EPRI | ELECTRIC POWER RESEARCH INSTITUTE

# Substation Security Architecture Reference Diagrams Version 1.0

**3002009519**

# Substation Security Architecture Reference Diagrams Version 1.0

**3002009519**

Technical Update, December 2016


EPRI Project Managers

A. Lee
J. Stewart
G. Chason
R. King



ELECTRIC POWER RESEARCH INSTITUTE
3420 Hillview Avenue, Palo Alto, California 94304-1338 ▪ PO Box 10412, Palo Alto, California 94303-0813 ▪ USA
800.313.3774 ▪ 650.855.2121 ▪ askepri@epri.com ▪ www.epri.com

## DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES



**This is an EPRI Technical Update report. A Technical Update report is intended as an informal report of continuing research, a meeting, or a topical study. It is not a final EPRI technical report.**

## NOTE

For further information about EPRI, call the EPRI Customer Assistance Center at 800.313.3774 or e-mail askepri@epri.com.

# ACKNOWLEDGMENTS

The Electric Power Research Institute (EPRI) prepared this report.

Principal Investigators
A. Lee
J. Stewart
G. Chason
R. King

This report describes research sponsored by EPRI.

EPRI acknowledges the collaboration of several organizations: National Rural Electric Cooperative Association (NRECA), American Public Power Association (APPA), Edison Electric Institute (EEI), and Utilities Technology Council (UTC) for their interest and involvement. EPRI also appreciates the input from utilities that have provided valuable information to guide this project.

---

This publication is a corporate document that should be cited in the literature in the following manner:

*Substation Security Architecture Reference Diagrams Version 1.0.* EPRI, Palo Alto, CA: 2016. 3002009519.

# ABSTRACT

The nation's power system consists of both legacy and next generation technologies, with devices that may be 30–50 years old, have no cyber security controls, and implement proprietary communication protocols and applications. Many of these legacy devices have significant computing and performance constraints that limit the type of cyber security controls that may be implemented. By contrast, the new technology may include modern information technology (IT) devices with commercially available applications and communication protocols. The new operations technology (OT) devices may also include commercially available applications and communications.

With this shift in technology, utilities are exploring methods to better address cyber security requirements. This exploration includes prioritizing the systems, performing a cyber security risk assessment, and determining the impacts of a cyber security compromise as part of a cyber security strategy.

Another component of the cyber security strategy is a cyber security architecture. Currently, utilities have enterprise architecture diagrams, but they have not typically developed a cyber security architecture. This technical update includes transmission and distribution reference cyber security architecture diagrams for legacy, transition, and future configurations. This report is a companion document to EPRI's *Cyber Security Architecture Methodology for the Electric Sector, Version 2.0* (3002007887).

**Keywords**
Cyber security
Risk assessment
Cyber security architecture
Cyber security controls
Attack surface

**Deliverable Number: 3002009519**

**Product Type: Technical Update**

# Substation Security Architecture Reference Diagrams Version 1.0

**PRIMARY AUDIENCE:** Power delivery system owners and operators

**SECONDARY AUDIENCE:** Research organizations and solutions providers

## KEY RESEARCH QUESTION

For grid modernization, increased interconnection in electric sector devices is required, resulting in a larger attack surface that may be exploited by potential adversaries such as nation-states, terrorist organizations, malicious contractors, and disgruntled employees. The focus of this document is to present a standardized security architecture methodology that has been applied to transmission and distribution substations and includes an approach for analyzing the attack surface. This report includes the transmission and distribution substation reference cyber security architecture diagrams for legacy, transition, and future configurations. The report is a companion document to EPRI's *Cyber Security Architecture Methodology for the Electric Sector*, Version 2.0 (3002007887), which focused on developing security use cases based on the National Electric Sector Cybersecurity Organization Resource (NESCOR) failure scenarios.

## RESEARCH OVERVIEW

Typically, an enterprise architecture does not address cyber security, in specific the overall attack surface, attack vectors, potential vulnerabilities, and applicable mitigation strategies. The challenge is to develop a security architecture methodology that augments, rather than replaces, current enterprise architecture methodologies and is at a level that is useful to utilities. This report includes the second version of a cyber security architecture methodology that may be used by utilities for existing and planned system architectures. The objective is to provide a common methodology applicable to utilities of all sizes—from large investor-owned utilities to smaller cooperatives and municipalities. EPRI is collaborating with other research efforts to ensure that the security architecture methodology does not conflict with ongoing work.

## KEY FINDINGS

- At present, there is no common security architecture methodology used throughout the utility industry. Several architecture frameworks are available, and each includes unique terms and definitions. In general, these frameworks are intended to be used to develop the enterprise architecture and not specifically a cyber security architecture.
- A reference cyber security architecture may be used in evaluating the current system configuration and defining transition and target configurations.
- A security architecture methodology is an important tool in a utility's cyber security risk management strategy.
- A reference cyber security architecture may be used to support utility situational awareness.

## WHY THIS MATTERS

A cyber security architecture methodology is one of the tools that can be used to assess the constantly changing threat and technology environments.

## HOW TO APPLY RESULTS

As utilities modernize the grid, they will need to assess the architecture to identify potential vulnerabilities that may be exploited by an attacker as well as appropriate attack mitigation strategies. This can be a difficult task without the use of a cyber security architecture methodology. Because the goal of this project is to develop a common methodology, participation in the project and provision of input will ensure that the product is useful to utilities.

## LEARNING AND ENGAGEMENT OPPORTUNITIES

- Collaborators: Edison Electric Institute (EEI), National Rural Electric Cooperative Association (NRECA), American Public Power Association (APPA), and Utilities Technology Council (UTC)
- Presentation materials: EPRI 2016 Cyber Security Technology Transfer Workshop, held November 1–2, 2016, in Dallas, TX
- EPRI 2017 Winter Advisory Meeting, held February 13–15, 2017, in Huntington Beach, CA

**EPRI CONTACTS:** Annabelle Lee, Principal Technical Executive, alee@epri.com

**PROGRAM:** Cyber Security, 183



**Electric Power Research Institute**
3420 Hillview Avenue, Palo Alto, California 94304-1338 • PO Box 10412, Palo Alto, California 94303-0813 USA
800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com

# ACRONYMS

| | |
|---|---|
| ANSI | American National Standards Institute |
| APPA | American Public Power Association |
| CCTV | Capacitance Coupled Voltage Transformer |
| DER | Distributed Energy Resources |
| DOE | Department of Energy |
| DVR | Digital Video Recorder |
| EEI | Edison Electric Institute |
| EPRI | Electric Power Research Institute |
| ICT | Information and Communications Technology |
| IDS | Intrusion Detection System |
| IEC | International Electrotechnical Commission |
| IEEE | Institute of Electrical and Electronics Engineers |
| IOU | Investor Owned Utility |
| IPS | Intrusion Protection System |
| ISO | International Organization for Standardization |
| ISOC | Integrated Security Operations Center |
| IT | Information Technology |
| NESCOR | National Electric Sector Cybersecurity Organization Resource |
| NIST | National Institute of Standards and Technology |
| NISTIR | NIST Interagency Report |
| NRECA | National Rural Electric Cooperative Association |
| OT | Operations Technology |
| PLC | Programmable Logic Controller |
| PMU | Phasor Measurement Unit |
| RTI | Remote Terminal Unit |
| SP | Special Publication |
| TC | Technical Committee |
| TOGAF | The Open Group Architecture Framework |
| UTC | Utilities Technology Council |

# CONTENTS

# LIST OF FIGURES

# 1
# INTRODUCTION

Currently, the nation's power system consists of both legacy and next generation technologies. This includes devices that may be 30-50 years old that have no cyber security controls and implement proprietary communication protocols and applications. Many of these legacy devices have significant computing and performance constraints that limit the cyber security controls that may be implemented. In contrast, the new technology may include modern information technology (IT) devices with commercially available applications and communication protocols. The new operations technology (OT) devices may also include commercially available applications and communications. To utilize this new technology, increased interconnection is required with the applicable cyber security controls implemented to address this larger attack surface that may be exploited by potential adversaries such as nation-states, terrorist organizations, malicious contractors, and disgruntled employees. The challenge and complexity of addressing cyber security risks has increased in part because the technology landscape and threat environment are constantly changing.

## 1.1 Document Purpose

This technical update includes the transmission and distribution reference security architecture diagrams for the legacy, transition, and future diagrams. This report is a companion document to the technical update *Cyber Security Architecture Methodology for the Electric Sector*, Version 2.0, 3002007887 that focused on developing security use cases based on the National Electric Sector Cybersecurity Organization Resource (NESCOR) failure scenarios.

The purpose of this document is to define a security architecture methodology that may be implemented throughout the electric sector by utilities of all sizes - large Investor Owned Utilities (IOUs), municipalities, and cooperatives. There are several architecture frameworks that are currently available, and each includes unique terms and definitions. In general, these frameworks are intended to be used to develop the enterprise architecture, and not specifically a security architecture. The frameworks that focus on security architectures typically do not include an approach for analyzing the attack surface and identifying attack vectors and potential vulnerabilities that may be exploited. The focus of this document is to present a standardized security architecture methodology that has been applied to transmission and distribution substations that includes an approach for analyzing the attack surface.

## 1.2 Document Content

This document contains the following sections:

- Section 1: Introduction
- Section 2: Substation Device Categories
- Section 3: Security Architecture Reference Diagrams

# 2
# SUBSTATION DEVICE CATEGORIES

There are a wide range of intelligent devices and systems in use at substations across the power grid. This document divides these devices and systems into a number of categories by role. Within each category, a number of example devices are listed to clarify the scope of the category. These lists are not intended to be comprehensive.

## 2.1 Automated Protection Systems

These systems have direct control or influence on the station switchgear and are designed to operate without requiring any manual actions. Typical equipment in this category is tasked with the protection of power system equipment or automated controls that help correct power system issues. The following list contains examples of protection systems.

1. Relays
2. Programmable Logic Controllers (PLC)
3. Substation Automation Controller

## 2.2 Manually Initiated Systems

These systems also have direct control or influence on the station switchgear but are designed to be operated manually. They are typically controlled by operators either locally or at one or more centralized control centers. The capability to access equipment remotely is important when evaluating cyber security for a substation architecture. The following list contains examples of devices that are manually initiated.

1. SCADA Remote Terminal Unit (RTU)
2. SCADA Gateway/Protocol Converter
3. Dedicated Human Machine Interface (HMI)

## 2.3 Monitoring and Measurement Systems

When operating an unmanned substation, many states and conditions must be monitored and recorded for a number of operational and maintenance reasons. The devices within this category are responsible for the collection of that data. From a hardware perspective, many of the devices in this category may be similar to those in both the automated and manual control categories. The key difference for these devices is the lack of direct control over, or operation of, the high voltage equipment.

Even though they do not have direct control, these devices play a critical role in the operations and maintenance of the power grid. Information from these systems may cause an operator to make a manual control decision. Additionally, measurements or conditions observed by these systems may be used as input to an automated protection scheme. The following list contains examples of monitoring and measurement systems. Included in this category are two subcategories based on the function that a given device is designed to support. System monitors

are used to report the state of the power system while asset health monitors are deployed to provide insight into the health of a key asset.

System Monitors

1. Power Quality Monitor
2. Phasor Measurement Unit (PMU)
3. Meters
4. Intelligent Transducer

Asset Health Monitors

1. Transformer Monitor
2. Circuit Breaker Monitor

## 2.4 Communications Systems

Communications are used to facilitate the exchange of information among devices in the other categories and systems external to the substation. This exchange of information may occur within the substation, between the substation and remote locations and between the substation and a control center. This category includes serial based devices, packet based devices, and devices used to translate between serial and packet systems. In addition to an array of devices, the infrastructure used for communications between the devices is multi-faceted. These facets can be broken down into two primary groups, range and ownership. Communications ranges from short to medium and long distances. Ownership can be any combination of Utility, third party, or a combination of the two. The following list contains some examples of communication devices.

1. Ethernet switches
2. Routers
3. Modems
4. Digital Protection Units (Pilot Protection Channels)
5. Terminal Servers
6. Channel Banks
7. Phone Line Switches
8. Fiber Optic Terminals
9. Microwave Terminals

## 2.5 Support Systems

The support system category contains the substation devices and systems that do not play a direct role in the operation of the grid, but can be critical to the proper operation of devices listed in the other categories. These devices provide primary and backup power along with providing a time reference where required. The following list contains examples of support systems.

1. Global Positioning System (GPS) Clocks
2. 48V-125VDC Battery Chargers

3. 48V-125VDC Power Distribution
4. 120VAC Station Service Distribution

## 2.6 Primary Power Equipment Systems

In the categories listed above, all systems and devices share the characteristic of being electronic and programmable. These systems and devices may also be called “cyber” assets. In addition to these systems and devices, a typical substation also includes primary power equipment devices. This equipment is responsible for carrying power and interrupting or reconfiguring the flow of power through the substation.

Many of the non-cyber systems and devices may evolve over time into processor-based assets. One such example is the instrument transformer. In its current form it uses electromagnetic induction to convert voltage and current down to a more convenient level for use by protection or measurement systems. This conversion is controlled by mechanical connections and the transformer does not contain any programmable components. In the future, some instrument transformers may be replaced with a programmable device that samples the current or voltage values using a high sample rate. The devices then publish the sampled values for use. Examples of non-cyber substation devices are listed below:

1. Instrument Transformer
2. Power Transformer
3. Circuit Breaker
4. Capacitance Coupled Voltage Transformer (CCVT)

## 2.7 Security Mitigation Strategies

While the categories included above contain systems that enable or support the delivery of power, security mitigation strategies contain categories focused on the protection of the substation devices and systems. The example systems listed below have been divided into two categories. The first category is focused on the cyber security of the substation while the second category is focused on physical security.

