# CYBERSECURITY FOR MODERN DISTRIBUTION AUTOMATION GRIDS

Jean-Luc BATARD
Schneider Electric - France
jean-luc.batard@schneider-electric.com

Yves CHOLLOT
Schneider Electric - France
yves.chollot@schneider-electric.com

Patrick PIPET
Schneider Electric - France
patrick.pipet@schneider-electric.com

Ludovic LAMBERTI
Schneider Electric - France
ludovic.lamberti@schneider-electric.com

Adam GAUCI
Schneider Electric - France
adam.gauci@schneider-electric.com

## *ABSTRACT*

*Strong evolutions are taking place for a modern Distribution Automation Grid, with increased missions generating more and more reasons for Cybersecurity.*
*New control technologies with fast and wide area communication will require a modern approach addressing cyber security aspects, for design as well as for operation phases.*
*This paper describes the perspectives for the design of distribution automation architecture and devices addressing the cyber security aspect of the modern grid.*
*It refers to topics such as data encryption, secured communication protocol implementation and routine security procedures to protect the distribution grid against cybersecurity attack and unintentional misuses.*

## AN ACTUAL CHALLENGE FOR MODERN DISTRIBUTION GRIDS

Distribution Grids are quickly evolving addressing new values:

### Enriching feeder capabilities

Deploying intelligent devices on the feeder increases Utilities' ability to manage assets remotely.
Sophisticated, meaningful data are shared among mobile field crews, remote operators, and maintenance centers thanks to smart communication standards.
More accurate information about asset behavior enables Utilities to reduce the number of costly field maintenance visits, and even more, to keep equipment operating efficiently with proactive actions.

### Optimizing assets

The MV/LV substation is becoming the cornerstone of distributed automation to help Utilities improve power quality and assets' lifespan.
Smart controllers (feeder RTU) can maximize the benefits of smart assets by hosting some local automation and by communicating with control centres or with other substations.

### Increased Cybersecurity needs

Distribution grid faces a lot of new challenges to integrate all these aspects in the coming years. Cybersecurity is clearly one of them:

- New control technologies with fast and wide area communication will require a modern approach of the distribution grid addressing cyber security aspects.
- This need is increased by the enlargement of applications addressed, multiplying the number of actors, accesses and data exchanges.
- Also interconnection needs are growing tremendously (e.g. interconnections with Information System and not only with Control Centre)

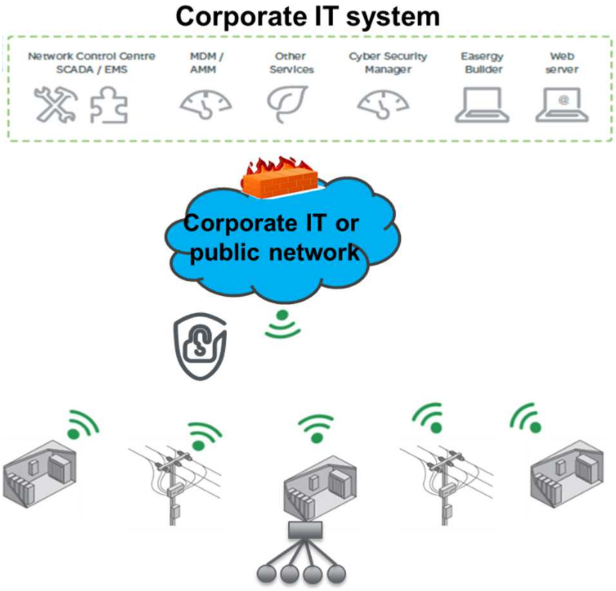


*Figure 1: Increased variety of interfaces & data flows*

Also:

- Cybersecurity aspects have to be addressed during definition phase to cover operational phases, but more globally it has to be considered during whole System lifetime, from definition to end of life. (especially as it copes with confidentiality aspects).
- Scope itself is quite significant as purpose is to protect against ill-intended attackers but also unintentional misuse.
- And all these points have to be addressed ensuring interoperability of components coming from various actors of different maturity levels, over a large diversity of device types, coping with consequent installed basis.

