CIGRE-432

2021 CIGRE Canada Conference & Expo
Toronto, Ontario, October 25-28, 2021

Realizing benefits from securing access and remotely managing devices across the Duke Energy enterprise

K. ANDRESON
Duke Energy
USA

A.C. WEST
SUBNET Solutions
Australia

SUMMARY

Deregulation-led competition and government compliance is forcing electric utilities to modernize their grid to meet customer demands for impeccable power reliability. Advanced Intelligent Electronic Devices (IEDs) provide a digital control infrastructure to support lightning fast restoration times. IED management challenges for utilities include lifecycle costs, cyber security and regulatory compliance, with an exponentially increasing device population and vendor diversity.

Duke Energy, headquartered in North Carolina, USA, embarked on an ambitious long-term vision to standardize management of 60,000+ IEDs within 4,000 substations across three disparate regions in the USA Midwest, Carolinas, and Florida for both NERC CIP cyber assets and pole top distribution devices. The goal was to implement a Secure Access and Device Management (SADM) system capable of multi-vendor integration of existing devices while seamlessly adding new multi-vendor device types in the future. Business drivers beyond compliance included workforce optimization, improved device security, direct cost savings and improved restoration times. Engineers needed the ability to perform device management functionality including automated password management, configuration management, firmware/security patch management, and integration with third party applications, all of which are performed within an electronic security perimeter. With a secure and optimized device management strategy, Duke Energy could effectively expand their multi-vendor network of IEDs and extend the smart grid use cases to continually improve customer reliability.

To achieve this goal, a robust business case was formulated, an RFP issued and an IED Management solution provider was selected. A cross-functional team met for a design workshop to document current system architectures and design a cyber-secure path to reach any edge device from a centralized data centre.

kevin.andreson@duke-energy.com

This paper reports experience gained by Duke Energy during the implementation of an integrated, corporate-wide system for secure access and management of IEDs. Four of the planned eight systems have now been deployed and are in production, with all eight scheduled for commissioning by Q2 2022. The paper focuses on the lessons learned during implementation and the operational benefits achieved by the system.

KEYWORDS

Intelligent Electronic Device (IED), Secure Access and Device Management (SADM), password management, remote access management, settings file management, firmware management, NERC CIP compliance, event file collection, multi-vendor, cybersecurity

1. Introduction

Duke Energy is one of the largest utilities in America, serving over 7.8 million customers. Duke owns 51,000 megawatts of generation capacity and employs over 27,000 employees to deliver power over their 104,000 square mile territory. For managing grid assets over their massive territory, Duke operates over 120,000 IEDs.

Constrained by NERC CIP Cybersecurity standards, which govern how North American utilities manage and interact with cyber assets that control the grid, Duke Energy was under immense pressure to adhere to the NERC CIP standards while minimizing device management costs. Securing and managing the Duke Energy owned IEDs for compliance purposes is a requirement of the SADM project.

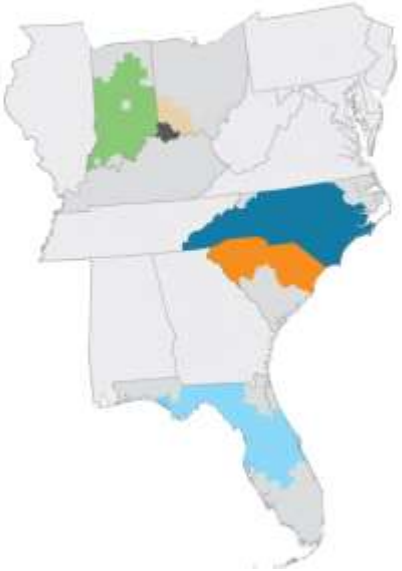


Figure 1: Duke Energy service territory

Duke Energy has experienced mergers and acquisitions over years that resulted in regional entities forging independent paths for technological implementations. The regional methods for device management included three different software systems, one for each region that independently secured device engineering access with varying degrees of cyber security and auditability. Managing three separate software systems to provide the device management was not a cyber secure and cost effective long-term solution. The vision that Duke Energy set out to achieve was to unify device management corporate wide under one management software that complies with and exceeds NERC CIP cybersecurity standards, and reduce engineering management costs. With one standard integration interface, Duke will save time and money on grid operations and improve the data available for engineering support. Compliance auditing and evidentiary support across the enterprise is dramatically simplified with one standard integration philosophy for all business units.

