21, rue d'Artois, F-75008 PARIS
http : //www.cigre.org

D2-112

CIGRE 2016

Experiences from Intelligent Alarm Processing and Decision Support Tools in Smart Grid Transmission Control Centers

Neven Baranovic, M.Sc.
HOPS, Croatia
neven.baranovic@hops.hr

Per Andersson, Ph.D.
GoalArt, Sweden
per@goalart.com

Igor Ivanković, M.Sc.
HOPS, Croatia
igor.ivankovic@hops.hr

Ksenija Žubrinić-Kostović, M.Sc.
HOPS, Croatia
ksenija.zubrinic@hops.hr

Domagoj Peharda, Ph.D.
Končar-Ket, Croatia
domagoj.peharda@koncar-ket.hr

Jan Eric Larsson, Professor
GoalArt, Sweden
janeric@goalart.com

SUMMARY

New technologies have a major impact on the improvement of transmission grids, and this impact will be even greater in the near future. The introduction of intelligence in the network, by wide application of information and communication technology, has led to the so-called "smart" grid. Power systems have indeed always been smart, (especially at the transmission level), but a massive penetration of smaller units, and an increased inflow of signals, measurements, and alarms in control centers, increase the need for control and coordination. A smart grid needs a smart control room.

In order for the operators in a control room to manage the grid and handle problems quickly and correctly, they need to understand the behavior and fault state of the grid, that is, they need to maintain situational awareness. One of the operator support systems is the alarm system, which displays fault indications in lists and graphical displays, often accompanied with warning sounds. In order to help the operators maintain situational awareness, the alarm system needs to display all important faults promptly, but it is equally important that it does not overload the operators with information. Ideally, they want to see the *real faults* only.

The Croatian Transmission System Operator (HOPS) has installed a new system for intelligent alarm processing (IAP) using real-time root cause analysis, a lightning detection system and a smart visualization system. The IAP system has been evaluated on-line during real operation. We present the results from one month of normal operation, and from four selected incidents during 2015.

The system for intelligent alarm processing with on-line root cause analysis displays less than 1 % of the number of alarms displayed in the SCADA system. All selected outages are correctly analyzed, and the algorithm displays the minimal set of root alarms, that is, "the real faults." In this way, it is possible to reach the Engineering Equipment and Materials User Association's (EEMUA) alarm rate criteria at all times, both during normal operation, and during incidents.

KEYWORDS

Alarm management – Control rooms – Human-machine interface – Intelligent alarm processing – Lightning detection – SCADA systems – Situational awareness – Smart grid – Visualization.

neven.baranovic@hops.hr

1. INTRODUCTION

During the last ten years, HOPS has enhanced its transmission grid, replaced classical remote terminal units in all substations with modern substation automation systems, introduced an optical infrastructure and a new telecommunication network, and connected renewable energy sources, especially wind energy. The goal is to have a smart transmission system, which is observable and controllable in all states. Its behavior should be known in real time and should be predicted for short-term and long-term time periods. To fulfill these demands, HOPS has installed a new SCADA/EMS system and integrated new decision support tools: intelligent alarm processing, lightning detection and smart visualization.

1.1 A Smart Visualization Concept

The HOPS visualization concept consists of world map displays, fixed displays, and geographic data views. In the national dispatch center there is a video wall (3x6 cubes with a total of 26 square meters) which provides real time operational status of the transmission network. The video wall is flexible and can show any picture in the system that the dispatcher currently needs. Data are presented in a way that allows operators to understand a situation and have quick access to all data, to make decisions, and to take effective actions, see Figure 1.