### *2.7.1 Cyber Security Systems*

Cyber security systems protect intelligent substation devices and data from any potential compromise of availability, integrity, and confidentiality. The following list contains examples of cyber security systems.

1. Firewall
2. Intrusion Detection System (IDS)
3. Intrusion Prevention System (IPS)
4. Security Gateway
5. Log Collector
6. Security Proxy Server

Physical security systems are deployed at substations to control and monitor physical access to the site. For this report, the focus is on data received from these devices and its correlation with data from cyber security systems. Therefore, these devices are included under Cyber Security Systems. The following list contains examples of physical security systems.

1. Card Access Readers
2. Card Access Controller
3. Video Camera
4. Digital Video Recorder (DVR)

# 3
# SUBSTATION SECURITY ARCHITECTURE REFERENCE DIAGRAMS

Included below are the substation reference security architecture diagrams with devices that are common to a substation. The diagrams are not intended to include all the various devices that may be located at a substation, rather they include devices that are representative of each device category listed above. These diagrams should be revised to replicate the specific planned and proposed substation configurations. There may be variations depending on the size of the substations and/or whether they are for transmission or distribution.

Included are three diagrams: legacy, transition, and future with the device categories highlighted in different colors. The device categories and color coding include:

Automated Protection Systems

Manually Initiated Systems

Monitoring and Measurement Systems

Communications Systems

Support Systems

Primary Power Systems

Cyber Security Systems

The differences between the three architectures are:

- Legacy substations typically consist of electromechanical control systems and a small number of single purpose programmable devices with limited resources and capabilities. Coordination among devices is typically done by wiring inputs and outputs between terminal blocks. All communication interfaces and protocols are relatively simple and often proprietary.
- Transition substations begin to leverage microprocessor based devices that may perform the functions of multiple electromechanical devices. Serial communications protocols have increased in complexity and evolved toward more use of open standards.
- Future substations rely on high speed sampling to convert inputs and outputs into logic states and values that can be exchanged among different multipurpose devices. As the function

each device performs becomes abstracted from the hardware, complexity in device software and configuration increases. Newer protocols leverage techniques like self-description to deal with the new complexity.

The diagrams were developed as a series of overlays, with each device category and the associated devices highlighted with a unique color, as noted above. In the companion document, the three high level diagrams include all the device categories in each diagram. In this document, the high level diagram is displayed first, and then there are separate diagrams for each device category.