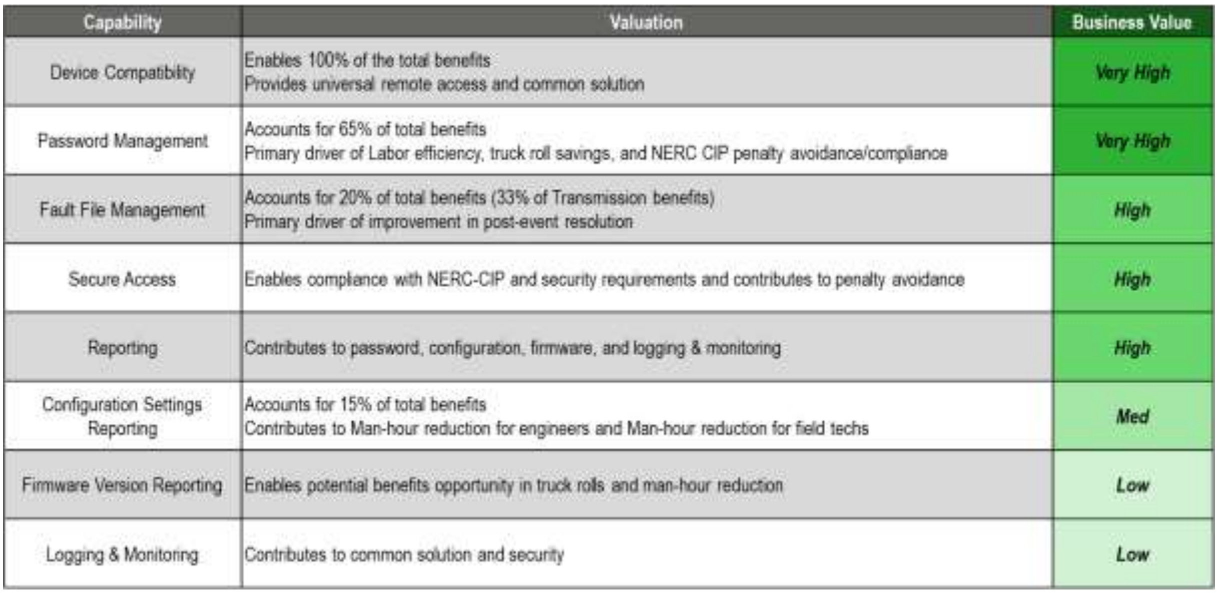
Securing any remote engineering access to grid devices was a major concern for Duke's security engineers. Remote access needs to be granted to authorized individuals for workforce efficiency but monitoring and restricting access is needed to ensure no unauthorized access is granted and no unwanted actions are taken. The blocking of certain commands (control operation) during remote user sessions was a system feature Duke desired in the final SADM solution but Duke was also aware of the difficulty the requirement posed to device management vendors.

2. **Internal consensus from all business units required**

To move the SADM project forward, Duke Energy enrolled stakeholders in all business units to come together for a common cause. Needs from the various business units were captured to create an RFP document that Duke Energy used to solicit bids from the industry. The process of getting the stakeholders consensus, evaluating the marketplace vendors available and creating the RFP, took 18 months to complete.

Stakeholders in the SADM project are not all from the same department. Many departments are affected and acquiring internal stakeholder consensus from different departments at different regional entities posed a significant challenge for the project. In order to meet compliance requirements, a well-engineered solution for universal device management was needed.

The business drivers determined by the SADM project stakeholders are listed **Error! Reference source not found.**:**Error! Reference source not found.**



Capability	Valuation	Business Value
Device Compatibility	Enables 100% of the total benefits Provides universal remote access and common solution	*Very High*
Password Management	Accounts for 65% of total benefits Primary driver of Labor efficiency, truck roll savings, and NERC CIP penalty avoidance/compliance	*Very High*
Fault File Management	Accounts for 20% of total benefits (33% of Transmission benefits) Primary driver of improvement in post-event resolution	*High*
Secure Access	Enables compliance with NERC-CIP and security requirements and contributes to penalty avoidance	*High*
Reporting	Contributes to password, configuration, firmware, and logging & monitoring	*High*
Configuration Settings Reporting	Accounts for 15% of total benefits Contributes to Man-hour reduction for engineers and Man-hour reduction for field techs	*Med*
Firmware Version Reporting	Enables potential benefits opportunity in truck rolls and man-hour reduction	*Low*
Logging & Monitoring	Contributes to common solution and security	*Low*

Table 1: Duke Energy business drivers for the SADM Project

Duke Energy developed a specification for the SADM project, which initiated a formal SADM Project Request for Proposal (RFP) process. During the business needs identification process, Duke identified a short list of capable device management vendors, to whom Duke sent the RFP.

