

SUMMARY REPORT

Testbed Overview

1.1 Objectives

The VIKING Testbed is a major delivery of the VIKING project. It is used to demonstrate and verify the work produced in the other Work Packages.

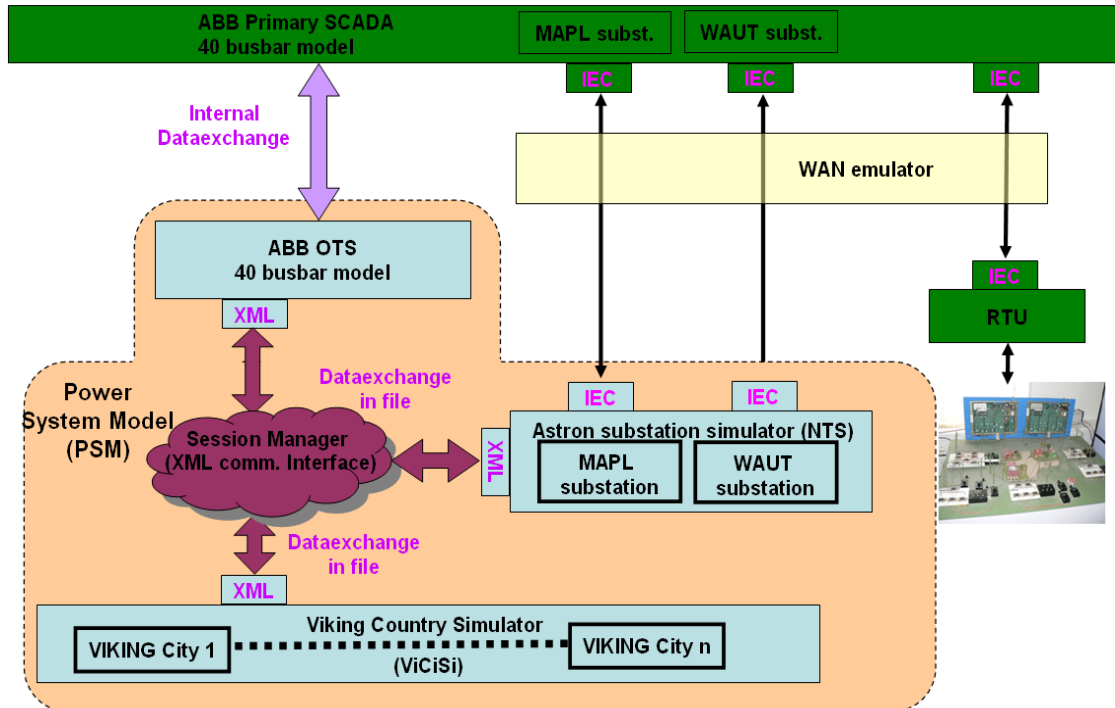
The VIKING Test bed has the following objectives:

- Demonstrate cyber attacks on SCADA systems and their consequences in the power network and in the society to project stake holders.
 - The main objective of the VIKING Testbed is to enable demonstrations of cyber attacks and their consequences to the power network and the society on a “real-life” SCADA system. This objective corresponds to the VIKING objective to increase awareness of threats from cyber attacks on control system that might endanger the operation of critical infrastructures in the society. With the VIKING Test Bed it is possible to introduce real attacks to the SCADA systems, to show their consequences on the electrical grid and to demonstrate the impacts of the corresponding power outages to the society. The different attacks have already described in corresponding Test Cases (see D5.3b)
 - To ease dissemination using the Testbed, remote demonstrations without having to move the physical equipment is possible. This feature will be used to show the results from VIKING on conferences and seminars and on visits to utilities and security organizations.
- Internal use for the VIKING security research and to investigate mitigation alternatives.
 - The VIKING Testbed has used internally within the VIKING project to study the behavior of a “real-life” SCADA system and its applications including communication and substation equipment. The Testbed is able to use to investigate and evaluate alternative mitigations proposed within the project work.
- Verification of models, tools and methodologies developed for VIKING purposes.
 - The VIKING Testbed is able to use to give proof of concept for the models, tools and methodologies developed within the project on a “real-life” SCADA system.

1.2 Design overview

The finally functional design of the VIKING Test bed is illustrated in the following figure.