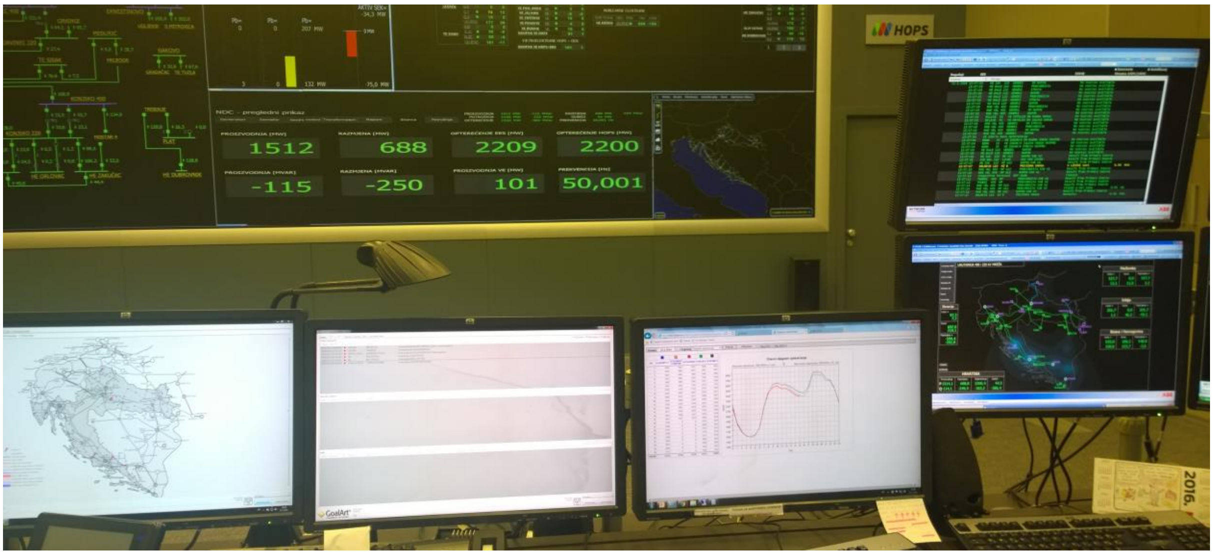


Figure 1. An operator workplace. The IAP tool is on the two left bottom screens (graphical overview and alarm list with root alarms and secondary alarms). The lightning detection tool is on the bottom right of the video wall. The smart visualization of voltage deviations is on the bottom screen on the far right.

There are “scenarios” of video wall display configuration. Different scenarios are used for different operational states. For example, in case of heavy storms, the lightning detection map is made larger than during normal operation.

1.2 Smart Visualization of Voltage Deviations

A new smart visualization tool provides a valuable picture of how voltages vary across the whole transmission system, and shades low voltage regions red and high voltage regions blue, (with so-called contour coloring). This view is useful for detection of impending voltage collapses and identifying areas with high voltages, see Figure 2.

1.3 Lightning Detection

Operators use real time lightning data (time, location and peak current of lightning strikes), to see where a storm is occurring and where it is going, and to determine if a specific lightning strike caused a persistent fault. The lightning detection system is connected with the SCADA system and correlation between breaker switching and lightning strikes is done in real time. This functionality may be used within seconds of the occurrence of lightning strikes, to help in decisions about reclosing, or over a period of years when used for long-term lightning incidence statistics. The result is a detailed world map display with lightning data and the positions of overhead lines, poles, and substations, see Figure 3, where there is a picture of lightning strikes and the movement of the storm during a three hour period, (the picture is from the Istra incident, described in Chapter 4.2.1).

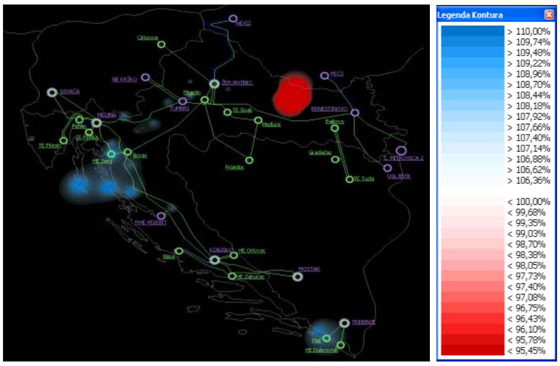


Figure 2. Smart visualization of voltage deviations.

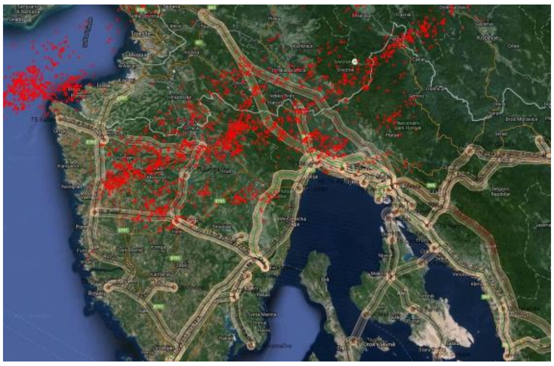


Figure 3. Lightning detection system.

2. INFORMATION AND ALARMS IN HOPS SCADA SYSTEM

A new SCADA/EMS system is installed in the National control center and four SCADA systems in the area control centers, in a multi-site configuration. The multi-site configuration consists of five SCADA systems with synchronized real-time databases and one network model for the whole transmission network. Each area control center controls its part of the network and the alarm and event lists are filtered to show that part only.

The basic idea is to collect as much operational and non-operational data from substations as possible, in order to understand the power system behavior, and have a full and detailed overview of the entire power system. The substations are unmanned and it is important to record and present all events and violations of analog limits, and to alert the operators. Most of the collected events are also alarms.

The HOPS control philosophy makes a distinction between the roles of a dispatcher and of an operator. Dispatchers are responsible for the safety of the grid, decision making, and keeping the balance between supply and demand. Operational data is the fundamental information for dispatchers, and used to measure the real-time status, and performance and loading of power system equipment. The operators continuously monitor primary and auxiliary equipment status, execute network topology change orders from dispatchers, and manage maintenance work. Non-operational data is the most important information for the operators' job. Alarms and event data in the new SCADA system are distributed between control centers on a geographical basis, and additionally in each control room between two operator workplaces and one dispatcher workplace.

