GE VERNOVA
Our portfolio of energy businesses

Cyberbezpieczeństwo w obszarze automatyki zabezpieczeniowej

Cezary Bryczek
GE Grid GmbH
Cezary.Bryczek@ge.com

Marzec 2024

GE VERNOVA
Our portfolio of energy businesses

Cyberbezpieczeństwo

Powstrzymywanie „złych aktorów” od robienia „złych rzeczy” ludziom i/lub organizacjom za pomocą metod cyfrowych.

GE VERNOVA
Our portfolio of energy businesses

IT versus OT Cybersecurity

Cyberbezpieczeństwo IT versus OT

GE VERNOVA
Our portfolio of energy businesses

IT

Dane i przepływ informacji cyfrowych

- Systemy informatyczne służą przede wszystkim do przechowywania i przetwarzania danych.
- Cyberbezpieczeństwo IT koncentruje się głównie na ochronie wrażliwych informacji, takich jak numery ubezpieczenia społecznego, wrażliwe informacje dotyczące zdrowia etc.
- Wpływ cyberataku na wrażliwe dane może na przykład skutkować utratą reputacji, kradzieżą, stratami finansowymi lub karami finansowymi.

OT

Procesy technologicze oraz urządzenia/maszyny służące do ich przeprowadzania

- Systemy OT kontrolują procesy technologiczne i zapewniają nadzór and urządzeniami IED.
- Cyberbezpieczeństwo OT koncentruje się na zapewnieniu bezpieczeństwa i niezawodności infrastruktury krytycznej w branżach takich jak ropa i gaz, chemiczna, elektryczna, transport i produkcja.
- Wpływ cyberataku na OT w organizacjach zajmujących się infrastrukturą krytyczną może skutkować tragicznymi konsekwencjami, w tym przestojami w zasilaniu/produkcji, awarią sprzętu, a nawet może spowodować eksplozje oraz zagrożenie dla życia i zdrowia ludzi.

IT (CIA)

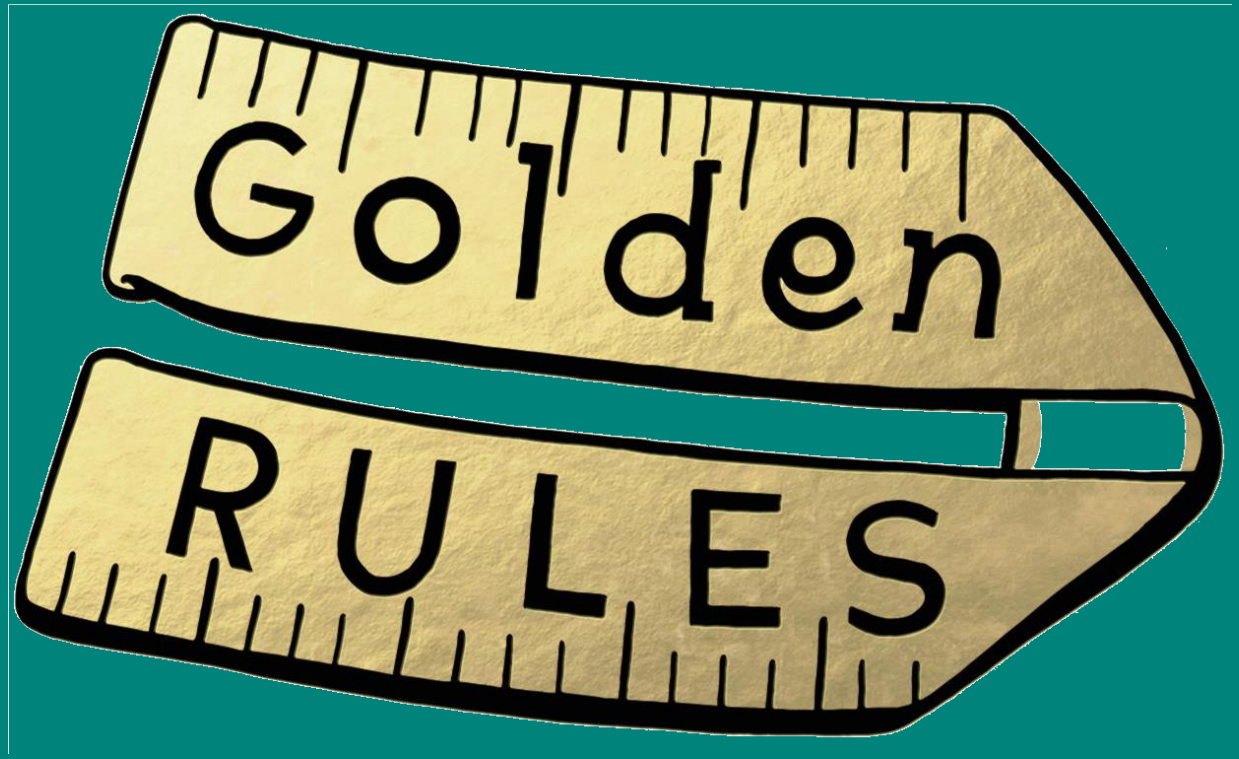
- Confidentiality
- Integrity
- Availability

