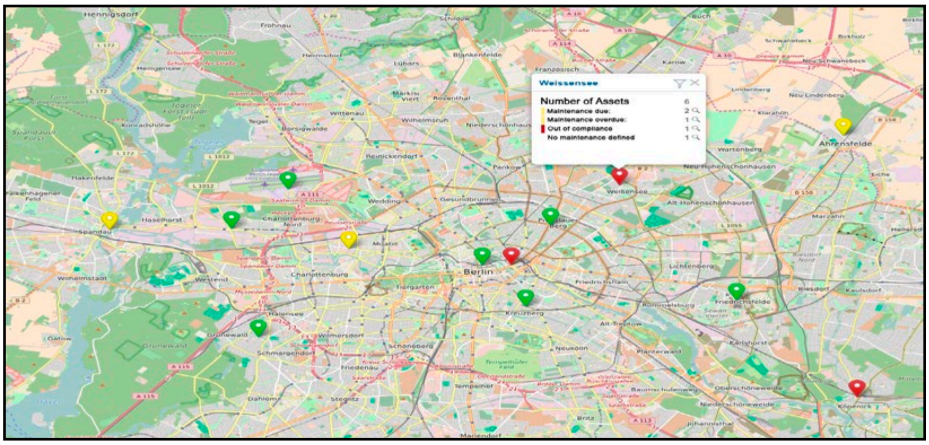
Figure 3 shows a typical asset and maintenance overview. Assets in a normal operating state are marked in green. The yellow symbol at circuit breaker 457397, protective relay 453571 and circuit breaker 453577 shows that the maintenance for these assets is due. The red x-symbol at power transformer 457433 means that it does not meet the recquired specifications and therefore, it is out of compliance. In the lower third of the window the timeline for the protective relay is shown, where the maintenance history can be tracked and the upcoming ones are shown at the same time. In this example the due date for the maintenance of this asset is in Q2/2019.

An integrated approach in accordance with the principle described above ensures that all the information is always up to date. Test and maintenance activities can be planned and managed centrally. Depending on their user rights, all users always have fast and easy access to the data which are important for them, and which they are allowed to work with. The system provides an overview of the maintenance status of the entire protection system, as well as for each individual component.

Client/Server structure

A standalone version running on laptops is available for service providers and smaller utilities. This means that a single user manages all the maintenance processes. In most cases, however, several people work in the maintenance and commissioning departments of protection technology, constantly alternating between the office and field work. They all need access to the data that are important for their tasks. Here the system is usually designed as a multi-user solution with a client/server structure that allows parallel access and synchronous working from several locations. Each user has a personal ID with which to establish a secure connection to the central server, in order to obtain exclusive access to the data for which they are approved (**Figure 4**).

Another important aspect is the exchange of data with the ERP or other systems. Data are imported and exported via secure data hubs.



Weissensee	
Number of Assets	6
🟨 Maintenance due:	2
🟨 Maintenance overdue:	1
🟥 Out of compliance	1
No maintenance defined	1

Figure 7. *The map function displays the geographical location of the substations together with an overview of the maintenance status of the equipment used there.*

They can be exported to the format of a spreadsheet program, to prepare individual reports or specific analyses (**Figure 5**).

Unrestricted offline use in the substation

It is often not possible to access the network in a substation, and it should actually not be allowed for the technical notebooks for reasons of cyber security. To enable the tester to work on site, an offline copy of the database is synchronized to the laptop that then contains the necessary instructions for the particular test. This includes test plans prepared in the office, relay settings, manuals, wiring diagrams, and other test data.

During the test, all the test results are saved in the offline database and can then be synchronized with the server again afterwards in the office, where they can be analyzed or further processed. This approach provides a uniform and consistent working environment that keeps the data constantly up to date for all users, both in the office and on site.

Possible analyses

As the protection system data are recorded in full and continually updated, they can be evaluated and visualized accordingly. In order not to overload the specialized software with functions and complexity, the analysis part is implemented in a web-based application. The data can therefore be extracted from the database in every conceivable way and then further processed, analyzed, and visualized. Filters enable the focus to be placed on particularly interesting areas, such as locations, voltage levels, installation types, injections, or certain time frames (**Figure 6**).