2.1 EEMUA Criteria

Average alarms per 10 min	Alarms during worst 10 mins	Classification
Less than 1 alarm	Less than 10 alarms	acceptable
Less than 2 alarms	Less than 20 alarms	manageable
Less than 10 alarms	Less than 100 alarms	over-demanding
More	More	unacceptable

Table 1. EEMUA alarm KPI criteria.

The EEMUA document presents key performance indexes (KPI) concerning the number of alarms presented per each operator workplace, [3]. There are two KPIs. The *average alarms per ten minutes* is used over longer time periods, while the *maximum number of alarms per ten minutes* is used for alarm cascades, see Table 1. The criteria also state that less than 10 long-standing alarms and less than 30 shelved alarms are acceptable.

EEMUA is not a standard or regulation, but globally accepted as the benchmark for best practice on designing and managing alarm systems. Currently, there are no recommendations directly concerning electrical transmission networks. However, some findings have been published. One utility reports that during normal quiescent behavior, 3-5 alarms are received by control staff every minute, [2]. This translates to 30-50 alarms per ten minutes ("unacceptable"). Another utility reports 2 000 average alarms per day, [12]. This translates to 14 alarms per ten minutes, (also "unacceptable").

2.2 Experience of Information Overload

In order to investigate the alarm load situation, the actual alarm rates were measured during November 2015 for the SCADA system in each area control center. Data from the Osijek area control center is shown in Figure 4.

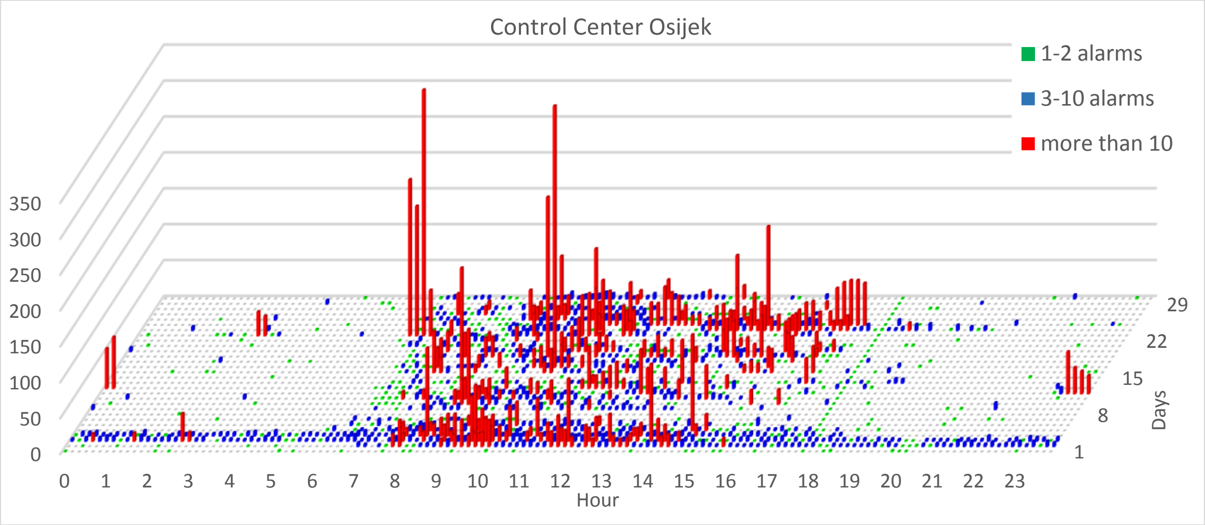


Figure 4. Number of alarms for each 10 minute period at the Osijek area control center, in November 2015. The x-axis shows 144 10-minute periods, the y-axis shows 30 days in the month of November, and the z-axis shows the number of alarms during each 10-minute period.

The alarm rate curve is not uniform during day and night. Generally, for all area control centers, the alarm rate is highest during work hours (08^{00}-16^{00}). It should be noted that during this period, the alarms were mainly caused by maintenance work.

3. INTELLIGENT ALARM PROCESSING FOR POWER SYSTEMS

The results of alarm rate measurements for all four area control centers indicate that the SCADA system generates more information than the operators are able to handle easily, especially in situations when there are one or many faults in the grid. There are several different kinds of alarm problems, and they each need different solutions.

- There may be too many alarms configured. At HOPS, these problems are handled by a so-called alarm rationalization process, see, for example, [3, 6].
- There may be problems with the tuning of alarm limits and other alarm parameters. This should be handled by alarm limit tuning, which may be a part of the alarm rationalization.
- Alarms may be irrelevant in certain operational states, for example, alarms from equipment that is switched off. These problems should be managed by state-based suppression of alarms. HOPS solves these problems by using an available SCADA feature, *test mode of operation*, where updating of the values in event and alarm lists are stopped. Unfortunately, this problem persists because maintenance personnel do not always use the test mode.
- Sometimes one or several faults in combination lead to consequential faults. This is the case in larger fault situations, where problems may spread through large parts of a power grid. Since all original and consequential faults create alarms, such a situation manifests itself as an *alarm cascade*, that is, a sudden burst of primary and consequential alarms. This problem has so far

been difficult to manage, but the new IAP technology described in this paper provides a technical solution to the alarm cascade problem.

