Rent a Brain
Intelligent ICT

TESTING OF SCADA DMS

6/28/2013

TESTING OF SCADA DISTRIBUTION MANAGEMENT SYSTEMS, A NECESSARY FIRST STEP IN REALIZING DEPENDABLE SMART GRIDS

TESTING OF SCADA DISTRIBUTION MANAGEMENT SYSTEMS, A NECESSARY FIRST STEP IN REALIZING DEPENDABLE SMART GRIDS

Future power grids need to be more secure and adaptive than ever before. Consumer demands and government legislation increase the need for extremely reliable power supply. Together with the future abundance of alternative energy sources this fuels the need for flexible, telemetered, remotely operated power grids. In the near future these grids will be software controlled rather than by human intervention.

A necessary first step in this development is implementing Distribution Management Systems (DMS) for Medium Voltage Grids (MVG).

This article is based on the experience of testing the implementation of DMS systems for two Dutch grid operators. These projects consisted in broad terms of:

- Implementation of a DMS system, one from Alstom and one from Siemens
- In one case implementation of an interface between the Asset Management System (Smalllworld) and the new DMS systems
- In the other case implementation of an interface between the Asset Management System (Smalllworld) and middleware, implementation of a new GIS system, an interface between the middleware and the GIS system (ESRI) and an interface between the middleware and the DMS system.
- Phasing out of paper diagrams of the medium voltage grids made in AutoCAD.

Generally speaking most pre DMS grid companies will have their grid related applications organized more or less as shown here (Figure 1). The Asset Management System and the Diagrams on paper in AutoCAD (or similar program) are connected to the Office LAN (OA). And EMS and SCADA are part of the technical network (TA). These two networks are, as a security measure, physically completely separated.

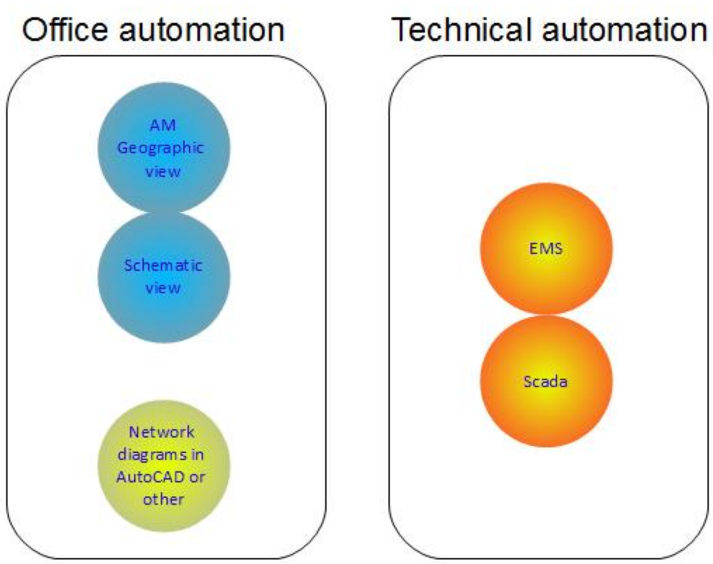

Figure 1

AM: Asset Management System
EMS: Energy Management System
SCADA: Supervisory Control and Data Acquisition

In the case of a DMS system the 2 separate networks (OA and TA) have to be able to communicate. And the paper network diagrams in AutoCAD or any other program will be replaced by electronic diagrams in DMS and in one case in ArcGIS.

