Application Note

CIARA

Cyber Industrial Automated Risk Analysis

IEC-62443-Based Risk Assessment in ICS/SCADA Networks

radiflow

radiflow

Table of Contents

OVERVIEW

Cyber-security standards were developed to establish the required procedures for tasks, ownership and reporting to reach and maintain the organization's cyber-security goals, whether merely demonstrating compliance or using the standard as a set of best practices for cyber threat management.

"The recommendation is to develop and implement an organization-wide cybersecurity management system (CSMS) that includes program elements to reassess risk and take corrective actions to eliminate the tendency for security levels to decline over time."
(IEC 62443-1-1; IEC 1294/09; IEC 1295/09)

CIARA was develop in response to the growing digitization of the production floor (Industry 4.0) that has led to a tide of cyber threats—all while risk assessment processes, which up to now were done manually, have failed to address the full scope of the issue. The complexity of today's Industrial networks calls for an automated cyber risk management process. Simply put, the era of "eyeballing" network risk is long-gone.

CIARA automates the process of examining hundreds of the most commonly used security controls against a simulation of hundreds of cyber threat types, while modeling against dozens of features in the digital network model including protocols, vulnerabilities, firmware versions, topology, device types and more.

These risk assessments are then factored against common OT risk scenarios including loss of availability, loss of control and damage to property (among others). The result is a matrix of tens of thousands of potential permutations that simply cannot be analysed by humans.

CIARA is able to evaluate your network risk and provide comprehensive, actionable reports in a matter of minutes.

Serving as a decision-support tool intended for stakeholders seeking to manage and reduce cyber-risk in ICS environments, CIARA enables risk-based prioritization of expenditure on security requirements.

THE CIARA SOLUTION

CIARA is designed to simplify the process of managing the CSMS security life cycle (see "Concepts" below).

Focused on supporting the IEC 62443 cyber-risk management process, CIARA automates major blocks in the security life cycle process, adding wizards and workflows to facilitate the on-boarding process.

Continuous ingress of information from network events and additional inputs like asset and change management systems build the digital image (model) that CIARA learns from and uses for simulating attack scenarios. The digital image is separated into Zones and Conduits, each assigned an Impact value by the user. Impact can be monetary, or HSE related derived from Cyber PHA.

The eventual risk score factors both the likelihood and the impact of a cyber-attack:

Likelihood		**Impact**		**Risk**
• Threat & adversary characteristics • Organization's locale & sector • Network vulnerabilities detected • Mitigation controls installed	**X**	Assessment of the damage caused by a cyber-attack, per zone and network-overall	**=**	Used by CISOs/stakeholders to assess the state of the network and the effectiveness of security measures

AUTOMATED CYBER-RISK MANAGEMENT

Automated cyber-risk management incorporates multiple sources for data on network topology, assets and vulnerabilities, adversaries and threat tactics, including:

- Inventory mapping
- Vulnerability mapping for likelihood scoring
- Network & protocol diagrams
- User and system behavior analysis
- Peer Benchmarking
- Virtual penetration testing (MITRE-ICS simulations)

THE CIARA WIZARD

CIARA features a step-by-step wizard that guides the user through the network acquisition & configuration stages using plain-language instructions:

1. Acquisition on network information: The user is asked to either connect to an instance of Radiflow iSID or upload a file (MS Excel, generated by iSID) that contains the digital image of the SuC (System Under Control).
2. Geo-location and industry sector: These two descriptors (e.g. "USA, Chemicals Sector") help identify the adversaries and ATT's (Adversary Tactics and Techniques) relevant to the SUC and prescribe a prioritized list of controls to mitigate the network's specific risks.
3. Assigning security levels target (SL-T) to Zones: Zones, as defined in IEC 62443, are delineated operational units (business processes) that share the same security requirements. The user is asked at this stage to assign an SL-T from 1 to 4 for each Zone (or override CIARA's initial assigned SL-T values). CIARA presents the relevant foundational/security requirements (FR/SR) needed to meet the designated Zone's SLT.
4. Planning and budgeting mitigations: Once all Zone's were assigned SL-Ts, the user is presented with multiple mitigation control "cards", prioritized by each control's contribution to minimizing overall network risk. The

user is given the option to enter cost and target completion date (by year-quarter) for each control, to meet budgetary constraints.