3.1 Alarm Management Based on Intelligent Alarm Processing

This paper reports the experiences of a software system using *intelligent alarm processing* and *real-time root cause analysis* of complex alarm situations. The system provides an alarm management technology with the following functions.

- SCADA alarms from a single grid object (generator, transmission line, bus bar, etc.), are grouped into single alarms, so the operator easily can see which objects have problems or are out of service.
- Nuisance alarms that are activated repeatedly over short time periods, so-called "chattering" alarms, are monitored by the system and shelved and un-shelved dynamically. Shelving means that the alarm is moved from the primary alarm list to a separate list for shelved alarms.
- Other alarms are caused by damaged or unused equipment and remain active for a long time, so-called "long-standing" alarms. These are also monitored by the system and are timed out after a fixed time period, currently four hours.
- The system contains a model-based algorithm that can analyze consequential alarm cascades, and show the root cause alarms ("the real faults") in a primary list, and consequences in a secondary list.

For readings on intelligent alarm processing with on-line root cause analysis, see [1, 4, 5, 7, 8-11].

The combination of these methods leads to a large improvement of the alarm situation. In complex fault situations, hundreds of alarms may be shown in the SCADA system, while the IAP tool only shows one or two primary root cause alarms.

3.2 Intelligent Alarm Processing and Root Cause Analysis Software Functionality

The alarm management algorithm uses knowledge of the physical structure of the power grid, which it acquires from a SCADA/EMS network model. At HOPS, the internal IAP model is derived from the existing CIM XML description of the SCADA/EMS network model. The algorithm also uses operational real-time data from the synchronized SCADA system database, such as analog and discrete signals (power flow, voltage, amps, breaker and disconnector positions, and protection signals), and the real-time alarm and event stream, see Figure 5.

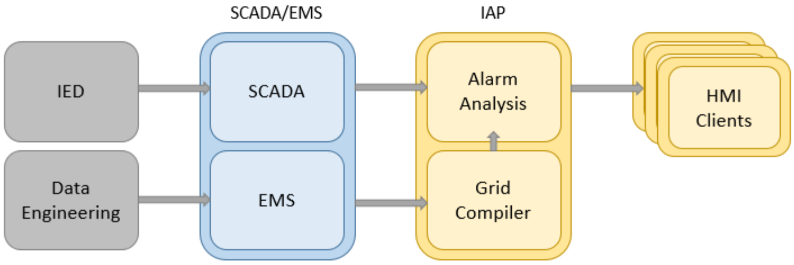


Figure 5. The IAP software integrates with the existing SCADA/EMS system.

All grid knowledge used in the calculations can be derived automatically from the CIM model. Whenever the CIM model is updated, it is imported to the system and compiled, which takes less than a minute. This means that the system needs *no manual maintenance.*

The real-time functionality consists of several software layers, which perform calculations on analog and discrete data to identify stale signals, bad data, delta changes, equipment which is out-of-service, faults states, and the global root cause analysis state for the whole transmission network.

3.3 Software Integration

The intelligent alarm processing system is a separate software application that can be integrated with a SCADA system in several different ways. It consists of a central server and one or several clients. The server executes on a separate computer. The server receives real-time data from the SCADA system via a network protocol. The results of the analysis for the whole network are stored in the server, and are distributed to all clients in all control centers in real time, see Figure 5.

3.4 Alternative Methods

The most common method to deal with alarm problems is to perform a so-called *alarm rationalization*, [3, 6]. This process is a manual analysis of all configured alarms. For each alarm you check the intention and what action the operator needs to take. If there is no need for an action, the alarm can be removed. Typically, an alarm rationalization may lower the everyday number of alarms per hour, but the effect will be small in upset situations.

In principle, it is possible to perform alarm reduction by programming in the built-in SCADA system language. However, without an explicit algorithm, this type of solution is incapable of reducing more complex alarm cascades. It is also possible to try rule-based system tools, but the work effort and costs are ultimately prohibitive.

A previous solution for intelligent alarm processing is described in [2, 13]. This application performs data concentration and flood recognition for a single substation bay. The main difference is that the real-time root cause analysis tool can handle problems that spread between substations and performs a *grid-wide* root cause analysis.

4. EXPERIENCES FROM INTELLIGENT ALARM PROCESSING

The intelligent alarm processing tool described above has been installed at the Swedish national grid since 2009. It was delivered to HOPS in October 2013 and real-time operations began in March 2014. During 2015, the tool has saved performance statistics, and the SCADA system has saved original alarm statistics. This allows us to present actual statistics on the alarm reduction and to calculate key performance indices based on the measured alarm data.

