Risk Management System™ with ASSESS Package

for Existing and Future Systems

Safe
Easy
Quick
Secure
Compliant

&

I know
Cybersecurity,
...
do you?

All-In-One & 1st True Solution for Industrial Cybersecurity

Manage Industrial Cybersecurity Risk, and Secure by Design all and the most critical industrial assets - start at any moment - and during the entire life cycle of the plant. Monitor zones and conduits in real-time for safety and security.

RMS

RISK MANAGEMENT SYSTEM

Comply and achieve the requirements of the most comprehensive set of international standards, national regulations and best practices with ease.

ISA/IEC-62443-X-X Series + NIST + NERC + C2M2 + ENISA + many more.

Enterprise Server

ZCM Site Server

ZCM Analyzers

WisePlant.com

Doc. BR.RMS.ASS.E.003 August 2024

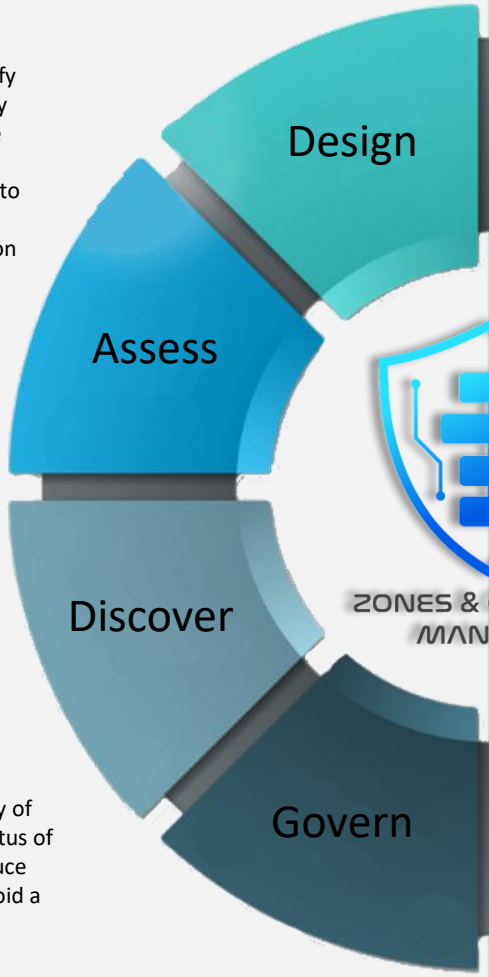
Systems to Secure

With a variety of non-intrusive methods and techniques automatically discover and identify 100% of the Cyber-Assets (PCI, PLCs, DCS, hardware, firmware, VMs, software, …) to clearly understand the systems to secure. View the systems with deepest granularity in the same way engineers does, complying with ISA95 Perdue Model, ISA88, ISA5.1 Cyber-Assets definitions clearly defining its hierarchical architecture from the edge devices (Level 0) up to plant management components (Level 3), and corporate (Levels 4 and 5). Manage, keep history and track inventory during entire Cyber-Asset Life Cycle from the system conception (Engineering), through operation period, and until decommissioning (Retirement).

Knowing your systems to perfection is an essential part in understanding your infrastructure, and a key step before evaluating industrial cybersecurity risk. Using a variety of methods and techniques, develop a complete vulnerability Assessment onto all Cyber-Asset. Start at earlier stages (Engineering Phase) before the systems arrives at the plant, or on existing systems (Operation), even if they are legacy completely isolated dinosaurs. Catch them all!

Assign Cyber-Assets to zones, sub-zones, conduits within the zone, and conduits interconnecting different zones, complying with international standards, such as ISA/IEC-62443. Document the preliminary Security Level Target (SL-T) by each node during a Hight Level Risk Assessment Study, improve your zones and conduits definition during a Detailed Cyber Risk Assessment as well as identify the current Security Level (SL-A) of each node. Track changes and keep history of each node, including those which have been decommissioned or re-defined. Clearly identify every communication interfaces (ethernet based and traditional non-ethernet) associated with each Cyber-Asset, including all Level 0 fieldbus communications.

