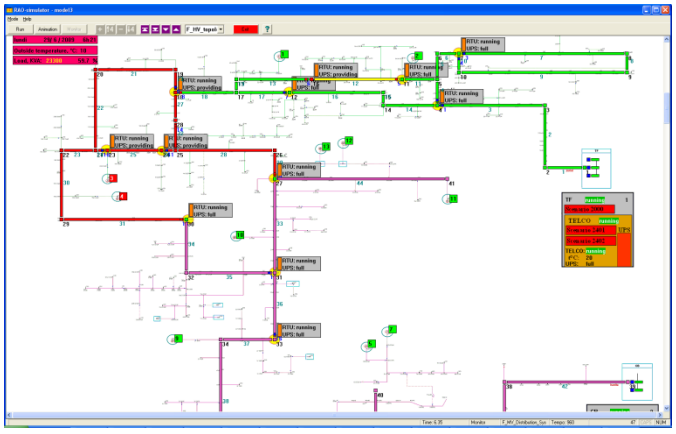
Heterogeneous simulation model for quality of service indicators calculation of electricity distribution grid controlled by SCADA under cyber attacks.

Estimation of quality of service (QoS) indicators of electricity distribution infrastructure while its communication infrastructure and SCADA are under cyber attacks is very important for risk management of grid utility and for final customers. Topology of electrical grid, communication network, SCADA, their devices, SCADA procedures, cyber attack scenarios should be taken into account to accomplish the task. Simulation model of such a complex heterogeneous system has been developed in CockpitCI project. The model "translates" probable behavior of SCADA/CCI devices and software under cyber attack in the expected behavior of electrical grid seen by electricity customers. Indeed, these customers don't care about electricity supplier cyber security problems. All they want is uninterrupted power supply or at least to know in advance about potentials power supply disruptions.



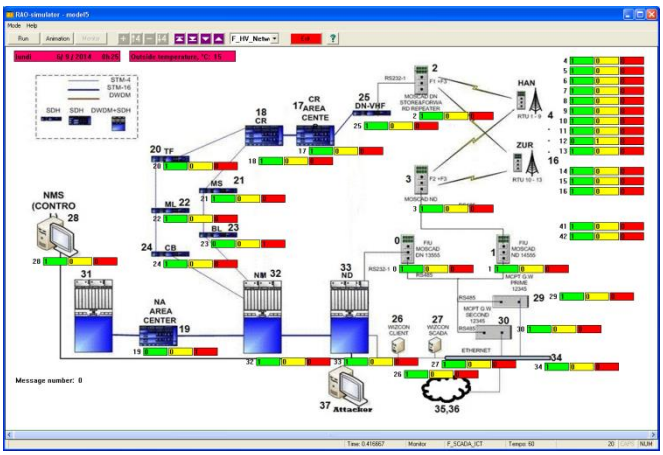
The Intelligent RAO Simulator is the tool used to develop the model. The tool is a hybrid of discrete-event simulator and expert system. System elements are described in this tool by resources having a set of parameters or state variables and the system behavior is described by modified production rules coming from Artificial Intelligence. A modified production rule describes in common case an action involving several resources. Using production rules gives great flexibility to the simulator, allowing one to describe processes of different nature as well as human reasoning and algorithmic procedures. The simulator has also an external messaging mechanism allowing communication with other simulation models and with any external software locally or remotely by network.

The model developed consists of:

- Data base: a set of objects describing system composition and state (200+ permanent objects + temporary objects created while simulating) belonging to 20 object types (substation, breaker, line, FIU, gateway, SCADA, message, route, etc.)
- Knowledge base: a set of activities describing system behaviour (200+ activities of 100+ types such as toggle breaker state, send a message, repair a line, transmit a message, etc.)
- Animation screens description to illustrate system state evolution (see screenshots above: one step of FISR process on electricity distribution grid (upper) and SCADA/CI under cyber attack (lower))
- Quality of service indicators and specific technical indicators definition

Multitel
A.S.B.L. fondée par la F.P.Ms

The model simulates a reference scenario (fault isolation and system restoration (FISR) process + cyber attack). To execute the FISR process remotely, dozens of commands are sent by SCADA to field RTUs which



open and close switches. Commands transmission and execution time depends on elements behavior under cyber attack. The model reproduces this process in details and calculates QoS indicators under various cyber attack scenarios and for various SCADA procedures. This provides the important input helping to increase awareness of electric grid management and final customers, to undertake possible countermeasures, thus reducing overall risks.

As the SCADA/CCI elements behavior under cyber attack is modeled in CockpitCI in a probabilistic way, the model includes all necessary logic to perform Monte-Carlo simulations. QoS indicators are then given by mean values and standard deviation of mean, allowing to estimate confidence intervals of indicator values.