## 3.1 Legacy Substation Security Architecture

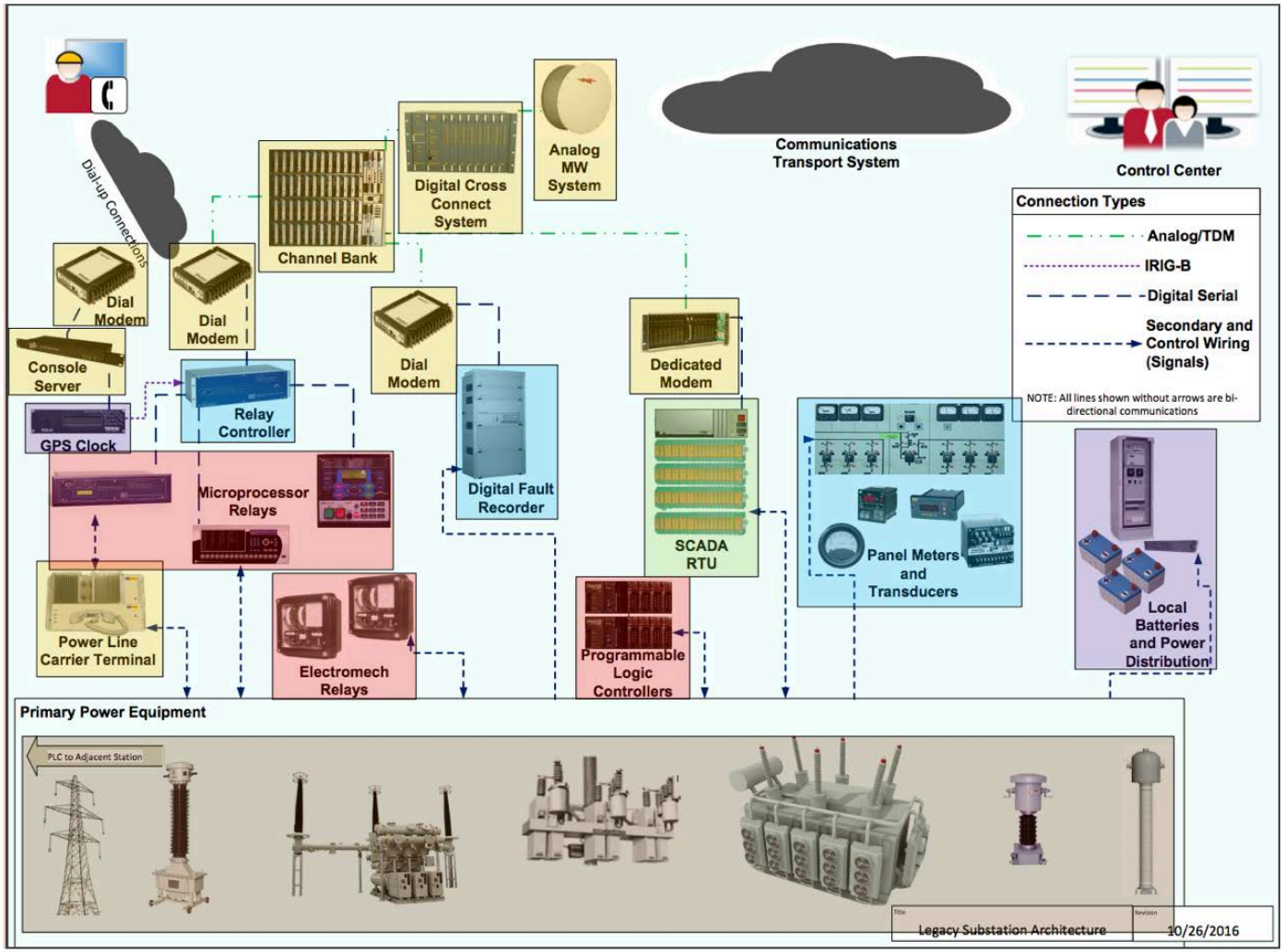


**Figure 3-1**
**Legacy Substation Security Architecture – all device categories**

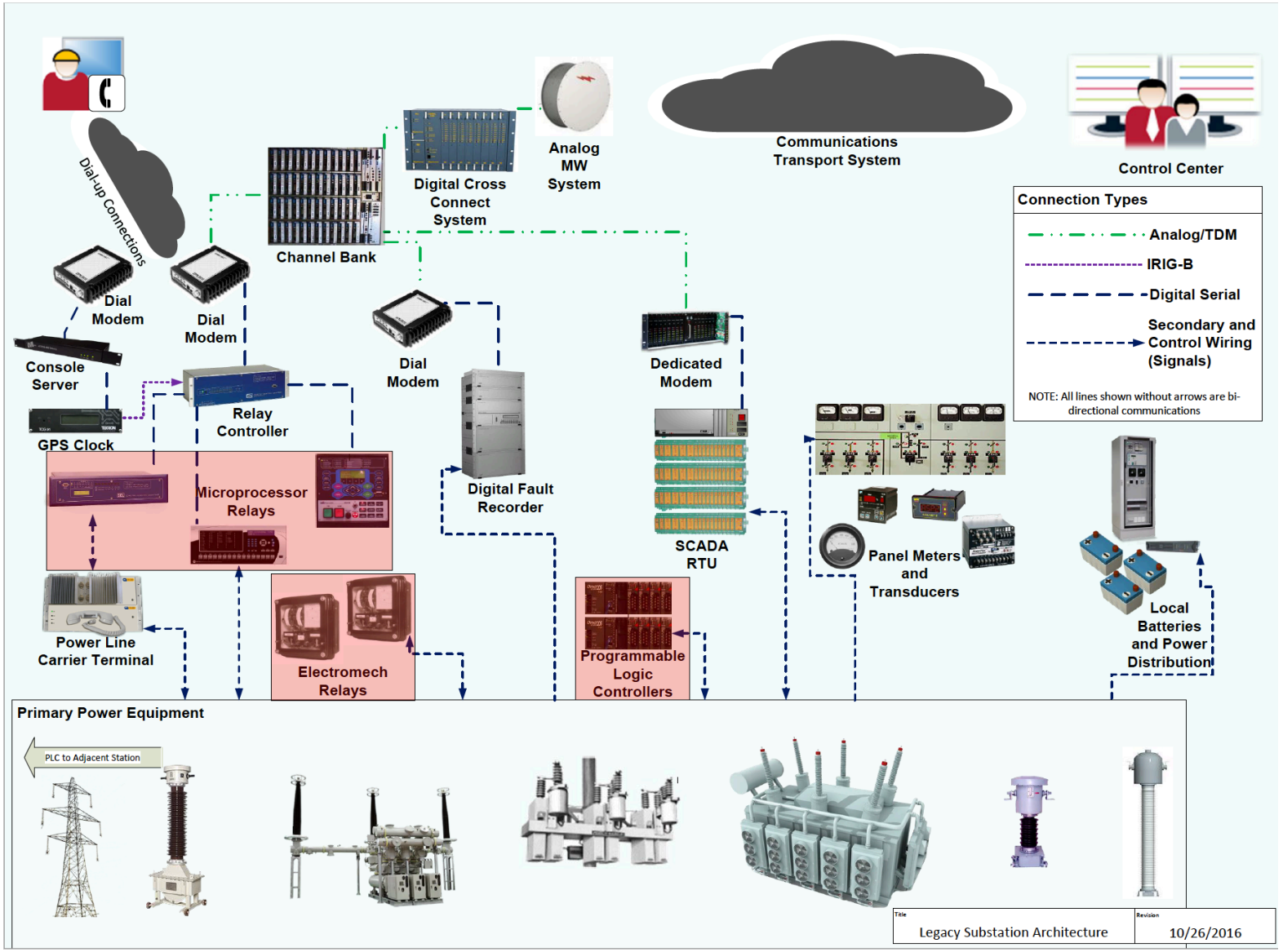


**Figure 3-2**
**Legacy Substation Security Architecture – Automated Protection Systems**

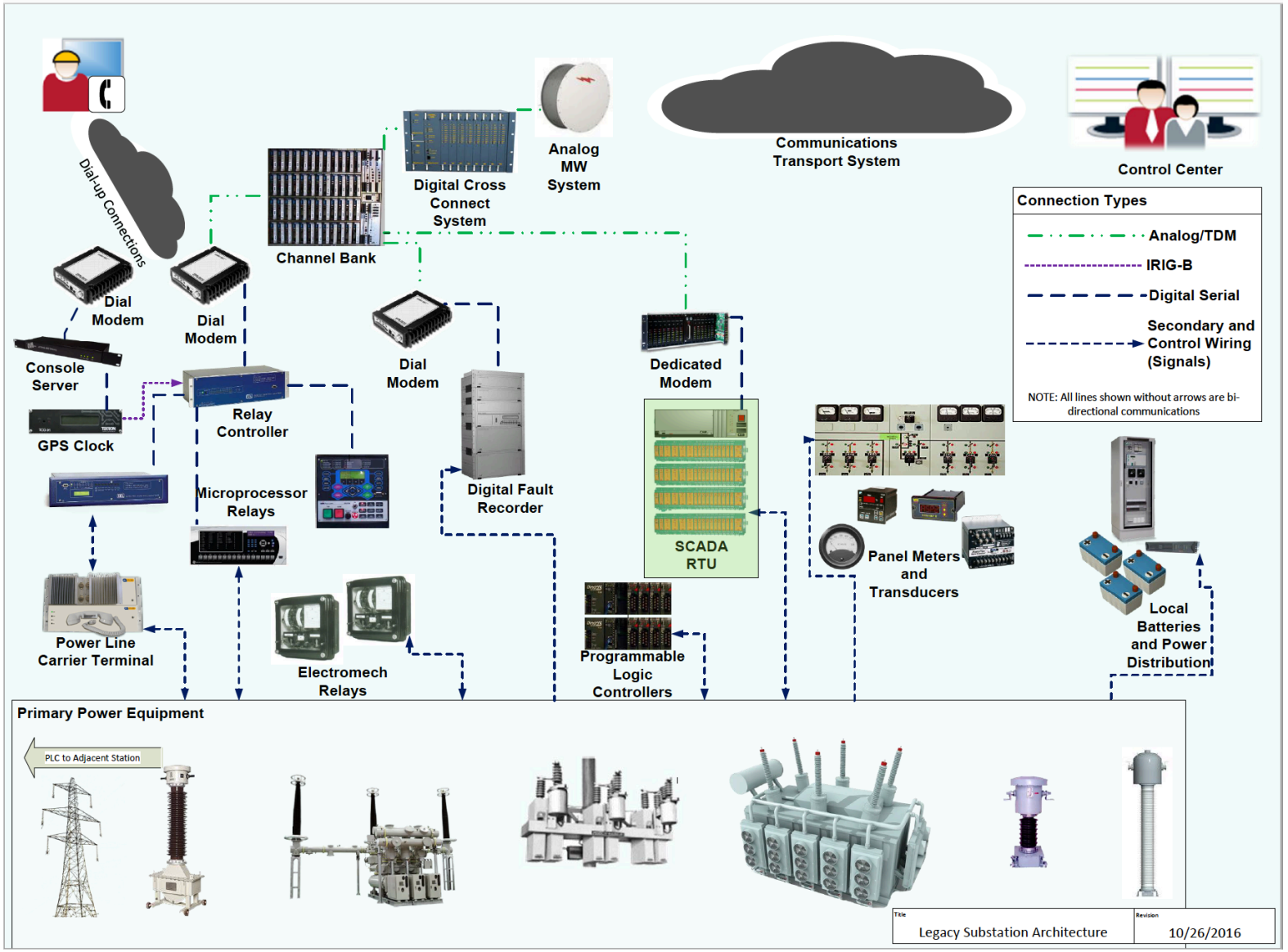


**Figure 3-3**
**Legacy Substation Security Architecture – Manually Initiated Systems**

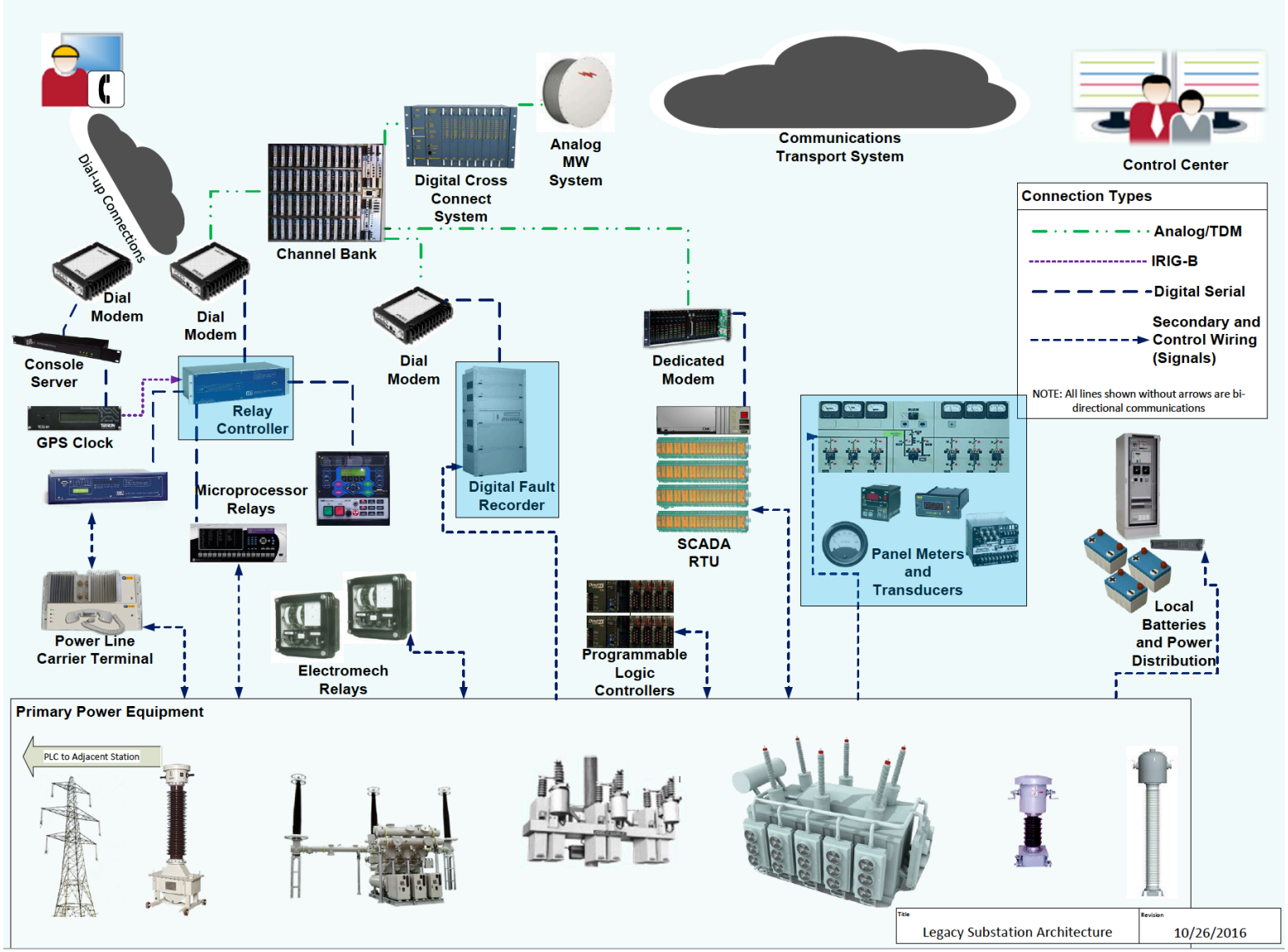


**Figure 3-4**
**Legacy Substation Security Architecture – Monitoring and Measurement Systems**

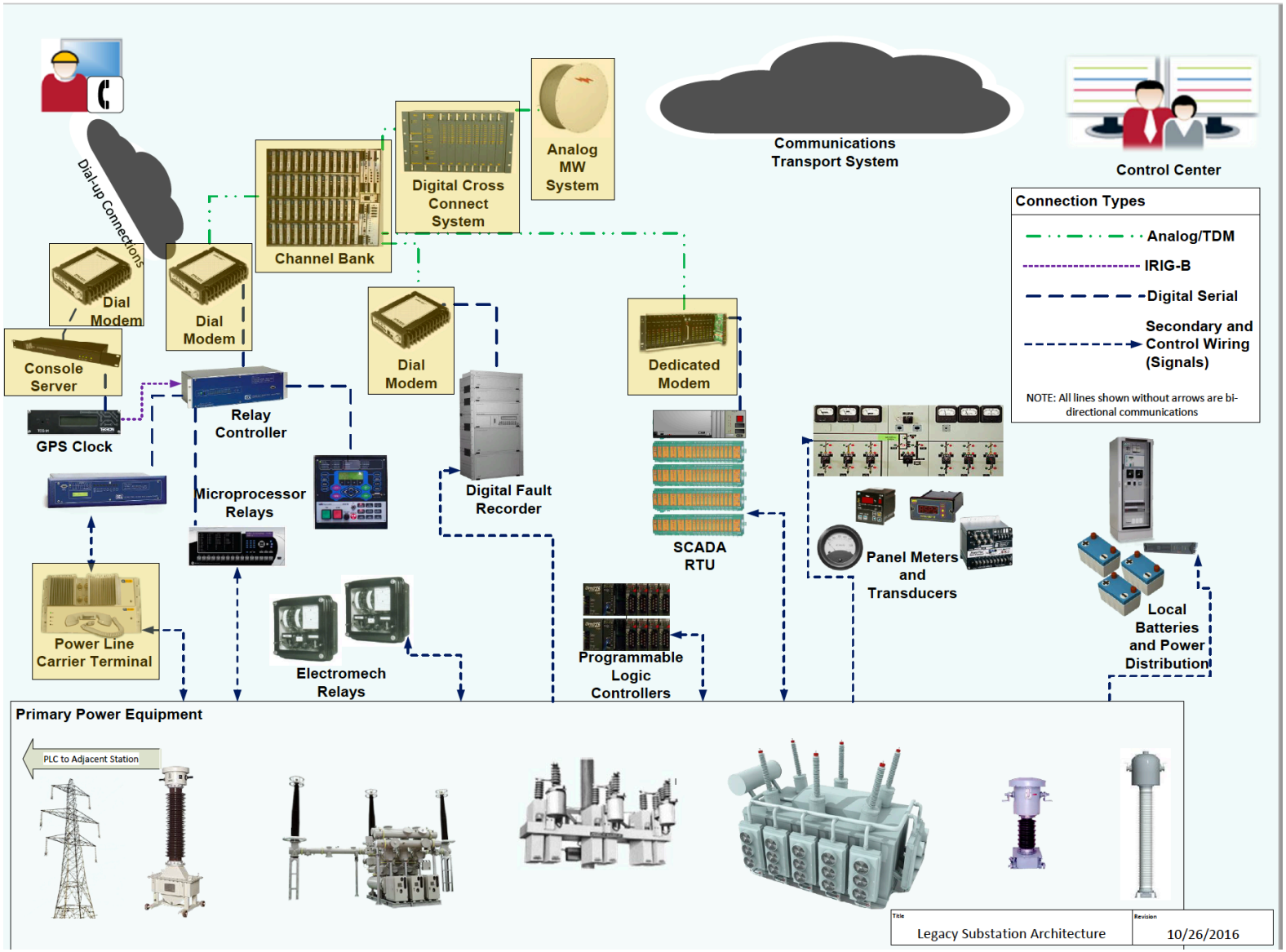


**Figure 3-5**
**Legacy Substation Security Architecture – Communications Systems**

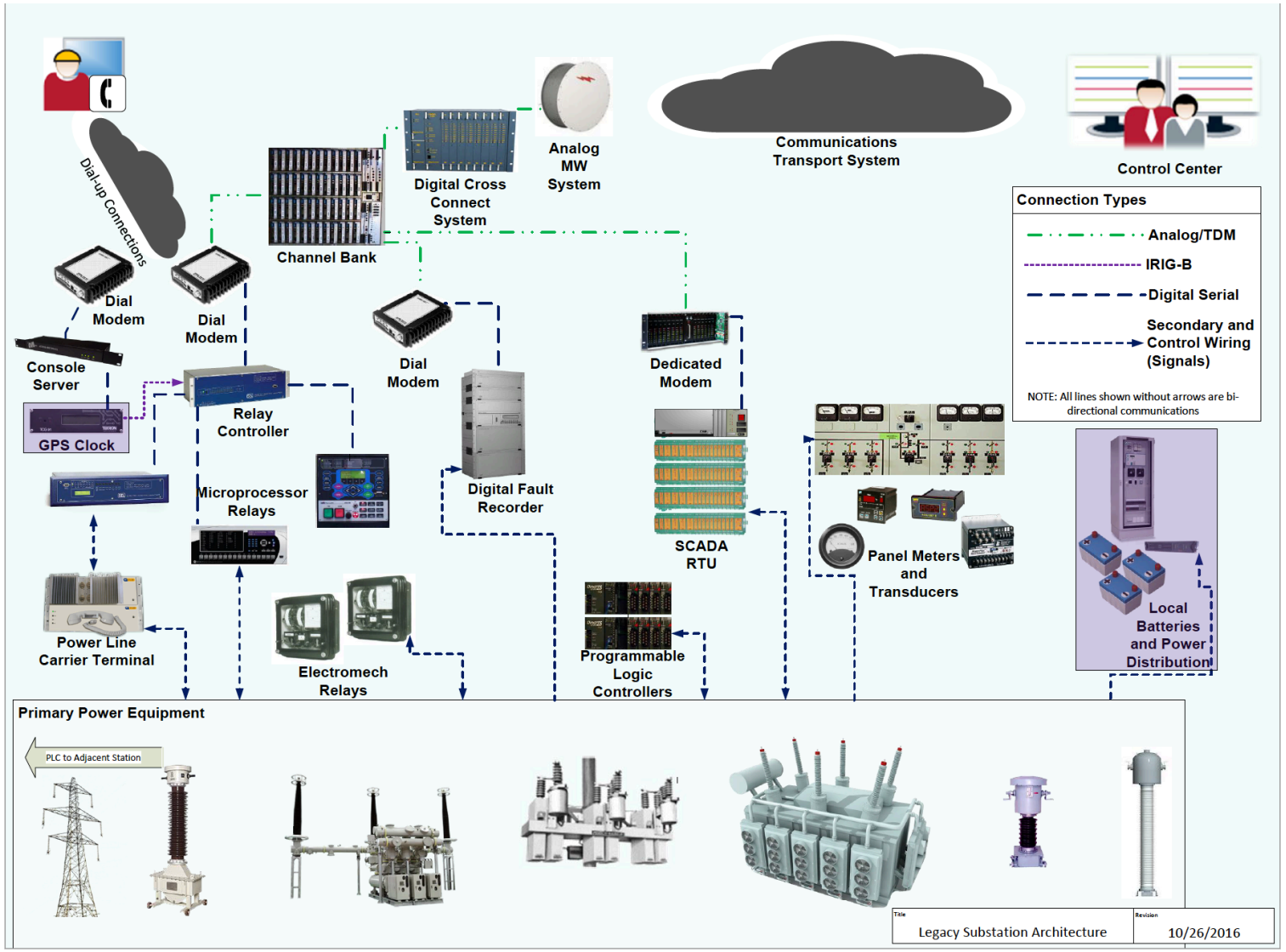


