CPS-CDC DESIGN DOCUMENT

PowerCyber

Adam Daniel
Brian Forsberg
Ian Pierce
Yehoshua Meyer

Faculty Advisor: Dr. Manimaran Govindarasu

Dec1407

Cyber Security Smart Grid Testbed

Dec1407

Adam Daniel

Brian Forsberg

Ian Pierce

Yehoshua Meyer

Version	Date	Author	Change
0.1	4/27/14	All	Initial Document

Table of Contents

1 Executive Summary

The CPS CDC is the combination of the Cyber Defense Competition (CDC) and a Cyber Physical System (CPS). The CPS CDC consists of several virtual and physical components which are connected through ISERink. ISERink is based on the ISEAGE testbed and provides a scalable VM environment with a routable internet and networking hardware.
For each competition there is an accompanying scenario. Each scenario has some sort of background story to keep things interesting. They also specify the responsibilities of each team.

2 Problem

Currently there are two isolated systems: ISEAGE and the PowerCyber testbed. Our goal is to integrate these two systems to create the CPS CDC.

3 Operating Environment

The PowerCyber testbed operating environment is located in Coover Hall. We are the fifth senior design team to work on and improve the testbed. The PowerCyber testbed was already implemented when we began our senior design project. We will expand the system by adding a few additional components in an effort to improve the PowerCyber testbed. The ISEAGE operating environment is also located in Coover Hall. We are the first senior design team to work on the combination of the ISEAGE and PowerCyber labs.

4 Indented Uses and Users

The intended users for the CPS-CDC are mostly undergraduate SE, CprE, and EE students. The primary use for the CPS-CDC will be to serve as a learning tool for students to grow their interest in power systems and security. Competition serves as the hook to draw in students and possibly lead them into SCADA systems security research. To supplement the competition we plan on creating learning modules to grow interest in power systems and security among students.

Competition Users

- Blue Team
    - Blue team consists of students, size often will range from 1 students to 8 students. The Blue team is responsible for protecting the systems given in a scenario.
- Red Team
    - Red team consists of professors and industry professionals. The Red team is responsible for attacking and exploiting the Blue teams.
- Green Team
    - Green team can consist of anyone interested in helping out with the competition. The Green team is responsible for being the general user, they test all the blue team systems.

5 Assumptions and Limitations

Assumptions

- That there will be access to ISERink
- Virtualized relays will be fully implemented and working
- All systems are working properly - SCADA control system, switches, RTS model, etc
- Virtualized devices will function exactly like physical devices
- Integration of SCADA environment with ISEAGE CDC is feasible
- Systems protocols provide the testbed system to accurately portray real-world protocols
- All PMUs and relays are capable of communicating with the Opal-RT physical models

Limitations

- We have two semesters for this project
- Only two physical relays and two PMU units are available
- Current virtualized substations can only be run for thirty minutes at a time
- Lab access for future CPS-CDC organizers

6 Expected End Product

By the end of this project term, we expect to have designed and implemented a scalable and portable cyber-physical defense competition. To solve portability and scalability problems, the system we create for this competition will be largely virtualized. The first CPS-CDC event is expected to take place during the Fall 2014 semester and involve only a small number of teams. The first CPS-CDC will also involve a relatively simple scenario in an effort to foster a positive learning experience for students and grow interest for future competitions. We plan to create extensive documentation for future use by subsequent teams and universities that wish to hold a CPS-CDC event.

7 Approach

Design Objectives

- This will allow us to run all hacks from a central framework that can share resources and allow multiple attacks at once on different parts of the network. Design a variety of CPS-CDC scenarios with increasing difficulty.
    - This will allow other schools to quickly start their own CPS-CDC
    - This will allow modules to easily be added to the CPS-CDC
- Design a standard implementation for scenarios
    - Scenarios should always include
        - Substations and relays
        - Communication Center
        - Attack objectives for Red Team *
        - Design objectives for Blue Team *
        - Test cases for Green Team *
- Incorporate the PowerCyber components into ISERink.
    - This will allow the CPS-CDC to actually become a reality.

* Further expiation of teams available in Section 4

8 Functional Requirements

- Scoring System
    - System for scoring of teams that can be used for all CPS-CDC.
- Virtualized Cyber-Physical Testbed
    - Design must consider resource constraints for when the CPS-CDC expands. A virtualized environment is much cheaper to scale up than one which requires a relay and PMU for each substation.
- Attack Impact Visualization
    - Attacks should be visualized in a way that it is visible to all involved with the CPS-CDC. This visualization can be as simple as a light turning off that can symbolize power being lost to a neighborhood.
- OPAL-RT Timeshare
    - System that can be used to organize the use of OPAL-RT among teams during the competition. System should be able to give teams scheduled time to run models on OPAL-RT. The running of models will also be scored and will be a part of the scoring system.
- Exploitable CPS
    - For this competition to work, there must exist viable attack vectors for red team to exploit. We will manually punch holes in the substation software before it is distributed to the teams if the inherent security flaws are not enough.