(Vital Infrastructure, Networks, Information and Control System Management)



Testbed functional design

The VIKING Test bed consists of real-life components (green) and simulated components (light blue), power system models and Wide Area Network (WAN) Emulator (yellow).

In the following sections the already implemented Testbed components are described, firstly in an overview manner and then in more details.

1.3 Functional components

The VIKING Test Bed consists of components from a real-life SCADA system and simulated components that use models to represent reality.

The real-life components are:

- A SCADA/EMS system consisting of redundant SCADA servers, Front Ends, Operator Workstations and a redundant Local Area Network. The SCADA/EMS system software includes SCADA application with data warehousing plus advanced power system applications for a high voltage Transmission System.
- Communication interfaces to the communication between Substation Simulator (NTS)/Remote Terminal Units (RTU) and the central SCADA system.
- RTU for collection of process data and communication to the main SCADA system.

(Vital Infrastructure, Networks, Information and Control System Management)

The modeled components are:

- A power system high voltage model that is used to model the characteristics of the electrical transmission system. This is a semi-dynamic model that models quasi-stationary characteristics of primary electrical components, e.g. rotating masses in generators. It includes generation control to balance generation to loads.
- A Substation (Network) Simulator (NTS) that models the internal configuration, equipment and the characteristics of an HV/MV electrical substation including operation of protection, interlocks and reclosures. The Substation Simulator also models 40KV/10KV feeders and the corresponding field devices.
- A virtual society model (ViCiSi). ViCiSi calculates the electrical loads in the society on different load points for different times and voltage levels. The main objective of ViCiSi is to calculate the consequences of outages in the society in the form of cost for missed BNP production. ViCiSi can be parameterized to model different countries inside the European Union using load and society statistics.
- A communication emulator. It emulates the communication traffic between NTS /RTU and SCADA. The reason to use an emulator in the Test Bed is to enable the possibility to disturb the communication with the Denial of Service (DoS) attacks in order to blind the SCADA system and to introduce false telegrams in the traffic to and from SCADA.

1.3.1 Hardware components

The ABB Network Manager system has already installed on six (6) PCs, one of which is a rack-mounted high performance server. Two machines are dedicated as the SCADA application servers and the remaining servers are used for the HMI Client, Data Engineering, Historian, and Active Directory server. No virtualization of servers in the main SCADA system is used in the Testbed.

Three PCs are dedicated for the ViCiSi, WAN emulator and the NTS.

The SCADA control centre network is isolated from the Internet and other local networks. A separate network is allocated to IEC 870-5-104 devices and performs the function of the "utility WAN". Access for maintenance and demonstration is provided using VPN and VLANs facilitated by a Cisco security appliance connected to the KTH ICS office network and accessible by authorized parties (e.g. Astron).

A Redundant Communication Module (RCM) is also connected to the SCADA Local Area Network (LAN). The RCM provides additional serial ports for connection of IEC 870-5-101 RTUs to the SCADA server.

(Vital Infrastructure, Networks, Information and Control System Management)

1.4 Power system models

The VIKING Testbed contains different models of the power system on all voltage levels. However, this is not one singular model but three different models due to the different tools that are using them. The following picture shows how the electrical models of the Testbed have interconnected.