Risk Management System™ suite provides many features for proper managing the security of the entire systems. Allows to perform your own vulnerabilities discovery and track the status of the mitigation and vendor remediation. With RMS cut CSMP costs by more than 60%, reduce time from months to weeks, and perform complex tasks in days, instead of weeks, and avoid a myriad of external resources (visitors, applications, scanning tools, etc.).



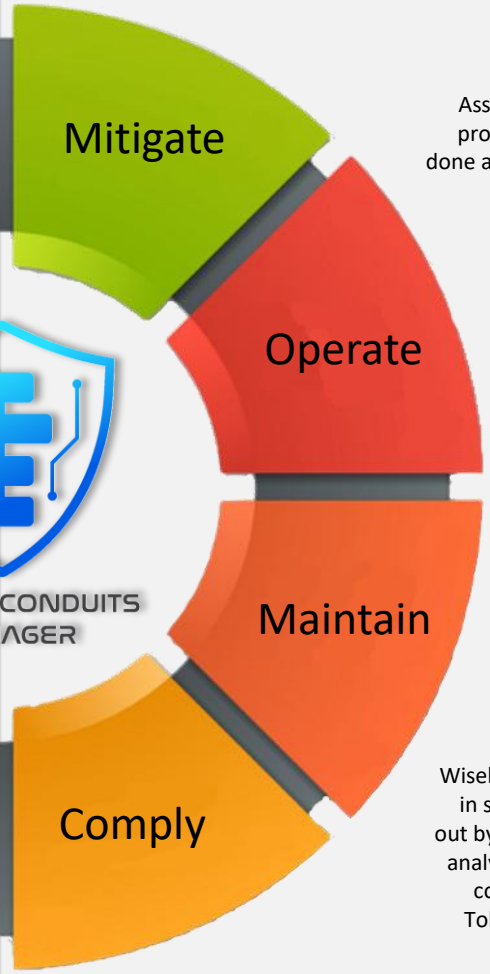
o protect the most valued Assets
ent infrastructure
pe of threats”

I know
Cybersecurity,
...
do you?

Processes
Environment
Workers/People

& Protect

RISK
MANAGEMENT
SYSTEM



Assets to Protect

Identify all the Assets from your facilities and business which can be affected by the Cyber-Assets, and clearly identify all the valuable assets that you need to track over time. It could be production equipment, buildings, processes, and people as some of the examples. This can be done as an engineering process through modelling techniques, or as a result of an on-going High-Level Risk Assessment or Criticality Studies.

Identify all Risk Receptors that needs to be protected, and prevent that bad things happens because of threat actions. This main activity is also typically performed during a High-Level Risk Assessment or a Criticality Study. The Risk Receptors will typically match with the plant or Corporate Risk Matrix.

Through proven engineering methods identify all potential consequences. This is key for evaluating the multiple Risk Scenarios, and for generating a reasonable and meaningful incident and response plan with prioritization of cyber-events based on realistic potential consequences. Get your Cyber Emergency Response Team and first line of response at the plant to be prepared to react to what matters most without false positives, and prioritizing appropriately, before it is too late.

Determine impact level as a measurement of specific and clearly defined consequences, using the corporate Risk Matrix. Formerly keep auditable records of all data and assessment results confidentially secured into Risk Management System Server without leaving the plant and have them only available to authorized users for risk analysis, design of mitigating methods, and eventually for incident and response actions.

Wisely use the consequence-based analysis to take good decisions, justify the right investments in security actions that really mitigates the risk on existing and future systems. Design the risk out by influencing the design of the zones and conduits, determine Security Level Targets (SL-T), analyze effectiveness of current existing countermeasures, determine necessary compensating countermeasures and/or eventually influence the design of the plant to meet the Corporate Tolerable Risk. **Run the systems/plant at tolerable risk first, and then monitor for intrusion**.

INDUSTRIAL CYBER RISK MANAGEMENT

International Standards
National Standards
Requirements
Best Practices
Technologies
Regulations
Capabilities
Guidelines
Controls
Rules
Laws

RISK MANAGEMENT SYSTEM

Security frameworks
Depending on the country, region, laws, regulations, its industry and the goals defined by the organization itself is that Z&CM can provide all the necessary tools to comply with different known global frameworks and/or develop a specific one tailored to the organization. Z&CM is an Integrated All-In-One Industrial Cybersecurity Solution.