**Figure 3-6**
**Legacy Substation Security Architecture – Support Systems**

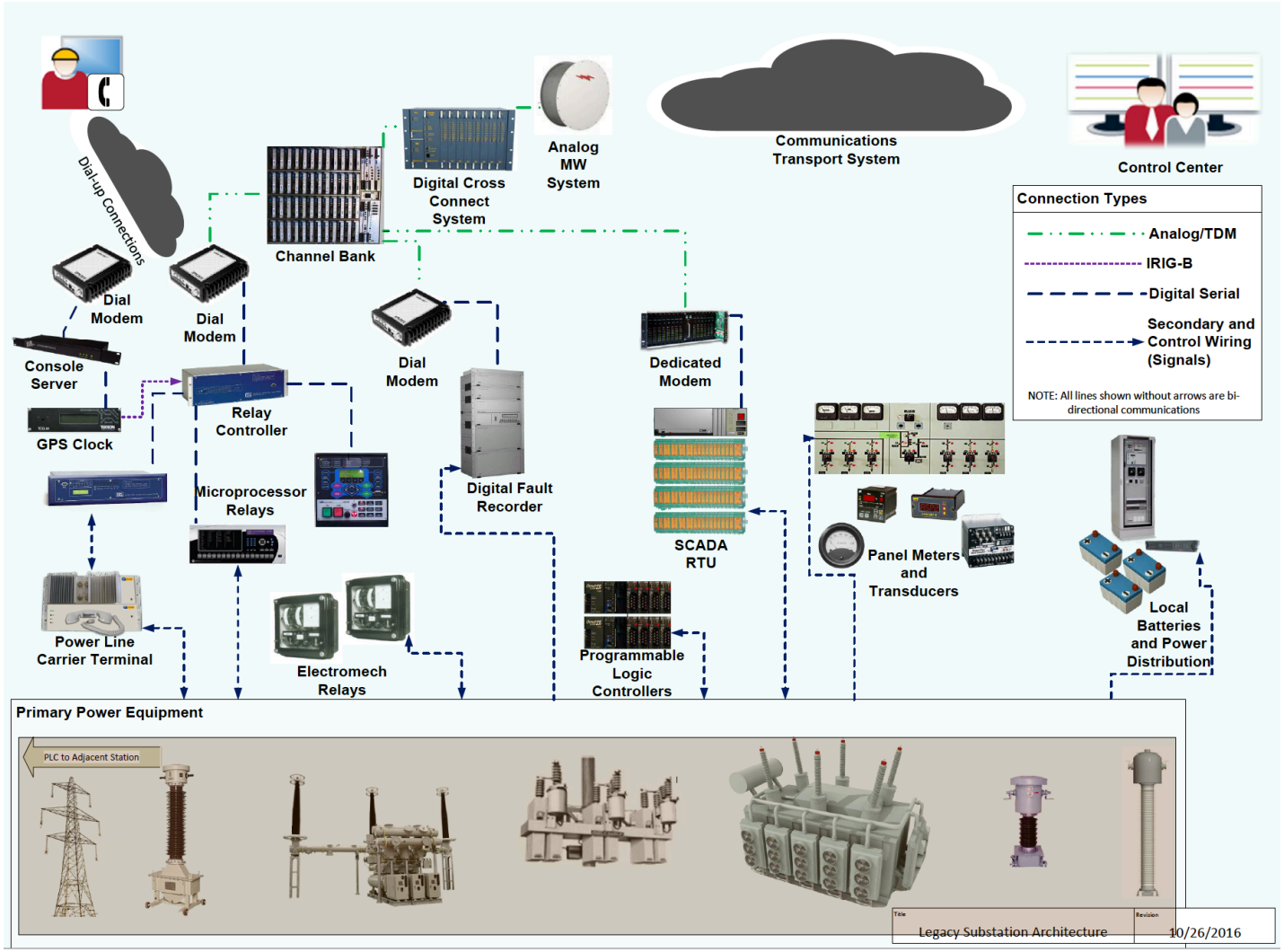


**Figure 3-7**
**Legacy Substation Security Architecture – Primary Power Systems**

## 3.2 Transition Substation Security Architecture

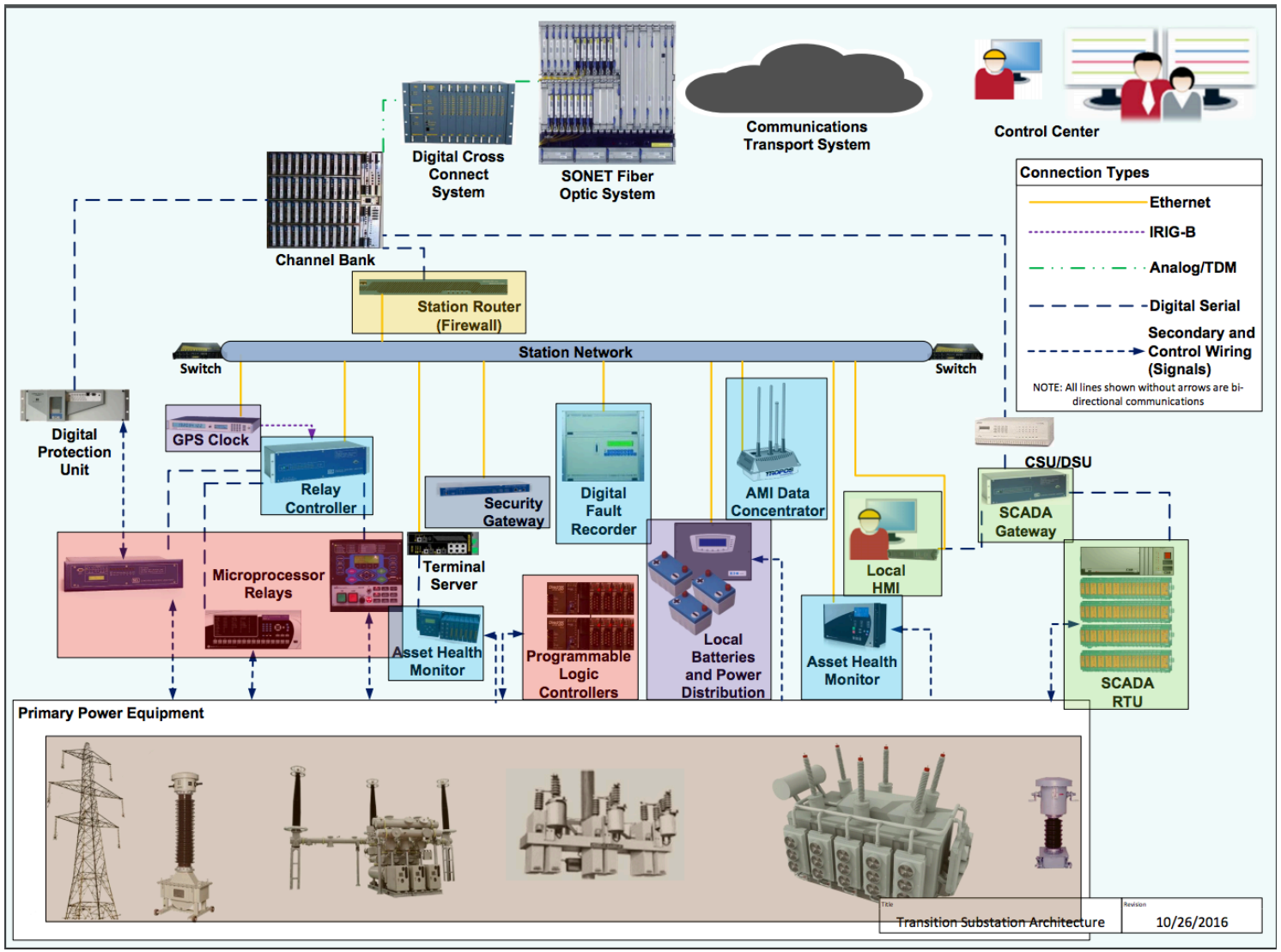


**Figure 3-8**
**Transition Substation Security Architecture – all device categories**

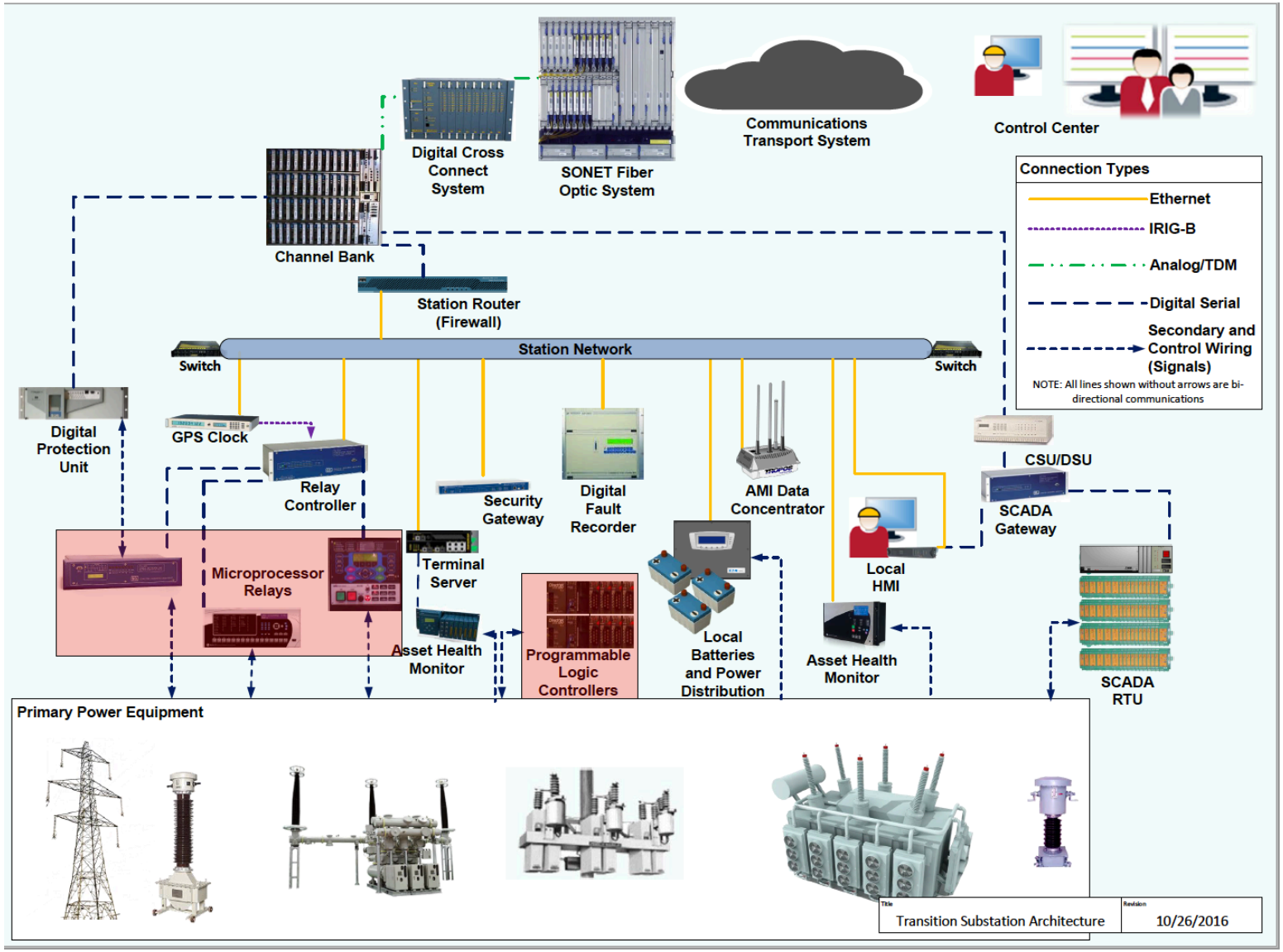


**Figure 3-9**
**Transition Substation Security Architecture – Automated Protection Systems**

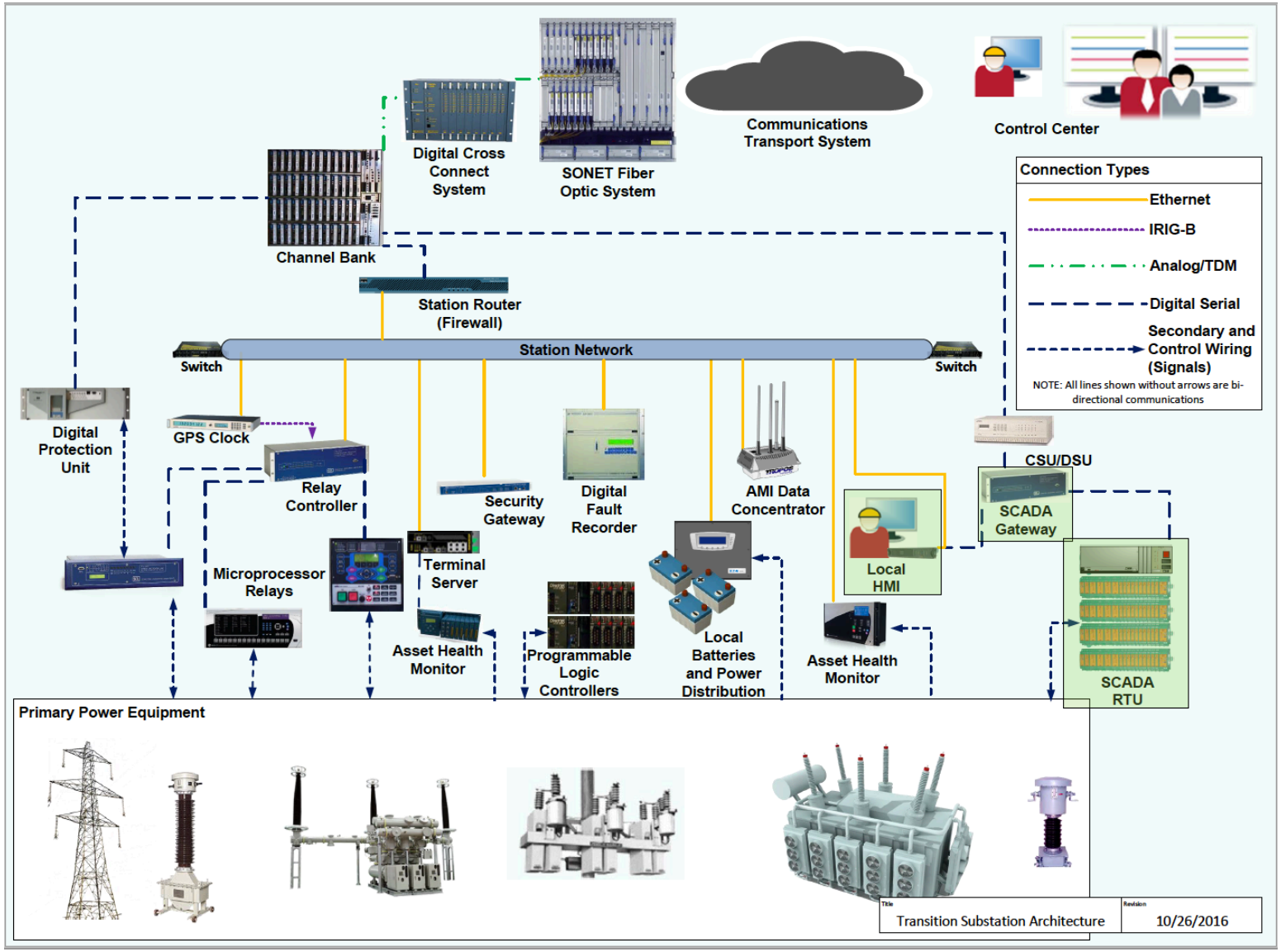


**Figure 3-10**
**Transition Substation Security Architecture – Manually Initiated Systems**

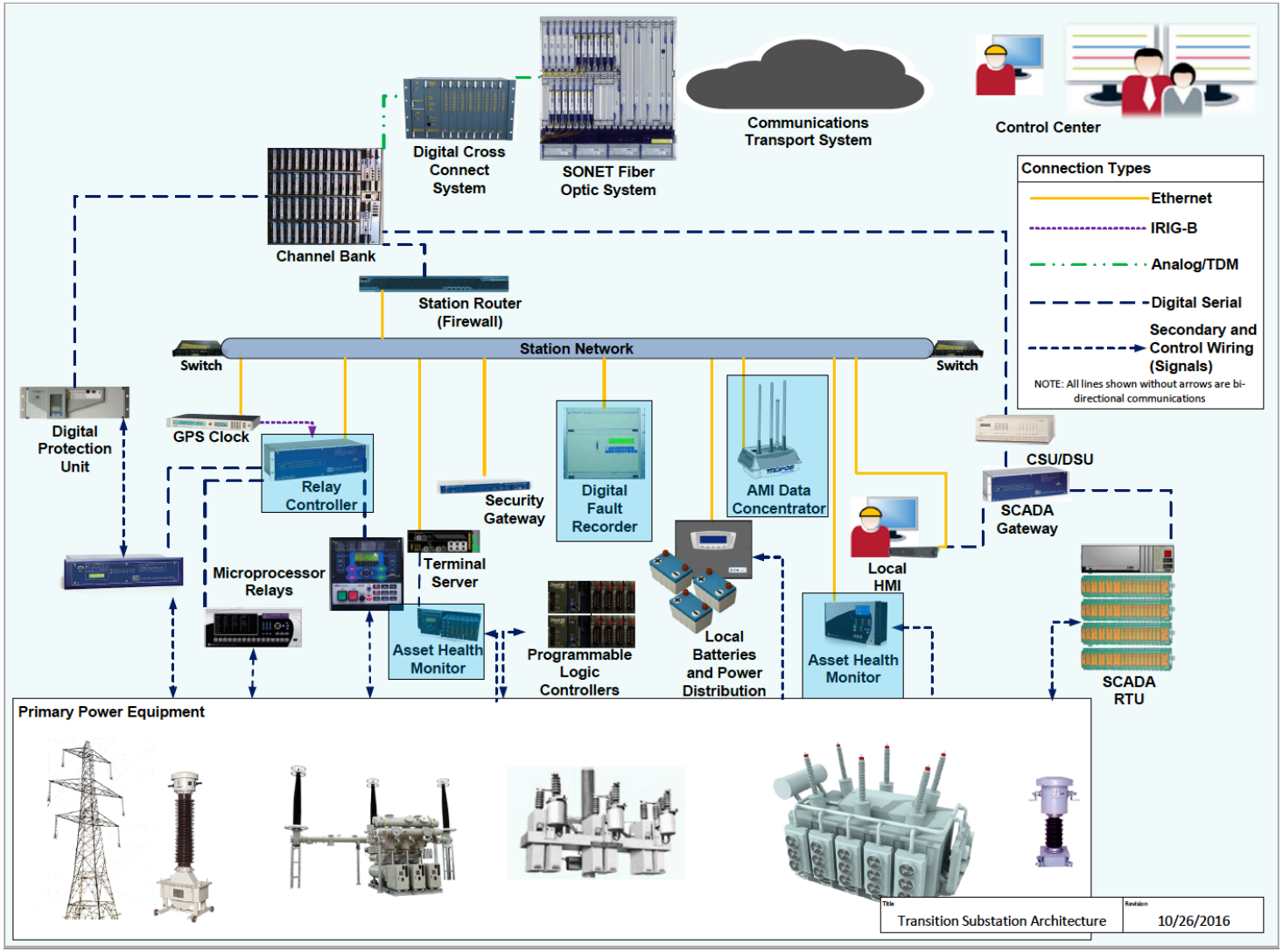


**Figure 3-11**
**Transition Substation Security Architecture – Monitoring and Measurement Systems**

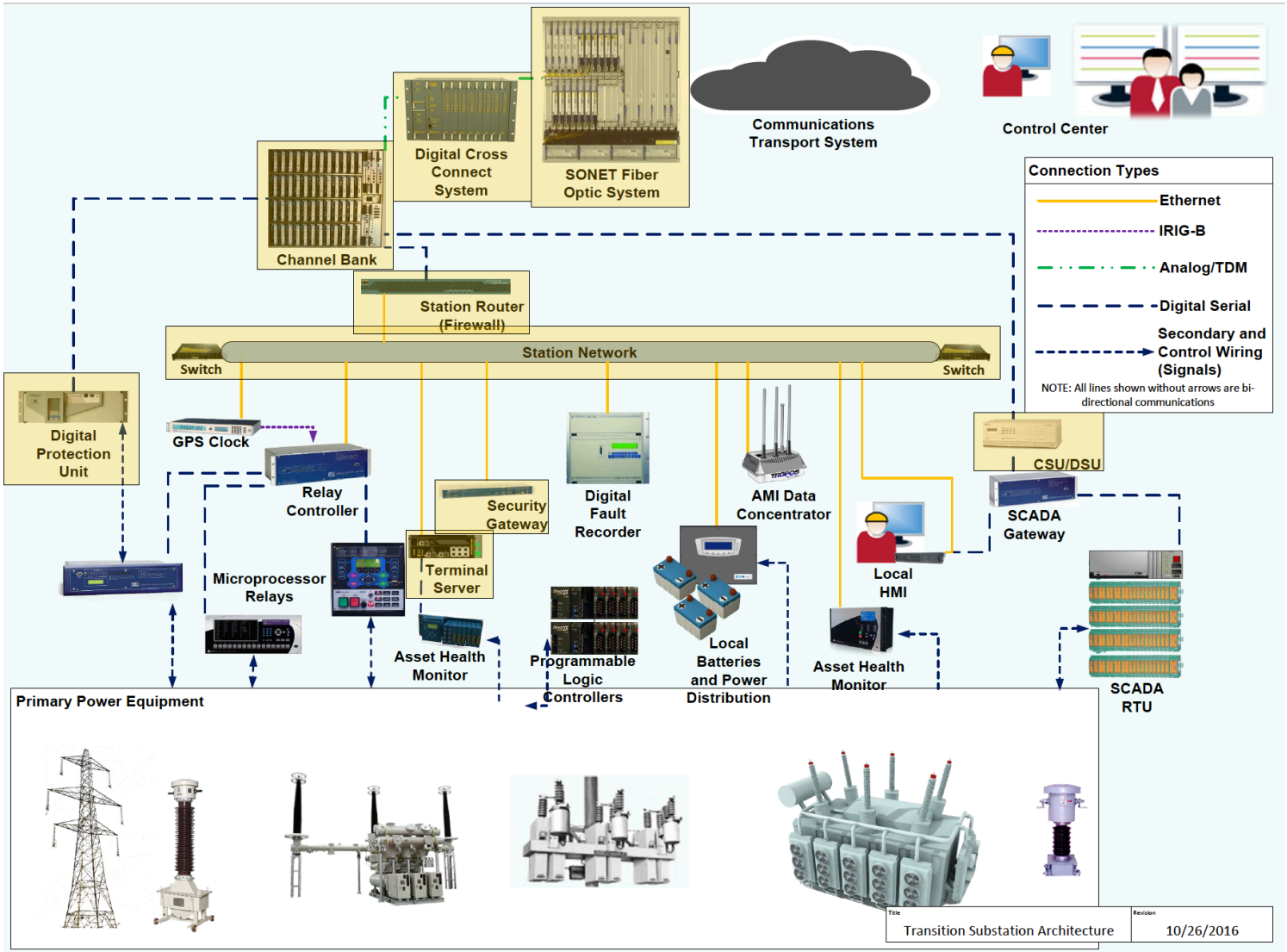