9 Non-Functional Requirements

- Scalable
    - Scenarios should be scalable to allow competitions consisting of a few teams all the way up to competitions containing many teams.
- Portable
    - The entirety of the CPS-CDC should be easily portable physically along in the sense of ease of portability to other schools. Other Universities must be able to host their

own CPS-CDC events without specialized power systems hardware (OPAL-RT, relays, PMU's).

- Well Documented
    - Well documented information to ease the set-up of CPS-CDC for future competition along with first time competitions for new schools.
- Learning documents to assist students come competition time
    - Vast documentation of many aspects on the competition to provide assistance to students due to the small number of students familiar with SCADA and power systems.
- Maintainable
    - All security holes in the CPS must be well documented and replicable. This documentation be used as a reference by those working on the CPS-CDC and also aid subsequent teams who research smart grid security.

10 Technical Consideratoins

ISEAGE - a cluster of nodes which are capable of simulating an arbitrary, reconfigurable, static routing topology that is abstracted away from the physical hardware

- Contains a suite of tools to research internet-scale cyber security events in a controlled environment
- *ISEFLOW* - The core of ISEAGE
    - Routes packets between the flows to ensure proper delivery
- *ISEBOX* - A portable version of ISEAGE
    - the virtual implementation of an ICLE
    - Consists of a high-powered server running the VMWare ESXi operating system

ICLE - the backbone of ISEAGE, simulating the routing infrastructure of arbitrary networks.

11 Cost

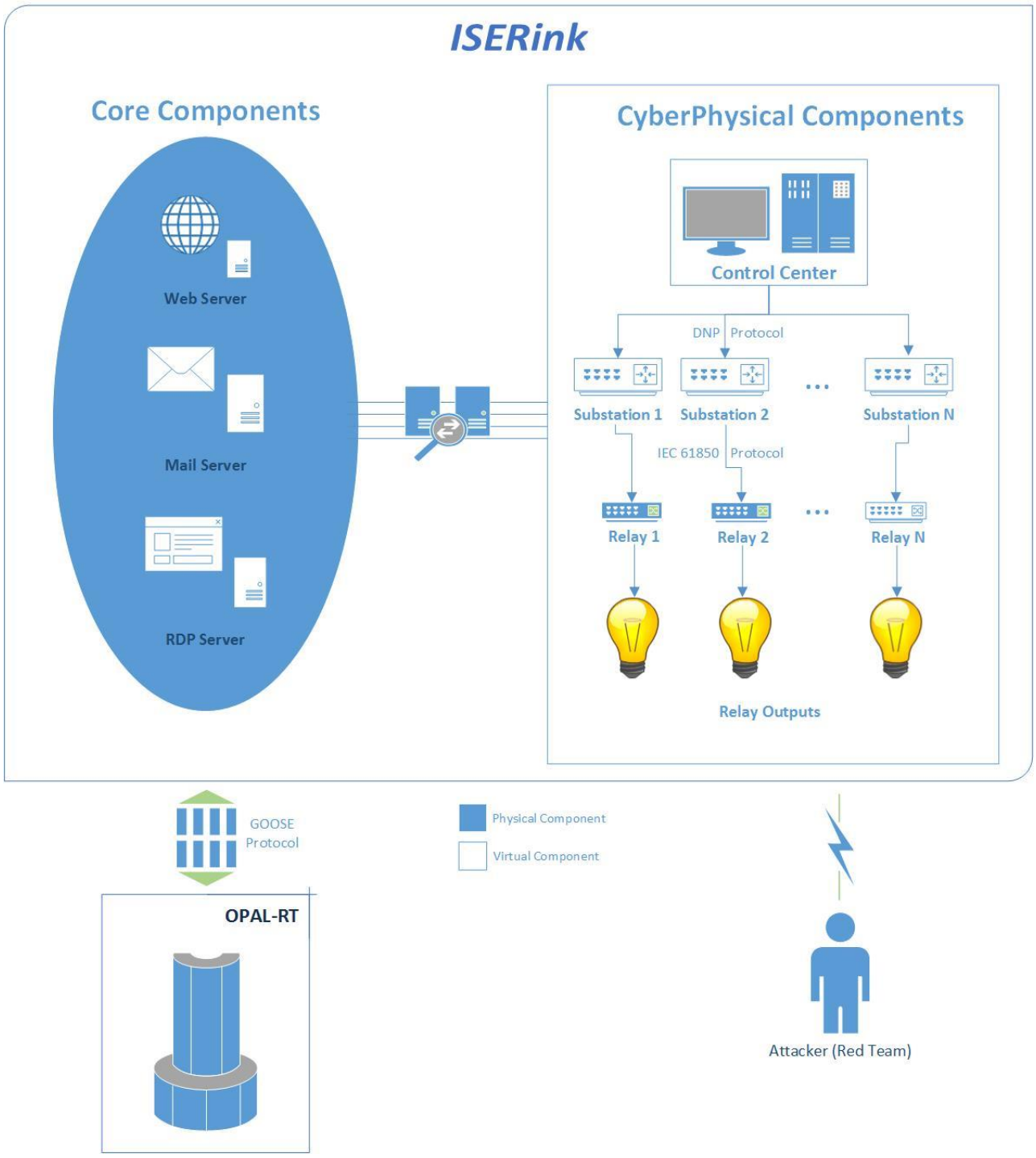
Due to the joint effect of the PowerCyber and ISEAGE labs, the overall cost of the CPS-CDC will be near zero. The largest cost will come from the electricity which is assumed to be covered by the lab.