These steps are described in more detail in the CIARA Step-By-Step section in this document.

In practice, CIARA measures the relevance of each security requirement (i.e. mitigation controllers) against a threat likelihood model. The likelihood of each threat is calculated according to the relevance of adversaries' geo-location and activity in specific sectors.

CIARA uses the ICS-MITRE framework's adversary tactics and techniques for attack vector likelihood, combined with information derived from the ICS-CERT database about the vulnerabilities (CVEs) detected in the system. By calculating the likelihood of dozens and hundreds of attacks, CIARA is able to calculate the effectiveness of security requirements (SR), and assess the risk-based ROI of procuring different security risk mitigation measures.

As the user goes through the wizard the network's overall risk posture is re-calculated and the effectiveness of current mitigation controls is re-evaluated regarding the ICS's specific threat landscape. CIARA provides full visibility of the current risk posture, accounting for both risk facilitators risk mitigators. The resulting CIARA cyber program planning screen greatly streamlines CSMS planning by adding impact priority and budget restraints.

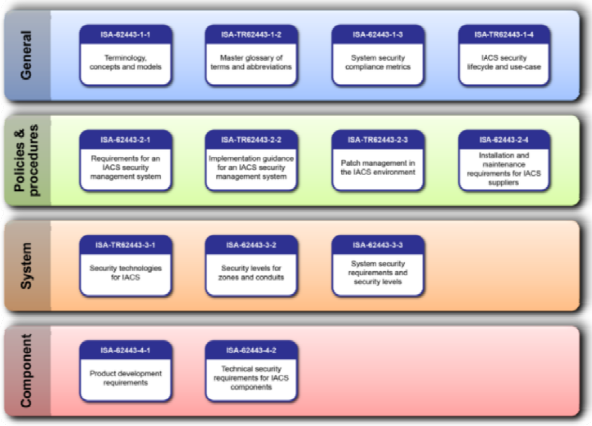
As every plan is subject to change (as the saying goes), CIARA accounts for new adversaries, vulnerabilities, changes in the process topology, and will dynamically update both the overall risk score and the risk-mitigation roadmap.

CSMS planning by impact priority and budget restraints can now be easily conducted with the CIARA cyber program planning screen.

CONCEPTS

THE IEC 62443 STANDARD

IEC-62443 is a series of standards (inc. technical reports) that provide a systematic and practical approach to securing Industrial Automation and Control Systems (IACS). The standard covers each and every stage and aspect of industrial cybersecurity from risk assessment to ongoing operations.



Structure and sections of the IEC 62443 standard

RISK TOLERANCE/AVERSION/APPETITE

"If you're willing to take a hit to the head, there's no need to invest in helmets."

What extent of risk can the organization stomach without investing in mitigating or transferring risk (i.e. buying insurance)?

SYSTEM UNDER CONSIDERATION (SUC)

Scope of the cyber risk management plan: what are the plan's boundaries—a single site, multiple sites, a single process, or an interdependent group of processes?

CYBER SECURITY MANAGEMENT SYSTEM (CSMS)

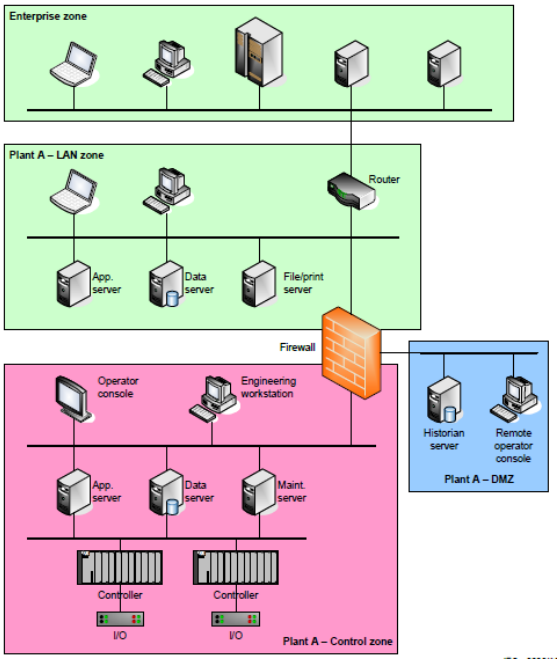
The five fundamental elements of a CSMS program are:

- High level risk assessment
- Establish cyber security policy, awareness, and organization
- Detailed risk assessment
- Implement counter measures – mitigation controls
- Continuously maintain and operate the CSMS program

ZONE

A zone is defined by a physical or/and logical boundary (62443-2-1 3.2.17).

A zone can be defined as a group of assets (e.g. PLCs), by functionality (DMZ, remote access), or as a production business process.



CONDUIT

A Conduit is a Physical or/and logical entity that serves as a communication channel (for protocols & services) between two zones.

SECURITY LEVEL TARGET (SLT)

A numeric level corresponding to the required effectiveness of countermeasures and/or the inherent security properties of devices and systems. SLTs are defined per zone or conduit.

Zone	Default SL-T
Enterprise	2
DMZ	3
Operations management	3
Supervisory control	4
Basic control	4
Safety	4
Remote	4

SECURITY LEVEL ACHIEVED (SLA)

The achieved security level of a zone or conduit depends on:

- The inherent security properties of devices and systems within the zone or conduit; and/or
- The properties of countermeasures used to prevent the zone or conduit from being compromised.

The SL(Achieved) is a function of time, and decreases in time due to degradation of countermeasures, new vulnerabilities, adjusted threats or attack methods, breach in security layers, and the inherent security properties of devices and systems pending review, update, or upgrade.

> *The objective is to ensure that at any given time the SL(achieved) of a zone or conduit is greater than or equal to the SL(target) for the zone or conduit.*

PROCESS HAZARD ANALYSIS (PHA)

For potentially hazardous processes, the results of the process hazard analysis (PHA) and functional safety assessments (as defined in IEC 61511-2 [8]) should be referenced as part of the initial cyber security risk assessment to identify worst-case impacts.

RISK MATRIX

Assessment of initial risk is often accomplished using a risk matrix that establishes the relationship between likelihood, impact, and risk.

Risk matrixes are used to qualitatively establish the SL. Starting with a reasonable estimate of SL (or none at all), the cyber security risk is evaluated considering the countermeasures implied by the SL. If the risk is not acceptable, the SL is raised (i.e. additional countermeasures are added) until the cyber security risk is acceptable. The SL derived from this analysis becomes the SL-T.

			Severity	
		A	B	C
Likelihood	5	High	High	Med-high
	4	High	Med-high	Medium
	3	Med-high	Medium	Med-low
	2	Medium	Med-low	Low
	1	Med-low	Low	Low

MITRE ATT&CK

MITRE ATT&CK® is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

CVE

CVE® is a list of entries, each containing an identification number, a description, and at least one public reference for publicly known cybersecurity vulnerabilities. CVE Entries are used in numerous cybersecurity products and services from around the world, including the U.S. National Vulnerability Database (NVD).

SECURITY LIFE CYCLE (NIST 800-55)

This concept refers to establishing and maintaining baseline configurations of hardware and software throughout the system's development life cycle, including inventories of organizational information systems.

Automation Security Life Cycle Stages:

Concept and Specifications	**Initial cybersecurity risk assessment**
Development and Design	Detailed cybersecurity risk assessment, mitigation control, recommendation, Security operations guidelines
Production Implementation	Automation of data collection, continuous monitoring
Support and Maintenance	Periodic detailed risk assessment, reporting, alerts, incident handling protocols, patches and upgrades, data collection, continuous monitoring
Retirement	Purge sensitive data, decommission security controls

DIGITAL IMAGE

A digital image is a digital replica of a physical entity, and more broadly to a digital replica of potential and actual physical assets, processes, assets, protocols, configurations, systems, and devices.