OT (CAIC)

- Control
- Availability
- Integrity
- Confidentiality

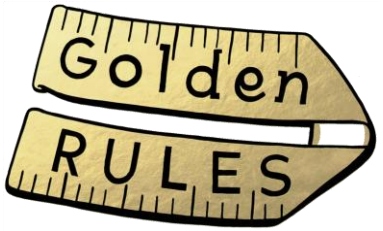
GE VERNOVA
Our portfolio of energy businesses

10 złotych zasad cyberbezpieczeństwa



Złote zasady cyberbezpieczeństwa

GE VERNOVA
Our portfolio of energy businesses



Zasada 1

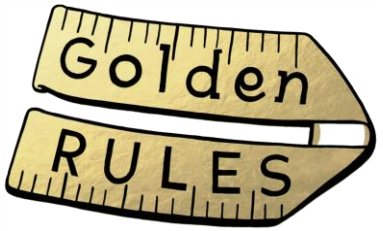
WSZYSTKO sprowadza się do RYZYKA. Ile ryzyka jest akceptowalne w porównaniu do tego, ile zainwestować w ochronę przed czymś co może się wydarzyć.

„To gra liczbowa – wszystko sprowadza się do matematyki. ”

Złote zasady cyberbezpieczeństwa

GE VERNOVA
Our portfolio of energy businesses

Zasada 2



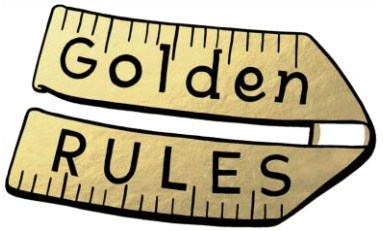
Zapobieganie cyberincydentowi jest o 1 000 000% lepsze i mniej kosztowne niż próba naprawienia sytuacji i powrotu do „znanego dobrego stanu”.

„Profilaktyka jest zawsze lepsza od leczenia. ”

Złote zasady cyberbezpieczeństwa

GE VERNOVA
Our portfolio of energy businesses

Zasada 3



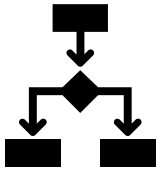
Nie zakładaj, że wszyscy „źli aktorzy” są „nieznani” lub spoza organizacji.

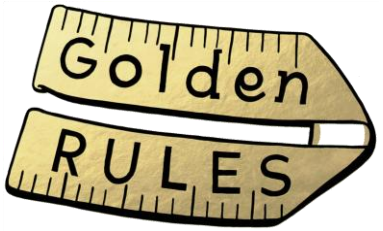
„Zagrożenia wewnętrzne mogą być równie złe a nawet gorsze niż zagrożenia zewnętrzne. ”

Złote zasady cyberbezpieczeństwa

GE VERNOVA
Our portfolio of energy businesses

Zasada 4





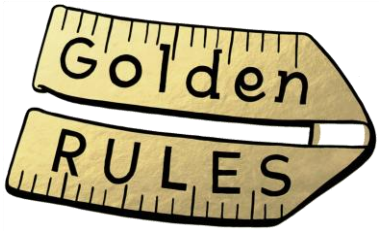
Różnica między dobrą a świetną strategią cyberbezpieczeństwa polega na uznaniu, że jedno rozwiązanie nie jest „tym” rozwiązaniem.

