

Structured approach to maintenance and modification of a railway traction IEC 61850 substation automation system

David Hewings¹ ✉, Andrea Poczapsky¹
¹Wales Route, Network Rail, Cardiff, UK

✉ E-mail: dave.hewings@networkrail.co.uk

eISSN 2051-3305
E-First on 3rd October 2018
doi: 10.1049/joe.2018.0148
www.ietdl.org

Abstract: Network Rail is currently electrifying one of the world's oldest main line railways, the Great Western main line between London and Cardiff. The traction system substations will incorporate full IEC 61850 functionality including the Rationalised Autotransformer Scheme: the world's first wide-area traction protection scheme operating using GOOSE messaging. The design and construction elements of a wide-area IEC 61850 system have been considerable. However, attention now focuses on future management of the IEC 61850 assets including the Substation Configuration Language files associated with the scheme. This study considers the IEC 61850 scheme of Network Rail from an asset owner's perspective. It sets out a structure for system modification and renewal which can be implemented by the in-house substation maintenance organisation for a complex IEC 61850 architecture. The system modelling and configuration control systems are described, along with a detailed examination of the management processes associated with future changes to IEDs and wide-area tripping logic.

1 Introduction

The Rationalised Autotransformer Scheme (RATS) provides a means of reducing switchgear requirements for new traction schemes, and utilising a wide-area protection scheme. Circuit breakers are replaced with load-break switches, and the resulting scheme makes use of a sequenced switching arrangement on detection of a fault to clear and then restore healthy lines, without any need for auto-reclose to be used as part of the fault detection and location process.

Development of this scheme has been a technical achievement for specialists in IEC 61850 and modern substation communication technology. However, now developed, the next significant challenge is for this scheme to be maintained and further developed by the Network Rail as the owning power system network utility. This is a challenge which utility organisations increasingly face; the need to increase IEC 61850 system knowledge.

2 Objectives

The objective of the maintenance process is to be able to act as the informed client of the Network Rail IEC 61850 network in the future. This means that the organisation must:

- be equipped to specify modifications to the system in a clear documented manner;
- be able to check and approve changes to the network provided by suppliers;
- communicate the structure and functionality of the RATS scheme to suppliers who may not have been involved in the original development; and
- be able to undertake minor modifications and system maintenance quickly.

The most important element of this methodology is the clear communication of the structure and functionality of the scheme. Given some of the inherent links to the Unified Modelling Language (UML) within the structure of the IEC 61850 standard documents, the structures of IEC 61850 are most readily formally documented using the graphical approach of UML. This provides a clear, unambiguous and yet very concise means of communicating structured system definitions and processes.

3 Scheme functionality model

The functionality of the scheme is shown in a modified object diagram in Fig. 1, which is known as a Scheme Functional Diagram (SFD). This shows a level of connectivity between logical node functions, which serves as a useful crossover diagram between the familiar logic diagrams of protection scheme design and the functional models of activity and sequence diagrams within UML. Fig. 1 gives an extract of the SFD for the RATS scheme, and shows a line current transformer (CT) object representation (CTR) and a busbar voltage transformer (VT) object representation (VTR), which are represented within an IEC 61850 system by the logical nodes TCTR and TVTR, respectively. Individual distance protection zones are shown as separate objects, so that the functionality and logic flows can be expressed without regard to their grouping within a single IED as a logical device. It is essential that a form of documentation to capture scheme functions and logic is maintained as part of a scheme, and management of changes to these diagrams from the first element of any structured maintenance modification.

The overall sequence diagram for the RATS scheme is shown in Fig. 2, and follows the UML sequence diagram approach for wide-area grouped protection schemes set out in the BS EN 50633 [1]. This is the overarching European Standard for the development of traction protection schemes, and makes use of the UML diagram approach for IEC 61850.

4 Scheme settings

With the functionality of the RATS scheme clearly defined in the functional diagrams, the settings of a particular section need to be provided. These are again given in the diagram form, representing the instance diagrams of the logical nodes, and therefore showing the individual settings associated with each device. At this stage, and given that settings are specific to a particular type of IED, the diagrams become specific to the types of devices in use. They, therefore, also provide reference to the IED capability description files for each device, which provides an audit trace of the device file system.