Digital images are used to conduct testing and simulations without affecting the actual production process.

METHODOLOGY

A successful risk assessment methodology should analyze all involved systems in a layered approach, starting with systems closest to the threat, and working inward. The basic risk assessment process consists of three steps:

- Assess initial risk.
- Implement risk mitigation countermeasures.
- Assess residual risk.

The organization should select a particular risk assessment/analysis approach and methodology that identifies and prioritizes risks based upon security threats, vulnerabilities and consequences related to their IACS assets. Asset owners may assign different levels of integrity protection to different components, communication channels and information in their IACS.

INITIAL RISK CYBER SECURITY ASSESSMENT (62443-3-2)

IEC62443 prescribes that users identify the worst case unmitigated cyber security risk that could result from the interference with, breach or disruption of, or disablement of mission critical IACS operations. (62443-2-1 4.3 ZCR 2)

For potentially hazardous processes, the results of the process hazard analysis (PHA) and functional safety assessments (as defined in IEC 61511-2 [8]) should be referenced as part of the initial cyber security risk assessment to identify worst-case impacts. The outcome of the Initial Level Risk Assessment is a defined set of Zones and Conduits in relation to Impact. The defined “impact zones” are assigned a security level target (SLT) dictates the security requirements (SR) needed to meet the SLT.

DETAILED CYBER SECURITY RISK ASSESSMENT 62443-3-2

- Identify a list of the threats that could affect the assets contained within the zone or conduit
- Description of the threat source.
- Description of the capability or skill-level of the threat source.
- Description of possible threat vectors.
- Identification of the potentially affected asset(s).
- Identify vulnerabilities
- Identify threat scenario, determine the consequence and the impact should the threat be realized
- Determine the unmitigated likelihood. This is the likelihood that the threat will materialize.
- Determination of unmitigated cyber security risk using a risk matrix that establishes the relationship between likelihood, impact, and risk.
- Compare unmitigated risk with tolerable risk
- Identify and evaluate existing countermeasures, existing countermeasures in the SUC shall be identified and evaluated to determine the effectiveness of the countermeasures to reduce the likelihood or impact.
- Reevaluate likelihood and impact, the likelihood and impact shall be re-evaluated considering the countermeasures and their effectiveness.
- Determine residual risk
- Compare residual risk with tolerable risk
- Document and communicate results, documentation that was instrumental in performing the cyber risk assessment (such as, system architecture diagrams, PHAs, vulnerability assessments, gap assessments and sources of threat information) shall be recorded and archived along with the cyber risk assessment.

ASSET-DRIVEN VS SCENARIO-DRIVEN

As mentioned, the likelihood of a threat materializing in relation to its impact makes up the risk score.

Most current likelihood assessment methodologies rely predominately on vulnerabilities (asset-driven) as likelihood facilitators and patch level as likelihood mitigators. CIARA goes one step further and combines asset and scenario driven likelihood calculations. Scenarios are based on MITRE ATT&CK adversary simulations and threat intelligence.

CONTINUOUS VS AD-HOC RISK MONITORING

Continuous risk monitoring, where logs and events are continuously sent to CIARA for analysis, enables the organization to observe risk score changes as new connections, assets, and business processes are added to the system. In addition, risk score and contextual information can be added to security alerts sent to the SOC.

