University of Exeter

Centre for Smart Grid

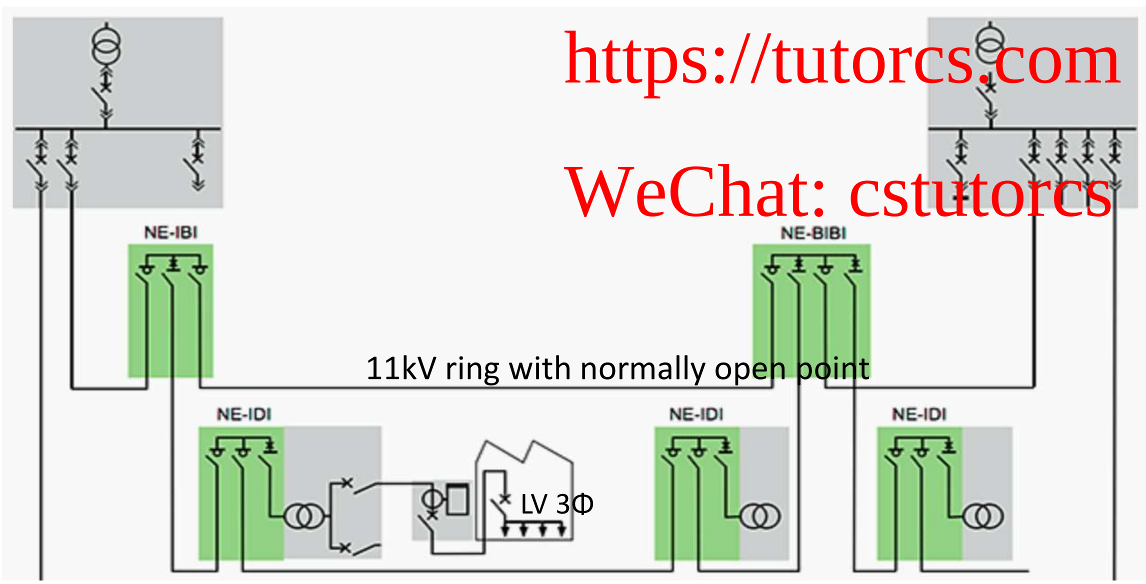
L5 ENGM031

Automation in Distribution Networks

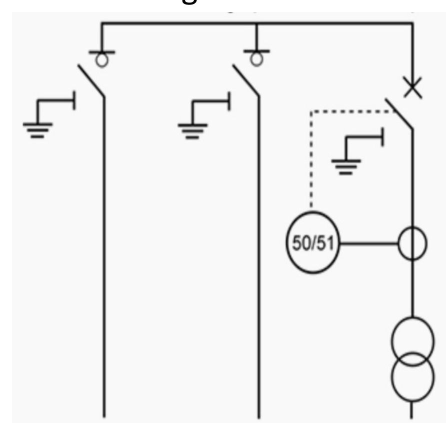
Prof Peter Crossley

Distribution Networks

- Distribution network links transmission (generation) to energy consumption and is made up of both overhead line (rural) or underground cable systems (urban).
- Secondary distribution is typically the last leg of the HV and LV networks through to the utility meter.
- For a UK DNO: EHV normally means 33kV or 132kV, HV means 11kV or 6.6kV and LV means 230V/400V. Note: International definition normally: MV = 1 – 36kV and HV = 36kV – 220kV.
- Protection and control of secondary distribution is typically through ring main units (RMUs) for underground cable networks and overhead switches for overhead lines.



Ring main unit:

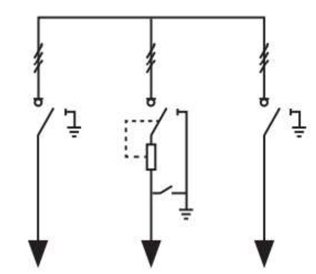


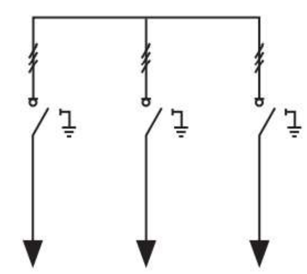
Automation in Distribution Networks

Types of MV switchgear:

- Switch is a piece of equipment used to open an electric circuit by a mechanical action, interrupting the flow of current, without causing damage to the equipment.
  - Switch may either be a disconnector/isolator or a circuit breaker.

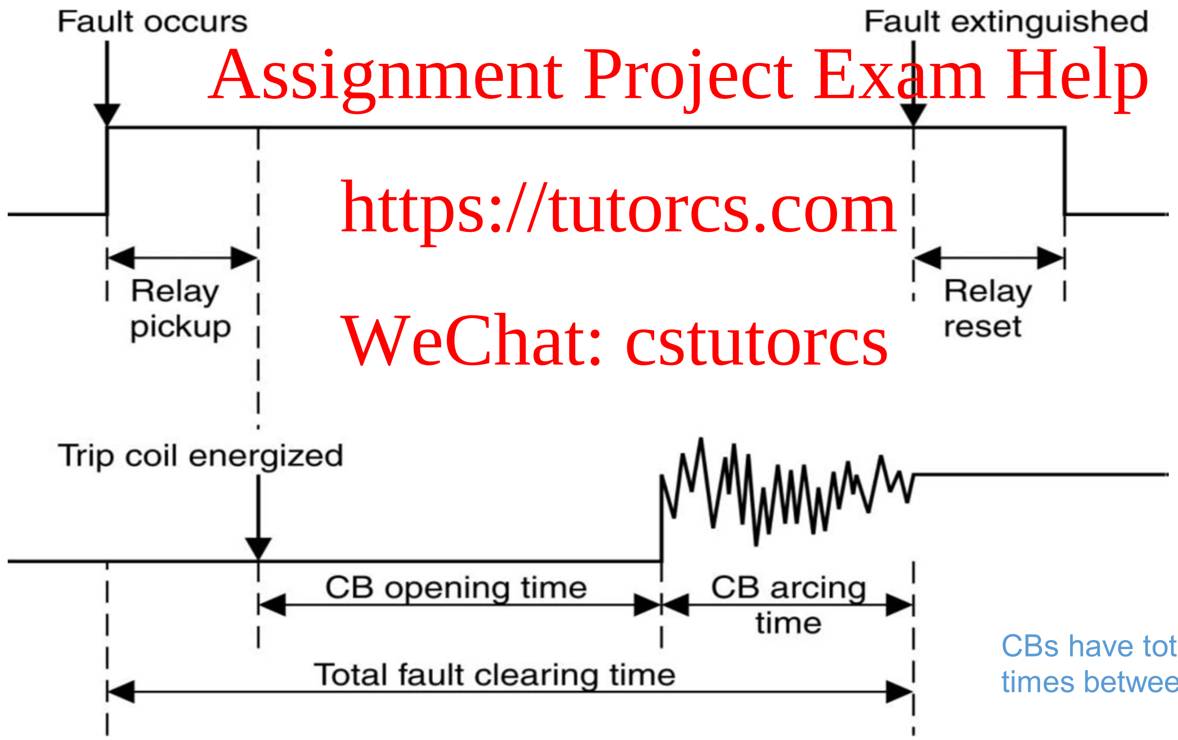
- Ring Main Unit (RMU) is metal enclosed switchgear used at the load connection points of a ring-type distribution network.
  - includes two switches that connect both sides of the load to the main conductors and a fusible switch or circuit breaker that tee-off to an MV:LV distribution transformer.
  - designs use air, vacuum, oil or gas "SF6" insulation and are applicable at 11 – 36kV.





Circuit Breaker:

- Circuit breaker (CB) opens an electric circuit under overcurrent or fault conditions.
  - usually occurs when a trip signal from a protection relay is received.
- CBs have a continuous full load current rating, a fault current rating for a limited time, as well as a fault making- and breaking rating.



CBs have total breaking “opening + arcing” times between 1 and 5 cycles

Secure, industrial grade communication networks are vital for digitization of distribution networks

- Ofgem and UK Government influence the Distribution Network Operators (DNOs) to ensure they satisfy societal requirements for:
  - reliable and resilient high quality electrical power for all consumers
  - affordable and environmentally appropriate electrical energy
  - cost effective integration of low-carbon sources of energy
  - green and sustainable technologies in all aspects of the energy chain
  - encourage greater use of distributed energy resources, especially low carbon sources and storage.

- DNOs want to improve power quality, reduce outage times, and lower operational and maintenance costs.

- These requirements together with changing demand patterns requires the integration of numerous smart devices into the existing electrical grid to ensure it is “future proof”.

- All these devices, including sensors, smart meters, switchgear and Volt/VAR controllers, remote terminal units (RTUs), SCADA outstations generate massive amounts of data.

- Consequently, DNOs need a higher degree of automation, with greater monitoring and control capabilities at all levels of the distribution grid.

- Industrial communication networks deliver reliable, high bandwidth, low latency bi-directional data exchange for distribution network automation and smart grids.