As well as protection settings, communication settings are also identified on this instance diagrams including details of addresses associated with GOOSE messaging. The full categorisation of parameters, which assists defining the areas of Substation

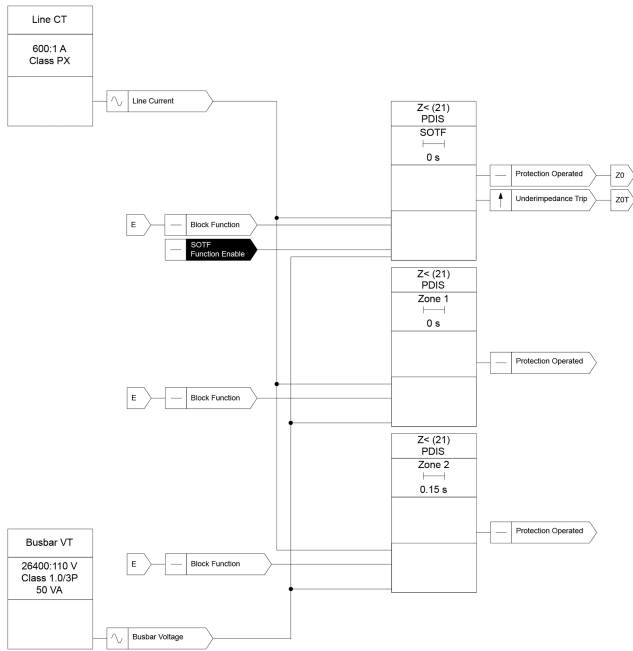


Fig. 1 RATS SFD

Configuration Language (SCL) change required are defined in IEC 61850-4 [2] as:

- system parameters;
- process parameters; and
- functional parameters.

5 System specification diagram Set

Within IEC 61850, the system specification is set out within the substation configuration description (SCD) file, and hence to some extent provision of the SCD file for a scheme should provide the full functionality and specification of that scheme. The diagrams described in the previous sections, when brought together, form a simplified, but comprehensive graphical view of the SCD file, and can be used as the starting point for further development and changes.

6 Use case development

To consider changes to the scheme, it is essential that a controlled change management approach is developed, with well-defined processes. A structured configuration management system proposed, based on the requirements of BS ISO 10007 [3], which sets out the general organisational requirements for configuration management. The overall description of the RATS system configuration in terms of the diagram structure and associated SCL files, together with the permitted forms of change and the detailed process requirements for each of those changes, together comprise the configuration management plan (CMP) as defined within BS ISO 10007. The core elements of this plan are given as:

- scope of application of the CMP;
- description of the IEC 61850 RATS system;
- indicative schedule of timescales for changes;
- references to scheme design documentation including UML diagrams;
- description of asset management change control organisation;
- role definitions and competency requirements;
- definition of system baselines and baseline documentation requirements; and
- definition of change processes including security requirements.

To define the permitted changes, specific use cases have been identified and modelled. These consider the future management of the IEC 61850 system from the perspective of Network Rail as the

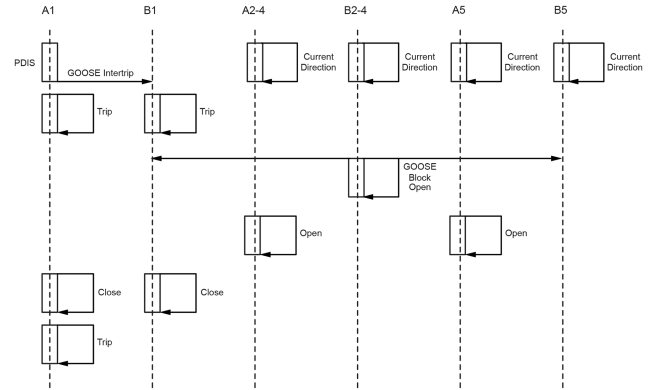


Fig. 2 RATS scheme sequence diagram

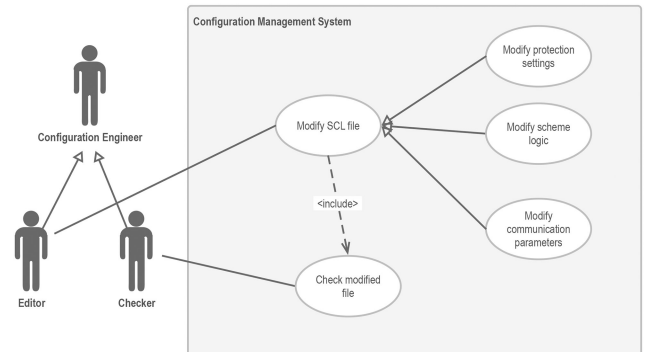


Fig. 3 Use case model extract

asset manager, and use the asset management requirements defined in ISO 55001 [4] as the basis for a structured view of system management through the full life cycle. Modifications of the hardware and functionality are then defined as specific use cases. Fig. 3 gives an extract of a use case model, one considering the processes around changes to the protection scheme and SCL files. There are more specific use cases covering the full asset life cycle, from initial commissioning of the scheme through to renewal.