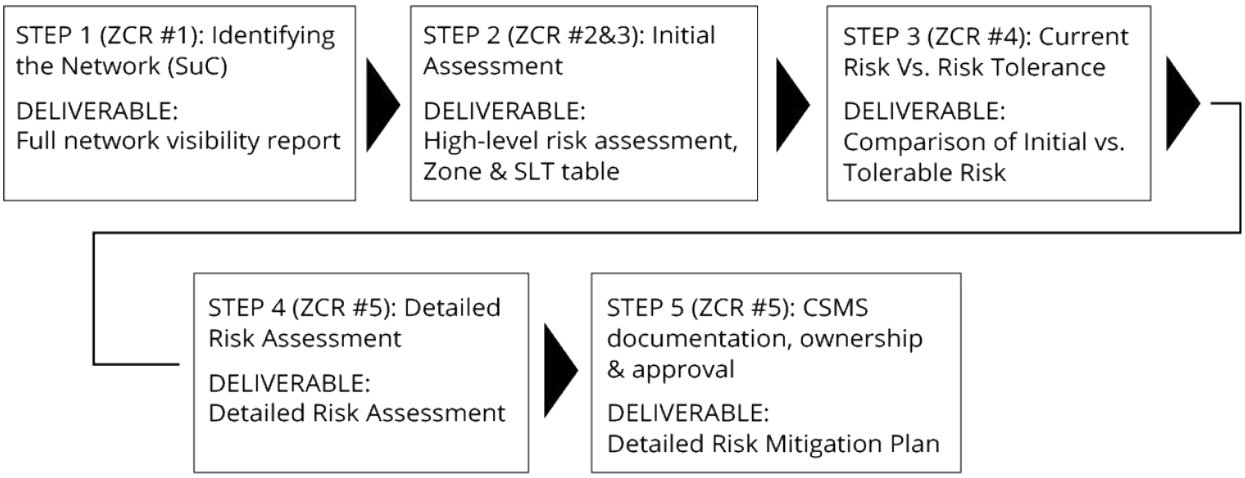
An ad-hoc methodology can be used as an assessments tool for Systems Under Consideration (SUC) by means of recording PCAPs and running then in CIARA. CIARA's resulting reports will then provide a risk snap-shot of the current system, along with risk reduction recommendations.

This process of recording PCAP files can be done as frequently as needed to verify the implementation of risk-mitigation recommendations.

Risk score and contextual information can be added to security alerts sent to the SOC.

CIARA – STEP-BY-STEP

CIARA's workflow steps were designed to follow the ZCRs (Zone & Conduit Requirements) defined in IEC 62443 3-2.



STEP #1(ZCR 1)

Requirement:

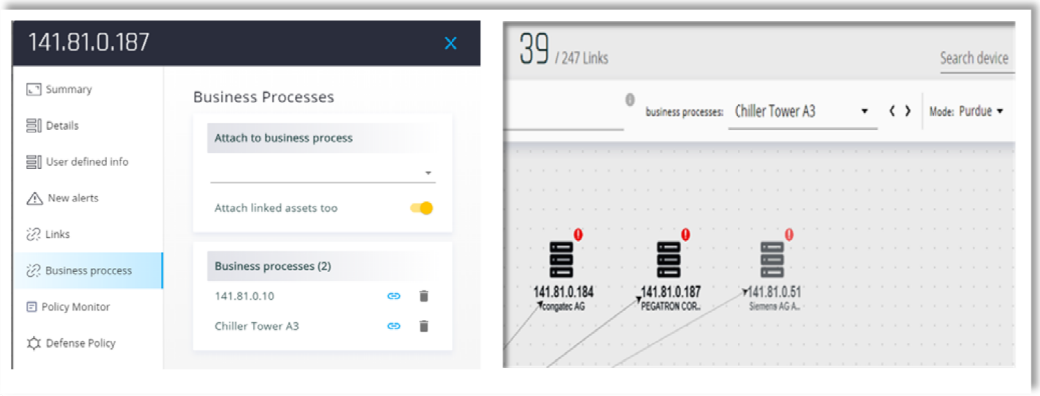
Identifying the system under control (SuC): The organization shall clearly identify the SUC, including clear demarcation of the security perimeter and identification of all access points to the SUC. (4.2.1.1)

Actions:

- Input PCAPs, traffic via a TAP or mirror port, CIARA API, or upload a flat file
- Define the SuC from the uploaded digital image

Deliverable:

At this stage the user is able to print from within CIARA a full network visibility report showing assets, protocols and links.