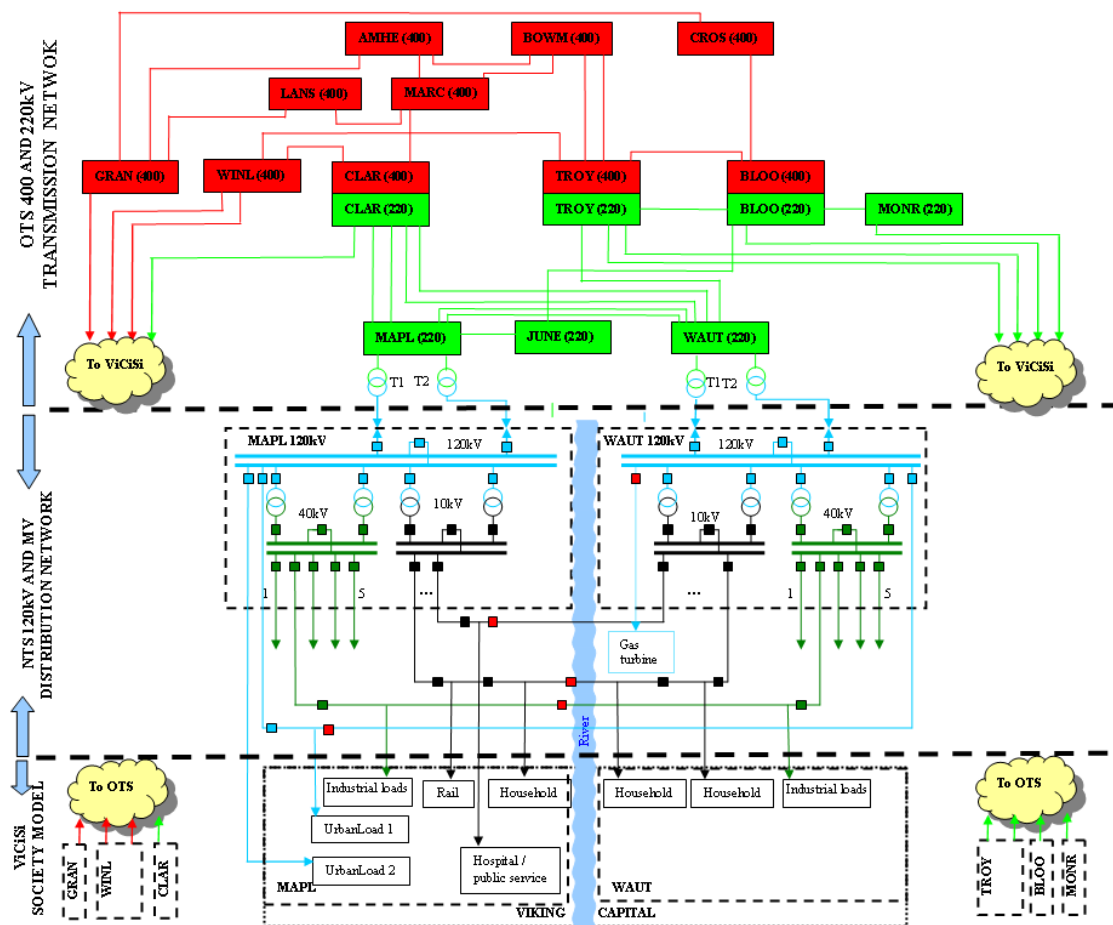


Figure 1 – Testbed finally power system model

A short description of these models follows below:

- The OTS 400KV and 220KV transmission network model includes generation, transmission lines and transformers. This network is based on the ABB 40 buses network that has been used in many international interoperability tests. This model is used by the ABB Training Simulator that models semi-dynamic behavior of the power network and includes continuous pseudo-stationary modeling of load-frequency balance and network power flow in normal and emergency operational state. The modeled transmission network

(Vital Infrastructure, Networks, Information and Control System Management)

is connecting to the NTS power network through two HV/MV substations, which are feeding the VIKING capital. Six HV substations are feeding directly the remaining VIKING cities with electrical power both on 400KV and 220KV level.

- The 120KV part of two HV/MV substations for VIKING capital and parts of the 40KV and 10KV distribution networks are modeled using the substation simulator (NTS). The NTS is able to simulate the behavior of the HV/MV substation with continuous modeling of the operation of substation primary and secondary devices, including protections/automatics (e.g. auto-reclosing). NTS also models the 120kV, 40KV and 10KV connecting feeders to VIKING capital as illustrated in the figure above.
- VIKING City Simulator (ViCiSi) model includes all types of consumers, e.g. residential, enterprises, public services, etc. in the virtual society. These consumers are fed with electricity through a model of the electrical distribution network on MV and LV levels. This is pure radial model. Based on individual consumer load profiles ViCiSi calculates active and reactive loads on arbitrary load points which are used as loads for the substation and transmission models.

1.5 Session manager

In order to control the flow of data between the modeled parts of the Testbed and the execution of the corresponding programs, a control program (called Session manager) implementation was required. For the real-life components no execution control or control of data flows is required since these components act as if they were in a real life situation acting on real-life data. These components have their in-built data flow control and execution control mechanisms.