The advantage of the use case approach is that it provides a very limited and specific set of change conditions. Any change which is more expressly considered in a use case is not permitted. Once defined, the actors on the diagram give a full view of stakeholders within the organisation involved in the change, and this sets the basis for a more detailed functional model of the change. Effectively, the use case diagram defines who is involved in a process, and their interrelationships.

Fig. 4 gives an extract of a sequence diagram for the SCL change. The sequence diagram follows the approach of UML given for the architecture specification, but now represents not the functionality of the protection and control scheme, but that of the management processes of the organisation undertaking a change to the scheme. It provides a clear graphical view of the process, and requirements for checking, approval and testing.

7 Wide-area scheme regression testing

One of the key challenges of providing an efficient configuration management structure for an IEC 61850 asset management system is the need to evaluate the effect of changes on the full IEC 61850 scheme. This is particularly relevant to a wide-area IEC 61850 scheme, where communication between IEDs in different sites may be affected by individual changes to communications, network and protection settings. Testing needs to be considered in terms of overall system risk. Whilst a traditional protection testing view would consider fully re-testing a protection scheme in the event of any change, the outage requirements for this for an operational wide-area scheme are not practicable, and so a level of overall scheme regression testing is required which can be accommodated within normal system outage times (typically up to 8 h), but which provide an adequate level of testing resilience. The level of testing

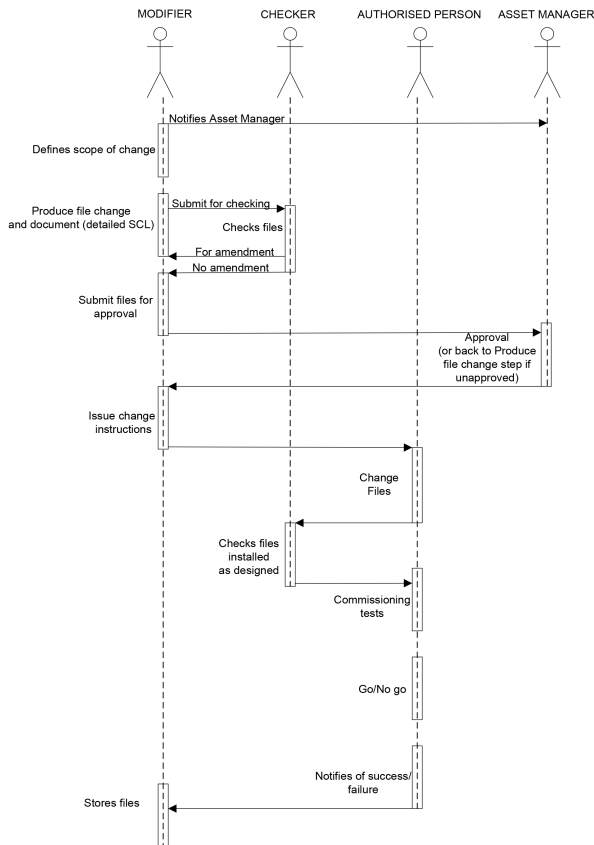


Fig. 4 Sequence diagram extract

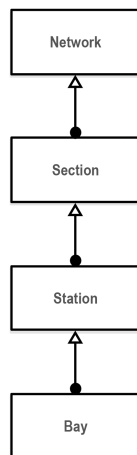


Fig. 5 SAT hierarchy

is, therefore, proportionate to the scale of the system change, and the potential risks, and can be defined as part of each use case, so that thereafter commissioning engineers are not given the unenviable task of providing individual system regression risk assessments for each change.

Fig. 5 gives the hierarchy of site acceptance tests (SATs), as defined in IEC 61850-4. For each level, an SAT definition is provided, dependent on the level of change undertaken. Hence, this structure is used to assist the process of reducing the level of required testing. The hierarchy has been modified to accommodate the GOOSE messaging between substations which is a feature of RATS. This introduces a new level of 'section', which represents the group of substations which act together for a single railway feeding section, and which in the RATS scheme comprise an extended station bus.