**Figure 3-12**
**Transition Substation Security Architecture – Communications Systems**

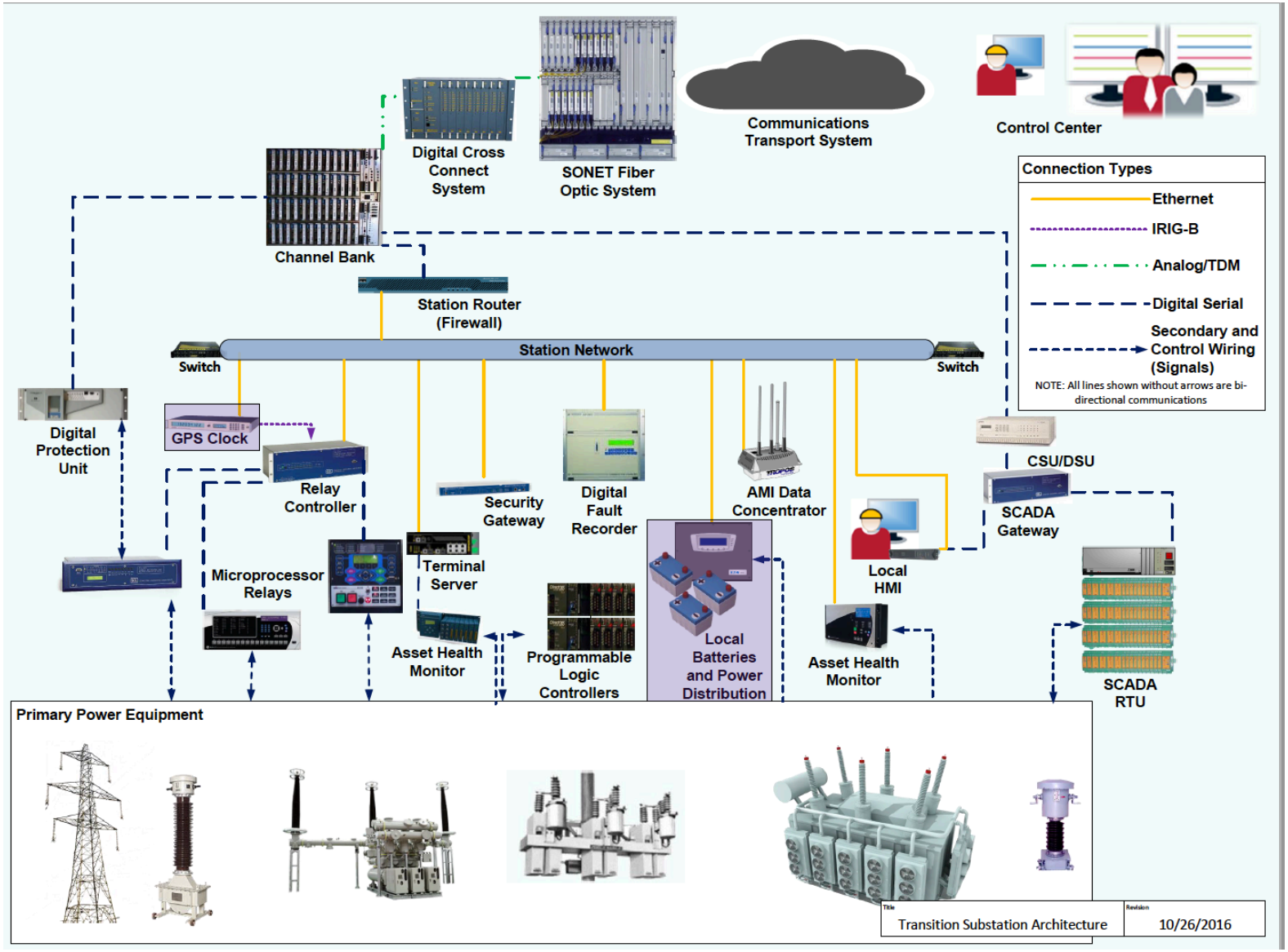


**Figure 3-13**
**Transition Substation Security Architecture – Support Systems**

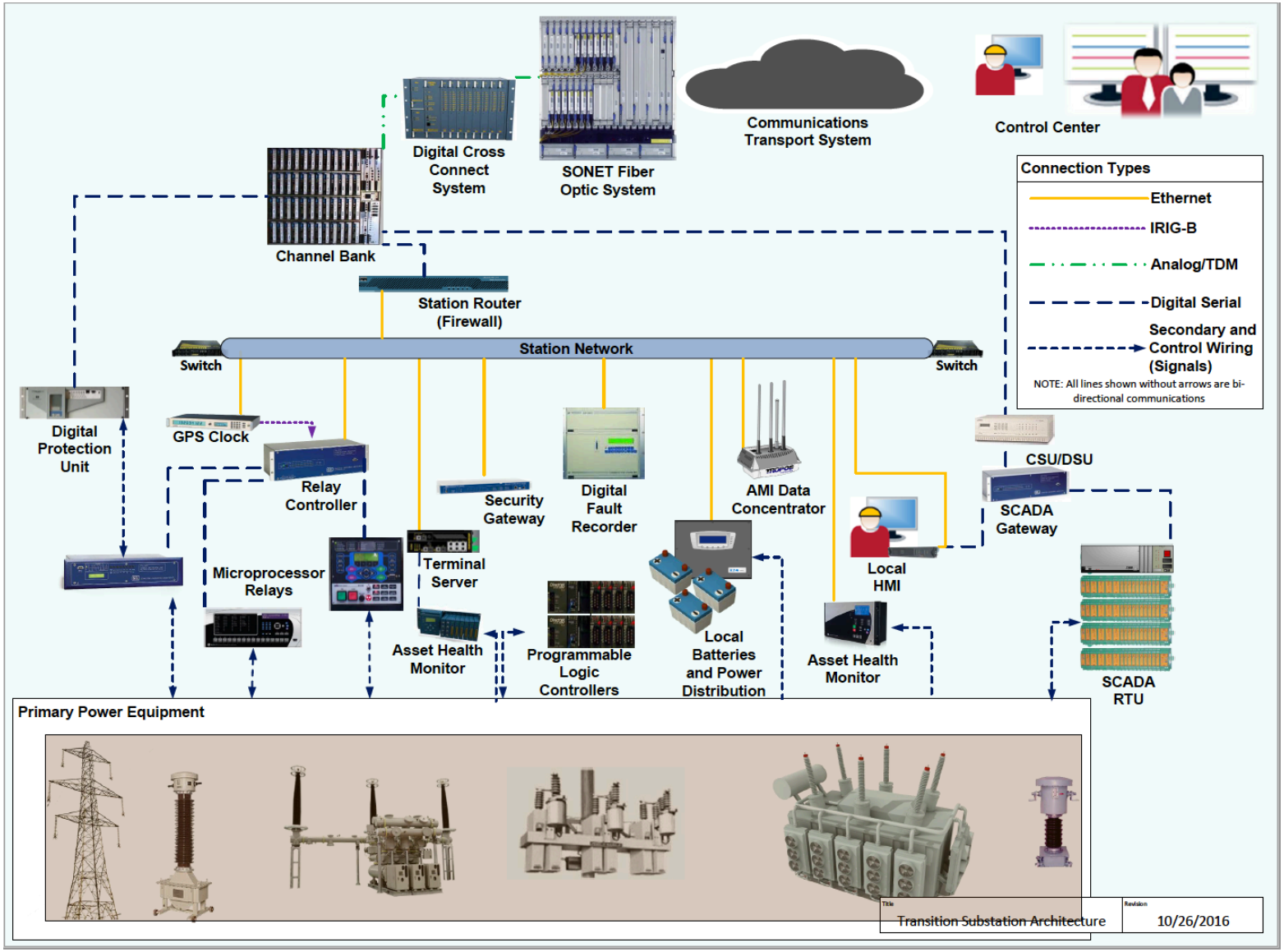


**Figure 3-14**
**Transition Substation Security Architecture – Primary Power Systems**

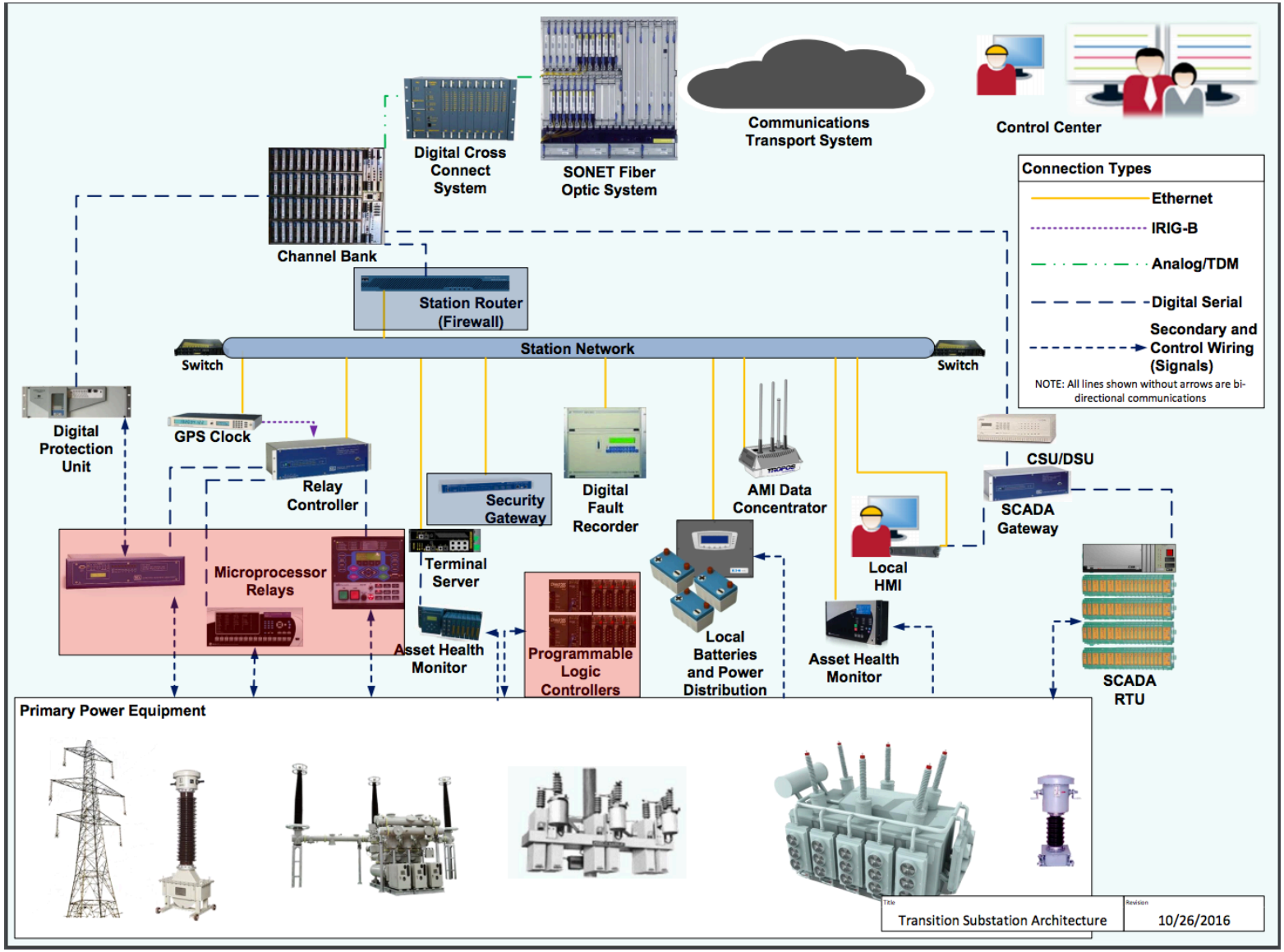


**Figure 3-15**
**Transition Substation Security Architecture – Cyber Security Systems**

## 3.3 Future Substation Security Architecture

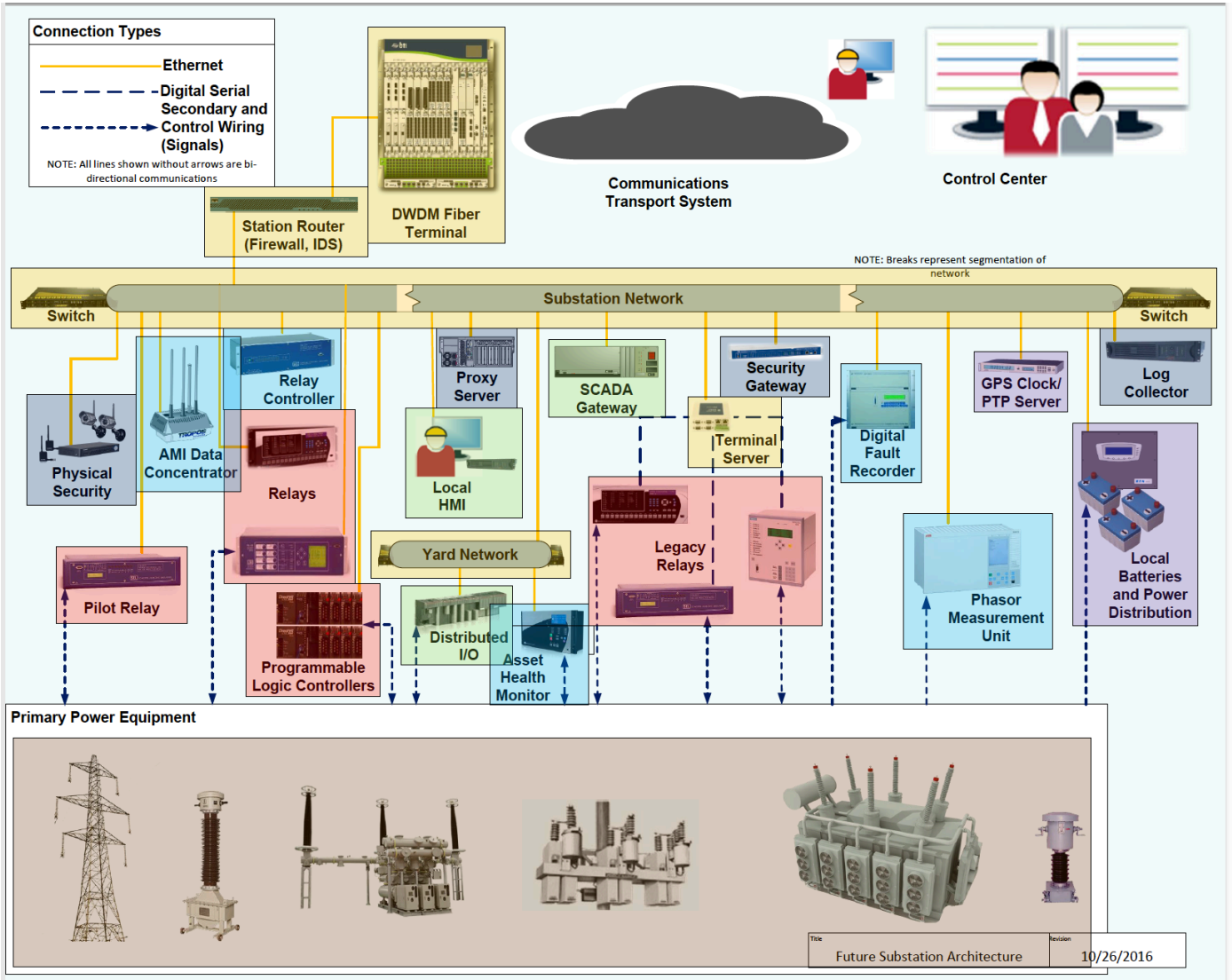


**Figure 3-16**
**Future Substation Security Architecture – all device categories**

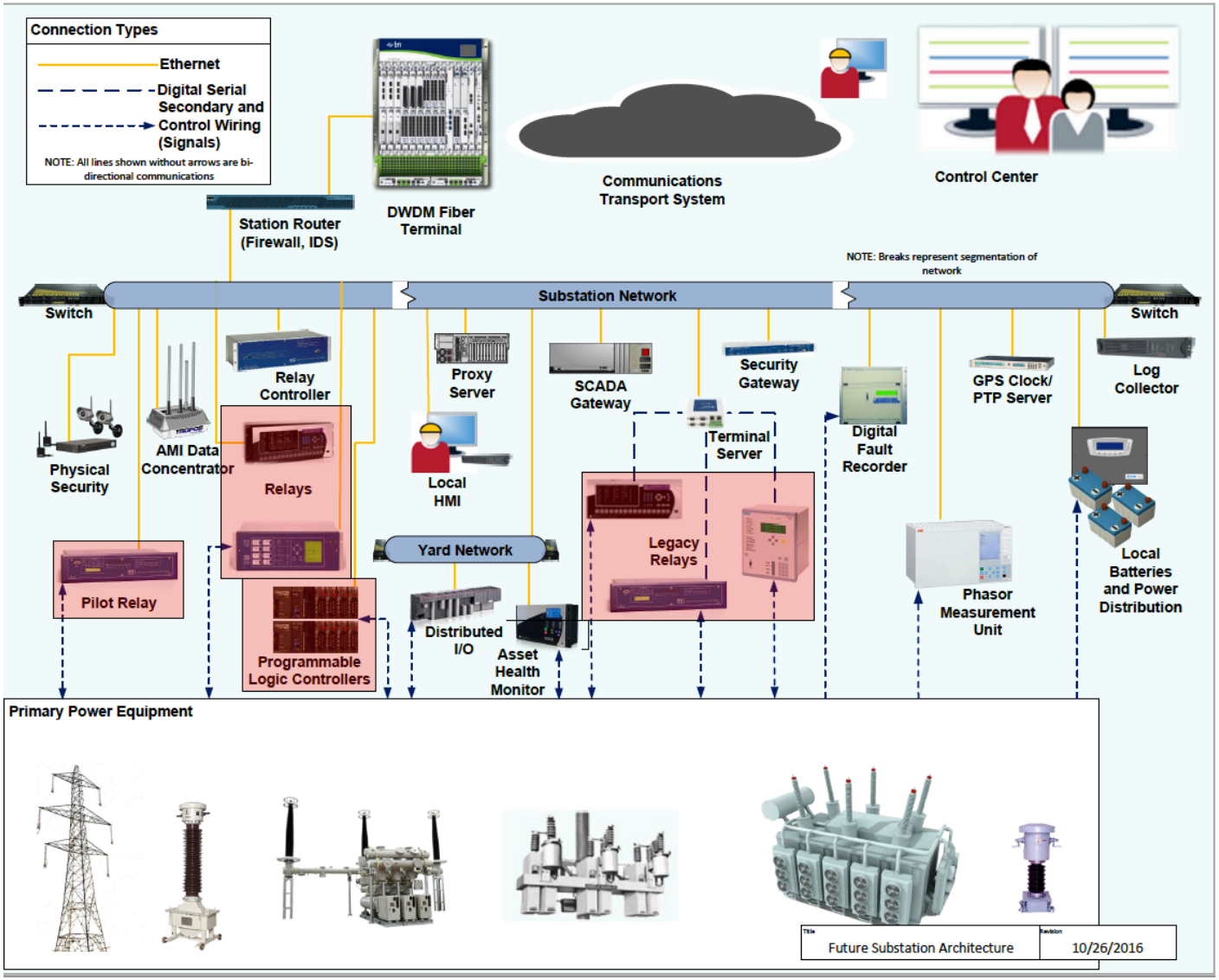