3. **Vendor Selection Process**

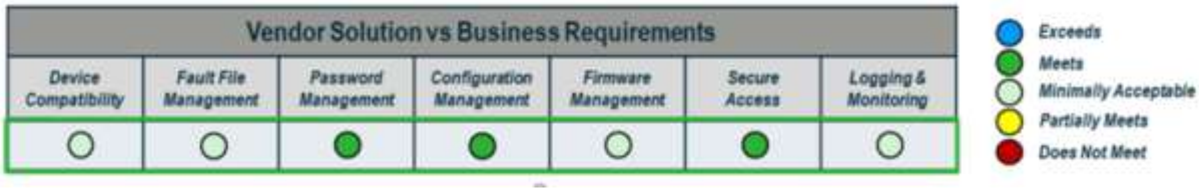
Some of the business units were satisfied with pre-existing device management vendor's performance and exhibited bias for one vendor over another. However, different business units did not all favour the same system and an aim of the project was to standardize on a common system across the utility. For Duke Energy's best interest, it was determined that the RFP process would perform an objective evaluation of features, costs and capabilities of each vendor’s offering, irrespective of opinion of any incumbent system. Based on the scoring in this evaluation, Duke determined the most appropriate solution.

Duke analysed the RFP responses and determined a scoring system for the offerings based on compliance to the following criteria:

- Technical requirements for the SADM project
  - Highly flexible environment
  - Capability for the solution to be customized by Duke
  - Configurability of the solution
  - Provision for application integration to other Duke Energy business systems
  - Satisfies the NERC CIP compliance requirements
- Functional requirements for the SADM project
  - Provides the full scope of requirements and functionality specified in the RFP
  - Compatible with the majority of the device inventory of new and legacy equipment
  - Scalable to provide for future growth to manage a significantly larger and increasing number and diversity of devices

It may be noted that technical and functional requirements were the dominant factors in the evaluation process.

A vendor scorecard was developed for summarizing each offering’s alignment with the identified business drivers. An example of such a scorecard is show in **Error! Reference source not found.**.



Vendor Solution vs Business Requirements						
Device Compatibility	Fault File Management	Password Management	Configuration Management	Firmware Management	Secure Access	Logging & Monitoring
○	○	🟢	🟢	○	🟢	○

🔵 Exceeds
🟢 Meets
○ Minimally Acceptable
🟡 Partially Meets
🔴 Does Not Meet

Figure 2: Sample vendor scorecard

Many vendors were interested in winning Duke’s business. Duke Energy’s vendor selection choices for remote device management ultimately broke down to being between vendors of devices that Duke Energy purchases for grid operations or an independent vendor-agnostic software solution, not affiliated with any of the IEDs Duke Energy purchases.

IED vendors typically offer tools to manage their devices and sometimes these tools provide limited functionality with other vendor’s devices. Device conflicts can ensue whereby only certain vendor’s products can operate within the confines of a single device vendor’s device management solution. A vendor-agnostic software-based solution can apply consistent features across the spectrum of Duke’s device types.

Duke’s technical selection criteria identified that no offering met all their requirements but the selected offering was the one that met the largest portion of their requirements.

Duke Energy’s need for corporate-wide device management. An enterprise license agreement for unlimited devices and unlimited installations was determined to be the best affordability for the long-term project. By purchasing an enterprise software license, Duke

Energy has fulfilled the requirements of the SADM project and future-proofed Duke Energy for growing needs of device management.

4. Staging the project

After the vendor selection process concluded, the project commencement phase began. The vendor selected offered a proven project implementation strategy. However, there was a project-based RFP that detailed many requirements, a design session was still required and a Design Document produced by the vendor.

Developing an agreed-upon design for all Duke Energy's divisions proved very challenging. Capturing the existing infrastructure needs at each division and incorporating their requirements into one holistic SADM system required a method to bring together all the information. For the design session, Duke brought all division technical stakeholders and the vendor together for a week in Charlotte, NC to work through all the technical details for the project. An initial draft of the Design Document was produced. Several iterations of the Design Document were circulated until all comments were incorporated and a final, agreed-upon version. With this document in place, project clarity is provided to all stakeholders and the SADM project management was simplified.