4.1 Normal Operation

To describe the experience with IAP under "normal" operation, we randomly selected the month of November 2015. There are a significant number of alarms even under calm circumstances, while the intelligent alarm processing identifies a small number of disturbances and their root causes. It is important to emphasize that this great improvement benefits both dispatchers and operators, but in particular the dispatchers, because of the different responsibilities described in Chapter 2.

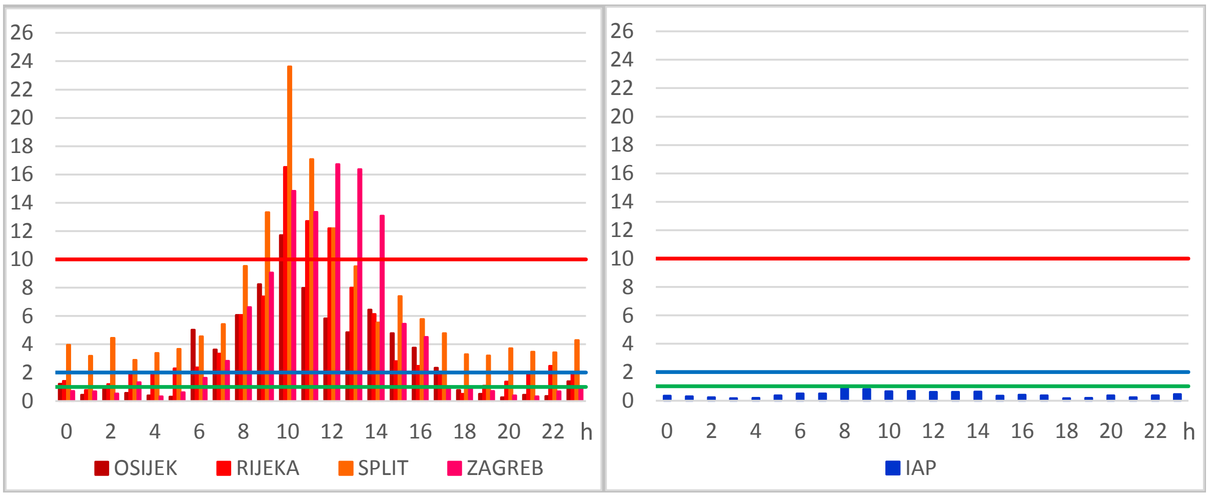


Figure 6. The average alarm rate per 10 minutes for each hour in November 2015, for SCADA alarms (left) and IAP alarms (right). The green, blue and red limits are the EEMUA limits for *average alarms*, see Table 1.

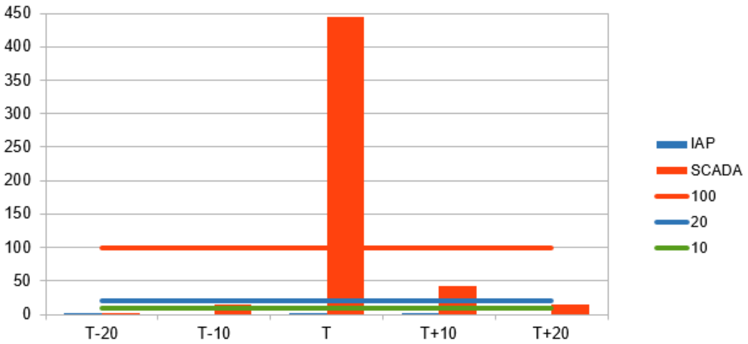
In order to see how the SCADA KPI and IAP KPI compare with the EEMUA recommendations, Figure 6 shows the alarm load for each hour during November 2015. It can be seen that the SCADA alarm loads often are outside of the optimal interval of less than one alarm per ten minutes (“acceptable”) and reach “unacceptable” regularly. The IAP tool consistently remains at the “acceptable” level.

4.2 Selected Alarm Cascades

Although the presented IAP algorithm provides an alarm rate reduction around 98 % in average situations, its performance is as good during disturbances and incidents. In order to investigate this further, we selected four incidents from 2015. These cases have all been analyzed with the intelligent alarm processing when they occurred. The results are as presented below. In these cases, we have counted the alarm rates for a single operator, because it is not possible to distribute the analysis of a cascade over several operators in an efficient manner. In the following, the SCADA alarm rates are per area, while the IAP alarm rates are for the entire Croatian grid.