International Standards
The World's Only Consensus-Based Automation and Control Systems Cybersecurity Standards.

- ISA/IEC-62443-X-X – Industrial Cybersecurity Series of Standards and Technical References
- ISA TR84.00.09 – Cybersecurity Related to the Functional Safety Lifecycle

National rules, guidelines and regulations could be used to assess the organization's current situation against the following national standards, regulations and laws from around the globe.

- ACC Guidance for Addressing Cyber Security
- API 1164 – Pipeline SCADA Security Guidelines
- AWWA Process Control System Security Guidance
- CFATS Risk-Based Performance Standards (RBPS-8)
- CSA Z246.1-09 from CSA Group
- NEI 08-09 – Cyber Security Plan for Nuclear Power Reactors
- NERC CIP Standards – Critical Infrastructure Protection
- NIST SP800-82 – Guide to Industrial Control Systems (ICS) Security
- NIST Cybersecurity Framework
- NRC Reg Guide 5.71 – Cyber Security Program for Nuclear Facilities
- TSA Pipeline Security Guidelines
- and many more

Maturity Models
The following maturity models are a case of security breach analysis. They seek to assess the organization's capabilities and identify points of improvement for the development of new skills and competencies at higher levels in the organizations and evaluate key suppliers.

- CCR (Cyber Resilience Review) Homeland National Security
- DOE C2M2 (Cybersecurity Capability Maturity Model)
- FFIEC (Federal Financial Institution Examination Council Assessment Tool)
- CCI (Industrial Cybersecurity Center, Spain)
- WisePlant's Suppliers Evaluation.

Generate, manage and access a collaborative environment for industrial cyber risk management meeting 100% with the requirements of the ISA/IEC-62443 standard series and others, while the Z&CM is providing updated accurate live information.

PERFORM LIVE

1 ASUC

Identify 100% of Cyber-Assets and clearly understand the System under Consideration by creating your Zones and Conduit diagram with ease. Analyze vulnerabilities and weaknesses in technology, processes, and physical security.

With Z&CM analyzers, detect and monitor Zones and Conduits in real time (intrusions, anomalies, unvalidated changes, etc.)

2 MGAP

Develop maturity studies, security audits, security breach assessments, and analyze your company's practices against standards, global best practices, standards, controls, requirements, laws, and compare results with peers.

3 HLRA

Develop your organization's asset model, identify the potential consequences for each of all risk recipients based on the corporate risk matrix, and perform high-level risk assessments. Determine Target Security Levels (SL-T).

4 CPHA

Develop detailed risk assessment optimally with Z&MC All-in-One without the need for additional tools, complying 100% with the requirements of the ISA/IEC-62443 series. Make consistent and sound decisions.

Develop a Cybersecurity Assessment is as easy as 1, 2, 3, and 4

ZCM Site Server

ZCM Analyzers

ZCM Analyzers are used in discovery mode over existing systems while performing a risk assessment. ZCM Analyzers will then run in Secure & Protect™ mode for mitigating the risk, safe and secure operation of the plant.

WiseCourses® Academy

I know Cybersecurity, ... do you?

Safe
Easy
Quick
Secure
Compliant

WisePlant®
Smart, Safe & Secure

CERTIFIED ASSESS

XX60 – Integrated Industrial Cyber Risk Assessment with RMS/ZCM

Lear **how to** perform the complete Industrial Cyber Risk Assessment into existing and/or future systems with ease, using Zones & Conduits Manager™. Streamline your engineering and security resources, reduce time, and maximize results of your Cybersecurity activities.

XX50
Industrial Cybersecurity and Critical Infrastructure

XX60
Integrated Industrial Cyber Risk Assessment with RMS/ZCM

XX61
Design and Implementation of Security with RMS/ZCM

XX62
Monitoring and Maintaining of Security with RMS/ZCM

WiseCourses.com

Doc. BR.RMS.ASS.E.003 August 2024