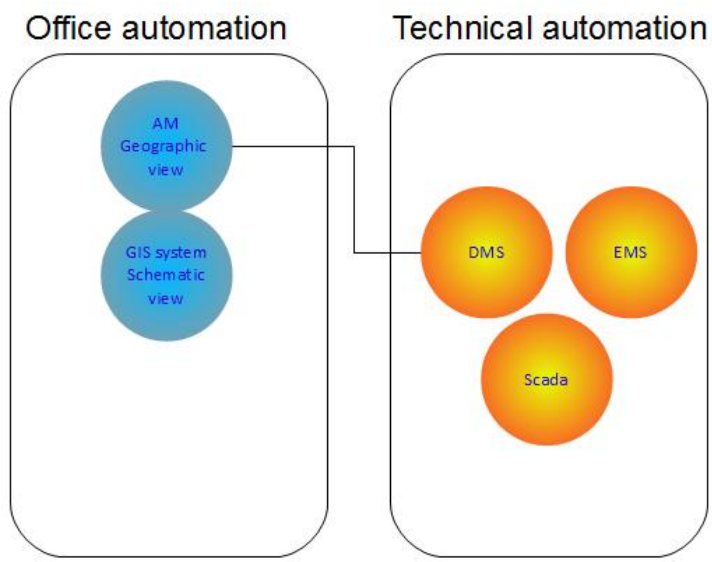

Figure 2
AM: Asset Management System
EMS: Energy Management System
DMS: Distribution Management System
SCADA: Supervisory Control and Data Acquisition

What sets testing of DMS systems apart? - The testing of DMS systems within the surrounding IT architecture has a number of aspects that need special attention. These are:

- Minimal outage time
- Fail over and recovery testing
- Usually poor data quality in the Asset Management Systems
- Continuous shifts of grid operators
- The Asset management systems require trained employees for input of the test cases
- No Test environment for grid components
- Big impact on the organization
- Security
- Performance

Test approach

Minimal outage time - Because of the mentioned increased need for reliability and flexibility and minimum outage time it is of the utmost importance that the DMS system together with interfacing asset management, GIS, EMS, and SCADA systems have near to zero defects over the entire chains of systems and business processes. This calls for extremely rigorous Factory Acceptance Testing) (FAT), Site Acceptance Testing (SAT), System Testing (ST), System Integration Testing (SIT), User Acceptance Testing (UAT), Process Cycle Testing (PCT), End to End Testing (ETE) and Failover and Recovery Testing (FRT).
But even then it is hard if not impossible to get to zero defects, as we have seen from, among others, an exploding Arianne rocket and malfunctioning Therac-25 Medical Accelerator. It's possible however to make sure the DMS serves the business requirements and has a technical quality level that will make it function without problems at a reasonable price. In order to select a DMS that meets the need of the business user an extensive set of Business Requirements (BR's) should be developed. To make sure this set is relevant to all stakeholders, that is business users, functional application- and system management, business management, internal accounting department etc. should all have a delegate in the team that develops the BR's. Once developed the BR's will be used not only for the selection process of the DMS but as a test basis for the User Acceptance Test (UAT) as well. And since the test team needs Business Requirements that are specific enough to be able to test them, a delegate from the test team should ideally be part of the team that develops the BR's. One of the main BR's will be the maximum allowed outage time. This should be tested with an extensive set of real life scenario's proving outages can be solved within agreed on time limits.

Fail over and recovery testing - Another aspect of the zero defects and as part of this 100% uptime is that all major components in the AM-EMS-DMS-SCADA configuration have to be completely mirrored, both logically and geographically. This means that data has to be mirrored on a constant basis over several environments. This has to be verified as part of the test. Fail over and recovery testing tests the readiness of the disaster recovery environment. This means the tests must prove that at any given time it is possible to switch to the disaster recovery environment instantaneously, or at least within a time frame deemed sufficient by the business. There are usually two types of recovery environments, on site (environment B) and on a geographically separate location (environment C and D). Which suggest at least four tests, from the test environment (A) to, B, C to D and D back to A. But it might be necessary to test from B back to A and from C back to A as well, or any other transition. An analysis has to be made which transitions exactly have to be tested. And, as important, which manual and/or automated recovery processes have to be tested. This analysis should be made with all relevant business stakeholders and based on the appropriate business requirements.

