ICS4ICS

Incident Command System
for Industrial Control Systems

Strengthening the Response to ICS incidents by Leveraging Established Emergency Frameworks

ETSI Security Conference 2022

Matjaz Demsar
SIEMENS Professional Services – Slovenia
Lukasz Kister, PhD
Woodward

Oct 5th, 2022

Brief introduction

ICS4ICS Overview

ICS4ICS

Incident Command System
for Industrial Control Systems

ICS4ICS Exercise

After Action Review (AAR)

Brief introduction

Two years ago, we created ICS4ICS…

The beginning of ICS4ICS

- Absence of a common response framework, making scaling nearly impossible
- The cost of poorly coordinated responses, unclear number of incident reponders
- Cyber was the only designated federal (US) disaster type not currently using Incident Command System for its response framework
- The need for consistent Cyber Incident Responder roles and typing based on knowledge and experience

It was enough to give the effort momentum, volunteers, and sponsorship through the ISA GCA.

ICS4ICS Today

- Over 1,000 global volunteers
- Completed first round of credentialing of Cyber Incident Commanders
- 1st ICS4ICS Exercise at S4 on April 18, 2022
- Utilizing FEMA OneResponder System
- Freely available

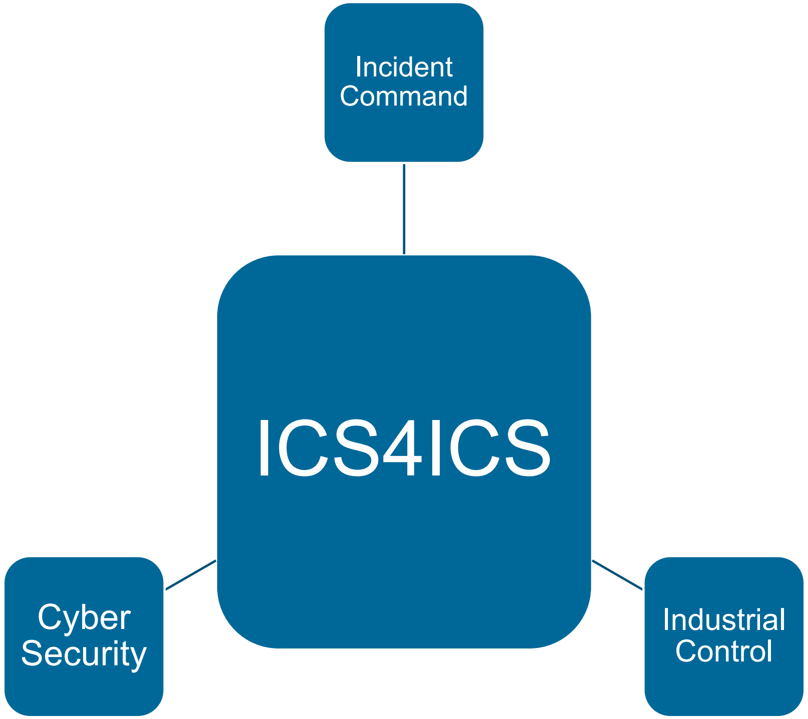
ICS4ICS

Incident Command System
for Industrial Control Systems

ICS4ICS Overview

ICS4ICS Improves response to ICS incidents

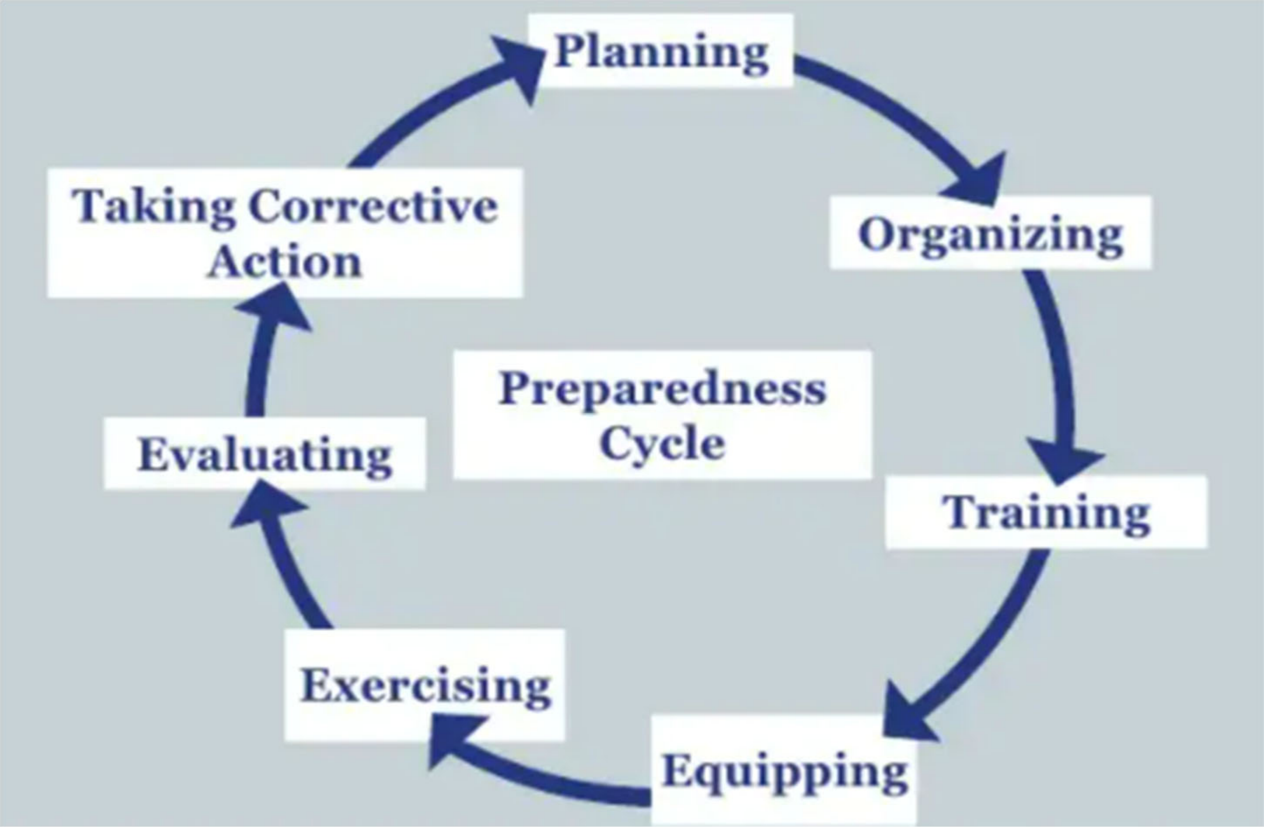
By leveraging 3 disciplines with proven capabilities



- Incident Command System
  - Command structure to manage incidents used since the 1970's
- Cyber Security: Computer Incident Response
  - Investigation capabilities to manage cybersecurity incidents that are widely used by IT organizations
- Industrial Control System
  - Experts with Industrial knowledge and expertise to respond to incidents

Mature Incident Command System methodology

Steps to prepare and implement a program focused on teams



Why use Incident Command System when managing Industrial Control System incidents?

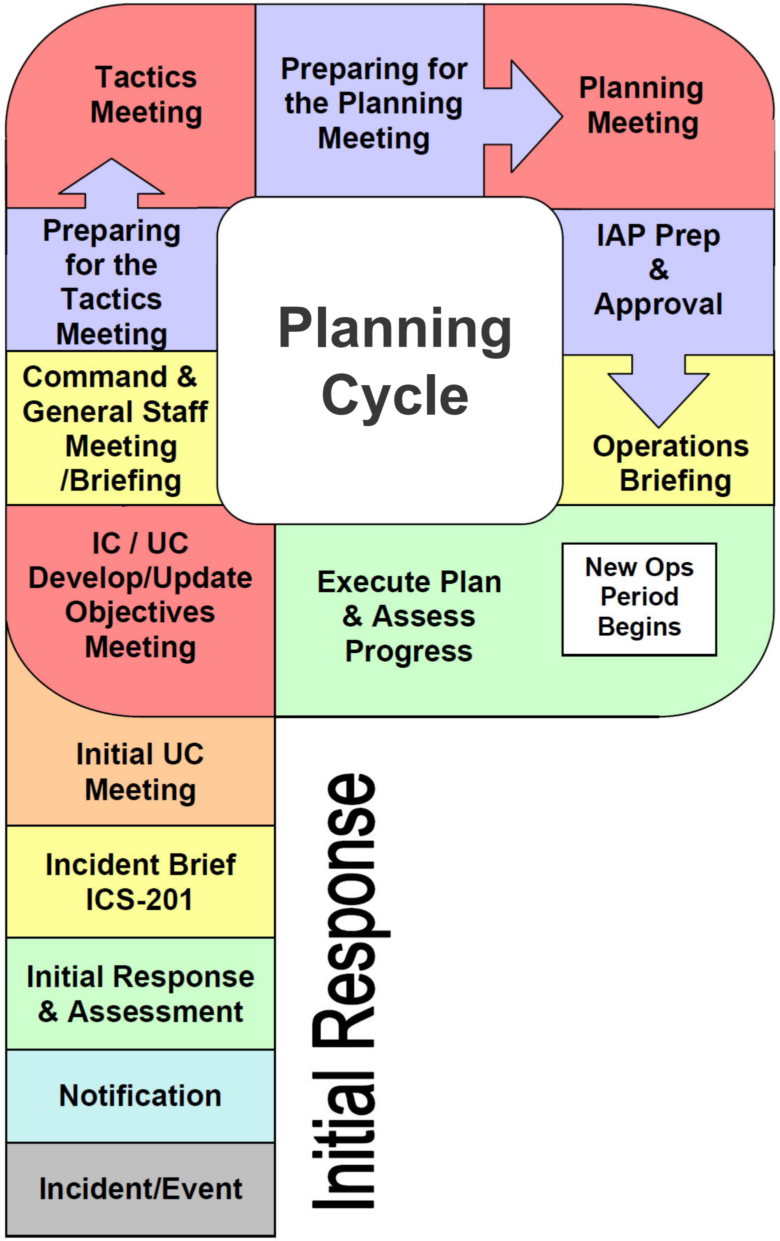
- Standard Approach
- Proven Effective
- Unity of Command
- Clarity of Responsibilities
- Span of Control
- Common Terminology
- Adaptability to size/complexity
- Planned and Unplanned events
- Unity of Effort
- Accountability