The Session Manager is responsible for the following tasks in the Test bed

- Polling of loads from ViCiSi /NTS and sending them to NTS and to OTS.
- Sending of outage information to ViCiSi based on outages in the network models, from NTS or OTS
- Time synchronization within the Test bed. The Test bed works with a simulated time that always runs in "real-time" but can be stopped and resumed.

1.6 Software penetration and analysis tools

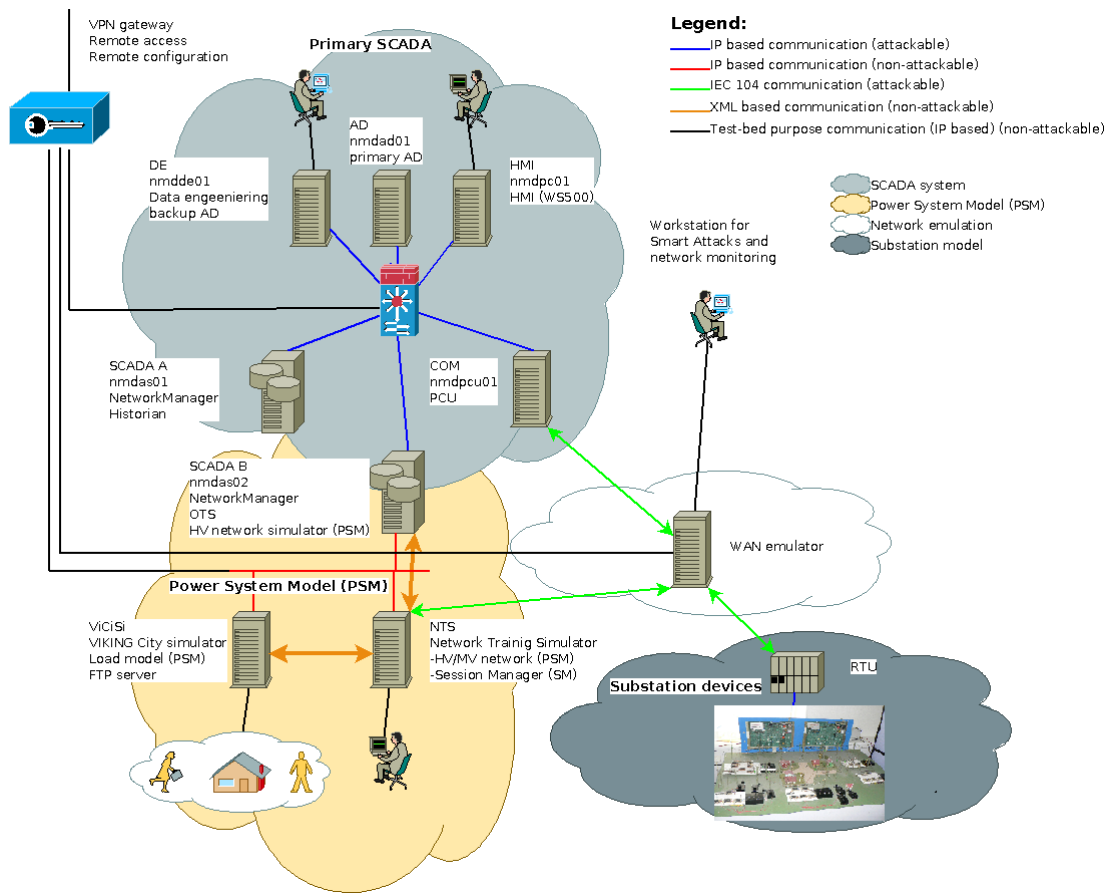
One of the main purposes of the Test bed is to introduce cyber attacks on the SCADA system or in the communication networks.

The Test bed gives a possibility for the Testbed user to apply different tools for analyzing the communication network. The communication emulator itself includes tools for traffic control and connection access is also available for intrusions (for example introduce of false telegrams).

(Vital Infrastructure, NetworkS, INformation and Control System ManaGement)

1.7 Functional components and configurations

The figures in the previous chapter show the Testbed components from a functional and from a Hardware point of view. Based on those previous figures and taking into account the functionality of each HW component the following groups can outline, what is shown on the figure below. We can observe in this figure the four functional parts of the Testbed, the HW components that are responsible for realize the mentioned functionality, and the network connections between them.



The Viking Testbed overview