„Wielopoziomowa strategia cyberbezpieczeństwa jest zawsze lepsza. ”

Złote zasady cyberbezpieczeństwa

GE VERNOVA
Our portfolio of energy businesses

Zasada 5



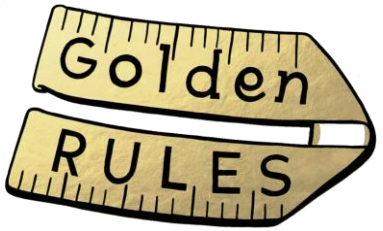
Ustanowienie dobrej „cyber-higieny” w swoim życiu osobistym i w swojej organizacji – poprzez szkolenia cybernetyczne.

„Nigdy nie przestawaj uczyć się o najlepszych praktykach w zakresie cyberbezpieczeństwa. ”

Złote zasady cyberbezpieczeństwa

GE VERNOVA
Our portfolio of energy businesses

Zasada 6



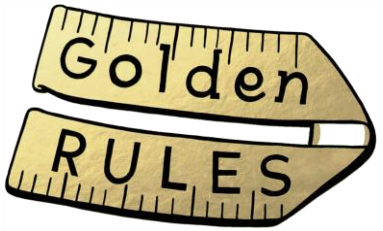
Źle zaprojektowane, zainstalowane i skonfigurowane rozwiązania cyberbezpieczeństwa doprowadzą do fałszywego poczucia bezpieczeństwa i doprowadzą do katastrofalnych zdarzeń.

"Przeanalizuj trzy razy zanim wprowadzisz rozwiązanie."

Złote zasady cyberbezpieczeństwa

GE VERNOVA
Our portfolio of energy businesses

Zasada 7



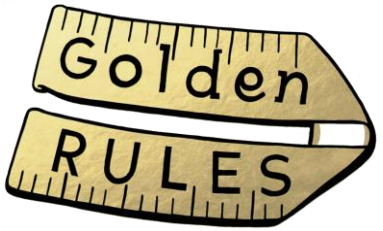
Ufaj, ale sprawdzaj . . . wszystkich i wszystko.

„Zastosuj podejście Zero Zaufania do cyberbezpieczeństwa. ”

Złote zasady cyberbezpieczeństwa

GE VERNOVA
Our portfolio of energy businesses

Zasada 8



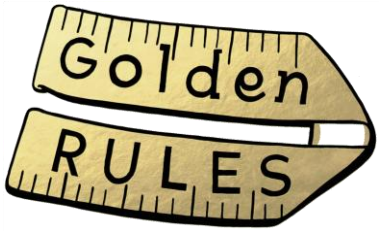
Przeanalizuj dokładnie, co należy chronić i dlaczego, a nawet przed kim, zanim podejmiesz decyzję w jaki sposób.

„Zacznij od dokładnego zrozumienia, co wymaga ochrony. ”

Złote zasady cyberbezpieczeństwa

GE VERNOVA
Our portfolio of energy businesses

Zasada 9



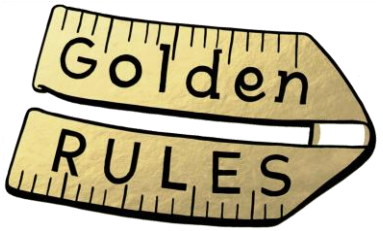
Pamiętaj, że skuteczne powstrzymanie jednego cyberataku nie oznacza, że powstrzymałeś wszystkie przyszłe cyberataki.

„Zli aktorzy są nieustępliwi i nigdy nie przestają. ”

Złote zasady cyberbezpieczeństwa

GE VERNOVA
Our portfolio of energy businesses

Zasada 10



Nie zakładaj i nigdy nie myśl, że jesteś „gotowy”.