Distribution Network Automation:

- As the societal requirement for Net-Zero impacts the electrical power industry, all GB DNOs are adopting solutions based on Distribution Network Automation (DA).
- Trends that drive the change include:
  - Environmentally-driven policy and consumer adoption of distributed energy resources (DER) requires bi-directional power flows on the distribution grid and DNOs need tools for flow management.
  - Empowerment of third-party alternatives to deliver utility-based power provision, providing consumers with more options. Always been true with industrial or commercial campus level networks, but in future will become common for housing estates etc.
  - DNOs need to engage consumers with new value propositions & programmes to retain their allegiance.
    - In GB, DNOs are hidden behind an energy supplier and consumers do not understand their role.
    - Will new build estates have private electricity networks with community based storage and DG, i.e. micro grids ?
    - What about legacy networks, will these continue to be operated by existing DNOs ?
    - In GB, a DNO is a private monopoly regulated by Ofgem, is this the correct model for a digitised Smart Grid ?
    - Local roads are built and managed by local authorities, why is your local HV and LV electrical grid different ?
    - What we have today was created in 1947, when local authority owned grids were grouped together into regional “nationalised” electricity utilities, e.g. SWEB “South Western Electricity Board. These were privatised in 1989 to form DNOs, ownership changed many times and the 14 licensed DNOs are now owned by six companies.
  - Extreme weather events: experts believe these are increasing in frequency, adding new urgency to improvements in system reliability and resilience to satisfy Ofgem regulatory performance metrics.
  - Grid modernization and utility challenges
  - Digital-age consumers: customers are accustomed to having options, diverse value propositions, rapid resolution of issues, and communications tailored to their specific needs.
  - DNOs must adopt new business processes and operational strategies supported by technology to meet these expectations.
  - Internet of Things (IoT): IoT and an increase in intelligent devices at the grid’s edge require a future facing distribution network designed to operate with real-time monitoring and control schemes.

Distribution Network Automation:

Ref:-usa.siemens.com/ruggedcom

SIEMENS
Ingenuity for life

- Distribution Network Automation (DA) integrated with a high-bandwidth, low latency, communication system is a cost-effective investment that satisfies many of the challenges in evolving passive distribution networks into the smart active grids required in a low-carbon future.
- DA delivers automated responses to power network anomalies and provides improved system visibility for grid operators.
- Challenge lies in selecting a trusted, authoritative advisor with domain expertise in cyber-secure critical infrastructure, industrial control systems (ICS) and strategic data communication networks designed for use in utilities.
- Obviously Siemens considers itself the solution provider for the future, but other companies have similar products and make similar claims.

DA benefits: from cybersecurity to the bottom line

DNOs require:

- **Cyber-secure operational networks** with the ability to detect, isolate and mitigate network intrusions and attacks, minimizing system impacts and boosting investor and consumer confidence in the security of the power grid.

- **Asset management capabilities** to increase system efficiencies and detect and prevent impending asset failures; hence improving reliability metrics, delivering consumer satisfaction and lowering operating costs (OpEx).

- **Fault location, isolation and service restoration** designed to minimise the impact of outages by rapidly restoring supplies to all consumers; again improving reliability metrics and consumer satisfaction.

- **Integrated volt/var control** optimizes distribution feeders to shave peak loads, reduce power losses and avoid voltage violations, operational strategies that lower OpEx and, by managing problematic feeders, can reduce or delay Capital Expense (CapEx).

Distribution Network Automation:

- **DER integration and anti-islanding measures** enable remote monitoring and control of interconnections for micro grids, solar arrays, wind turbines, energy storage to prevent operational challenges from distributed resources.

- **Distribution SCADA** systems are augmented by proper integration with Distribution Automation to achieve a greater degree of functionality in monitoring, controlling and protecting distribution system assets and performance.

- **Substation Visibility** refers to grid operators' ability to monitor substation assets and their status, performance and condition – is strengthened when a Field Area Network (FAN) is implemented in support of Distribution Automation.

- **Mobile workforce automation** enables field technicians to remotely receive work orders, access technical information and securely communicate with their operations center, cutting time, labor and OpEx.

Distribution Network Automation

Ref:-usa.siemens.com/ruggedcom

1. Direct Transfer Trip / Distributed Generation
2. Automatic Transfer Systems
3. Fault Location, Isolation, and Service Restoration
4. Volt/VAR Optimization
5. Substation Automation
6. Distribution SCADA
7. Mobile Workforce
8. AMI Backhaul
9. Subtation Backhaul

How to ensure fast and reliable feeder automation:

- An important function in Distribution Automation is FLISR (Fault Location Isolation and Service Restoration).
- It involves the detection of a faulty segment in a distribution line, then isolation of the fault by performing topology changes in the distribution grid (opening and closing of specific circuit breakers) and finally restoration of the initial topology once the faulty condition has disappeared.
- In the past, when a permanent fault occurred on a feeder, a repair crew had to manually restore the faulted section and this usually required a few hours.

- In modern digital grids it is desired that an automated FLISR algorithm detects and isolates the faulted segment within 100 milliseconds or less.
- Such performance is possible with the use of a distributed architecture with Intelligent Electronic Devices (IEDs) using communications to exchange their status via IEC 61850 fast GOOSE messaging.
- There are examples of real projects in USA and other countries where Siemens industrial wireless communications, both public 4G and private WiMAX, helped to achieve the self healing grid.

Ref:-usa.siemens.com/ruggedcom

Which wireless technology can be used, when no fibre or wired infrastructure.

- Depending on the geographical region and population density there may not be fiber optic or similar wired telecommunications infrastructure to interconnect devices in the secondary distribution grid.
- Wireless communications is a natural choice in such cases. However there is a wide selection of wireless technologies that could potentially be used.
- It is obvious there is no 'one solution fits all' in terms of wireless communications.
- Depending on economical and technical criteria, a choice has to be made between private wireless networks and public cellular networks.
- Private wireless communications such as WiMAX offer higher reliability, high security and OPEX (Operational Expenditure) optimization.
- While public cellular are attractive because of lower CAPEX (Capital Expenditure), faster deployments and good coverage in most parts of the country.
- What is clear, however, is that the solution should be standard based, interoperable, scalable and should support multi-service network infrastructure.

Ref:-usa.siemens.com/ruggedcom

Design of Communication Network for Distribution Automation:

- When designing the network for Distribution Automation, it is important to look closely at the requirements of the different applications that will use the communications architecture.
- Requirements should include number of nodes to be supported, type of ports to be supported (Ethernet, RS232 serial, etc.), required reliability, required data bandwidth, maximum tolerated latency, network redundancy options, time synchronization protocols, need to support multicast traffic, need to restrict data flows to specific locations or devices, monitoring and self-diagnostic requirements, etc.
- In terms of software features, scalability will imply that a rich set of layer 2 and layer 3 communication protocols may be needed.

Ref:-usa.siemens.com/ruggedcom

Supply restoration following a short circuit fault:

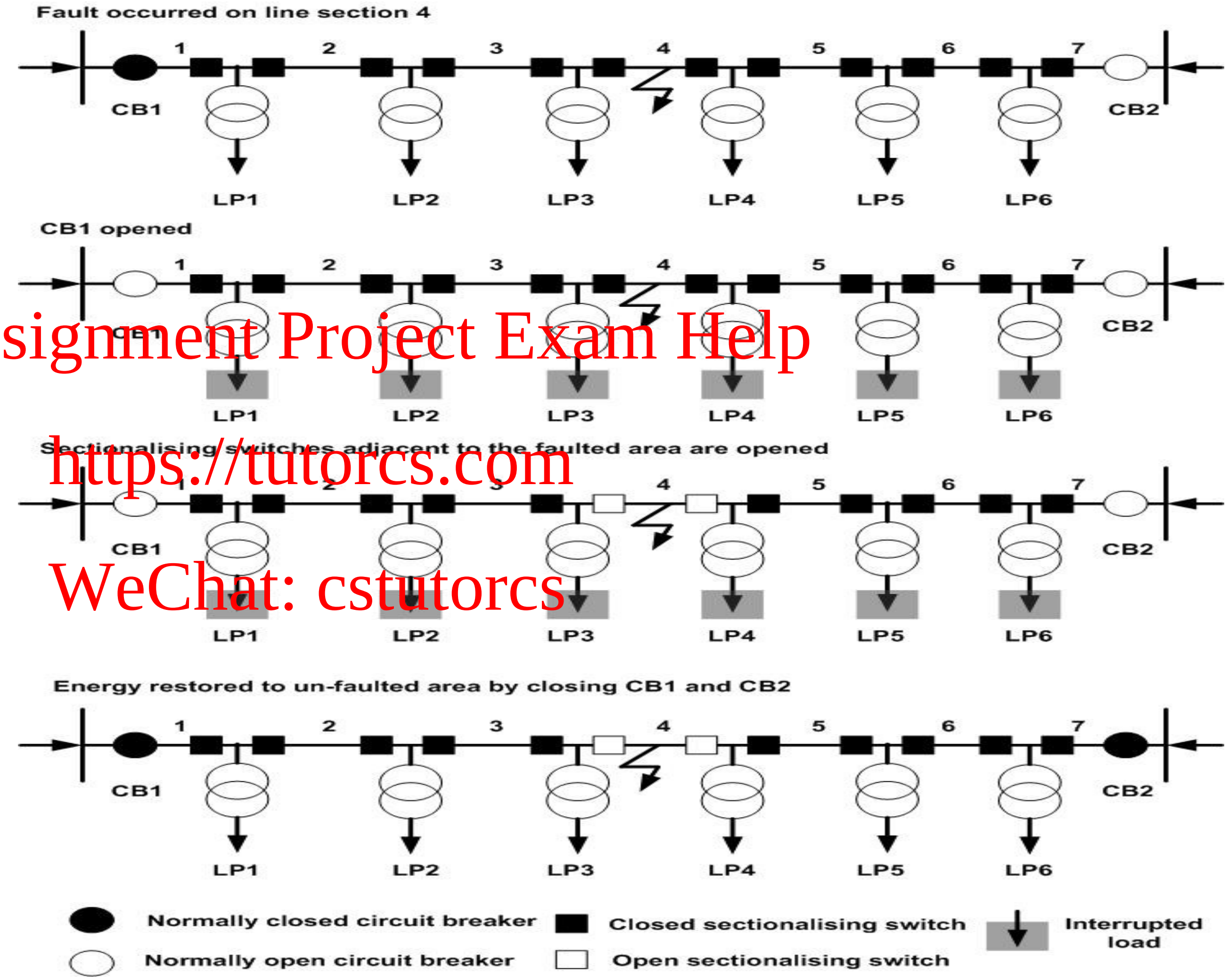
A1. Radial feeder supplied via closed CB1 (CB2 open)
A2. Permanent Fault at 4