Therefore, modern distribution grid will address critical security issues, company process making security requirements a must for the various devices and infrastructure of the distribution grid.

It is then of outmost importance to be aware that Cybersecurity will rely on Devices & System features, but also strongly on Process and People aspects, generating need for adequate services. Current article will focus on design aspects both at Device and System level).

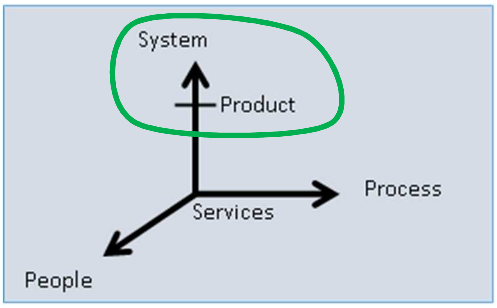


*Figure 2: A multidimensional problematic*

Please refer to [1] for considerations on process.

## TECHNICAL PREVENTION MEASURES TO AVOID BLACKOUT

The distribution automation architecture is made of thousands devices installed on large areas for underground and overhead electrical stations.

First of all, Distribution Grid plays a key role on security and energy availability.

Typical risks could be unwanted operation of switchgear or setting change making transfer automatism not operational. Both of them could lead to blackout, by opening a line or not switching to backup source.

Compared to a pure information system, Distribution Grid faces numerous keypoints:

- Access to each distribution RTU may prove difficult, often spread geographically, in isolated locations and visited only occasionally,
- Communication channels are often of limited bandwidth,
- Power consumption is critical, especially to ensure a good autonomy on batteries when main power is down to enable quick diagnosis and power restoration,
- Devices mostly embeds a single firmware with proven performances, ensuring functional safety missions.

The modern grid approach will as any information system identify key system vulnerabilities, assess the threats, evaluate the consequences of cyberattack and implement countermeasures or mitigation actions. But solutions shall take into account the specificities listed before.

Part of prevention may be done at design time, be it at device or system level. More will be achieved by permanently monitoring vulnerability alerts and upgrading system accordingly. And defining appropriate incident response management process & plan will prove necessary.

For doing so modern Distribution systems will leverage technologies of all grid components, from RTUs to Client devices, such as SCADA/DMS, a mobile maintenance actor or an Information System actor.

See [2], IEC 27000-1 standard for complete view about classical problematics to be solved.

Basic design policies will typically include:

- Robust design with clear interfaces and data check
- Access Control based on Roles, with limited access rights per user depending on its assigned roles
- Closing any unused com protocol ports
- Logging and monitoring of security related events
- Secured protocols implementing authentication and data encryption (SSH, Https over TLS, …)
- Testing against ill-intended penetration attack

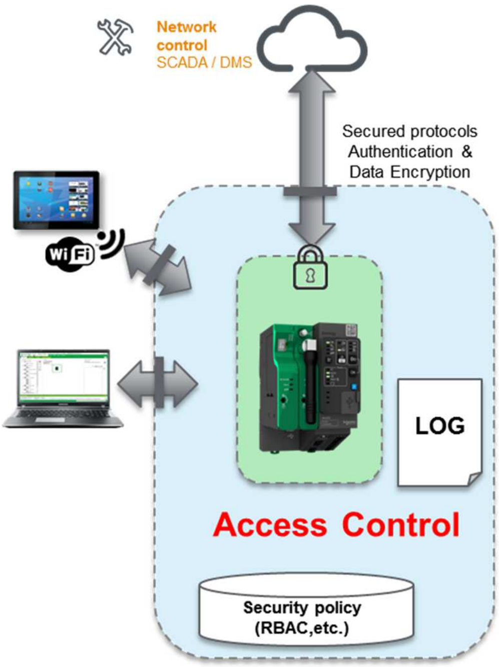


*Figure 3: Role Based Access Control& secured protocols*

Special focus shall be put on Web applications.