The general SADM project architecture was as follows.

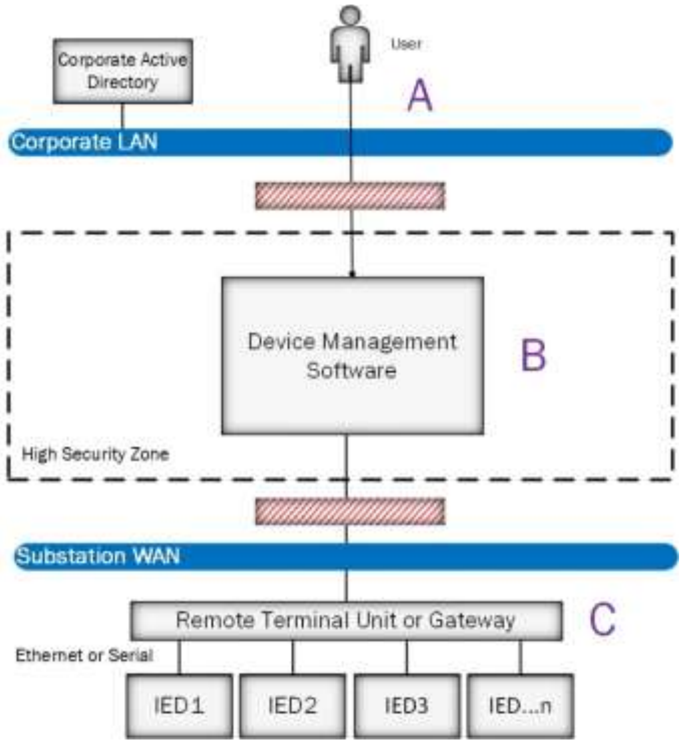


Figure 3: General SADM project system architecture

The user connects to edge IEDs from a central location (i.e. high-availability data centres). The user authenticates (Figure *3*: A) into a high security zone using Active Directory credentials and Multi-Factor authentication. Once in the network DMZ, users navigate to devices within the Device Management software (Figure *3*: B) and select the operation they wish to perform. The system validates the request and automates a secure endpoint connection to the edge IED by tunnelling through any intermediate devices such as RTU’s or gateways (Figure *3*: C) and completes the desired job. Once a path to the edge IEDs was architected, a matrix of device management functions was determined.

The SADM project required benefits to be realized right away and not wait until all the features are in place. Enhancements would be staged to roll-out over time. The initial installation was for a Minimal Viable Product (MVP) followed by a series of revisions adding automation functionality for devices as additional drivers and features are developed.

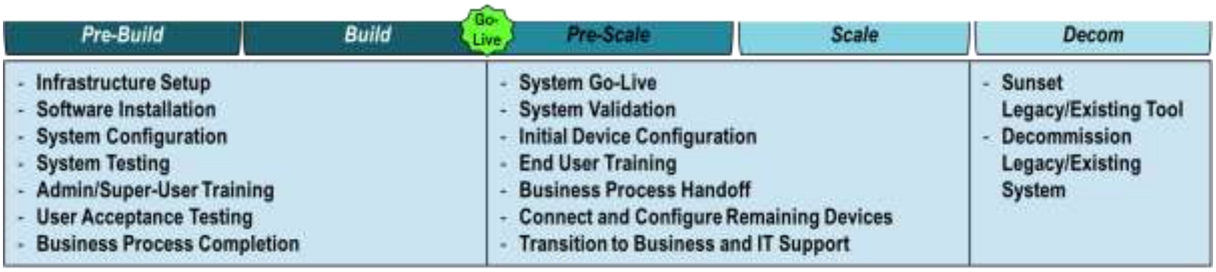
The project’s regional roll-out is:

Region	**Division**
Carolina’s West	Transmission
Carolina’s West	Customer Delivery
Carolina’s East	Transmission
Carolina’s East	Customer Delivery
Florida	Transmission
Florida	Customer Delivery
Midwest	Transmission
Midwest	Customer Delivery

Table 2: Regional SADM Project deployment locations

The extent of the project necessitated a multi-year implementation plan. Staging the project with MVP followed by enhancements allows for early benefits to be realized. The project management team incorporated planned upgrades of existing sites so that when the project is completed, all sites will be on the same version.