4.2.1 Lightning Strikes in Istra

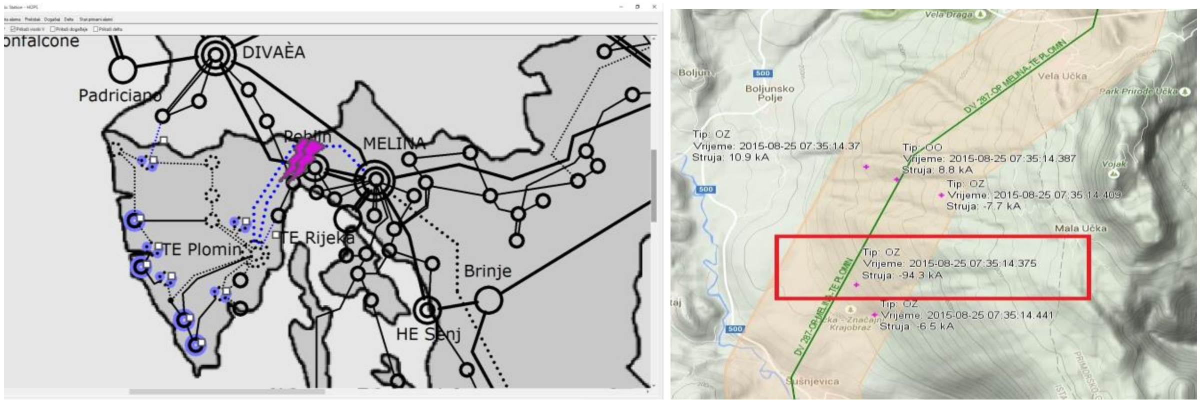
On August 25, 2015, lightning struck two parallel overhead lines in the Istra area. Both lines where hit within a few seconds, which caused them to disconnect and cause a subsequent disturbance as seen in Figures 7 and 8.



Time	SCADA RIJEKA		IAP HOPS	
T-20 min	🟢	2	🟢	1
T-10 min	🔵	15	🟢	0
T	🔴	445	🟢	2
T+10 min	🔵	43	🟢	1
T+20 min	🔵	14	🟢	0

Figure 7. Alarm load per ten minutes for SCADA alarms (red) and IAP alarms (blue), during the Istra incident, August 25, 2015, (green means less than 20, blue less than 100, and red more than 100 alarms see Table 1).

The Istra incident was followed by a cascade of 502 SCADA alarms during eighteen minutes (distributed over three 10 minute intervals, see Figure 7). During the same time interval, there were three IAP alarms in the same area. The intelligent alarm processing correctly identified the two disconnected lines as the root causes of the alarm cascade, see Figure 8. The third IAP alarm was an independent problem in the same area.



Tip: OZ
Vrijeme: 2015-08-25 07:35:14.37
Struja: 10.9 kA

Tip: OO
Vrijeme: 2015-08-25 07:35:14.387
Struja: 8.8 kA

Tip: OZ
Vrijeme: 2015-08-25 07:35:14.409
Struja: -7.7 kA

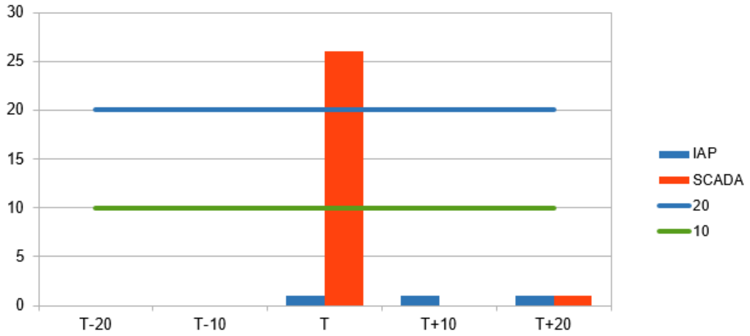
Tip: OZ
Vrijeme: 2015-08-25 07:35:14.375
Struja: -94.3 kA

Tip: OZ
Vrijeme: 2015-08-25 07:35:14.441
Struja: -6.5 kA

Figure 8. Screen shots of the Istra event, from the graphic presentation of the IAP tool (left) and the lightning detection tool (right). The locations of the two root faults are shown with pink lightning strikes in the IAP tool, and with pink plus signs in the lightning detection tool.

4.2.2 Lightning Strike in Vinodol

On September 5, 2015, a lightning strike caused a protection relay to activate and disconnect lines.



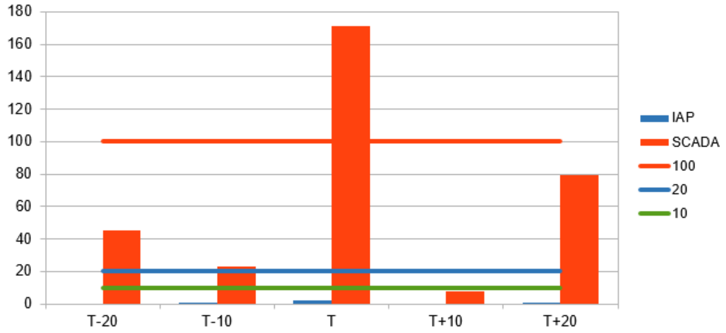
Time	SCADA RIJEKA		IAP HOPS	
T-20 min	🟢	0	🟢	0
T-10 min	🟢	0	🟢	0
T	🔵	26	🟢	1
T+10 min	🟢	0	🟢	1
T+20 min	🟢	1	🟢	1

Figure 9. Alarm load per ten minutes for SCADA alarms (red) and IAP alarms (blue) see Table 1, during the Vinodol incident, September 5, 2015.