**Figure 3-17**
**Future Substation Security Architecture – Automated Protection Systems**

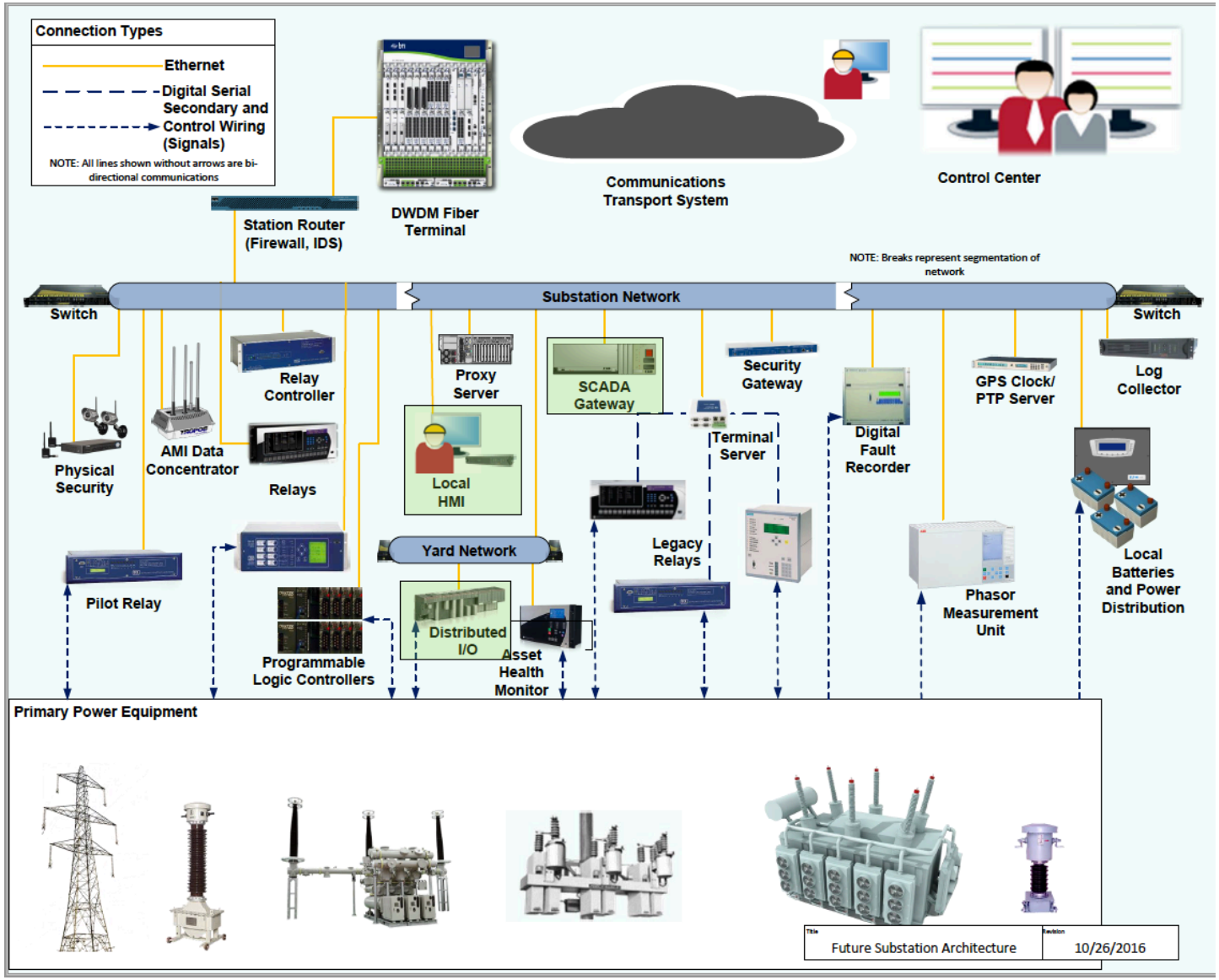


**Figure 3-18**
**Future Substation Security Architecture – Manually Initiated Systems**

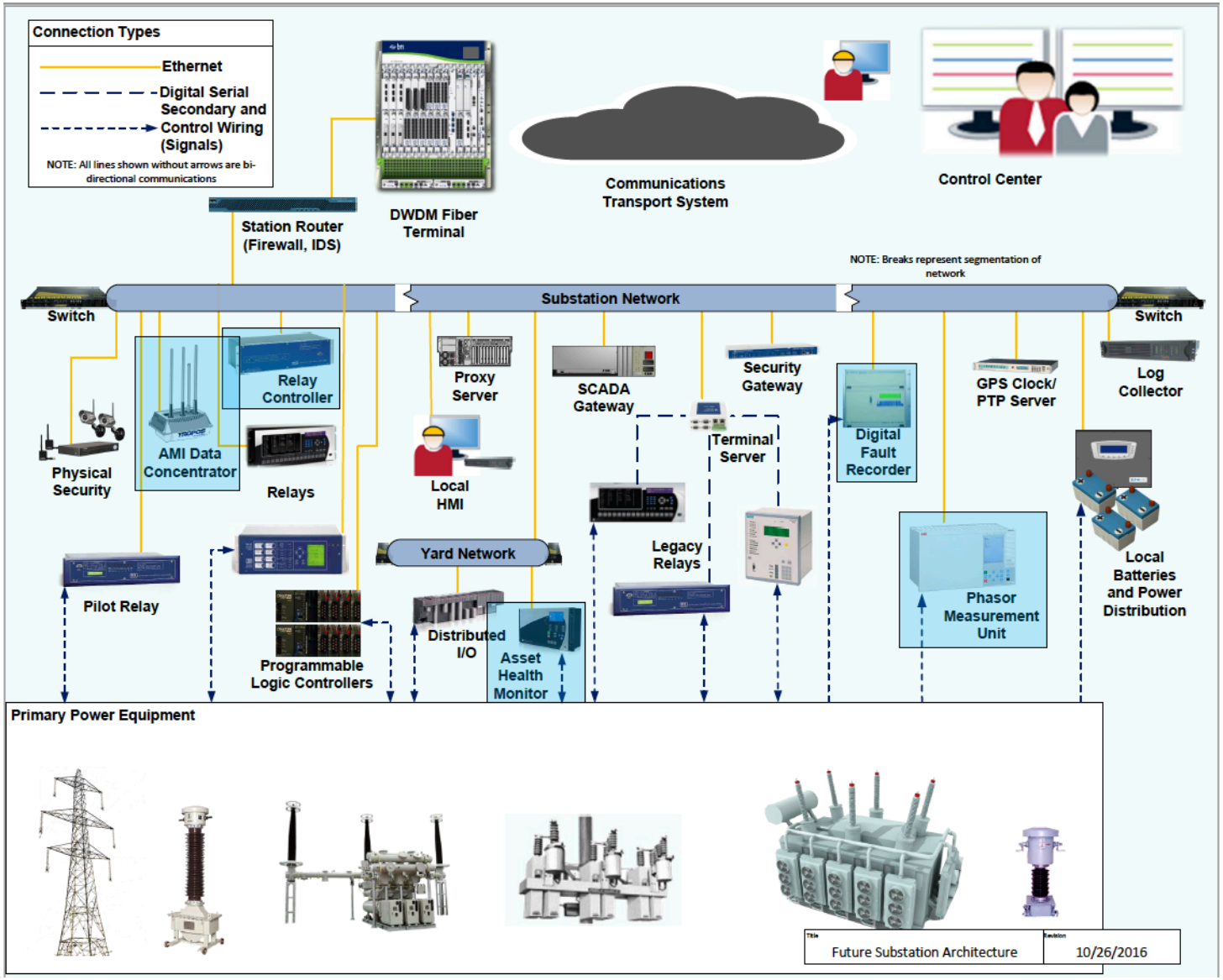


**Figure 3-19**
**Future Substation Security Architecture – Monitoring and Measurement Systems**

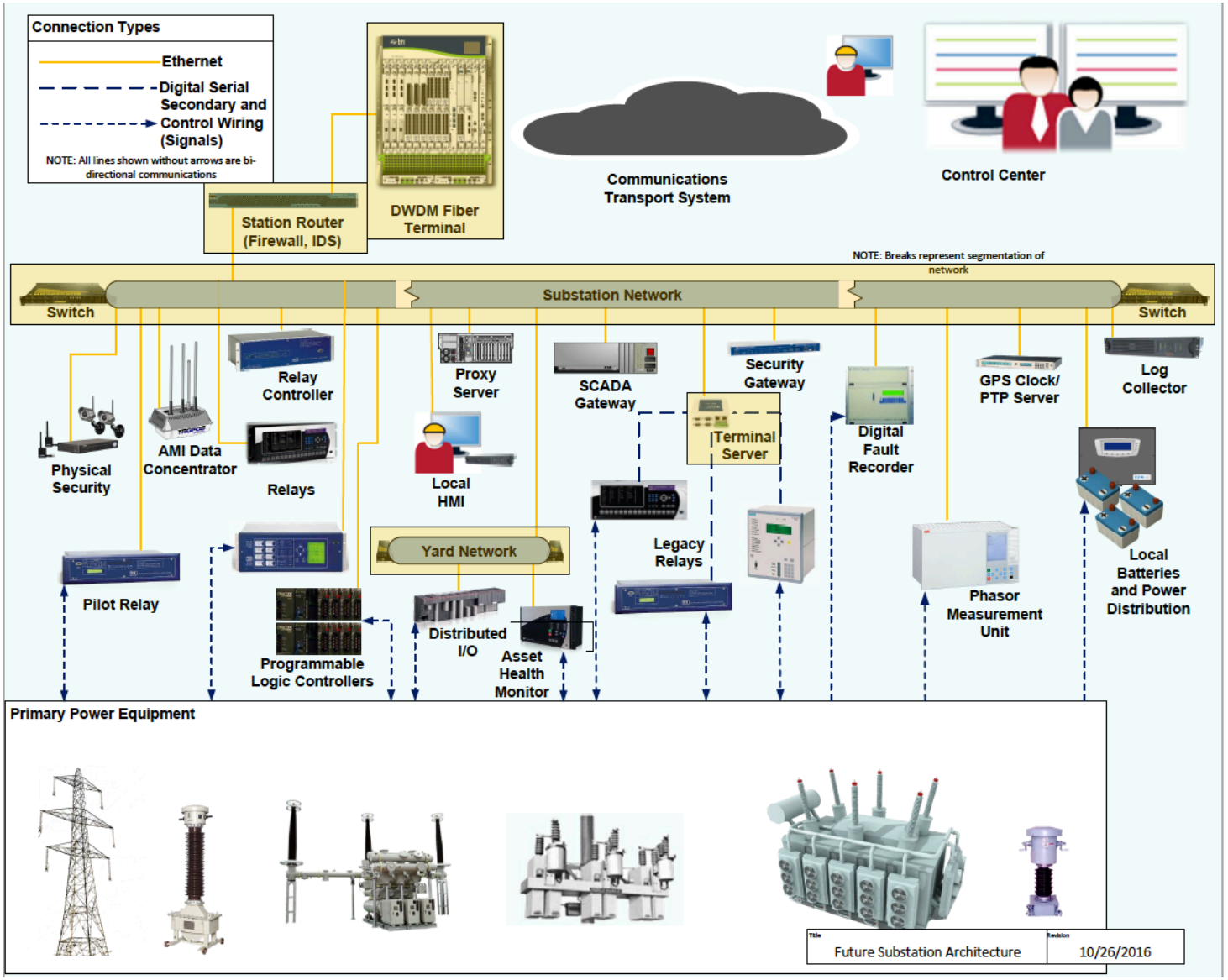


**Figure 3-20**
**Future Substation Security Architecture – Communications Systems**

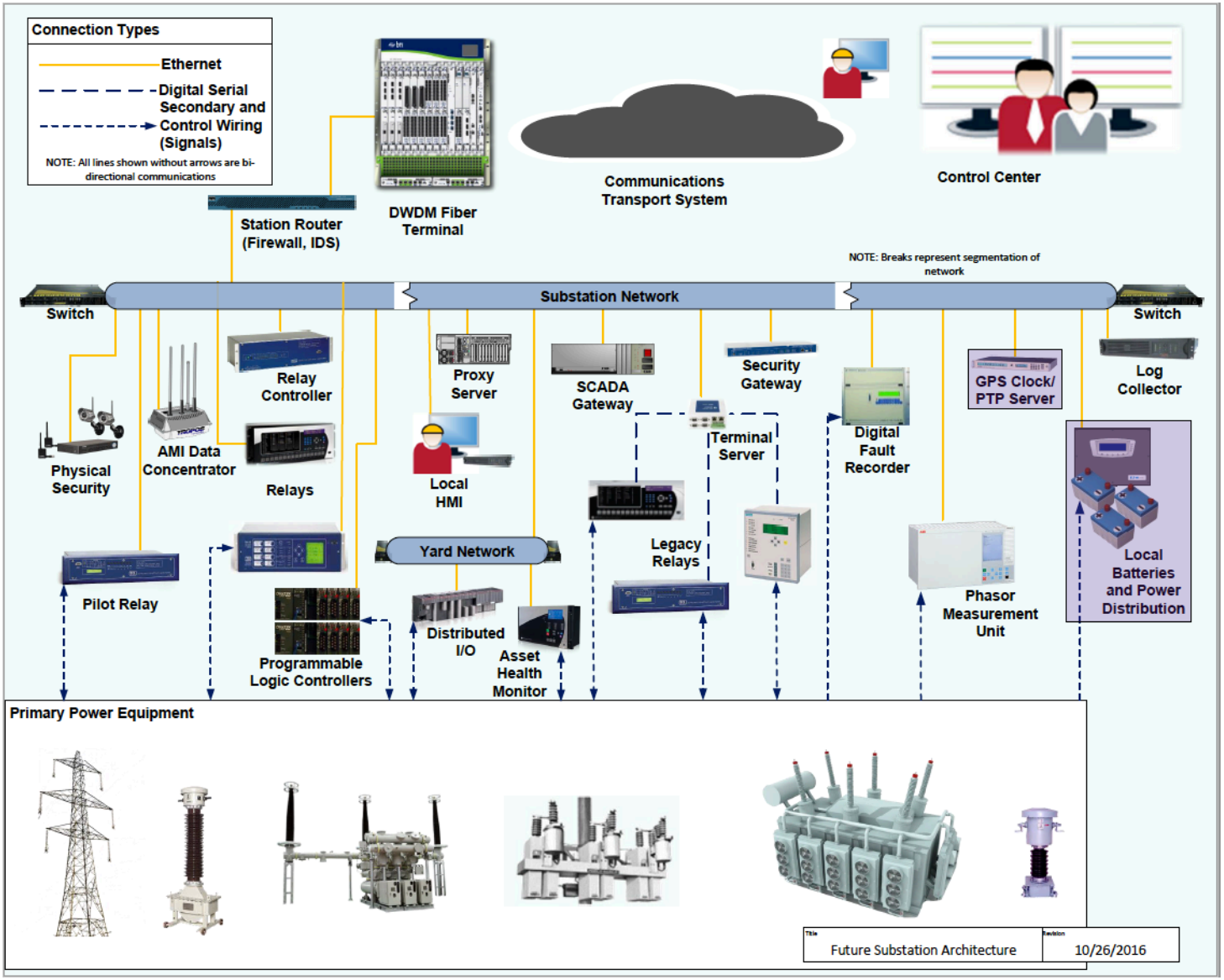


**Figure 3-21**
**Future Substation Security Architecture – Support Systems**

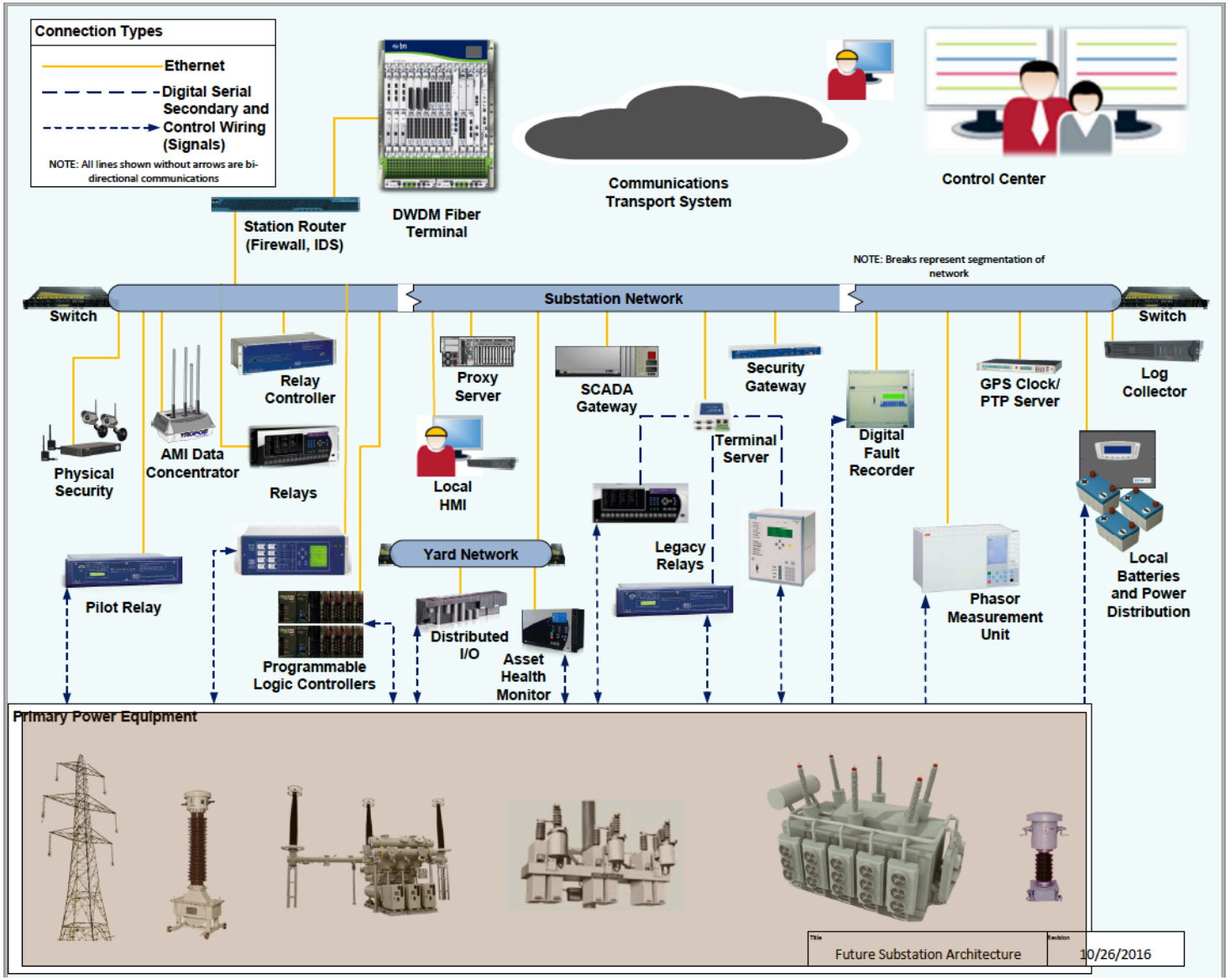


**Figure 3-22**
**Future Substation Security Architecture – Primary Power Systems**

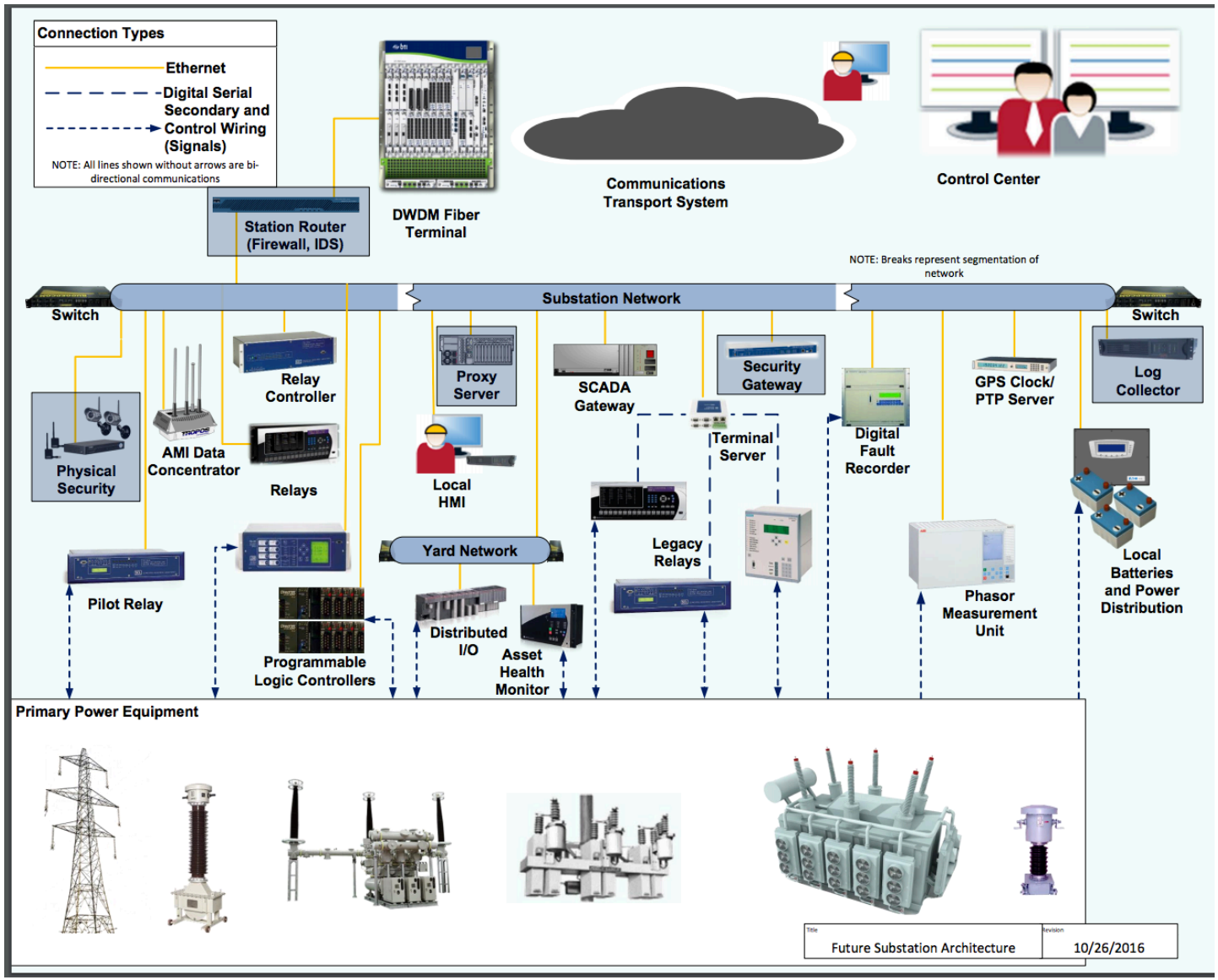