12 Integration Testing

Throughout the set up process of the CPS-CDC different modules of the competition will be mocked out. Through mocking out the various components it will allow testing. Items that can be mocked out include the relays, substations, and control centers.

13 Detailed Design

The diagram on the next page defines the structure of a typical CPS-CDC. We have split ISERink into its core (traditional) components and the new CyberPhysical components. Outside of ISERink is the OPAL-RT model which persists changes to the power grid using the GOOSE protocol. The CyberPhysical component will typically consist of a control center and multiple virtual substations. The control center will communicate with the substations via the DNP protocol. Each substation will have a single relay. Substations and relays will communicate using an IEC 61850 protocol. Currently we have two physical relays and are planning on incorporating additional virtual relays when available. These relays will be connected to some sort of output such as a light or switch.


ISERink
Core Components
Web Server
Mail Server
RDP Server
CyberPhysical Components
Control Center
DNP Protocol
Substation 1
Substation 2
Substation N
IEC 61850 Protocol
Relay 1
Relay 2
Relay N
Relay Outputs
GOOSE Protocol
OPAL-RT
Physical Component
Virtual Component
Attacker (Red Team)

14 Closing Summary

The Cyber Physical System - Cyber Defense Competition is largely based around the combination of PowerCyber components and the ISERink system. This combination of these two key components allows for future continued learning for students which is one of the largest goals of the CPS-CDC. We are attempting to ease the learning process by designing additional learning material that will accompany the CPS-CDC. There needs to be improved virtualization of a few of the modules including the relays and substations.

15 Definitions

SCADA - Supervisory Control and Data Acquisition

Smart Grid - Electrical grid that uses information and communication technology to gather and act on information

Testbed - A platform for simulation of large developmental projects that cannot be experimented on in their real world/implemented versions