Poor data quality in Asset Management (AM) System - The extent to which this is true will vary per grid operator. In general the data quality will be poorer than desired because of two reasons:

1. Traditionally grid companies didn't have much need for automating asset management and grids. This means computerization of the technical infrastructure started quite recently. And there wasn't the need for data quality on the level that a DMS system requires.
2. There has been a stream of mergers and acquisitions between grid companies in the last 10 to 20 years. This also meant merging of data that used to be handled and collected by different companies with their different asset management systems and different ways of modeling network and network objects.

The usually poor data quality in the asset management systems mentioned above can hamper testing in two ways. Firstly it can make execution of certain test cases impossible because inconsistent data will be rejected by the interface checking consistency of the data. Or it will pass through the interface but will be rejected by the DMS system. In case the inconsistent data it is accepted by DMS this can result in errors in the DMS. Secondly it will be hard to distinguish between errors stemming from functionality and errors stemming from inconsistent data. Making the analysis and fixing of defects time consuming.
This can be avoided in two ways. Both starting with the same action. Development of a set of data consistency rules to which the data entry within the AM system has to adhere. These data consistency rules should be based on the DMS data structure and translated to the AM System data entry GUI's. The best way to implement these rules is of course validation of the data entry in the AM system and data cleaning of the data already in the system according to these rules. Since the input validation on the AM system almost certainly has to be changed or added to be compliant with the established rules this means development in the AM system. In both studied cases this was outside the scope of the projects and too big to add to the project. Leaving two solutions, the first solution is to model a new part of the network according to the developed set of consistency rules. The second method is to take a certain part of the network and change the data according to the developed rules. Which is the better solution will depend on the actual situation. In both projects we chose to use the second solution.

Continuous shifts of grid operators - The grid operators that have to participate in the Site Acceptance, User Acceptance Test and Process Cycle Testing work in continuous shifts which make it necessary to plan weeks to months in advance to have them planned out of their shifts and into the test project. This also means that delays in project execution will mean re-planning of the grid operators and will again cost weeks to months. This makes it important to avoid delays at any cost.

Data entry in AM system - Correct input in the AM system requires a great deal of experience. This makes it important that end users from AM data entry department are available from the start of the System Intergration Test (SIT) until the end of the project. Since the input, without input validation in the AM system, has to comply with the newly developed consistency rules Technical Application Managers of DMS have to check the input as well.
As with all tests the easiest way to ensure a rapid execution of the tests is having all participants together in one room. In case of DMS this presents some specific challenges because of the variety and number of participants, AM data entry employees, a technical application manager of the AM system, of DMS and of the middleware/interface, a business representative, testers, grid operators and the test manager, all are needed, preferably on a fulltime basis for the duration of the project.
Together with the continuous shifts of the grid operator this calls for excellent planning, on schedule project and test execution and timely preparation. In one case on the other hand the DMS vendor's documentation didn't include the data model which meant the data model had to be re-engineered by trial and error and validations for input in the AM system were unknown. Along with some other uncertainties this may in certain cases suggest an Agile approach at least up to the User Acceptance testing and a more traditional linear

methodology during UAT, PAT and implementation.

No Test environment for grid components – Although the grid itself is an integral part of the test scope it's not feasible to have a test version of the grid or even of a scaled down test version of the grid. In fact even a test version of a secondary station is a rarity which means that an important part of the scope, the operation of the grid and collecting data from the grid, can only be tested implicitly
What makes this an important issue is that you want to be absolutely certain that DMS is addressing the right telemetered components in the field. That is to say that if on the DMS screen you are switching circuit breaker X in secondary station Y in the physical world circuit breaker X in secondary station Y should be switched and not for instance circuit breaker Z in secondary station W.
Having no test version of the grid presents us with a challenge. There are several options to cope with this, either connect to components in the real grid, use a test Remote Terminal Unit (RTU) or have a test version of a secondary station. Either of these solutions have specific advantages and disadvantages. In general the best solution is connecting to the real grid. But this has the disadvantage that only certain statuses can be tested. An open circuit breaker, for instance, can be tested to receive an "open" command. But a "close" command can only be ordered if there is no impact on the state of the grid, and there probably will be an impact. This makes it impossible to execute the "close" command. One big advantage of this approach on the other hand is that it tests if all telemetered grid components are linked correctly to the DMS objects, even though not all possible states can be tested. If there is a test station testing on the telemetered components of the test station will make sure all possible commands can be executed. But is limited to the components and there possible states in the test station. In combination with addressing components in the real grid this would provide the maximum test coverage. If there is no test station, which is likely, a good and cost effective option is testing with a test RTU, preferably one of every type used in the grid in combination with addressing the real grid components.