STEP #2 (ZCR 2&3)

Requirements:

The organization shall perform a cyber security risk assessment of the SUC or confirm that a previous initial cyber security risk assessment is still applicable, in order to identify the worst case unmitigated cyber security risk that could result from the interference with, breach or disruption of, or disablement of mission critical IACS operations. (4.3.1.1)

The organization shall group IACS and related assets into zones or conduits as determined by risk. Grouping shall be based upon the results of the initial cyber security risk assessment or other criteria, such as criticality of assets, operational function, physical or logical location, required access (for example, least privilege principles) or responsible organization (4.4.2.1).

Actions:

CIARA will automatically maps network assets into Zones and Business Processes. The user is able to fine-tune CIARA's mapping as needed.

CIARA will ask the user to enter your Industrial sector and Geo-location. Once entered, CIARA will scour the MITRE ATT&CK database for adversaries, regions, and attack techniques relevant to the system analyzed. The resulting ATT (Adversary Tactics and Techniques) will be simulated on the digital-image.

At this stage you can start defining Zones and Conduits based on your initial risk assessment (see above "initial risk assessment"). CIARA's initial configuration proposes several out-of-box zones, which are assigned predefined IEC-62443 SLTs. Users can define additional zones (for additional business processes) with custom names and SLTs.

Zone	Default SL-T
Enterprise	2
DMZ	3
Operations management	3
Supervisory control	4
Basic control	4
Safety	4
Remote	4

Deliverable:

Upon completion of this step, the user is able to print a high-level report (See Methodology section, "Initial Cybersecurity Risk Assessment) as well as a Zone & SLT table.

STEP #3 (ZCR 4)

Requirements:

The purpose of this step is to determine whether the initial risk is tolerable or requires further mitigation (4.5.2.2). The tolerable risk level is defined as the risk level acceptable to an organization.

"Risk tolerance e.g. levels of risk, types of risk, and degree of risk uncertainty that are acceptable. Risk-based decisions within organizations often reflect the blending of the risk tolerance of senior leaders/executives and the risk tolerance that is embedded within the culture of organizations". NIST 800-39

Note that the term Risk Tolerance is purely qualitative, as engineers do not try to find a describing function for this value. Unlike risk value calculations that can be done according to PHA (Process Hazard Analysis) and the likelihood of cyber breach, "Tolerance" is a subjective value entered by the user.

Actions:

CIARA will compare the Initial risk score with the user's input of Tolerable risk. This information will be used later for the detailed risk assessment and recommendations for risk mitigators.

> *The term Risk Tolerance is purely Qualitative, as engineers do not try to find a describing function for this value.*

STEP #4 (ZCR 5)

Requirements:

This stage defines the detailed risk assessment requirements for the IACS, and provides rationale and supplemental guidance on each requirement.

The requirements in this ZCR apply to every zone and conduit. If zones or conduits share similar threat(s), consequences, and/or similar assets, it is allowable to analyze groups of zones or conduits together if such grouping enables optimized analysis. It is permissible to use existing results if the zone is standardized (for example, replication of multiple instances of a reference design).

Actions:

At this stage CIARA's wizard that will help the user to go through the FR/SR for each zone.

As in step #2, if an SLT (security level target) has been defined for a zone, CIARA will present only the FRs/SRs needed to meet that SL-T (i.e. it will not present measures meant to exceed the SL-T.)

This information will be used by CIARA to:

- Perform a gap analysis between the FR/SR entered as implemented and the mediators that are needed to meet the SLT
- Re-calculate the risk score for a detailed risk assessment report
- Produce a mitigation score and a completion score to meet the desired SLT
- Calculate the best ROI for the planning of security mitigators that will maximize risk reduction

Deliverable:

At this point the user will be able to produce a detailed risk report containing:

- ZCR 5.1: Identify threats
- ZCR 5.2: Identify vulnerabilities
- ZCR 5.3: Determine impact
- ZCR 5.4: Determine unmitigated likelihood
- ZCR 5.5: Determine unmitigated risk
- ZCR 5.6: Determine SL-T
- ZCR 5.7: Compare unmitigated to tolerable risk
- ZCR 5.8: identify and evaluate existing countermeasures
- ZCR 5.9: Re- evaluate likelihood and impact
- ZCR 5.10: Determine residual risk
- ZCR 5.11: Compare residual risk to tolerable risk
- ZCR 5.12: Identify Additional cyber security countermeasures

STEP #5 (ZCR 6 & 7)

This step describes the processes of process documentation, ownership and approval needed to refine and finalize their CSMS (risk mitigation) plan.