ISEAGE - Internet-Scale event and Attack Generation Environment

PMU - Phasor Measurement Unit

RTDS - Real Time Digital Simulator

CPS-CDC - Cyber Physical System, Cyber Defense Competition

Opal-RT - Software, hardware, and target node used for real time simulations

VMWARE - Software that allows for virtualization of operating systems

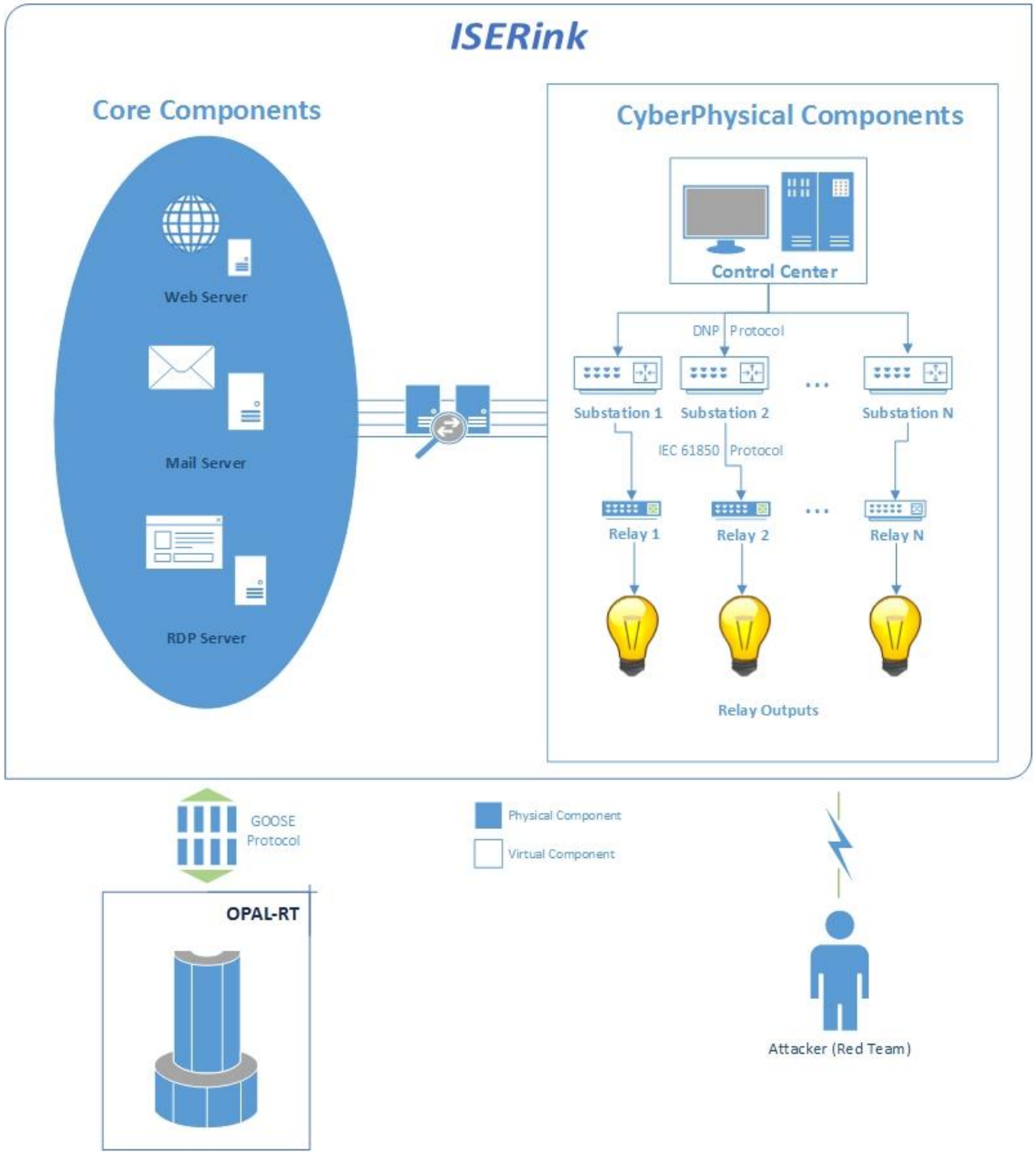
GOOSE - Generic Object Oriented Substation Events that utilizes the IEC 61850 and OPC 61850 protocols

16 Appendix A, Scenarios

16.1.1 Scenario 1

Massive Electric, LLC

Architecture:



Blue Team Description:

You have been brought into replace workers who were all recently fired. Previous employees were fired because they were found to be traitors and corporate spies. Welcome to Massive Electric! You along with your team have been assigned to the Mid-West central substation located in Ames, Iowa. Here at Massive Electric we pride ourselves on non-stop accessibility to our services for customers. However, we fear that many of our previous employees have left us very open to attack which would serious damage our reputation. Your team's job is to find and patch all systems. A majority of systems cannot simply be replaced because of our need for constant uptime, which means we are counting on your team to go through our systems with a fine tooth comb and straighten any crazy hairs. You substation is responsible for a variety of systems ranging from web servers, accessed by our customers, to the SCADA substation that provides our customers' power.

Blue Team Defends:

- Webserver used by green team.
- SCADA substation
- Flags placed in various locations
- RDP that will be used by Massive Electric HQ

Red Team Attacks:

- Webserver used by green team
- Blue team substations
- Substation traffic coming from and going
- Flags
- RDP