B. Protection opens CB1, fault de-energised, but not cleared.

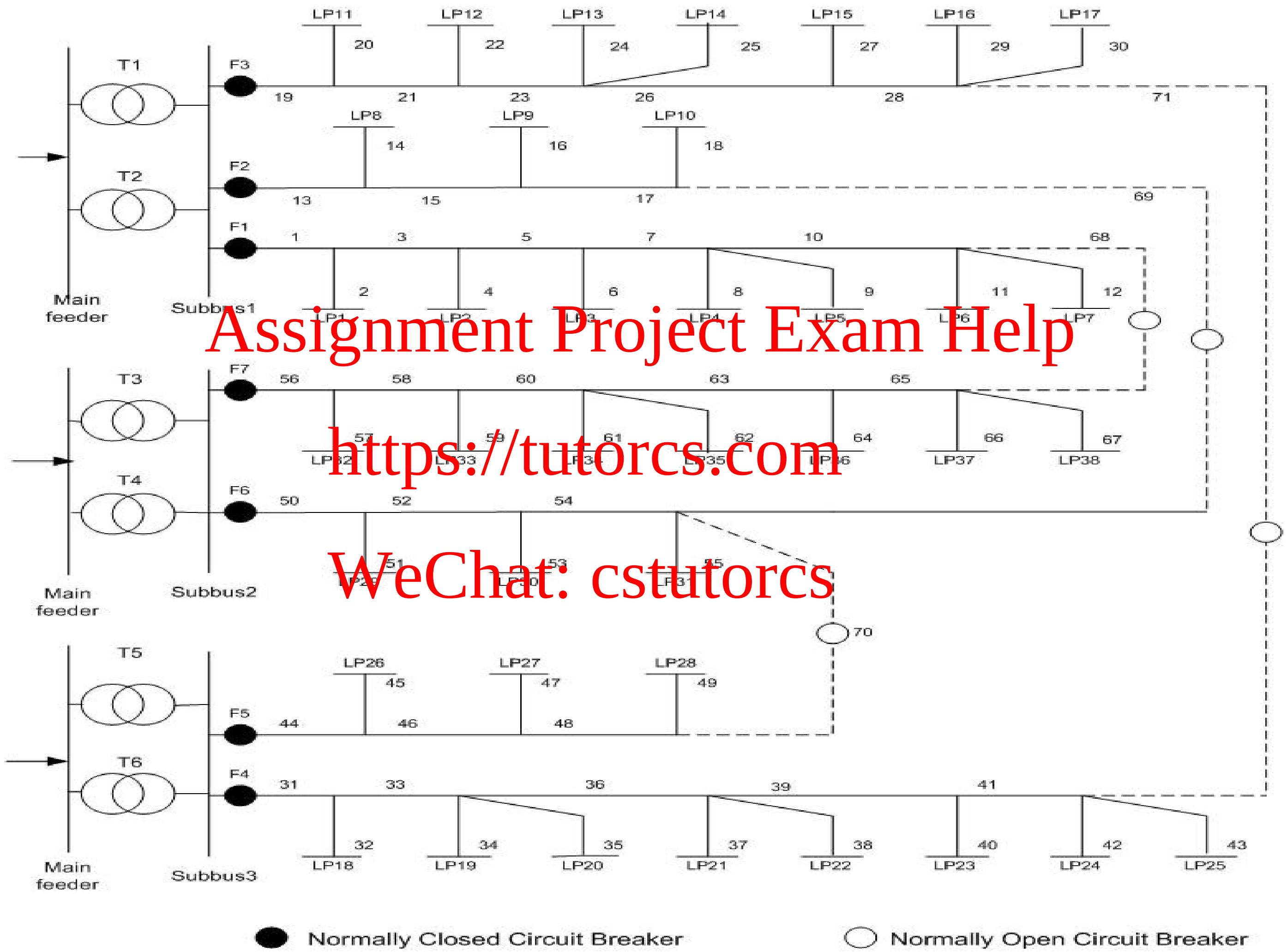
C. Open feeder 4 sectionalising switches using LP3 & LP4 RMUs.

D. Close CB1 and supply LP1, LP2 & LP3.
Close CB2 and supply LP4, LP5 & LP6.

E. Maintenance crews fix line at fault point 4.

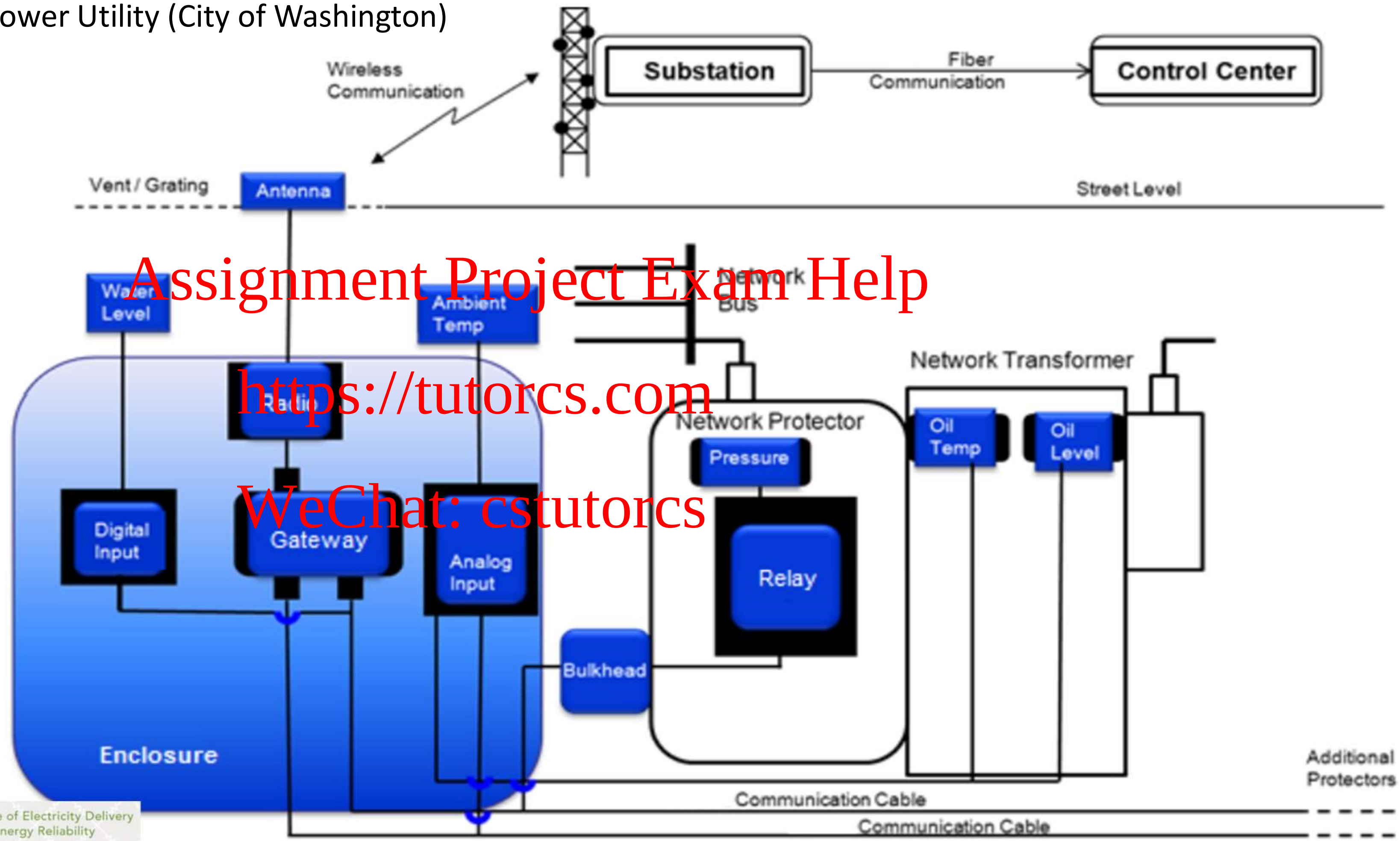


Structure of an urban 11kV distribution network operated radially:



Pepco: Equipment Health Condition Monitoring

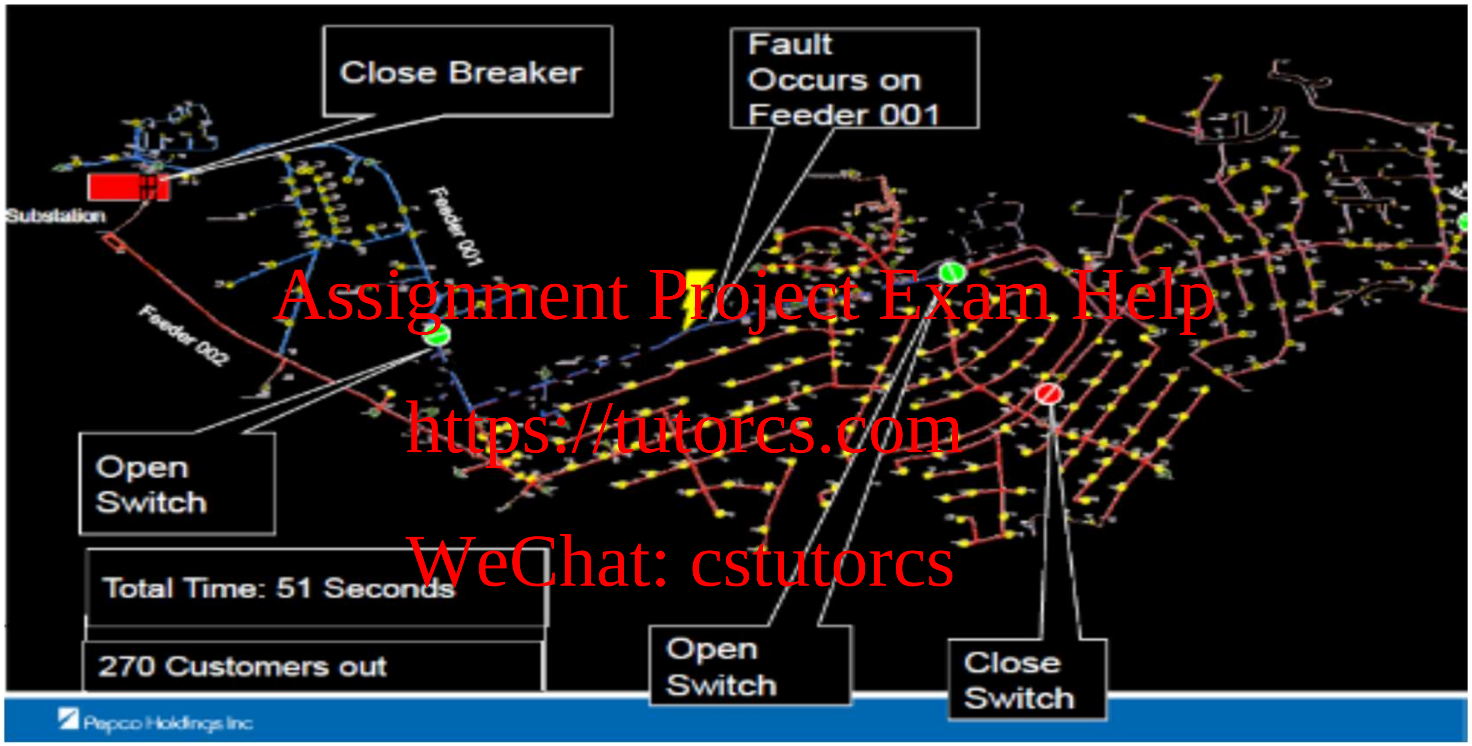
Pepco: Potomac Electric Power Utility (City of Washington)



Distribution Automation
RESULTS FROM THE SMART GRID INVESTMENT GRANT PROGRAM
September 2016

SMARTGRID.GOV U.S. DEPARTMENT OF ENERGY Office of Electricity Delivery and Energy Reliability

Pepco Automatic Sectionalizing & Restoration Schemes Enable Fault location-isolation and service restoration (FLISR):



- FLISR uses an Automatic Sectionalizing & Restoration (ASR) scheme, which segment feeders into 1, 2 or 3 four sections using closed remote-controlled switches or automatic reclosers.

- After the fault has been cleared by supply breaker, ASR opens closed switches to isolate the faulted section. Then, it restores the non-faulted sections by reclosing feeder breakers and/or closing open tie switches to other feeders.

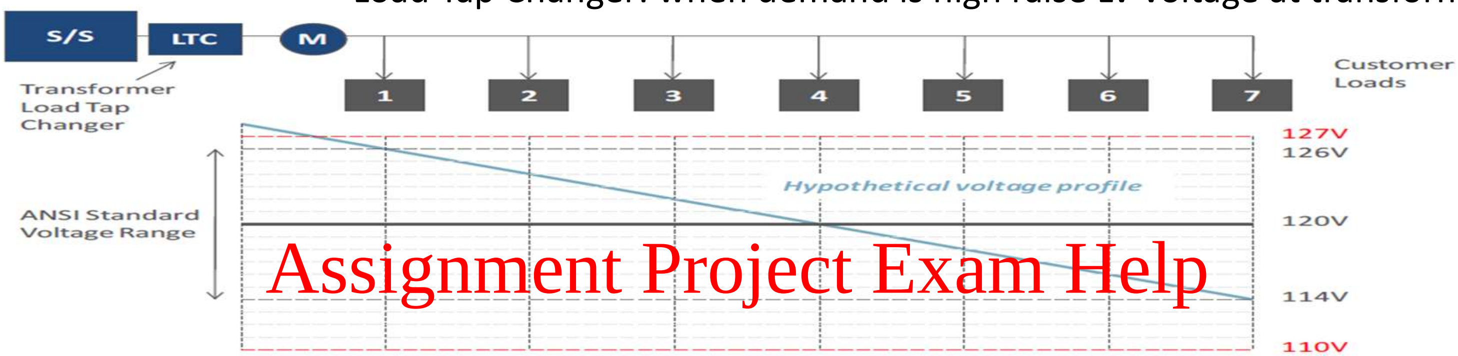
Conservation Voltage Reduction (CVR):

- CVR optimizes distribution asset utilization by using monitoring and automated controls to reduce feeder voltage levels, improve the efficiency of distribution systems, and reduce energy consumption during peak periods or for longer-duration operations.

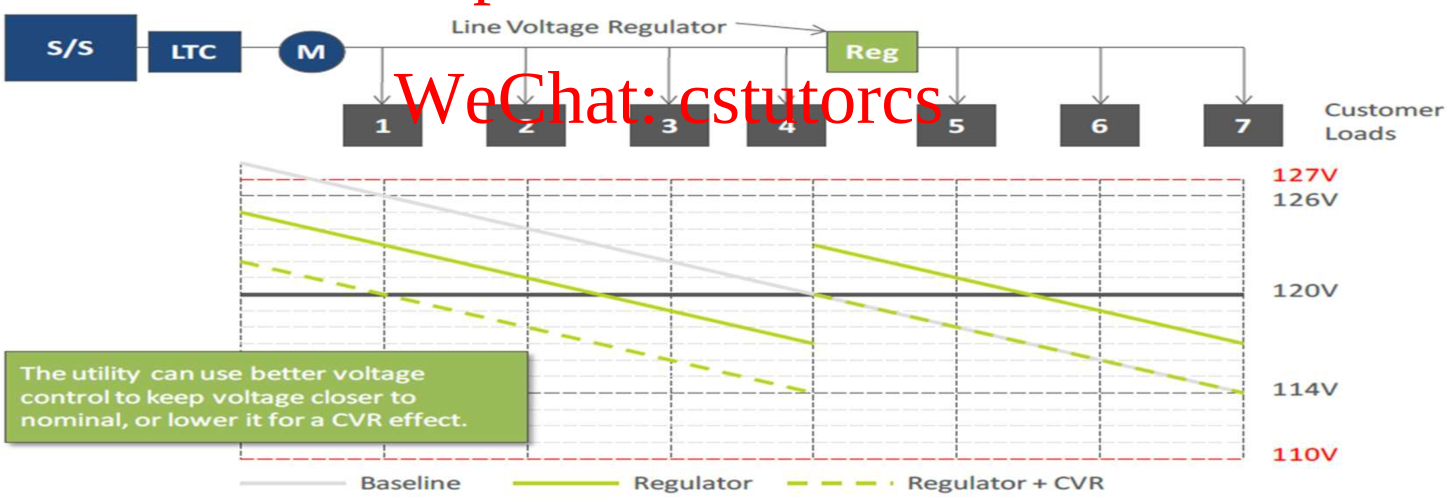
- Typical objectives of CVR include:
  - Management of peak demands through service voltage level reductions, which can reduce electricity consumption of end-use appliances and equipment and reduce customer bills.
  - When implemented during peak hours, CVR actions can supplement traditional demand-side management programs such as direct load controls, time-based rates, and incentive based programs.
  - Duke Energy refers to its CVR actions as "Distribution System Demand Response" for this reason. Duke energy provides electricity to nearly 8m customers in 6 US states.
  - Line loss reductions through feeder voltage level reductions and reactive power management results in lower electric resistance, which improves system energy efficiency and saves energy.

Load Tap Changers and Voltage Regulators:

Load Tap Changer: when demand is high raise LV voltage at transformer:

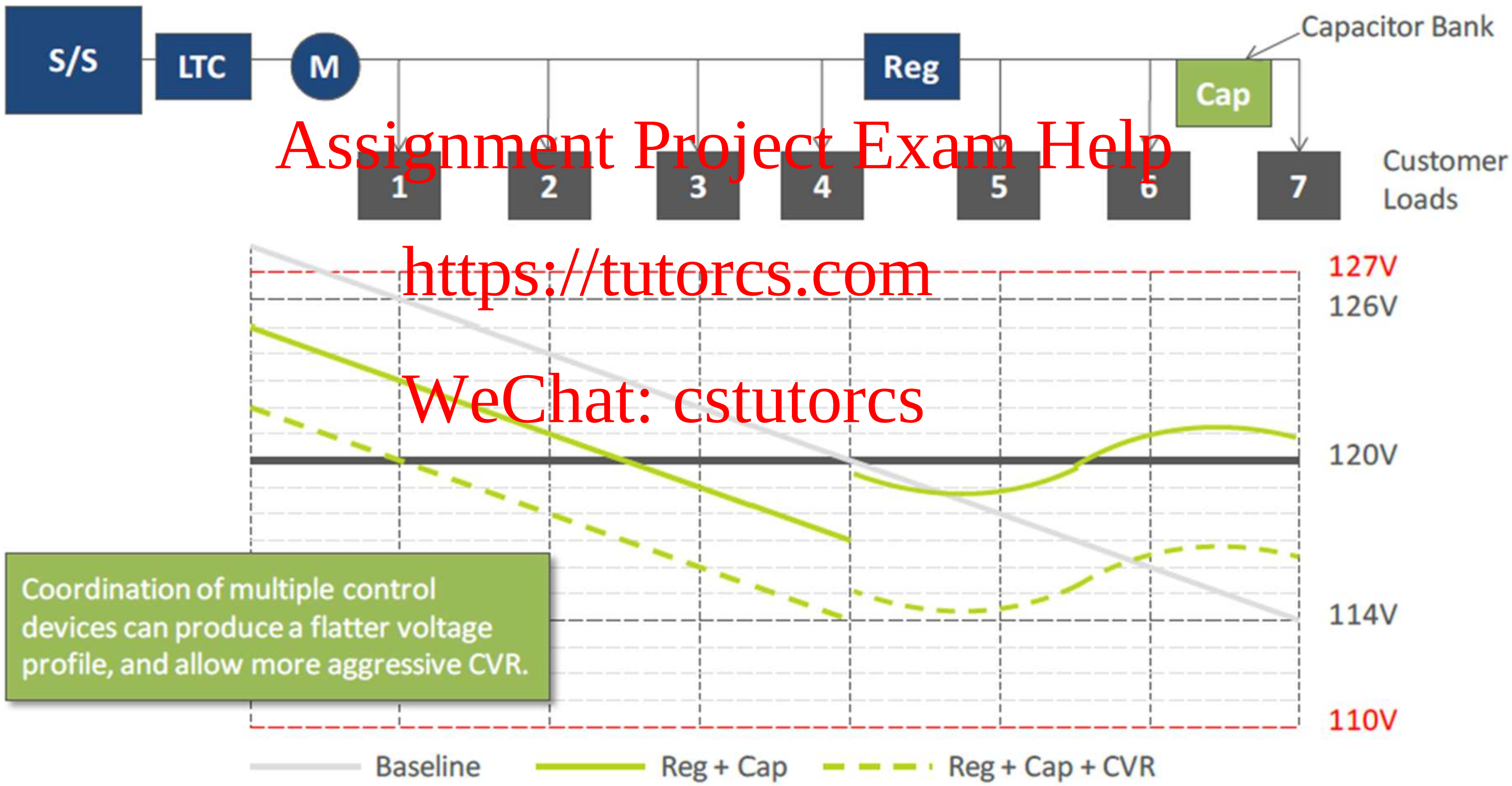


Voltage Control with Load Tap Changer and Line Voltage Regulator:



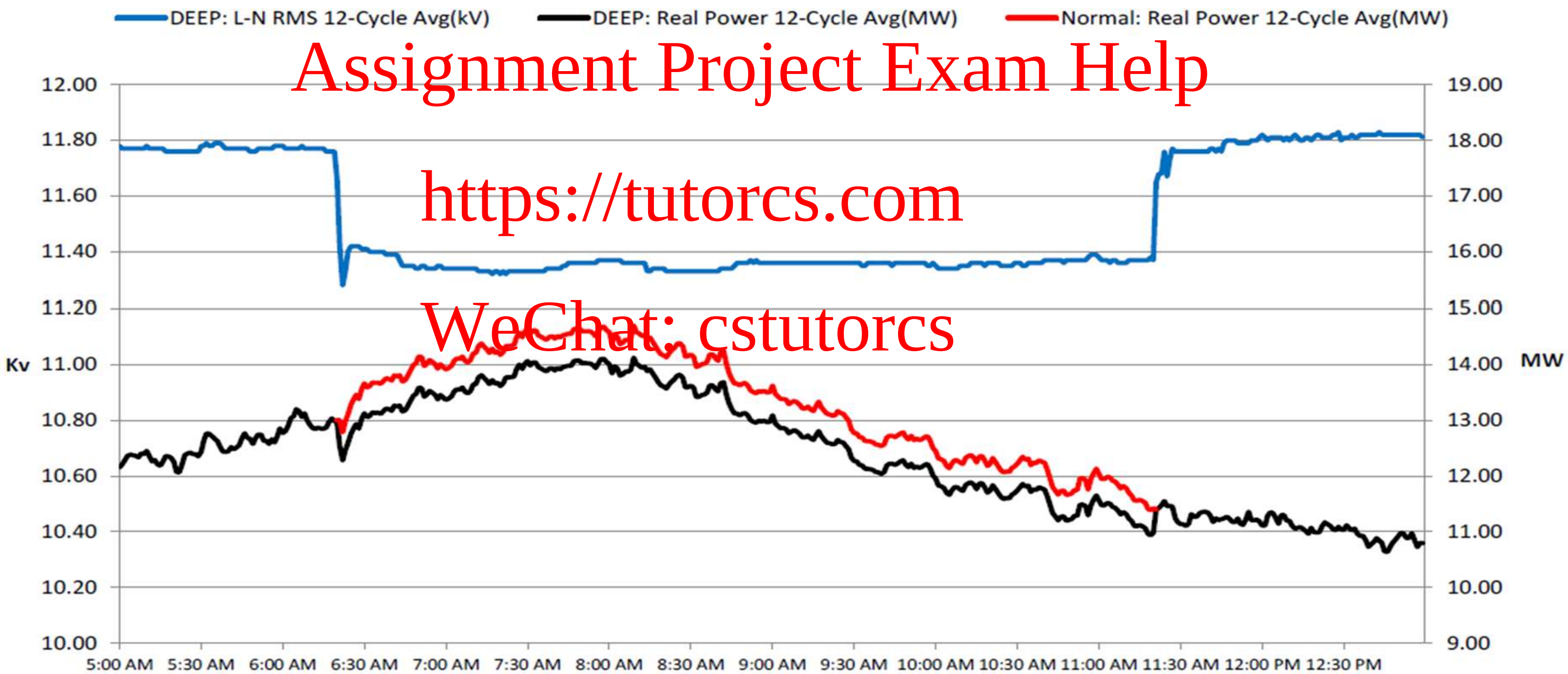
Feeder Voltage Profiles with load tap changer, voltage regulator and capacitor bank:

- Operators can also use capacitors to compensate for reactive power caused by inductive loads; capacitor banks placed along a feeder supports voltage profiles both downstream and upstream.



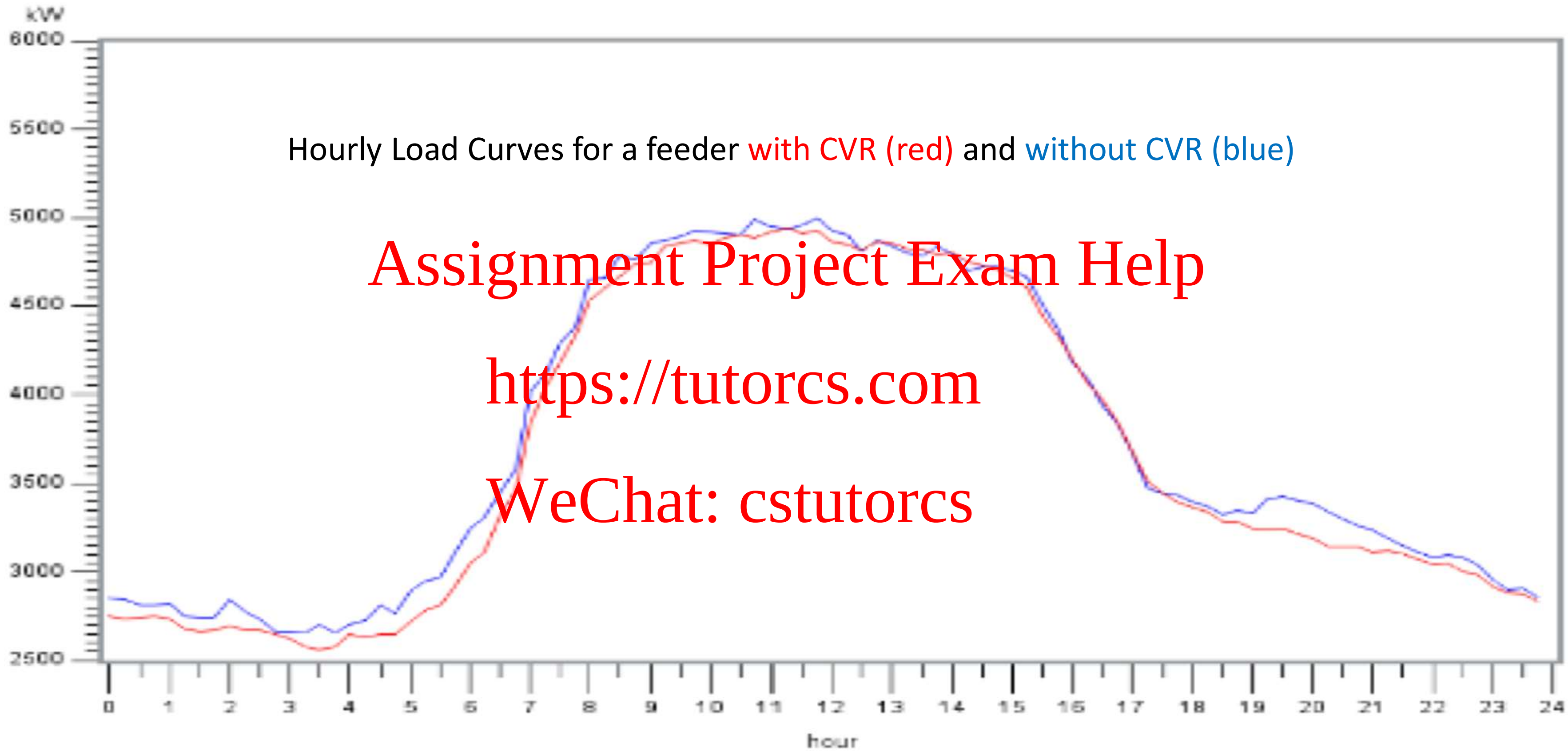
CVR lowers peak load during extreme weather:

- Southern Company (USA) used CVR to shave peak load during extreme weather Jan 2014.
- Load was 20% higher than the forecasted peak load due to low temperature.
- CVR reduced the voltage by 5% for 5 hours, delivered 300 MW of peak reduction
- Reduction helped Southern avoid manual load shedding.