Big impact on the organization - Large parts of the organization are affected by the introduction of a DMS system. This is caused by the fact that information without a DMS can be gathered during implementation of new grid components or restoration of existing grid components. Whereas in the case of DMS a bigger part of the data has to be available beforehand. And by the fact that updating of paper network diagrams is done in a much different way than updating the DMS diagrams. To give an example, in one of the cases an analysis was made of what data was needed throughout the entire processes of altering existing grid components, building new ones and taking out of service existing ones. Be it entire stations, transformers, circuit breakers or other components. Throughout these processes around 200 different parts of information had to be gathered. With DMS in place 80% of this data had to be available beforehand. Which means redesign of processes affecting several departments within the organization. Therefore the Process Cycle Test and End to End test need to be sufficiently robust.

Security – The interfacing of the OA and TA is necessary to get the full advantage of installing a DMS. It is however also a serious breach in security. There are several ways around this such as a proxy server and demilitarized zone between TA and OA where data from TA is available in OA through the proxy server but data in TA is not directly accessible from OA. Whichever solution is chosen, it should be tested extremely well for 2 reasons. The first obviously is security itself. The second is the acceptance of the interfacing of OA and TA by the application managers of TA. Who are naturally opposed to the idea of unlocking the formerly completely separated TA domain to the outside world. For these reasons a third party specialized in security and penetration testing should design and execute the tests.

Performance – The relatively small number of consecutive users for the DMS system will usually not lead to poor performance. The interface between the AM system and DMS may very well face performance problems. This will depend on the number of daily mutations that have to go through the interface. In both projects we saw that the number of mutations of normal day to day operation would fit in the nightly available time window for the ETL (Extraction, Transformation and Load) process between the AM system and DMS. In a couple of cases bulk mutations were triggered by for instance renaming of a transformer that was present in most parts of the grid. These bulk mutations couldn't be handled in the available time window and led to a redesign of the ETL process.

Some other considerations

Vendor selection - Most power grid companies will have an EMS system with a Scada interface towards the grid. In theory it will be possible to have an EMS Scada system from vendor X and a DMS Scada system from vendor Y. In practice this is extremely inadvisable since there most certainly will be interfacing problems between the two. This presents a problem because of the implicit vendor lock in. This can only be avoided by including in the selection process of the new system the explicit option for both a new EMS and DMS. Although EMS systems have more or less the same functionality there is a broad variety in functionality of DMS systems. Ending up with sub optimum choice of DMS can only be avoided by taking in account the possibility of changing the EMS system. Although in the short term this will be more expensive it may well turn out to be an excellent long-term investment.

The less interfaces the better – This means on the OA side both geographic and schematic view should be in the AM System and on the TA side calculation and simulation functionality should be in the DMS instead of in separate applications.

About the author

Jacco Peters studied tax law at the Erasmus University in Rotterdam. And started working at Cap Gemini afterwards. Where he specialized in test management, test process improvement and software process improvement. Jacco has over 10 years experience as a test manager and test coordinator in the financial and utilities sector. This article is based on his experiences as at test manager and test coordinator for the Dutch grid companies Alliander and Stedin.

Many thanks to Dirk Kriek (3S Systems) and Albertjan Peters (Bijvanck Consultancy) for proofreading this article.

www.rentab.eu
jacco.peters@rentab.eu
Mobile: +31683233428