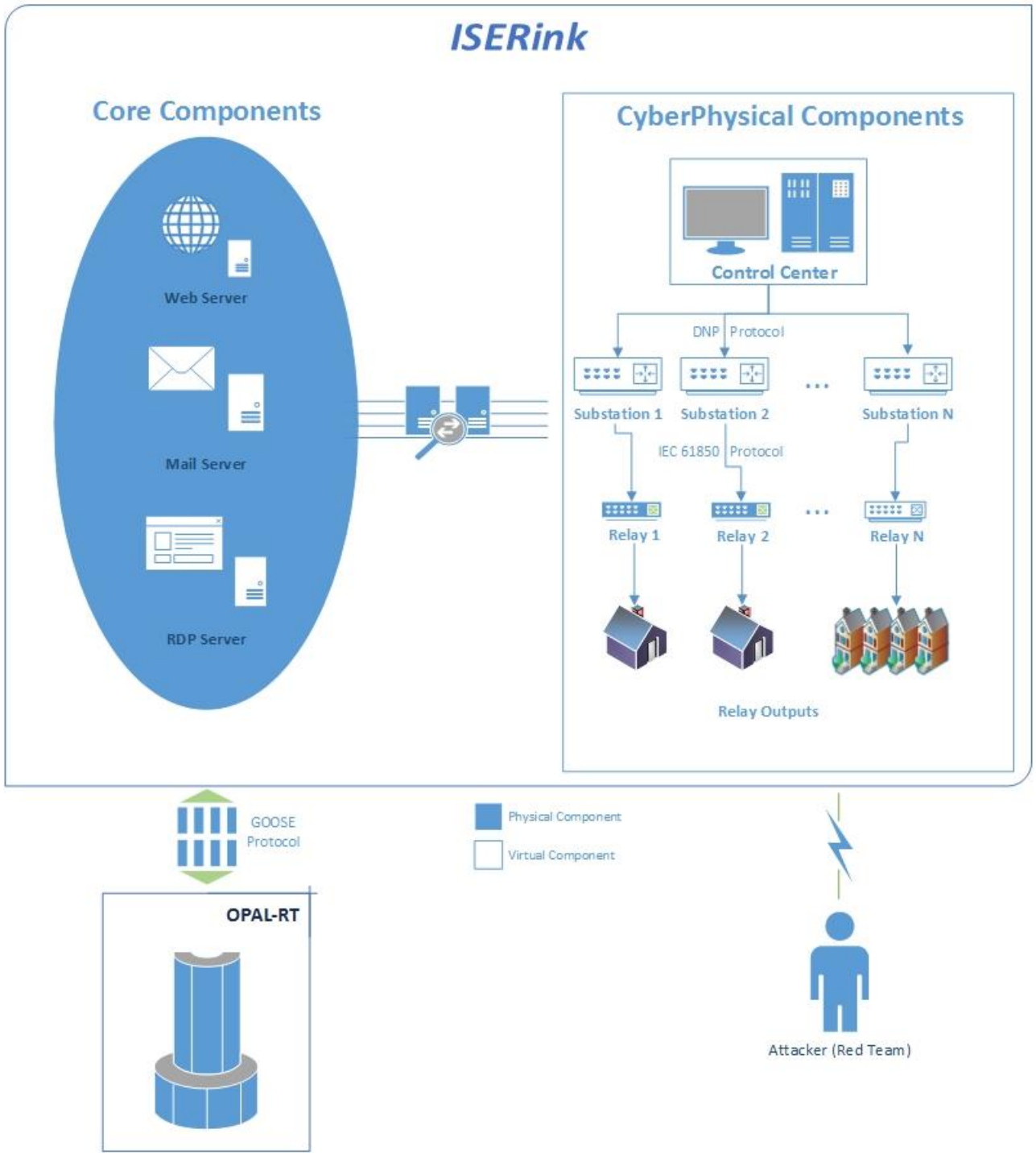
Green Team Tests:

- Webserver
- Accessibility to electrical utilities
- RDP

16.1.2 Scenario 2

Eco Electric

Architecture:



Blue Team Description:

You and your team have been brought on to help in the growth of Eco Electric. Here at Eco Electric we pride ourselves on providing clean energy to our customers while sponsoring renewable energy research nationwide. However, despite all of our progress and continued growth, we've picked up a few haters along the way. There are many companies out there that would like to see Eco Electric fall short of its goals. It is your job to protect Eco Electric from its haters.