The map function (**Figure 7**) shows the geographical location of the substations in a certain region, as well as the maintenance status of each one. Colored markings highlight those substations requiring special attention. For example, yellow indicates that maintenance is currently due, red that maintenance is already overdue. Widgets and filters like these can be saved and reused, so that standard methods of analysis are also readily available to other users, without giving them access to the actual data.

This turns the database into an extremely powerful tool for protection system management. The tester and planner use it to optimize their maintenance work, and to receive support in the life cycle management and the allocation of capital for assets. This also improves staff planning.

A software system for maintenance management is also one of the best ways to successfully pass an audit in accordance with the latest standards and to qualify for the related full certificate of conformity.

Cyber security - the "secure data island"

IT security specifications according to IEC ISO 27001/271019 standards stipulate that the systems of critical infrastructures must be set up in such a way that the office IT environment and the IT environment with the technical data are kept strictly separate. This means that the maintenance data of the protection systems, as well as those for the technical environment, must come neither into direct nor unprotected contact with the data of the office environment. The standards also demand the use of a systematic maintenance tool which guarantees the traceability of tests and maintenance work and provides documentation that is protected against manipulation.

A "secure data island" could well be a good metaphor for the stipulated approach. A vivid example from the "real" world would be the artificial island "Jumeirah Palm Island" off Dubai in the United Arab Emirates, which uses similar structures (Figure 8). The island is surrounded by a protective ring to shield it from the unpredictability of the open sea. The only way to get to the island from the mainland is via a road with a drawbridge that controls access. All traffic is monitored and must request and obtain approval before being allowed to pass. This controlled access acts as a secure interface for all inward and outward movements from other environments. The island itself has a spine that integrates all the central services. Fanning out from this are the "palm leaves" with plots of land for private use.

Transpose this to data management and the following picture emerges. Information technology protects the secure data island in every direction, so there is no possible way to access it apart from entering the spine that only grants access to authorized persons or data. This spine integrates all the central services, such as the server with the network data, and the technical and maintenance data. The "palm leaves" correspond to the individual parts of the network, i.e. locations, substations, assets, and all the work tools of the protection engineers. In other words, all those areas where technical and maintenance work is carried out.
Data can only be integrated and exchanged via the secure data interface. The requisite data are imported from the ERP system into the maintenance system, and in return,