The Vinodol incident was followed by a cascade of 26 SCADA alarms during twenty seconds, see Figure 9. During the same time interval, there was a single IAP alarm in the same area. The intelligent alarm processing correctly identified the protection relay alarm as the root cause of the alarm cascade. The IAP alarms during the “T+10 min” and “T+20 min” time periods were from another area.

4.2.3 Heavy Storm in Konjsko

On June 9, 2015, intensive lightning strikes during one hour caused protection relays to activate in the Konjsko substation, which caused several small alarm cascades.



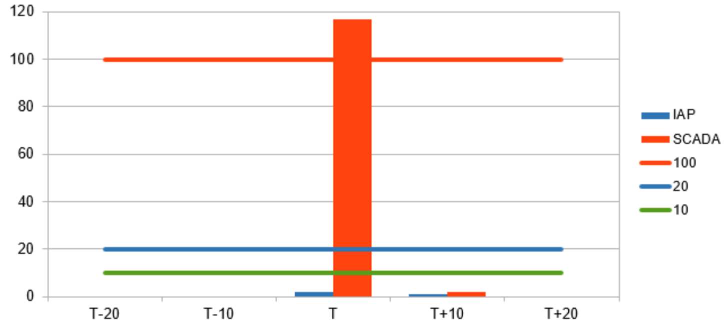
Time	SCADA SPLIT		IAP HOPS	
T-20 min	🔵	41	🟢	0
T-10 min	🔵	23	🟢	1
T	🔴	141	🟢	2
T+10 min	🟢	8	🟢	0
T+20 min	🔵	79	🟢	1

Figure 10. Alarm load per ten minutes for SCADA alarms (red) and IAP alarms (blue) see Table 1, during the Konjsko incident, June 9, 2015.

The main Konjsko incident was followed by a cascade of 141 SCADA alarms during three seconds, while during the same three-second time interval, there was a single IAP alarm in the same area, see Figure 10. The intelligent alarm processing correctly identified the protection relay alarm as the root cause of the alarm cascade. The other IAP alarms are from another area.

4.2.4 Strong Winds around Vrataruša Wind Farm

On November 23, 2015, strong winds broke an overhead grounding wire, and caused several protection relays to activate.



Time	SCADA RIJEKA		IAP HOPS	
T-20 min	🟢	0	🟢	0
T-10 min	🟢	0	🟢	0
T	🔴	117	🟢	2
T+10 min	🟢	2	🟢	1
T+20 min	🟢	0	🟢	0

Figure 11. Alarm load per ten minutes for SCADA alarms (red) and IAP alarms (blue) see Table 1, during the Vrataruša incident, November 23, 2015.

The Vrataruša incident was followed by a cascade of 117 SCADA alarms during seven minutes, see Figure 11. During the same seven minute time interval, there was a single IAP alarm in the same area. The intelligent alarm processing correctly identified the protection relay alarm as the root cause of the alarm cascade. The other IAP alarms are from another area.

4.3 Summary of Experiences

A summary of the experiences from the month of November 2015 is shown in Table 2, while the four selected incidents are shown in Table 3.

Nov 2015		Day	KPI	Classification	Night	KPI	Classification	Total
IAP *		1 216	0,56	● acceptable	673	0,31	● acceptable	1 889
SCADA	Osijek	11 953	5,53	● over-demanding	2 119	0,98	● acceptable	14 072
	Rijeka	14 435	6,68	● over-demanding	3 743	1,73	● manageable	18 178
	Split	21 158	9,80	● over-demanding	7 956	3,68	● over-demanding	29 114
	Zagreb **	18 843	4,36	● over-demanding	1 595	0,37	● acceptable	20 438

Table 2. Alarm statistics for the month of November 2015 in the IAP tool and the four area control centers. The KPI columns show the *average alarm rate per ten minutes*. Daytime is 07^{00} – 19^{00}. Nighttime is 19^{00} – 07^{00}. *IAP normally is not filtered per area. **Zagreb has two separate SCADA alarm lists and operator workstations, with approximately equal alarm load.

During November 2015, there were a total of 81 802 alarms in the four area control centers and 1889 IAP alarms (root causes of disturbances). The result is that in the normal operation there is an average alarm load of 4-10 alarms per ten minutes in the day time, see Table 2, for which the EEMUA classification is "over-demanding." The IAP alarm rate is significantly lower (98 %) than the SCADA alarm rate, and represents a great improvement for operators and especially dispatchers.

In the November 2015 case, there are some IAP nuisance alarms, that is, independent root causes with no consequences and relatively little information value. The main reason for IAP nuisance alarms are local circuit breaker switching at the bay or substation level, where commands from SCADA are not issued. Consequently these events are interpreted by the IAP system as a spontaneous topology changes, (outages or disturbances).

Each of the cascading events were located in a single area, and the analysis of a cascade cannot easily be distributed between operators. The Vinodol incident ranks as "over-demanding" while the other three are "unacceptable," see Table 3.