Feeder voltage (blue) dropping ≈11.75kV to ≈11.35kV (3 – 4%) and power dropping ≈ 0.6MW at peak predicted load 14.6MW i.e. ≈ 4%

Avista Utilities expects CVR to save 42GWh in 2014 on feeders that serve residential, commercial, industrial and agricultural customers in Spokane & Pullman, Washington State.



Guess: hourly saving ≈ 100kW for demand varying from 2.6MW to 5.0MW, i.e. 2 - 4% saving depending on time of day. Important times are demand pickup 6am – 8am and heavy load period 8am to 4pm.

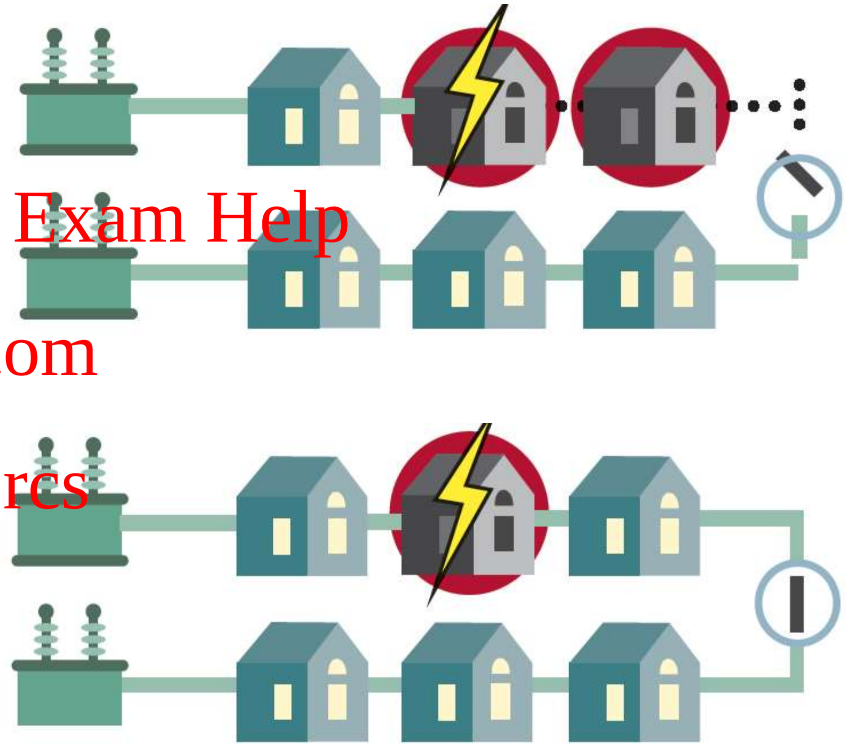
Problem: largest % saving at night when demand is low (kWh cost also low) and voltage probably high.

Making Self-Healing Grids a Reality

S&C IntelliTeam SG Automatic Restoration System

Feeder without Self-Healing:
Automation equipment, e.g. S&C's IntelliRupter® fault interrupters, improves feeder segmentation, resulting in fewer outages for customers upstream of HV main-line faults; but homes downstream of the fault unnecessarily experience a sustained outage every time there's a permanent fault.

Feeder with Self-Healing:
Faults are immediately identified, isolated, and restored to all downstream customers without any human interaction.
By the time a DNO repair crew is notified of the exact location of the fault, most customers are back online.



With a deployment of three automated switches per feeder—two mid-line switches and one tie-switch—DNO may see up to a 50% improvement in reliability on those feeders.

Making Self-Healing Grids a Reality

S&C IntelliTeam SG Automatic Restoration System

When utilities build a self-healing grid, there are three system options: centralized, regional & distributed:

- Centralized systems, such as a Distribution Management System (DMS), take a long time to deploy and are inherently slow.
- Regional systems, such as a substation controller-based solution, are successful for simple circuits but are difficult to scale for complex ones.
- Utilities need a distributed solution where ALL the restoration logic is predefined and resides in the field devices themselves, which makes it fast, reliable, and easily scalable.

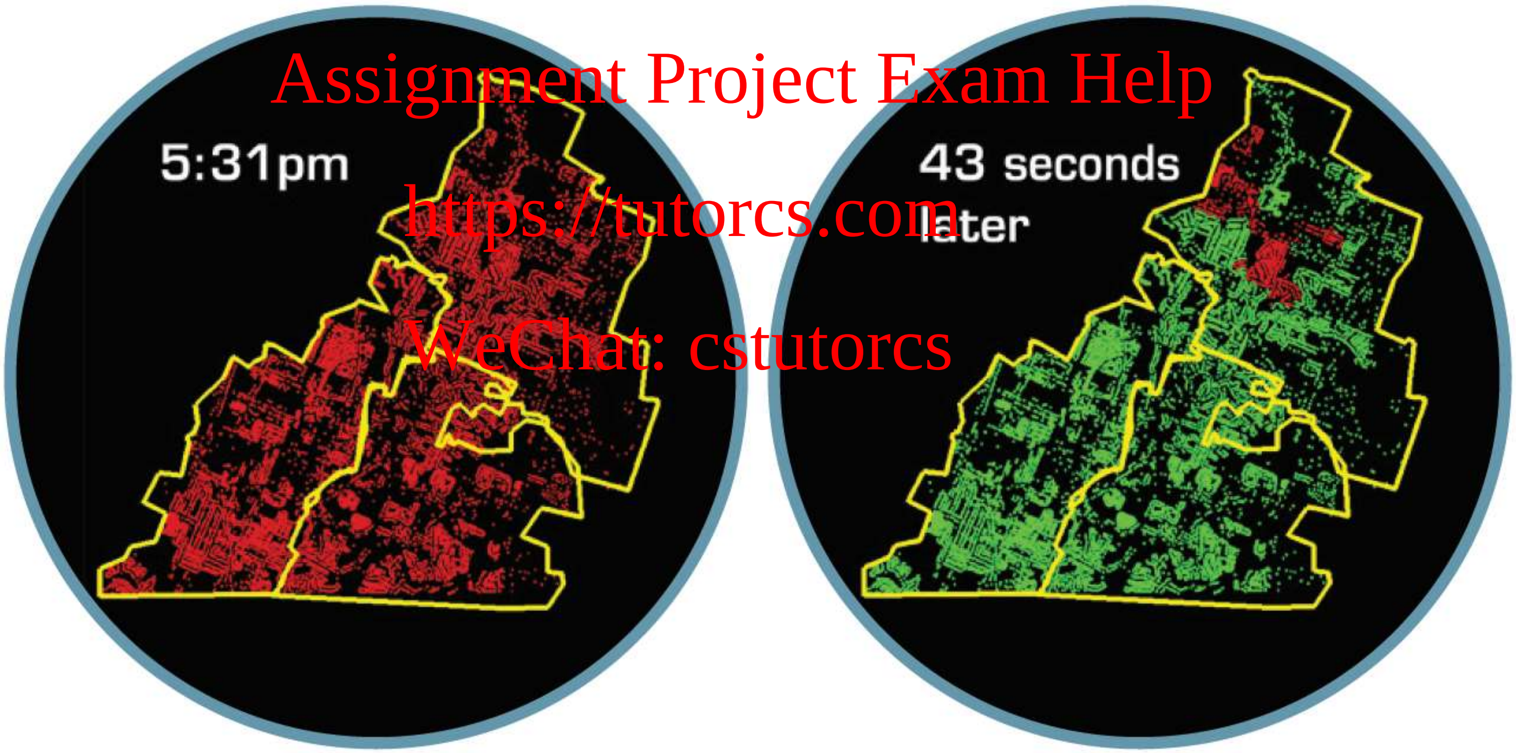
Solution is the IntelliTeam SG Automatic Restoration System.

- IntelliTeam SG system uses advanced controls, network communication, and distributed intelligence to quickly isolate a fault and then restore service to the maximum possible amount of load.
- Distributed approach places logic inside devices, improving scalability and enabling decisions to be made at the edge of the grid.
- Because communications are between local devices, decisions are made faster and more reliably, allowing restoration times of < minute.

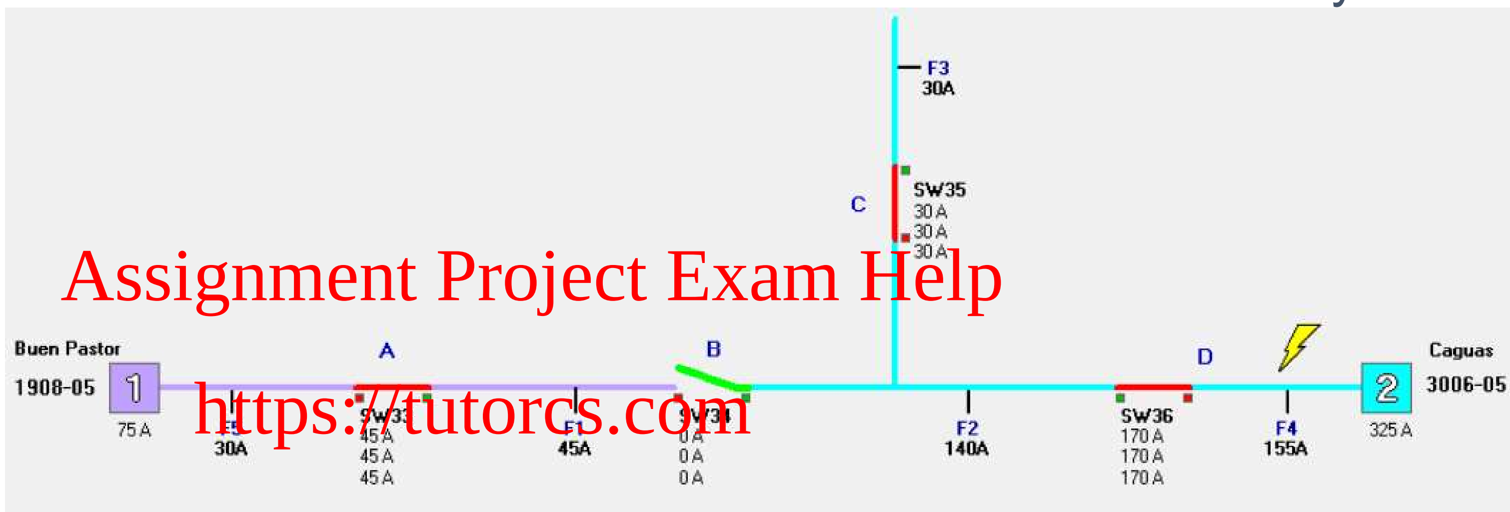
Making Self-Healing Grids a Reality

S&C IntelliTeam SG Automatic Restoration System

- Example: In Jan 2013, a storm knocked power out to more than 11,000 homes and businesses.
- Some 43 seconds later, 95% of these customers were brought back into service.