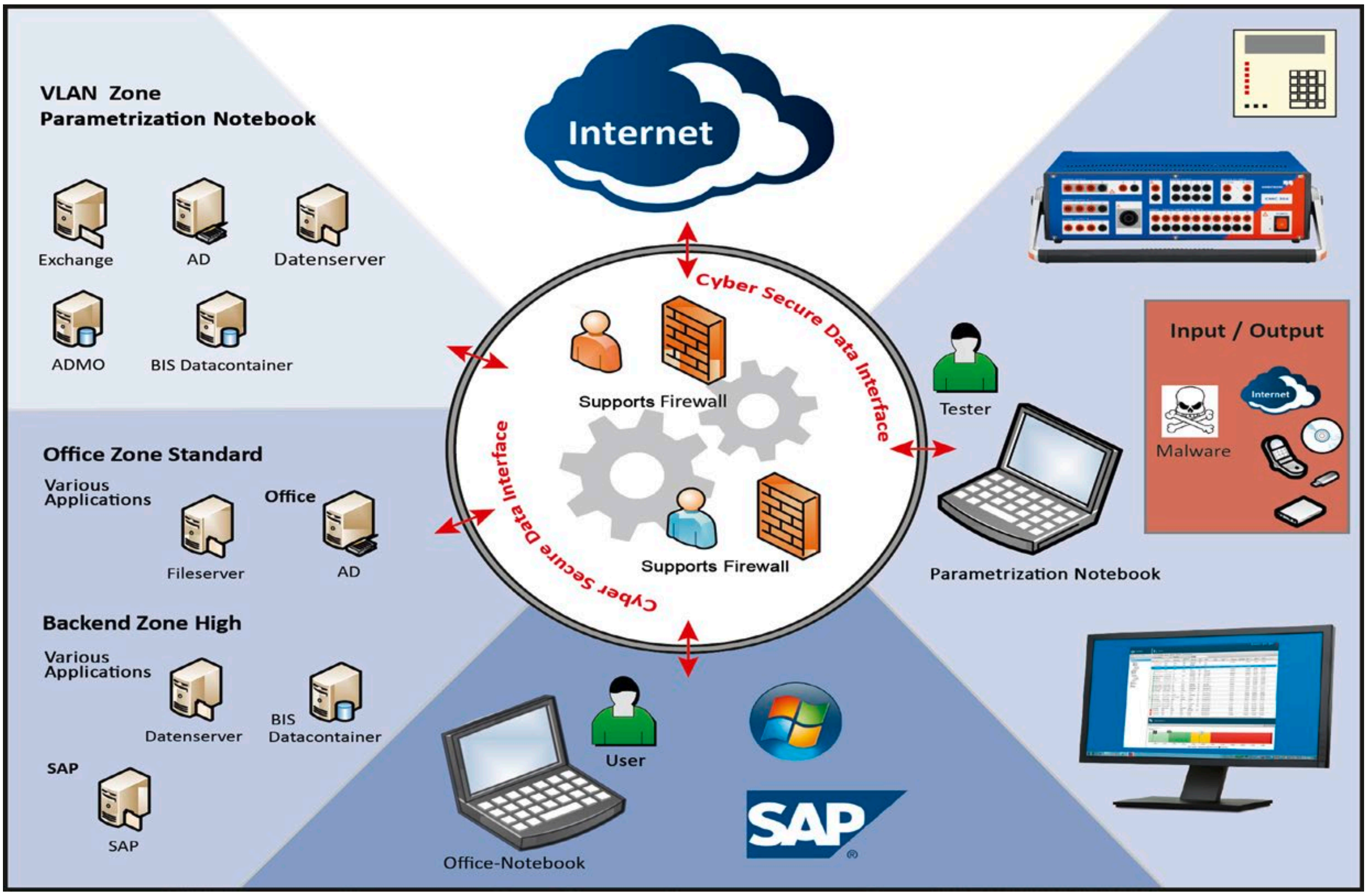


Figure 8. *The sensible structure of a data management system enables maximum security, as required by law - both with regard to the permanent access of authorized persons and with regard to the prevention of unauthorized access.*

the maintenance and status data from the technical environment are exported back into the ERP system. The company-wide ERP system and a specialized database for technical experts are therefore not mutually exclusive, instead they rather complement each other in implementing maintenance management that is as efficient and secure as possible (**Figure 8**).

The database of the maintenance system is located on a central server in the "technical zone", that is, outside the normal office IT environment, from which it is also clearly separated. Among IT experts, an area like this is called Demilitarized Zone (DMZ), as it is cut off from outside access and normal data traffic. All data relevant to the protection system belong in this area, from the operating data, to the relay settings, to the test equipment, and the test results.
User account management controls the respective access rights of testers, planners, and managers, and a conflict management solution ensures that access runs smoothly. This also means compliance with the security specifications of the standards that demand traceability for work completed and data exchanged.

Conclusion

Protection systems play a crucial role in the reliability of electric power systems. But it is often extremely difficult to retain an overview of the required maintenance intervals and dates, to keep the many assets of the protection system in good condition, to document tests and their results, or to complete maintenance work on time. The use of traditional manual systems with spreadsheets and paper documentation is prone to errors. In the wake of modernization and with the possibilities of modern technology, it is useful to replace these processes with an integrated software solution.
This provides to the utilities as "operators of critical infrastructures", the ability to meet the requirements of the standards and comply with the demands of cyber security. All teams involved in the maintenance of a system are then always up to date, and can work together in a multistage process more efficiently. This leads to more efficient and reliable results in the maintenance management and analysis, and simplifies decision-making processes for the further development of the protection systems.

Dipl.Ing. **Stefan Schlichting**,
Business Development
Data Management,
Omicron electronics GmbH,
Klaus

Dipl.Ing. **Klaus Jotz**,
Marketing Communications,
Omicron electronics GmbH,
Klaus

>> stefan.schlichting@omicronenergy.com
>> klaus.jotz@omicronenergy.com

>> www.omicronenergy.com