	SCADA	KPI	Classification	IAP	KPI	Classification
Istra	502	445	● unacceptable	3	2	● acceptable
Vinodol	26	26	● over-demanding	1	1	● acceptable
Konjsko	141	141	● unacceptable	2	2	● acceptable
Vrataruša	117	117	● unacceptable	2	2	● acceptable

Table 3. Alarm statistics for the four selected incidents. The SCADA and IAP columns show the alarm total during the incident. The KPI columns show the *worst case alarm rate per ten minutes* in the SCADA system and the IAP system.

In the intelligent alarm processing tool, the alarm load is consistently "acceptable," both during normal operation, and (notably) also during the incidents. When we compare the number of alarms in the SCADA alarm list with the number of alarms in the IAP primary list, there are around 98 % fewer alarms, both during normal operation and incidents. These numbers are corroborated by experiences in other domains. For a thermal power plant, the corresponding fractions during upsets were 97-99 % and during normal operation 75 %, [7].

5. CONCLUSIONS

In order for dispatchers and operators to manage a power grid correctly and efficiently, they need to understand the behavior and current state of the grid, that is, they need to maintain *situational awareness* at all times. To do this, they need alarms from the important faults, but the total number of alarms needs to be limited, to avoid information overload.

A new intelligent alarm processing system using online root cause analysis has been installed at HOPS and was evaluated during 2015. The results from the month of November and from four selected incidents have been presented. The amount of alarms in the IAP tool is very low, which means that the alarm load fulfills the EEMUA criteria, even under upset situations. The IAP identified the correct original faults in each case. The conclusion is that intelligent alarm processing with on-line root cause analysis provides a way of fulfilling the EEMUA criteria, and thus is an ideal tool for supporting the operators and dispatchers in maintaining situational awareness.

The experiences of the installed IAP tool have been very positive. However, the evaluation has also provided several new ideas for improved functionality. Concerning the software itself, the principal vendor is developing additional functionalities, such as light web clients, improved possibilities for replaying events, and efficient generation of reports.

Decision support tools installed in HOPS grid control rooms are: smart visualization, intelligent alarm processing and lightning detection. They are a great improvement of the operational conditions in the control centers, for all operators and especially for the dispatchers. The understanding of events is enhanced, the reaction time is reduced, and decision making is facilitated.

BIBLIOGRAPHY

[1] Andersson, P. and J. E. Larsson, "GoalArt System Proven during Outage," 13th International Workshop on Electric Power Control Centers, EPCC 13, Bled, Slovenia, 2015.

[2] Candy, R., and J. Taisne, "Advanced Alarm Processing Facilities Installed on Eskom's Energy Management System – IEEE PES Power Africa 2007," Conference and Exposition, Johannesburg, South Africa, 2007.

[3] EEMUA, "Alarm Systems: a Guide to Design, Management, and Procurement," Publication 191, Third Edition, EEMUA, London, 2014.

[4] Larsson, J. E., "Diagnostic Reasoning Strategies for Means-End Models," *Automatica*, vol. 30, no. 5, pp. 775-787, 1994.

[5] Larsson, J. E., "Diagnostic Reasoning Based on Explicit Means-End Models," *Artificial Intelligence*, vol. 80, no. 1, pp. 29-93, 1996.

[6] Larsson, J. E., "Simple Methods for Alarm Rationalization," Proceedings of the IFAC Symposium on Artificial Intelligence in Real-Time Control, Budapest, 2000.

[7] Larsson, J. E., "Primary Faults in Alarm Cascades," Final report, Energy Research and Swedish Energy Authority, 2016, to appear.

[8] Larsson, J. E., "On-Line Root Cause Analysis for Large Control Centers," Proceedings of the 8th International Workshop on Electric Power Control Centers, EPCC 8, Les Diablerets, Switzerland, 2005.

[9] Larsson, J. E. and J. DeBor, "Real-Time Root Cause Analysis for Complex Technical Systems," Proceedings of the Joint 8th Annual IEEE Conference on Human Factors and Power Plants and 13th Annual Workshop on Human Performance / Root Cause / Trending / Operating Experience / Self Assessment, Monterey, California, 2007.

[10] Larsson, J. E. and S. Lee, "Managing Information Overload in Power Grid Control Centers," 9th International Workshop on Electric Power Control Centers, EPCC 9, Ullensvang, Norway, 2007.

[11] Larsson, J. E., B. Öhman, and A. Calzada, "Real-Time Root Cause Analysis for Power Grids," Proceedings of Security and Reliability of Electric Power Systems, CIGRÉ Regional Meeting, Tallinn, Estonia, 2007.

[12] Southam, T., "Alarm Management Presentation - An Introduction," PTP-Global, 2013.

[13] Taisne, J., "Intelligent Alarm Processing for DMS Based on the Chronicle Concept," Proceedings of CIRED, the 19th International Conference on Electricity Distribution, Vienna, 2007.