Blue Team Defends:

- Webserver used by green team.
- SCADA substation
- Flags placed in various locations+

Red Team Attacks:

- Webserver used by green team
- Blue team substations
- Substation traffic coming from and going
- Flags

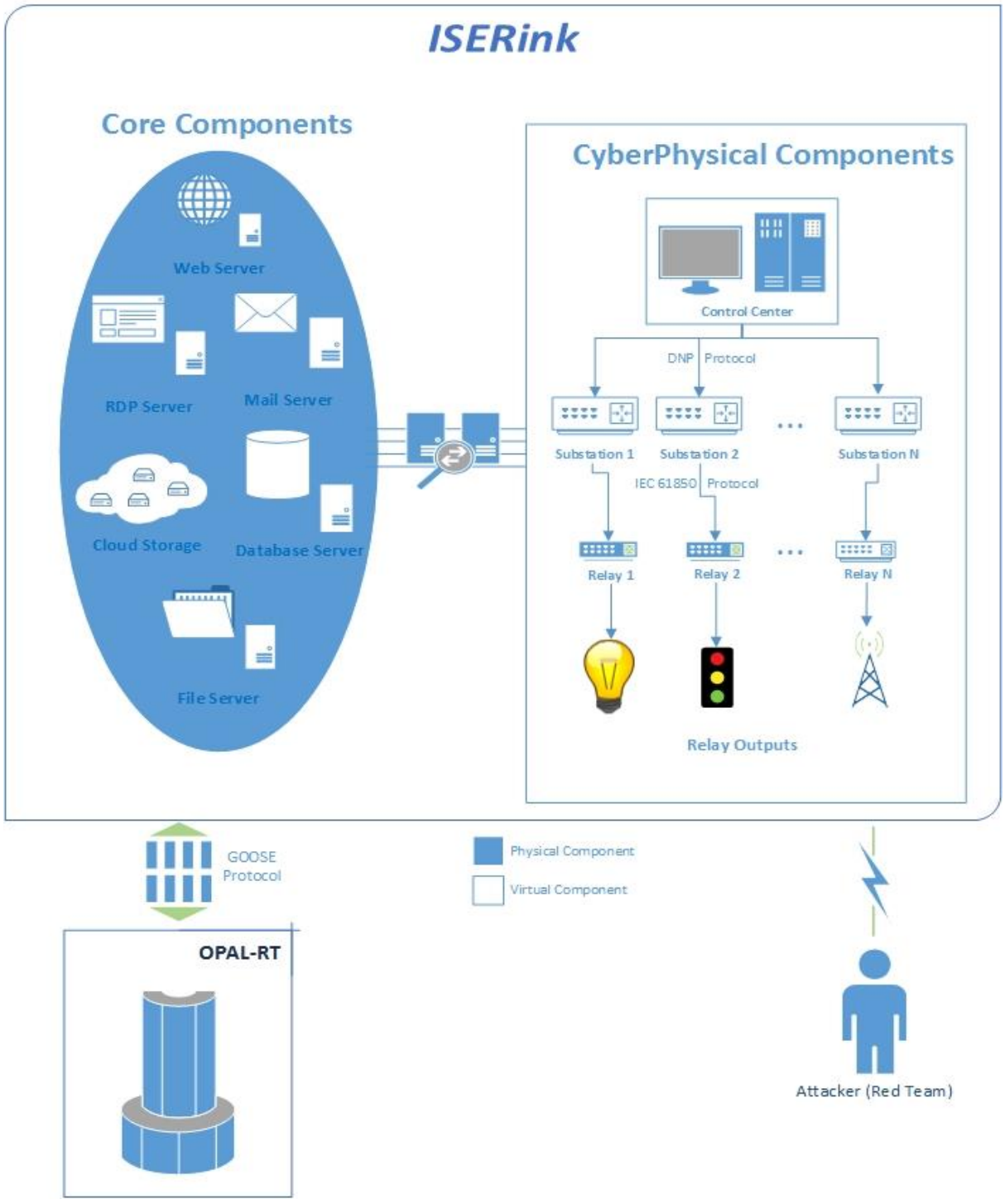
Green Team Tests:

- Webserver
- Accessibility to electrical utilities

16.1.3 Scenario 3

Gigantic Corp

Architecture:



Blue Team Description:

Welcome to Gigantic Corp one of the world's largest and oldest corporations. We hold monopolies in many sectors and remain unchallenged due to our heavy lobbying. Because of our size we have have many large campuses located all over the country. During a recent audit of our Iowa City campus the entire IT team was found to be completely incompetent and was let go. Your team needs to fix many of our IT sectors in order for the Iowa City campus to remain viable. Since we are such a gigantic corporation we have many systems to protect. This would include our own cloud storage, database, and file servers.