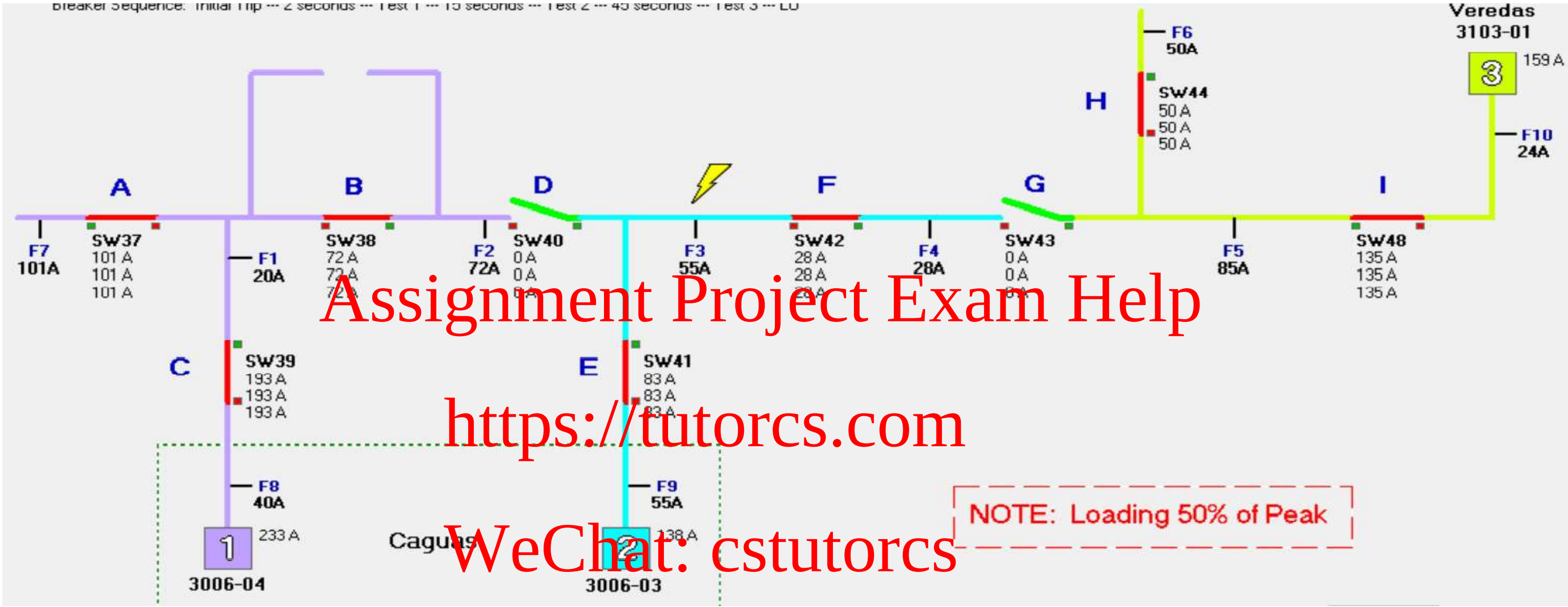


Site Automation Test Proves IntelliTeam® SG Performance at Puerto Rico Electric Power Authority



- Loss-of-voltage event was simulated on the Caguas 05 Circuit.
- After the configured time delay, IntelliRupter D—the switch closest to the substation— opened to isolate the normal source.
- IntelliTeam SG then initiated “Rapid Self-Healing,” and normally open IntelliRupter B closed to restore the entire circuit.
- Normally closed IntelliRupter C did not operate.
- Results were confirmed in real time through SCADA, and it was established that from the time IntelliRupter D opened, restoration took approximately 2 seconds.

Site Automation Test Proves IntelliTeam® SG Performance at Puerto Rico Electric Power Authority



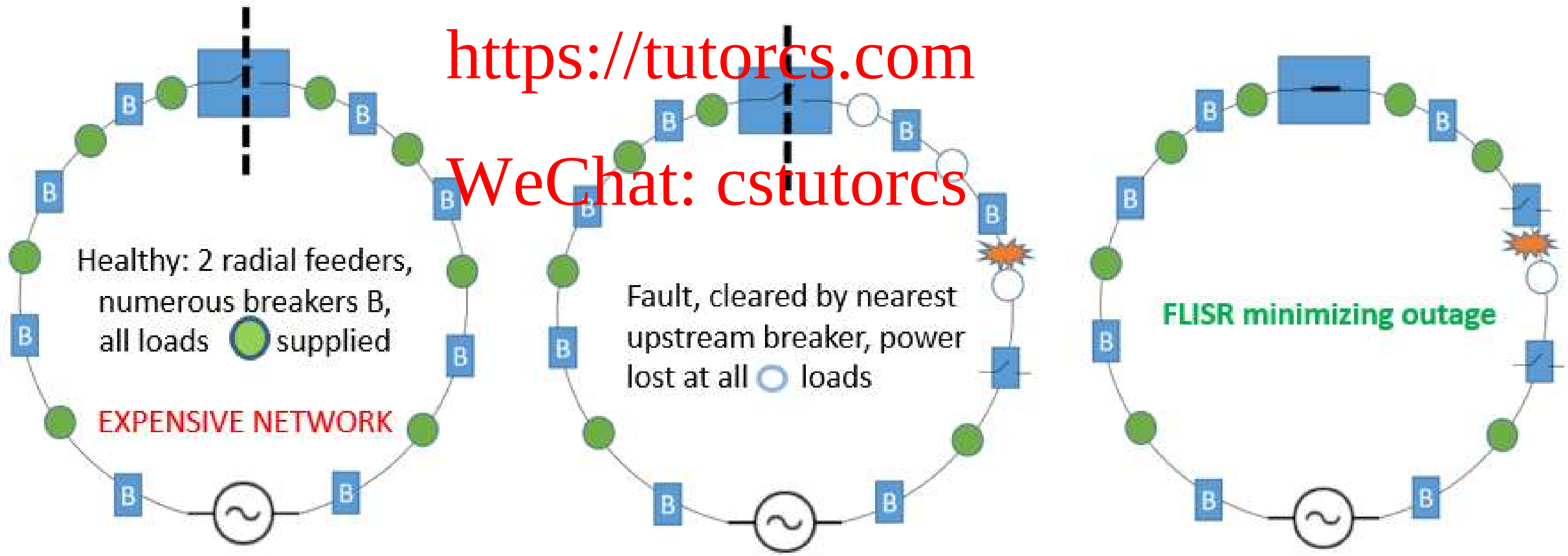
- Fault occurred on Caguas 03 Circuit, downstream of IntelliRupter E.
- After IntelliRupter E locked out due to overcurrent, IntelliTeam SG initiated automatic restoration.
- To isolate faulted section, IntelliTeam SG opened IntelliRupter F, <1s after IntelliRupter E opened.
- Then IntelliTeam SG closed IntelliRupter G—the tie switch to adjacent source.
- Restoration took approximately two seconds..

Cyber Security Considerations for Self-healing Smart Grid Network

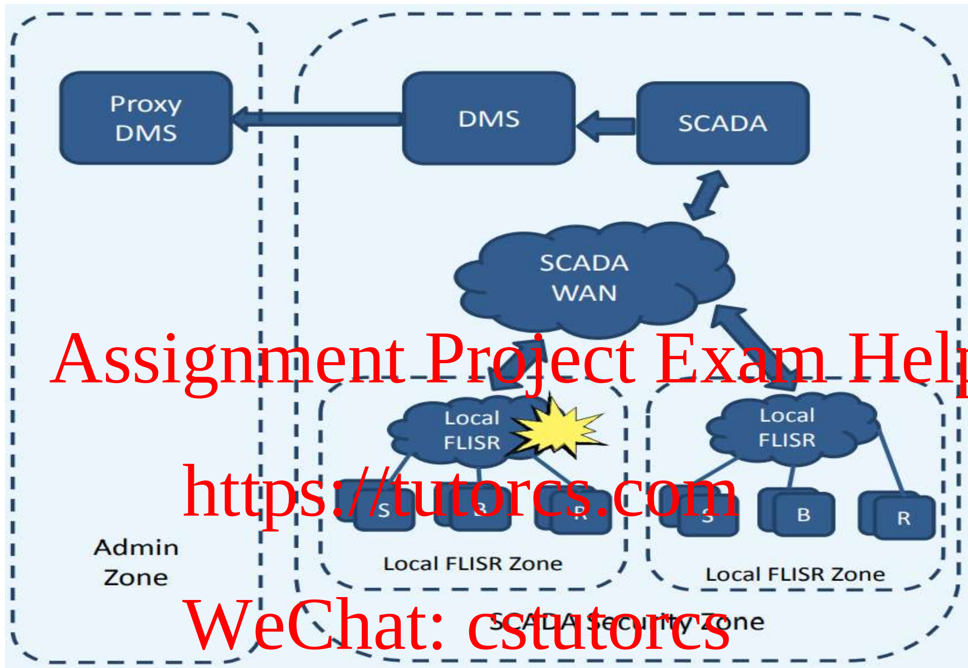
SINTEF

Martin Gilje Jaatun, Marie Elisabeth Gaup Moe, Per Erik Nordbø (2018). DOI: http://dx.doi.org/10.1109/CyberSecPODS.2018.8560668

- Distribution Management System (DMS) is the workhorse of the DSO, enabling real-time monitoring and control of the distribution grid, typically from the DSO control room.
- Paper from SINTEF, Norway addresses particular challenge of how self-healing mechanisms affect the cyber security of SCADA & DMS.
  - Discusses pros and cons of alternative self-healing configurations: Centralised, Decentralised and Local.
- Functional steps in FLISR solutions are:
  - Step 1: Based on sensor input automatically detect the Fault Location
  - Step 2: By means of breakers – automatically isolate the faulty component/segment.
  - Step 3: Maximum Service Restoration by energizing the new topology of the net.