„Zagrożenia cybernetyczne stale ewoluują; tak samo powinno być w przypadku cyberbezpieczeństwa. ”

GE VERNOVA
Our portfolio of energy businesses

Przykładowe incydenty cybernetyczne w sektorze energetycznym

Colonial Pipeline - 2021

GE VERNOVA
Our portfolio of energy businesses

- Udany atak ransomware przez: DarkSide
- Colonial Pipeline zapłacił okup 4,4 miliona dolarów w Bitcoinach.
- **Przyczyna**: Brak ram cyberbezpieczeństwa zarówno w zakresie przygotowania, jak i reagowania na incydenty
- Luki w zabezpieczeniach, wykorzystanie starego nieużywanego konta
- **Skutek**: Zakłócenia w dostawach ropy naftowej na wschodnim wybrzeżu USA

Inne ostatnie cyberataki w sektorze energetycznym

GE VERNOVA
Our portfolio of energy businesses

Saudi Aramco – nieudana próba wymuszenia

Sellafield Ltd

Sellafield (UK) –atak przez hakerów (**Chiny i Rosja**)

ignitis group

Litewska państwowa grupa energetyczna Ignitis

ЕНЕРГОАТОМ ENERGOATOM

Ukraińska energetyka jądrowa Energoatom

δesfa

Największy dostawca gazu ziemnego w Grecji DESFA

Israel Company ➔

UNITRONICS

Unitronics PLCs

Inne cyberataki w sektorze energetycznym

GE VERNOVA
Our portfolio of energy businesses

Cybersecurity incidents against global commodity industries

March 2017 through June 2023

Affected industry

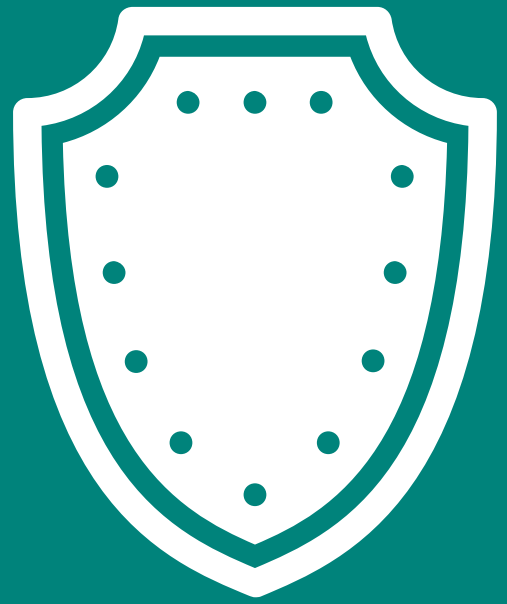
- Petchems
- Oil
- Nuclear
- Power
- Shipping
- Metals
- Gas

Source: S&P Global Commodity Insights

S&P Global
Commodity Insights

GE VERNOVA
Our portfolio of energy businesses

Cyberbezpieczeństwo Defense-in-Depth



Podejścia do Cyberobrony

GE VERNOVA
Our portfolio of energy businesses

Outside In

- Podkreśla ochronę obwodową
- Większy budżet na cyberbezpieczeństwo wydawany na zewnętrzne kręgi
- Założenie jest takie, że większość cyberataków pochodzi z zewnątrz, powstrzymaj je, zanim posuną się zbyt daleko

Inside Out

- Podkreśla wewnętrzną ochronę aktywów
- Greater cybersecurity budget spent protecting asset
- Zakłada się, że aktywa muszą być chronione za wszelką cenę lub że zagrożenia wewnętrzne mogą spowodować największe szkody

7 Warstw Cyberbezpieczeństwa

GE VERNOVA
Our portfolio of energy businesses

Warstwa	Nazwa Warstwy	Opis Warstwy
1	Edukacja/szkolenie użytkowników*	Szkolenie / Edukacja użytkowników w zakresie różnych „najlepszych praktyk” w zakresie cyberbezpieczeństwa, w tym różnych metod cybernetycznych ukierunkowanych na użytkowników.
2	Fizyczna / Kontrola dostępu*	Chociaż nie ma charakteru „cyber”, kluczowe znaczenie ma zapewnienie fizycznego dostępu do technologii, takich jak systemy sprzętowe i różne infrastruktury IT i OT.
3	Zabezpieczenia obwodowe	Ochrona i kontrola dostępu do sieci za pośrednictwem routerów, bram, przełączników i zapór sieciowych.
4	Bezpieczeństwo sieci	Ochrona rzeczywistej infrastruktury sieciowej i ruchu sieciowego (np. danych), który w niej przepływa.
5	Bezpieczeństwo punktów końcowych	Ochrona rzeczywistych urządzeń, w tym ich systemów operacyjnych (np. komputerów, urządzeń IoT/IIoT, urządzeń SCADA, urządzeń IED), które są podłączone do sieci.
6	Bezpieczeństwo aplikacji	Zabezpieczanie i ochrona różnych aplikacji oraz oprogramowania systemów działających w sieci.
7	Bezpieczeństwo danych	Ochrona i zabezpieczenie przechowywania i transmisji wszystkich typów i form danych przepływających przez sieć.