The implementation approach, summarized in Figure *3*, is repeated for each division. Pre-Build/Build start and duration will be dictated by preceding regions Go-Live. Pre-Scale/Scale success will be dictated by business readiness of each region. Product enhancements are applied to the base product in each region with inflight regions being upgraded to the current version when the release becomes available.



- Infrastructure Setup
- Software Installation
- System Configuration
- System Testing
- Admin/Super-User Training
- User Acceptance Testing
- Business Process Completion

- System Go-Live
- System Validation
- Initial Device Configuration
- End User Training
- Business Process Handoff
- Connect and Configure Remaining Devices
- Transition to Business and IT Support

- Sunset Legacy/Existing Tool
- Decommission Legacy/Existing System

Figure 4: Project implementation approach

5. SADM Project Benefits – Realized and Envisioned

There are many business drivers for the SADM project initiative. Many of the business drivers come with related benefits in cost savings or other areas. Duke Energy strives to lower greenhouse gases and improve safety and the SADM project assists those initiatives. Table 3 below lists categories of benefits the SADM project realizes and is expanding further as the project matures:

Benefit	Description
NERC CIP & Internal Duke Standard Compliance	Duke Energy has internal standards for compliance the SADM project must meet. Many external standards (NIST, NERC) are also required for Duke Energy to meet. The SADM project is an integral component of the following NERC CIP compliance items: CIP-002-5.1 — Cyber Security — BES Cyber System Categorization CIP-005-5 — Cyber Security – Electronic Security Perimeter(s) CIP-007-6 — Cyber Security – Systems Security Management CIP-008-5— Cyber Security —Incident Reporting and Response Planning CIP-010-2 — Cyber Security — Configuration Change Management and Vulnerability Assessments CIP-011-2 — Cyber Security — Information Protection
Truck roll reduction	The SADM project provides secure remote accessibility to the IEDs. In cases where an engineer would drive to the site to perform work with the device or acquire an event file from the device, those truck-rolls are now avoided saving time, reducing fuel costs, reducing emissions and reducing driving time, which reduces traffic and field accidents, thus improving safety.
Standardization across business units	Duke Energy has incurred many additional costs with disparate systems and lack of business synergy. The SADM project will bring together the divisions and consolidate Duke onto one platform for device management efficiency. Cost savings with standardization for reduced training requirements and improved clarity and understanding across regional business units. Compliance reporting standardization is key to improving compliance audit performance.
Business system integration	Integration with existing Duke Energy business intelligence systems is cost prohibitive is many different systems in use by Duke. With standardizing on one single vendor SADM platform, additional cost-effective business system integration and automation is available for Duke.
Improved Cyber Security	Cyber security risks have ever-growing threat vectors and Duke needs systems to thwart potential intrusion attempts. The SADM project requires multi-factor user authorizations for role-based access into the system. There are three primary cybersecurity benefits from using the application driver technology for device management. First, the application driver automatically enters the connection information and credentials for the end-user. This feature alleviates users as a potential insider threat vector since they no longer need to know the IP address or the password of the IEDs they are accessing. Second, user access is controlled by role-based controls that allow for granular user permissions for both user access to devices and functionality exposed to the user during an active remote session to a device. Third, the application drivers block restricted commands or software menus and hide unauthorized devices on a user-by-user basis.

Improved Grid Reliability (SAIDI)	The SADM project validates the devices on the grid are operating properly, configured properly, accessed properly and are in compliance. By ensuring device integrity, Duke is improving grid reliability (improved System Average Interruption Duration Index (SAIDI)) by eliminating a previous source of mis-operations. Forensics show that a percentage of all mis-operations of grid devices are resultant from mis-configuration of the edge device. The SADM project will validate the edge device's configurations to remove problems associated with IEDs being incorrectly configured. The vendor device application driver technology included with the SADM solution allows Duke Energy users to be blocked from certain commands so accidental trip operations during remote engineering access sessions can be eliminated.
Improved Grid Resiliency (SAIFI)	A SADM project goal is to retrieve event file records from devices seeing a disturbance on the line. Automatic detection that the disturbance file is available with immediate retrieval and forwarding to responsible parties aids in outage restoration and System Average Interruption Frequency Index (SAIFI) scores.
No local hardware	The deployed SADM solution is a centralized software solution with no local hardware needed. An SADM project goal was to not disturb the substation environment. A centralized software solution was a much simpler and cost-effective option.
Project cost savings	The SADM project execution was very efficient. From the design phase to the development phase and right through to production implementation, the SADM project has been ahead of scheduled and under budget. Many projects do not flow smoothly and the SADM project was a notable exception. The well-engineered project design is credited with smooth project execution. Having competent staff involved makes for short work when project issues are identified and resolutions needed.
Workforce Efficiency	Beyond saving time driving to/from the station, a key operational efficiency benefit of was a significant reduction in the number of engineer's steps required to manage any substation IED through automation. The automated tasks included collecting faults, sequence of events, firmware and device configuration without requiring the end-user to enter device specific data such as IP addresses, TCP port numbers and passwords.