Blue Team Defends:

- Webserver used by green team.
- SCADA substation that provides power to the campus
- Flags placed in various locations
- RDP used by green team
- Cloud storage that utilizes SFTP/SSL

Red Team Attacks:

- Webserver used by green team
- Blue team substations
- Substation traffic coming from and going
- Flags

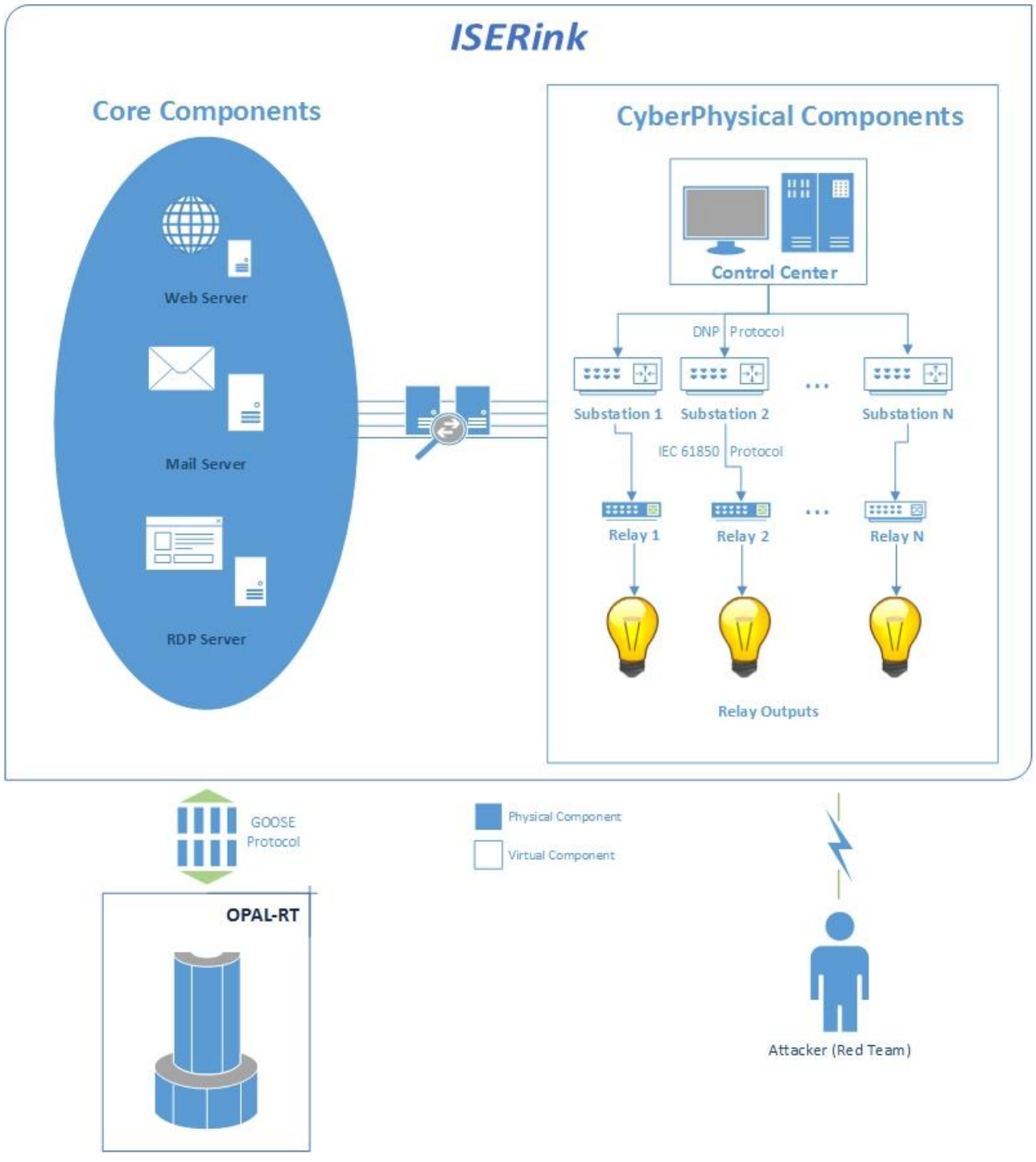
Green Team Tests:

- Webserver
- Accessibility to electrical utilities
- RDP
- FTP

16.1.4 Scenario 4

Promotion

Architecture:



Blue Team Description:

The manager of your regional SCADA control center has retired. Using the documentation the manager left behind, you need to take over management of the control center in addition to your previous duties. These duties include managing a substation, web server, and remote desktop server.