**Figure 3-23**
**Future Substation Security Architecture – Cyber Security Systems**

# 4
# REFERENCES


1. National Institute of Standards and Technology, *Framework for Improving Critical* Infrastructure *Cybersecurity Version 1.0*, February 12, 2014 [report]
2. National Electric Sector Cybersecurity Organization Resource, *Electric Sector Failure Scenarios and Impact Analyses, Version 3.0,* December 2015. [report]
3. National Institution of Standards and Technology Interagency Report (NISTIR) 7628, *Guidelines for Smart Grid Cyber Security,* Rev. 1, June 2014. [report]

**The Electric Power Research Institute, Inc.** (EPRI, www.epri.com) conducts research and development relating to the generation, delivery and use of electricity for the benefit of the public. An independent, nonprofit organization, EPRI brings together its scientists and engineers as well as experts from academia and industry to help address challenges in electricity, including reliability, efficiency, affordability, health, safety and the environment. EPRI members represent 90% of the electric utility revenue in the United States with international participation in 35 countries. EPRI's principal offices and laboratories are located in Palo Alto, Calif.; Charlotte, N.C.; Knoxville, Tenn.; and Lenox, Mass.

Together…Shaping the Future of Electricity



3002009519

**Electric Power Research Institute**
3420 Hillview Avenue, Palo Alto, California 94304-1338 • PO Box 10412, Palo Alto, California 94303-0813 • USA
800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com