Implementation of similar protections on messaging protocols will depend on interoperability constraints and state-of-the-art and develop over time.

In order to maintain the system prevention level and react on alerts, system components will also provide necessary features to support system upgrade such as:

- Easy Firmware upgrade or patching, checking files integrity and robust to abort,
- Back-up and Restore facilities, for managing configuration data and firmware,

• Means to manage user accounts from a central point to ensure consistency.

**Robust Design**

Robust design with well-defined interfaces and data check is fundamental. E.g. it is the key to:

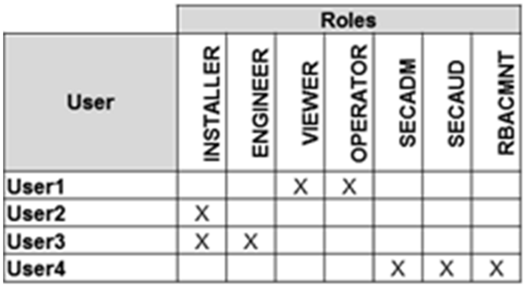
• Avoid penetration by letting attackers alter product behaviour by introducing wrong data in exchanges

• Enable to close com ports not used in a given configuration so reducing again the possibility for attackers to find entry doors (this may be defined through static rules depending on the configuration choices)

**Role base access control (RBAC)**

RBAC is at the core of the measures at device level, limiting the probability of misuses like unwanted setting change which may change the behaviour of system like fault detection, conditions to start a transfer automatism, …

Every user is limited to the access rights related to its role Every access is logged in the security log, enabling to discover attack attempts.



| | Roles | | | | | | |
|---|---|---|---|---|---|---|---|
| User | INSTALLER | ENGINEER | VIEWER | OPERATOR | SECADM | SECAUD | RBACMNT |
| User1 | | | X | X | | | |
| User2 | X | | | | | | |
| User3 | X | X | | | | | |
| User4 | | | | | X | X | X |

*Figure 4: Assigning Roles to Users*

**Efficient Firmware Upgrade requirement**

Providing ways to upgrade the firmware remotely e.g. through webserver or SSH commands to ensure some automation of deployment will enable to deploy countermeasures when new vulnerabilities are found. Devices will protect themselves in case of abort with possibility to restart on previous firmware version.

Then there is no need to visit each distribution substation individually.

Firmware upgrade has however to be executed under full responsibility and control of the Utility, from within its private secured Information System.

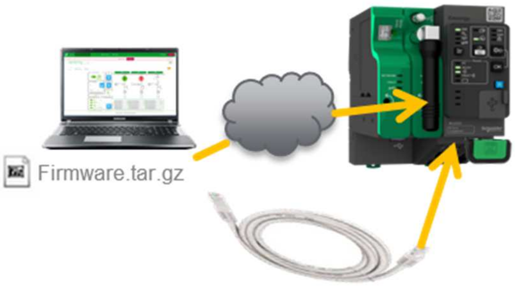


*Figure 5: Efficient firmware upgrade requirement*

**Secured protocols**

Usage of Secured protocols implementing authentication and data encryption is fully necessary to secure Web Applications and file accesses, as they may be clear open doors to intruders once the Utility Information System is penetrated.

It was more disputable for messaging protocols within systems dedicated to electrical industrial domain requiring a specific encoding. Nevertheless, securing also this communication channel becomes more and more valid. Usage of these protocols in a secured version as defined in IEC62351 standards over IPSEC or TLS will deploy progressively, when corresponding protocol stacks will be made available and included in both SCADA's and RTUs.

**Backup & Restore**

Ability to provide Backup and restore facilities of device configuration & settings both on external devices and local copies ease and secure changes and firmware upgrades, enabling to return easily to validated configurations. It also enables for incident response to check if settings have been modified against reference version and reload them in case of doubt.