- ZCR-6: Documentation of cyber security requirements, assumptions, and constraints within the SUC as needed to achieve the SL-T; provision of rationale and supplemental guidance for each requirement. (4.7.1)
- ZCR-7: Asset owner management who are accountable for the safety, integrity, and reliability of the process controlled by the SUC shall review and approve the results of the risk assessment. (4.8.2.1)

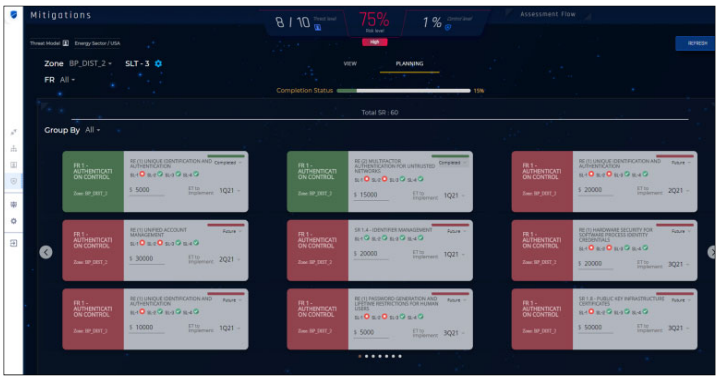
CIARA presents the top risk zones, level of mitigation controls and likelihood of breach due to vulnerabilities and threat adversaries.

Incomplete FRs/SRs will be presented to the user in a “to-do” checklist format. For each item (card) the user can add expenditure cost, and target completion date. Cards can be filtered by impact, risk, cost, and target date.

CIARA will dynamically change the network risk score as mitigation controllers are added/subtracted. Each controller has a pre-calculated (machine-learning) mitigation weight, which is assigned is according to its calculated effectiveness against the topmost likely scenario.

In this way, CIARA enables users to plan and budget their cyber-mitigation measures, and prioritize procurement according to mitigation control effectiveness and budgetary restraints.

> *CIARA enables users to plan and budget their cyber-mitigation measures, and prioritize procurement according to mitigation control effectiveness and budgetary restraints.*



CIARA’s Planning screen, displaying prioritized mitigation controls with cost and completion date for each

ORDERING INFORMATION

US and Canada:
Tel: +1 (302) 547-6839
sales_NA@radiflow.com

EMEA:
Tel: +972 (77) 501-2702
sales@radiflow.com

UK:
Tel: +44 (0) 800 246-1963
sales_UK@radiflow.com

Germany, Austria & Switzerland:
Tel: +49 (160) 109 75 65
sales_DACH@radiflow.com

Southern Europe Region
Tel: +39 (340) 7319727
Sales_SER@radiflow.com

France:
Tel : +33 1 77 47 87 25
sales_FR@radiflow.com

ABOUT RADIFLOW

Radiflow develops trusted Industrial Cybersecurity Solutions for Critical Business Operations. Our portfolio of game-changing solutions for ISC/SCADA networks empowers users to maintain visibility and control of their OT networks while increasing overall security expenditure ROI. Our intelligent Threat Detection and Analysis Platform for industrial cybersecurity minimizes potential business interruptions and loss within your OT environment.

Radiflow's team consists of professionals from diverse backgrounds, from cyber-experts from elite military units and automation experts from global cybersecurity vendors.

Founded in 2009, Radiflow's solutions are successfully deployed by major industrial enterprises and utilities protecting more than 4,000 critical facilities worldwide, and endorsed by Tier-1 customers & external labs. More at www.radiflow.com