Table 3: SADM project benefits

6. Additional projects resulting from the initial SADM project

The success of the initial SADM project has seen Duke Energy come together to find related beneficial projects.

Bulk Device Management (BDM) – The BDM project spawned off a need to update many devices in bulk. Consistent use cases occur where Duke needs to update the configuration or firmware of an IED type and there are many, maybe hundreds or thousands, of that IED type to update. Extensive time is spent making updates manually and the effort becomes a barrier to implementing the changes needed. The BDM project will enhance the SADM solution to issue the required IED updates and then validate the update is implemented and the IED is working properly.

CIP Local Password Tool (CLPT) – CIP compliance password management for IEDs not connected to Ethernet communication is another requirement by Duke Energy. Having the same system manage non-connected devices has many synergy benefits for Duke. The tool will enable engineers and technicians automated ways to change passwords on IEDs when connected directly to the IED. The password change will then sync with the main system so all passwords are managed in the same compliant manner.

7. Conclusion

Providing a vendor agnostic secure access and device management solution to Duke Energy has already proven to provide many benefits and improved workforce efficiency. Duke Energy is please to future proof their company from anticipated increased grid monitoring various with IEDs. Working in a multi-vendor environment where any vendor with a compliant product can bid on Duke Energy's business facilitates the open marketplace vision for Duke Energy project procurement.

There are several key take away points from this paper:

- Universal IED management is available. Being stuck in a single vendor proprietary solution is a situation that utilities no longer need to deal with. Technology exists that can manage the password of any device.
- Automation is key to workforce efficiency improvements. It is no longer acceptable for manual interaction for every configuration or firmware change too an IED. Automation of IED management frees up many hours of labor by not having to drive to site to take action with an IED that could actually be done remotely. Direct cost savings are realized by not having to travel to the site. The opportunity savings for other work that could be completed instead of driving are indirect and sizable.
- Software solutions are cheaper and easier to install and maintain for managing device password and compliance. No station drawings to update, no trips to the substation, no wires to run to connect the IEDs are all great benefits of using a centralized software solution. Maintainability and issuing updates are other major benefits to a centralized software solution. When updates are needed, updating many field hardware devices can be costly and time consuming. Updating a centralized software solution is fast and easy in comparison with a download and apply the patch. With high availability architecture, in many cases the user is unaware the system was updated or patched.
- Improved security by eliminating possible mis-operations in vendor applications. Granting remote access sessions is beneficial for utility engineering but accidental trips have occurred during remote access sessions. Elimination and blocking of the potential mis-operation vector is preferred versus a workflow that indicates trip operations are not to be completed during remote access sessions. Application driver technology provides role-based access within the vendor's applications to restrict the ability of the user from initiating a trip command, whether they are intentionally being malicious or an accidental operation.
- Duke synergy – By standardizing on a universal multi-vendor device management system for all regions, Duke will bring the disparate divisions together for a common cause. Corporate identity is lost during mergers and acquisitions and the

SADM project brings the various divisions together for a common cause. With all stakeholders' inputs recognized, the SADM project bridges the corporate divides and addresses the needs of all.

- Improved compliance reporting – Compliance is of paramount concern and being compliant was made more difficult with different business systems operating and reporting in separate ways. With consolidation of reporting, compliance reporting is becoming standard across the business. Large amount of time are saved by providing a standard level of compliance documentation at each division

BIBLIOGRAPHY

[1] Duke Energy Wikipedia - https://en.wikipedia.org/wiki/Duke_Energy

[2] Duke Energy statistics - https://www.duke-energy.com/Our-Company/About-Us

[3] 2020 Annual Report and Form 10-K - https://desitecoreprod-cd.azureedge.net/annual-report/_/media/pdfs/our-company/investors/de-annual-reports/2020/2020-duke-energy-annual-report.pdf

[4] Duke Energy corporate website - https://www.duke-energy.com/Our-Company/About-Us