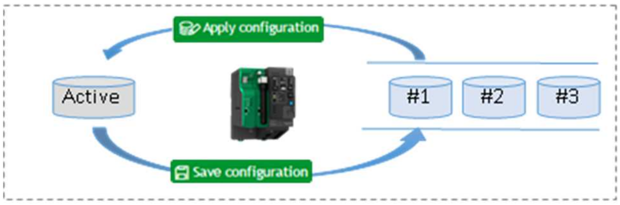


*Figure 6: Flexible Configuration Backup & Restore*

**System Architecture first**

At system level, architecture definition is of course a key step, e.g. separating or not the different information flows and subsystems. Consistent interfaces have to be specified in details.

Thorough analysis has to be made to implement barriers and countermeasures at relevant levels, avoiding to overload every system component with unrealistic features and constraints.

This is especially relevant for Distribution Automation, considering the number of distributed devices and global cost of the architecture compared to classical information systems.

We have to imagine Utility managing hundreds of RTUs in their system! Solutions shall prove efficient and realistic to cope with platform prices, bandwidth usage and consumption constraints.

E.g. typically RBAC policy has to be supported at RTU level to restrict operation access at process level.

At the contrary, it would be counterproductive to integrate firewall in RTU. Such barrier make sense only at relevant interfaces in the system, typically to insulate Electrical Distribution process part from Information System and extranet accesses.

So definition of addressed scope is always a must when considering an actual installation deployment.

## LARGE IMPACT ON UTILITIES AND OTHER ACTORS: BE FUTURE READY

Impacts on the different actors are quite broad to ensure an actual Cybersecurity management. Some typical but not exhaustive key points directly related to the technical part are presented hereafter:

### Be ready for significant investments

Too many control devices in use on today's grid do not have the bandwidth, processors and capacity to be upgraded in order to apply state of the art cybersecurity features. They will have to be replaced.

- This will require at manufacturer level to provide new richer & robust devices, embedding relevant security features, together with associated tools and documentation
- This means for Utilities to be ready for progressive & cost significant upgrade of existing grid control system,
- Contractors & System Integrators shall ensure that proposed solutions are robust and consistent, providing adequate documentation to their customer for safely starting and operating the delivered subsystem. They shall pay express attention to interoperability aspects.

### Need for global Cybersecurity Management Policy

All actors shall become ready for key implementation steps:

- Well identify system levels and subsystems
- Well identify responsibility perimeters
- Identify and manage related Interoperability requirements
- Take into account cybersecurity aspects for Request for Projects, selection of components and suppliers
- Implement System Hardening at installation time, typically resetting default user accounts
- Archiving of configurations

### Efficient firmware upgrade deployment

A typical impact on Utilities will be the need to upgrade installed basis at relevant pace or on critical events.

This is a very significant change compared to common usages to stick to an already qualified version. It will also require definition of efficient and robust means and processes to achieve these upgrades.

Impact is also quite larger as what we know in our day to day life on personal computers, considering the fact that devices firmware's are not really designed for local patch management as on laptops operating systems.

Firmware upgrade has to executed under full responsibility and control of the Utility, from within its private secured Information System.

Utility shall implement an offline test process based on its own configuration and application to approve any firmware updates that may need to be applied.

Also risks of impact on day to day operation and functional safety has to be taken into account.

### How will Utility manage all its users through time?

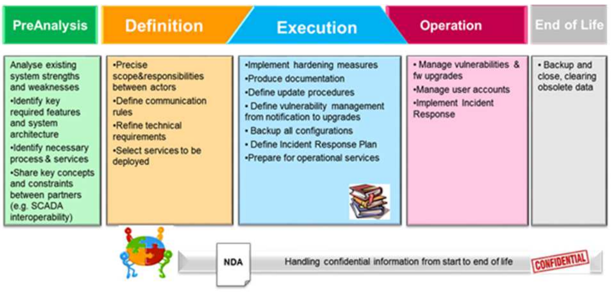
Constraints appear until end of life as for example user accounts and access rights have to be managed, not putting at risk other system parts remaining active neither proving information on company's security data (e.g. many Utilities have the requirement to remove access to systems within 48 hours after employee departure).