* = Nie specjalnie cyberbezpieczeństwo; ale krytycznie ważne i związane z cyberbezpieczeństwem.

Defense-in-Depth - Przykład

GE VERNOVA
Our portfolio of energy businesses

Sieć Publiczna

Sieć Prywatna

HACKER

HACKER

GE VERNOVA
Our portfolio of energy businesses

Standardy Cyberbezpieczeńsywa

Najczęściej stosowane standardy

GE VERNOVA
Our portfolio of energy businesses

ISA / IEC

- ISA/IEC 62443 standard cyberbezpieczeństwa definiuje procesy, techniki i wymagania dla Industrial Automation and Control Systems (IACS)
- IEC 62351 seria norm obejmuje technologie cyberbezpieczeństwa dla protokołów komunikacyjnych zdefiniowanych przez IEC TC 57.

NERC CIP

- NERC 1300 od CIP-002-3 do CIP-009-3(CIP=Critical Infrastructure Protection). Standardy NERC CIP zostały opracowane w celu ochrony krytycznej infrastruktury sieci energetycznej Ameryki Północnej.

NIS 2

- Dyrektywa NIS 2 jest ogólnounijnym aktem prawnym dotyczącym bezpieczeństwa cybernetycznego. Przewiduje ona środki prawne mające na celu podniesienie ogólnego poziomu bezpieczeństwa cybernetycznego w UE.

NIST

- The NIST Cybersecurity Framework to zbiór wytycznych dla firm z sektora prywatnego, których należy przestrzegać, aby lepiej przygotować się do identyfikacji, blokowania, wykrywania, reagowania i usuwania/zmniejszania skutków ataków.