An important element of testing for such a scheme is the use of software 'injection' testing. This is defined as a third form of injection testing, to complement the established primary and secondary injection tests, but utilising state changes implemented

through software such as injected GOOSE messages to initiate system tests. In such a way, a level of automated system testing can be defined for any change, and hence even complex wide-area scheme tests can be undertaken in a relatively short time. For each use case, the testing schedule is developed as a generic requirement, along with any system test equipment configuration files required to assist automated testing. As far as possible, the tests should be designed so as to provide a go/no-go check on the configuration change. Taken together, the output confirmation of all of the tests provides sufficient evidence for approval of the change by the commissioning engineer, and then to approval by the asset manager.

8 Document management

The structured UML diagram set, together with associated SCL files and process documentation, is maintained within a document management system. The key principle of this is that the discipline of the CMP is contained within the document structure itself and its contents, not within the file storage structure. Corporate file storage systems are subject to continual advancement and change, and so to provide for a future-proofed architecture an evaluation of the options has been considered. From this it is proposed that the document management is undertaken within the latest corporate document management system, rather than a stand-alone system. This gives:

- inherent system back-up and security facilities;
- inherent integration with enterprise-wide data storage changes; and
- minimised system management requirements.

The specific requirements for the document management system to support the CMP are:

- back-up and version control for all documents, with automatic storage and retrieval of previous versions;
- access control; and
- logging of changes to each file.

9 Role-based competency development

The process approach using UML provides an easily readable, graphical view of change management and the ability to readily communicate the new scheme and its changes to new organisations. A key skill requirement is, therefore, for all in the process to have a working understanding of the UML diagrams. This does not require proficiency in software engineering to the extent of developing the diagrams or translating complex systems for software design, but rather the ability to read and interpret provided UML drawings. Key competencies can be defined as follows:

- read an UML object diagram and provide a written statement defining the architecture hierarchy, parameters (attributes) and functionality given by the diagram;
- read an UML use case diagram and provide a written statement of the use case, concisely defining the use case, its constraints and inherent logic and the interaction by each of the actors;
- read an UML sequence or activity diagram and interpret as a written process description, defining the order of events, interfacing of data between actors and decision points; and
- read an SFD diagram, together with associated system sequence diagrams, and provide a clear written description of the functionality of the protection scheme and the key settings required for operation of each function.

In addition, there are practical competencies required in understanding IEC 61850 communications within substations, router settings, integration with supervisory control and data acquisition remote terminal unit interfaces, use of IEC 61850 test equipment and software, and the security requirements and processes associated with the communications system, and access

to devices. In particular, a structured approach to changes in an IEC 61850 system should comply with the methodology to security set out BS EN 62351:2014 [5]. This includes the use of role-based access permissions.

These are defined in a system configuration competency profile, which is developed for each role within the actors of the use cases. In this way, the structured use case approach becomes the defining approach for each role competency, and can be used as a tool to continually reassess competencies as the technology develops.

10 Conclusions

Implementation of a wide-area IEC 61850 system to a power system asset management organisation requires its own structured approach, equivalent to that used as the design process, and in line with the system project management requirements set out in IEC 61850-4 [5]. This paper has set out the structured methodology developed within Network Rail for implementation of the wide-area RATS scheme, based on utilising the discipline and rigour of the UML as a concise language. The UML methodology provides a means of defining:

- architecture, functionality and settings of the system, for communication to new organisations as part of future changes, and for internal reference;
- processes and controls for maintenance and renewal of the system, forming an UML-based CMP; and
- organisational requirements for competencies required to support the CMP.

A clear prediction of protection and control technology in the IEC 61850 era is that obsolescence and system-wide change will progress at a rate not previously seen in power system protection engineering. This is a new area of protection and control asset management. However, there are developed standards in IEC 61850 project management [2], configuration management [3] and cyber-security for power system data systems [5]. These, if brought together and built into an asset management model, give much of the structure required to manage data-based substation automation systems. This structured approach is designed to provide a robust and transparent system which can be developed to accommodate the changes to protection engineering, and which can maintain pace with the engineering technology.

11 Acknowledgment

The authors are grateful for the support given by the Network Rail to the development of this work and its publication.

12 References

- [1] BS EN 50633: 'Railway applications – fixed installations: protection principles for AC and DC electric traction systems' (BSI, London, 2016)
- [2] BS EN 61850-4: 'Communication networks and systems for power utility automation: system and project management' (BSI, London, 2011)
- [3] BS ISO 10007: 'Quality management: guidelines for configuration management' (BSI, London, 2017)
- [4] ISO 55001: 'Asset management – management systems: requirements' (ISO, London, 2014)
- [5] BS EN 62351: 'Power systems management and associated information exchange: data and communications security' (BSI, London, 2014)