Emerging implementation of known solution from IT world (e.g. tools using Radius servers) will enable to manage them from a central point ensuring consistency through whole system, provided sufficient bandwidth is available.

This means actors have to take into account all these elements for every new project starting from definition phase to end of life.

Of course very significant impacts also exist regarding process and people not addressed here like:

- Managing confidentiality aspects and data exchange
- Training People
- Identifying and Managing vulnerabilities,
- Managing User accounts through evolution of the organization



| PreAnalysis | Definition | Execution | Operation | End of Life |
|---|---|---|---|---|
| Analyse existing system strengths and weaknesses<br>•Identify key required features and system architecture<br>•Identify necessary process & services<br>•Share key concepts and constraints between partners (e.g. SCADA interoperability) | •Precise scope&responsibilities between actors<br>•Define communication rules<br>•Refine technical requirements<br>•Select services to be deployed | •Implement hardening measures<br>•Produce documentation<br>•Define update procedures<br>• Define vulnerability management from notification to upgrades<br>• Backup all configurations<br>• Define Incident Response Plan<br>•Prepare for operational services | • Manage vulnerabilities & fw upgrades<br>•Manage user accounts<br>•Implement Incident Response | • Backup and close, clearing obsolete data |

*Figure 7: Constraints appear through whole lifecycle of the Distribution Grid System (examples)*

## ORGANIZE: A MUST FOR A CONSISTENT PROGRESSIVE APPROACH

Cybersecurity has to be addressed ensuring interoperability of components coming from various actors of different maturity levels, over a large diversity of device types, coping with consequent installed basis.

Therefore, a common framework and understanding mixing device manufacturers, solution providers and Utilities/Large Private Customers would help to deploy and ensure consistency, through a progressive steps approach both for new & retrofit installations.

First step is certainly to raise common awareness of all actors to ensure adequate information exchange and scheduling for each new project and more global roadmaps.

Deployment of Cybersecurity shall recognize the installed basis, diversity of actors and infrastructures
Keypoints are:
➔Ensuring interoperability between clients and servers
➔Provide consistent solutions enabling deployment of realistic and efficient processes
➔Be ready and able to find compromises between security and interoperability
➔Keep sufficient agility to cope with diversity of requirements and evolution speed of environment

Basis is:
• to rely on fully recognized international standards, typically IEC62351 series,
• to manage clear versioning at system level of technical features, standards and processes,

However, being aware that:
• Definition and implementation of such standards goes at different paces
• Cybersecurity is an ever-moving battlefield against attackers
• Leaving sufficient freedom to address local specificities is necessary (telecom infrastructure, distribution system size, …)

All features may not be activated all at the same time, nevertheless Future’s ready devices shall be deployed to open the path for progressive implementation.

Such organisms like NIST or OWASP already registers known vulnerabilities of key software components like SSL libraries.
Similar approaches could be followed for messaging protocols according to IEC 62351 standard series, with smoother approaches to cope with upgrade constraints of installed basis, including functional safety.

## CONCLUSION

Addressing Cybersecurity aspects for Distribution Grids is challenging but unavoidable. It is already on the way and some solutions are available corresponding to today’s state of the art.

Key technical features and precautions at device level enable to reduce significantly the risks, nevertheless main aspects rely in Grid global information System, relevant process deployment and people awareness and skills, through whole grid lifecycle.

Securing the Distribution Grid systems will require a long term resolution of all actors, always keeping in mind however that it is an ever-moving field where genius attackers are proving constant innovation.

Impact on installed basis, diversity of distribution grids and involved actors is anyway so significant that it requires to go through a progressive approach.
Interoperability based on open standards together with consistent version management is a must.

## REFERENCES

[1] A.Gauci, Mathieu Salles, Sébastien Michelin, 2017, " Addressing the Challenge of Cyber Security Maintenance through Patch Management", CIRED conference, 252

[2] ISO/IEC 27001, 2013, “Information technology - Security Techniques - Information security management systems — Requirements”.