Blue Team Defends:

- Substation and connected RTU
- Control Center
- Web server
- RDP server

Red Team Attacks:

- Blue team substations
- Blue team control center communications
- Web server
- RDP server
- Flags on each system

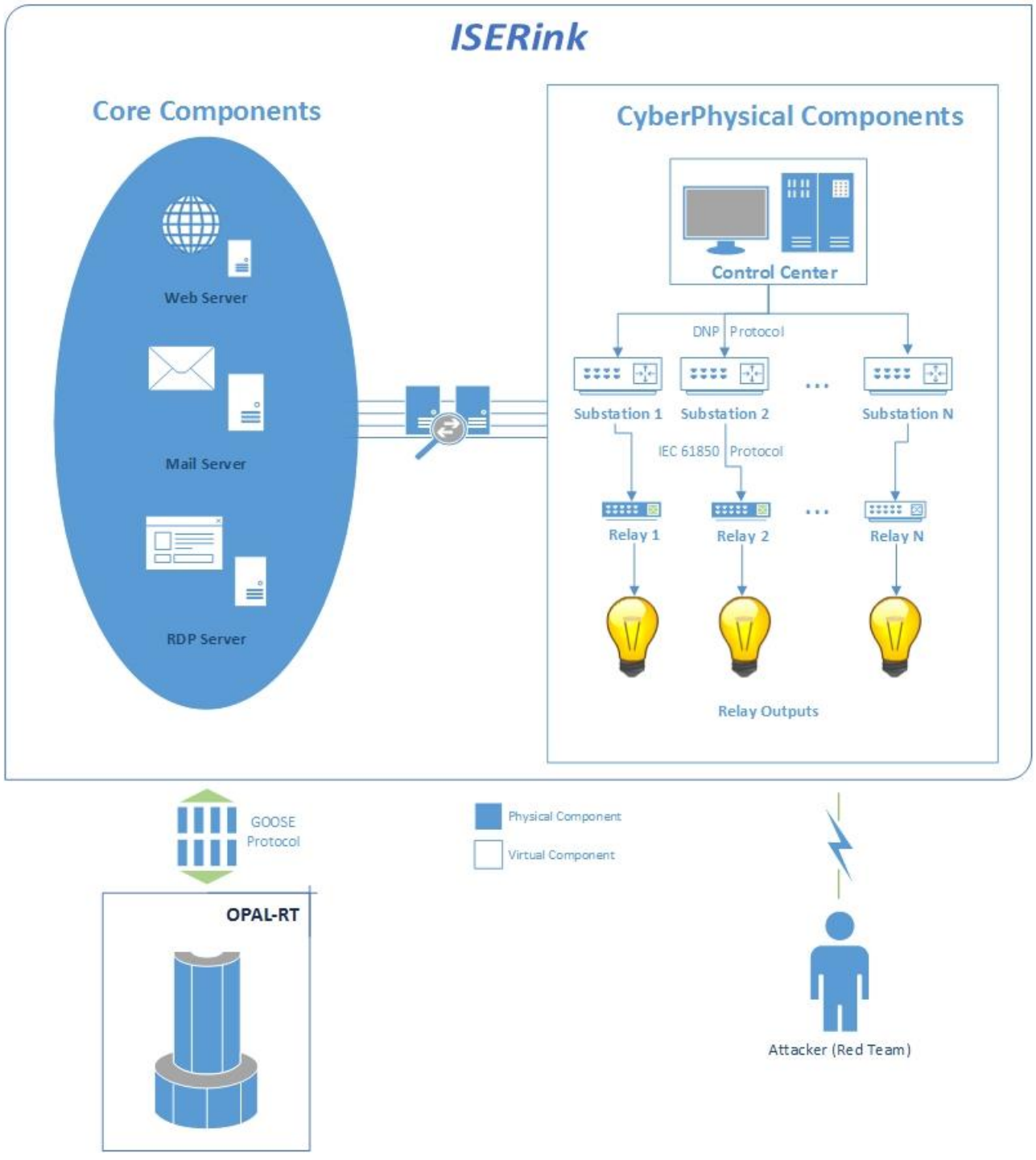
Green Team Tests:

- Control Center communication
- Substation permissions
- SCADA simulations
- Web server access
- RDP server access

16.1.5 Scenario 5

Executive Action

Architecture:



Blue Team Description:

All control center and substation operators in the USA mysteriously disappear. The only remaining qualified engineers happen to be on your team. You are ordered by the president to assume control of the national power grid (one control center and multiple substations), effective immediately.

Blue Team Defends:

- Multiple substations and RTUs
- Control Center
- Web server
- RDP

Red Team Attacks:

- Blue team substations
- Blue team control center
- Web server
- RDP server
- Flags on each system

Green Team Tests:

- Control Center communication
- Substation permissions
- SCADA simulations
- Web server access
- RDP server access