ISO / IEC

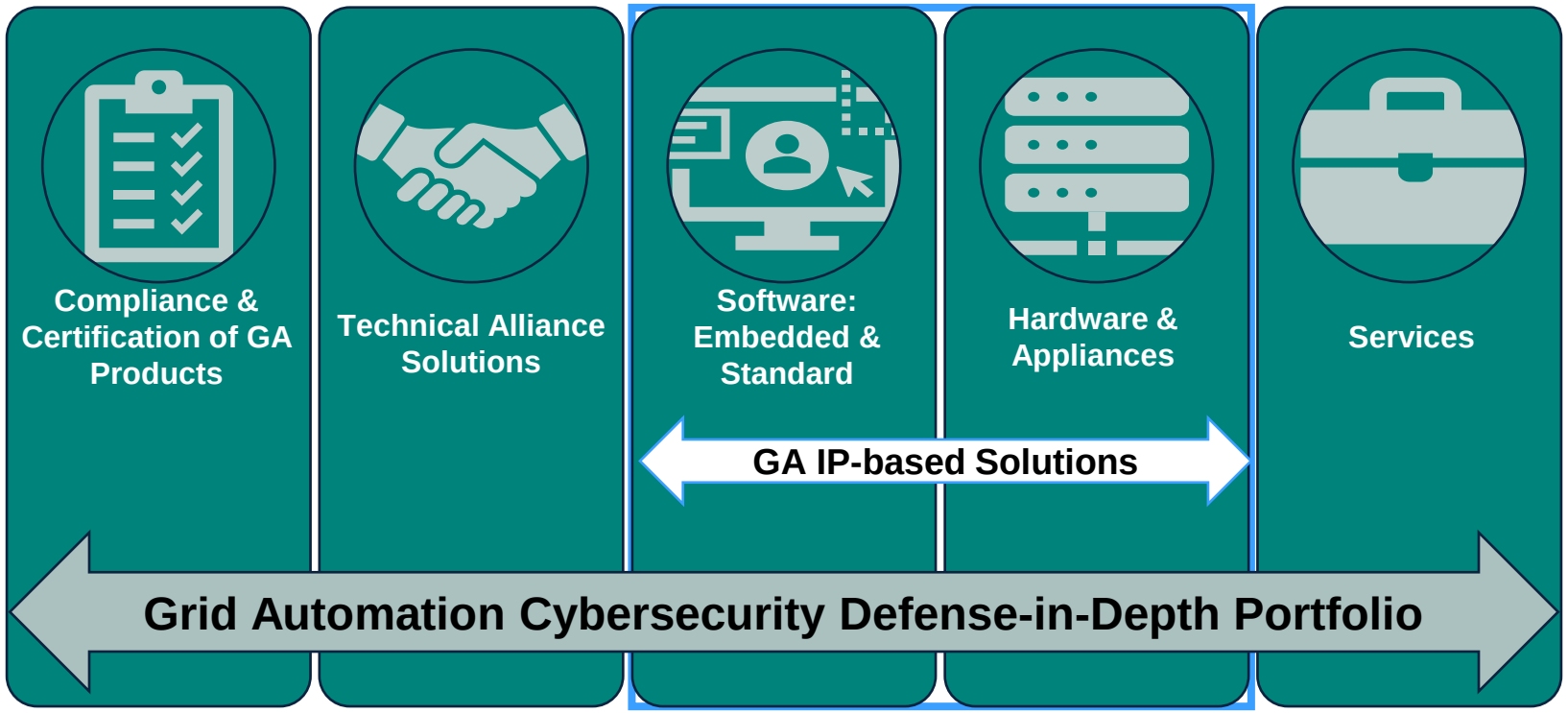
- ISO/IEC 27001 to zbiór regulacji do stosowania, których głównym celem jest zapewnienie zaimplementowania i późniejszego utrzymywania i doskonalenia w organizacji systemu zarządzania bezpieczeństwem, informacji .

GE VERNOVA
Our portfolio of energy businesses

GE Grid Automation - Wizja Cyberbezpieczeństwa

Grid Automation Defense-in-Depth

GE VERNOVA
Our portfolio of energy businesses



Ochrona cybernetyczna od krawędzi do rdzenia:

- Certyfikacja produktów Grid Automation pod kątem zgodności z cyberbezpieczeństwem
- Dostarczanie dojrzałych, sprawdzonych i solidnych rozwiązań w zakresie cyberbezpieczeństwa
- Innowacyjne rozwiązania z zakresu cyberbezpieczeństwa (Oprogramowanie i Sprzęt)
- Kompleksowe usługi w zakresie cyberbezpieczeństwa

GA - Cyberbezpieczeństwo Aktualna oferta

GE VERNOVA
Our portfolio of energy businesses

Produkty i Rozwiązania:

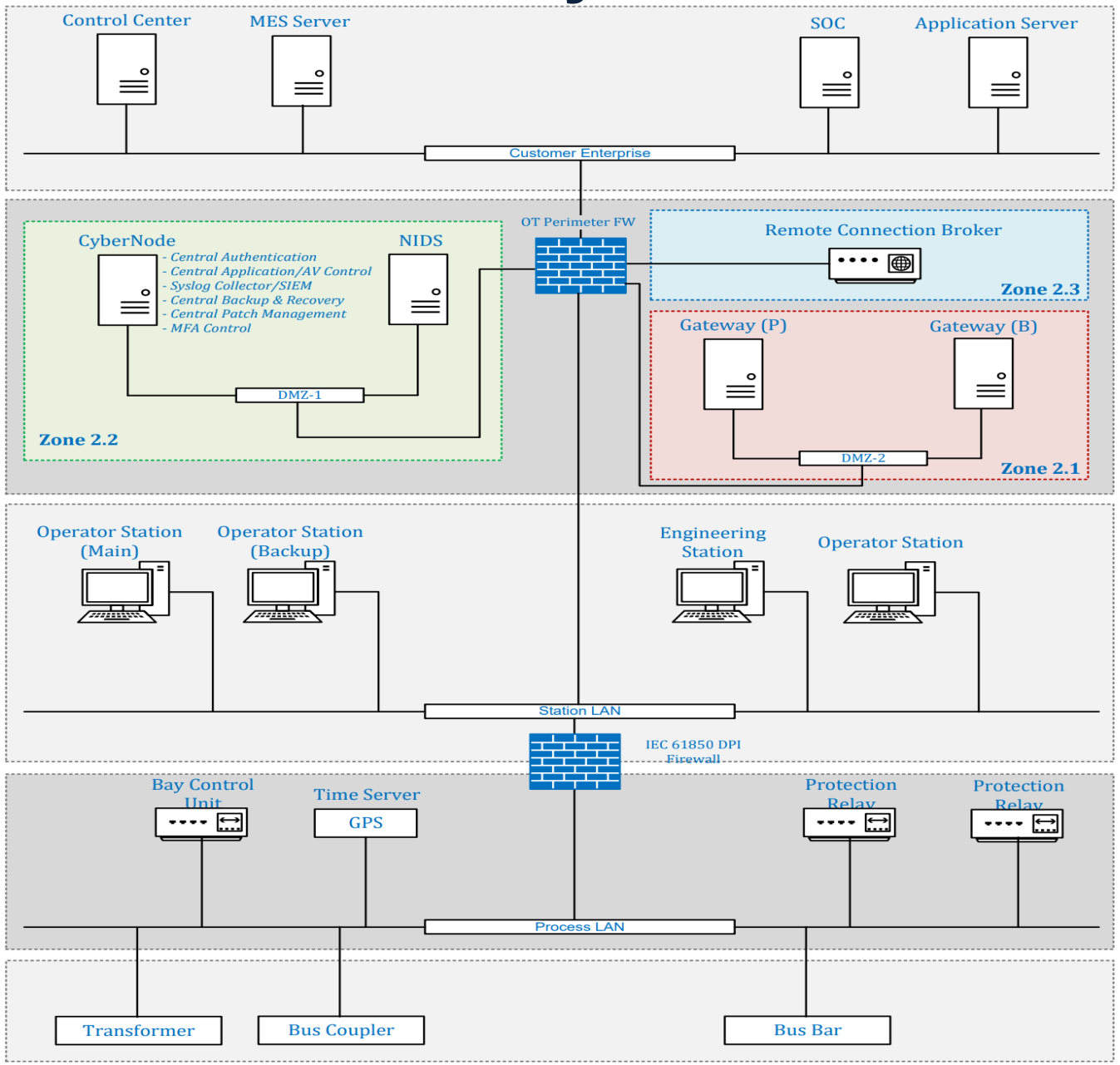
- Next Generation Firewall (NGFW)
- Monitorowanie bezpieczeństwa sieci(aka: NIDS)
- Host Intrusion Detection & Prevention (HIDS/HIPS)
- Kontrola Dostępu & Autentykacja Multi-factor (MFA)
- Bezpieczny zdalny dostęp klasy przemysłowej
- Anti-Virus / Anti-Malware

Usługi:

- Backup & Recovery
- Planowanie reakcji na incident
- Audyt cyberbezpieczeństwa i zgodności
- Analiza luk w cyberbezpieczeństwie przemysłowym i ocena ryzyka
- Ocena sieci przemysłowej pod kontem cyberbezpieczeństwa
- Opracowanie polityki i procedur
- Opracowanie “białej listy” dla aplikacji
- Hartowanie węzła końcowego
- Industrial Patching / Patch Management

Grid Automation - Przykładowa Architektura

GE VERNOVA
Our portfolio of energy businesses



Zone 3.x
Customer Enterprise Zone

Zone 2.x
DMZ
2.1 – Gateway DMZ
2.2 – Central Security Management DMZ
2.3 – Remote Access DMZ

Zone 2
Station LAN

Zone 1
Protection & Control LAN (substation bus & process bus)

Zone 0
Process

GE VERNOVA
Our portfolio of energy businesses

Cyberbezpieczeństwo a eksploatacja i zapewnienie wysokiej dostępności

Pytania?

GE VERNOVA
Our portfolio of energy businesses

GE VERNOVA

Our portfolio of energy businesses