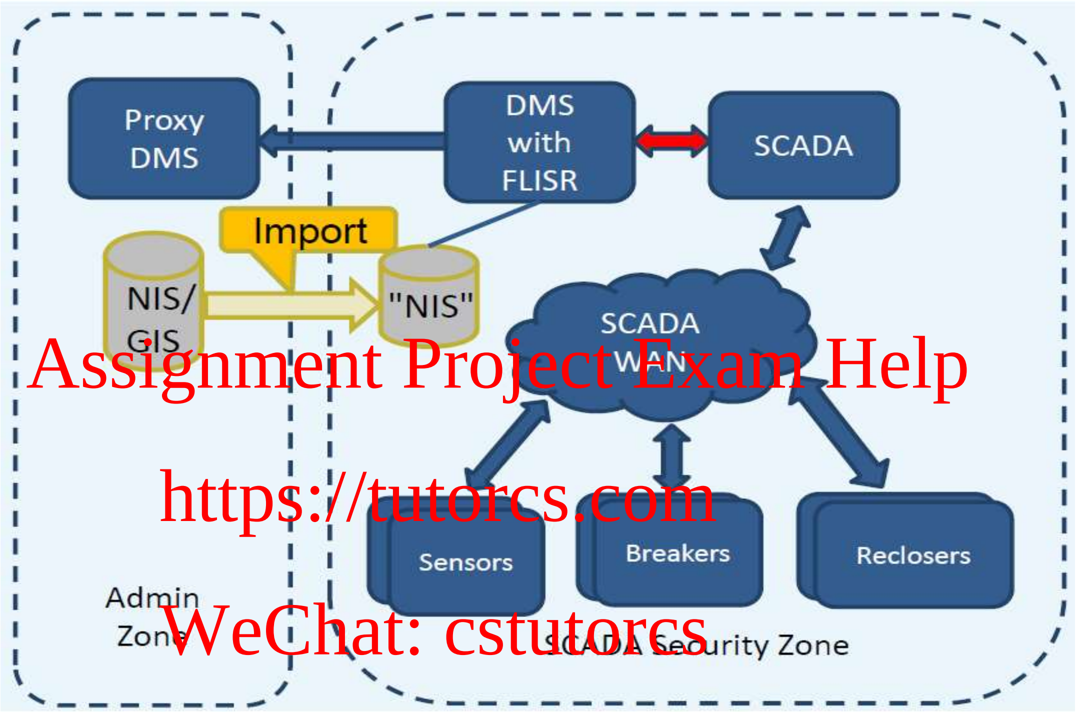


Cyber Security Considerations for Self-healing Smart Grid Network: Local FLISR

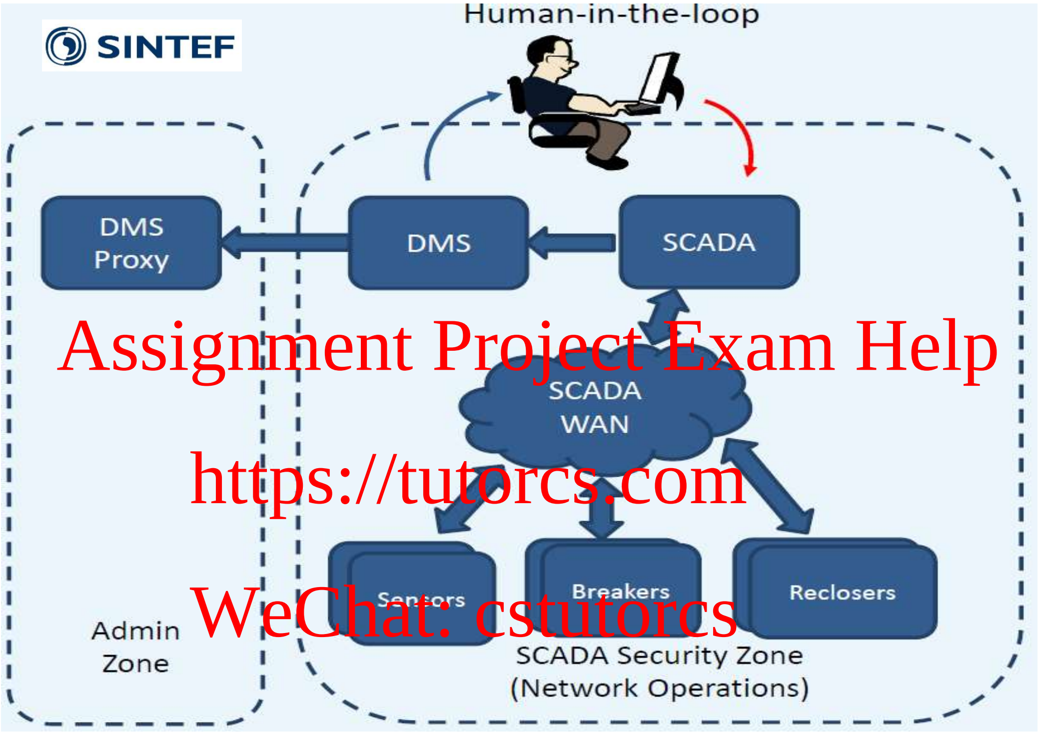


- Local FLISR controllers are collectively in charge of carrying out breaker and recloser operations until service is restored.
    - Only breaker status is reported back to the SCADA system, describing the new topology of the autonomous area.
    - Since messages sent to the SCADA system are status messages, the SCADA system can protect itself from local FLISR domains by only accepting status messages.
    - Implies solution is less vulnerable to cyber-attack than solutions that require DMS to be able to modify breakers directly.
    - If sensor data manipulated in local FLISR solution, malicious/wrong commands can be sent to breaker/reclosers, but the problem would not spread since the autonomous region only reports status to the central SCADA system.

Cyber Security Considerations for Self-healing Smart Grid Network: DMS-based FLISR



- Centralised FLISR solution where the intelligence resides in the DMS, requires the DMS to be able to actively manipulate breakers in the SCADA network.
- Decentralized FLISR solution relies on central analysis function residing in DMS or dedicated system assisting logic in a local FLISR domain, used to complete all steps in FLISR.
- If the central analysis function is in the DMS it will introduce the same security issues as with centralized FLISR solutions, and from a security point of view, there is no difference between decentralized and centralized solutions.



- Currently, good practice at Norwegian DSOs dictates it should not be possible to control SCADA network from the DMS.
  - Necessary because DMS generally is connected to the Internet (via firewalls), and could be compromised by an outside attacker.
  - Most DSOs currently require a human-in-the loop when performing system restoration operations.

Cyber Security Considerations for Self-healing Smart Grid Network: *Communication between SCADA and DMS*

SINTEF

- Typically, one-way connection initiated from the SCADA to the DMS is used to regularly update information on breaker settings.
- Since a DMS-based FLISR is doing the analysis based on the up-to-date GIS/NIS database, this must be maintained and used in a security zone below the SCADA zone,
  - introduces the problem of how to do a daily import of the up-to-date topology that can be trusted.

- Importing a manipulated GIS/NIS database into the DMS can have dramatic impact on erroneous breaker operation and outage if manipulation is not detected and changes are executed in the SCADA system.
  - Manipulation could be detected by operator inspection of the day-to-day evolution of the topological changes, by a human-in-the loop.
  - Automatic detection of manipulation is also a possibility, for instance with intrusion detection systems based on machine learning algorithms.

- Importing manipulated data can also be automatically prevented by whitelisting or rate limiting the number of allowed changes.

- Breaker and sensor data for FLISR analysis will normally be received by SCADA and forwarded to the DMS/FLISR.
- Even though end-to-end security, signatures and certificates can protect against man-in-the-middle attack, physical tampering at the location and spoofing of analogue lines interfacing RTUs cannot be detected and remains a problem.

research reported in SINTEF paper is supported by the Norwegian Research Council's ENERGIX program through the Flexnett project (project number 245412).

Q & A

Thanks:

Any questions on Automation in Distribution Networks?

Comments:

- Automatic Fault Location, Isolation and System Restoration (FLISR) is becoming increasingly important

- Reliability and Resilience is critically important, how do we ensure GB distribution networks can cope with physical and cyber attacks?

- What about extreme weather events, e.g. flooding or lightning storms.

- Will our distribution networks be as reliable and resilient in 2040, as they were in 2020.
    - Perhaps customers will learn to cope with short interruptions
    - What happens in a city centre if a local “black-out” lasts days, especially if your apartment is heated/cooled by electricity and the lifts stop working etc etc.