Planning P process

Incident Command Process

The Planning P provides a proven structured process to manage any incident with a standardized approach to organizing and executing work

- Order of meetings & briefings
- Incident Command System forms & worksheets to complete
- Team member's action and/or work products



Planning Cycle

Tactics Meeting

Preparing for the Planning Meeting

Planning Meeting

IAP Prep & Approval

Operations Briefing

New Ops Period Begins

Execute Plan & Assess Progress

IC / UC Develop/Update Objectives Meeting

Command & General Staff Meeting /Briefing

Preparing for the Tactics Meeting

Initial UC Meeting

Incident Brief ICS-201

Initial Response & Assessment

Notification

Incident/Event

Initial Response

ICS4ICS Exercise

ICS4ICS: Exercise Purpose, Mission, Objectives

Purpose: To explain proposed approach to coordination, collaboration, information sharing, and response capabilities of ICS4ICS in the context of a significant cyber incident that might result in physical threats to life, safety, and property.

Mission: Highlight the approach that ICS4ICS is recommending to manage a Cyber Security Incident for Industrial Control System

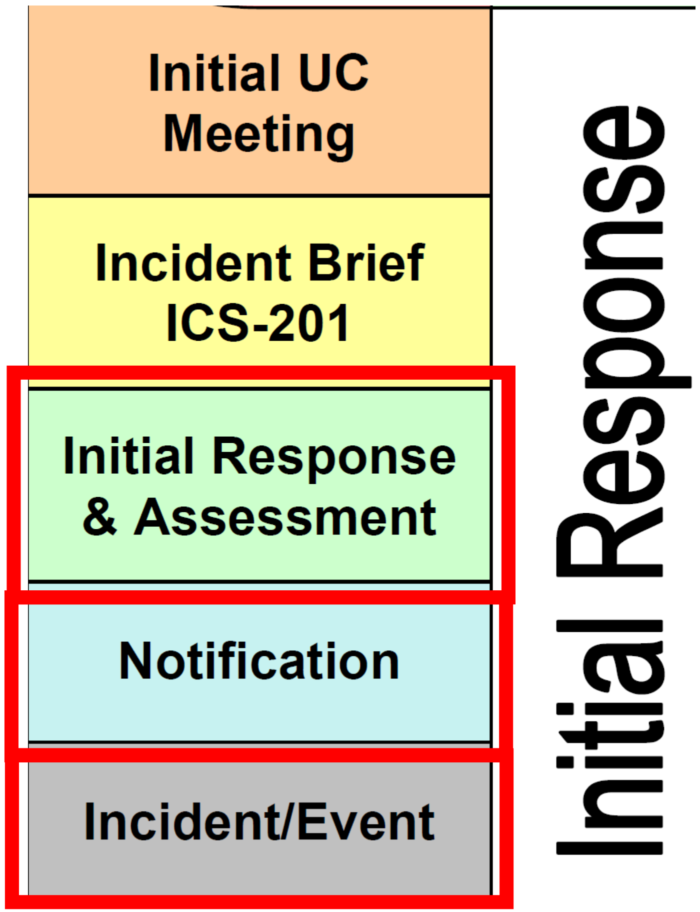
Objectives

1. Monitor events to identify possible incidents
2. Perform Notification to engage ICS4ICS Team
3. Complete an initial Assessment of the event and declare Incident if appropriate
4. Manage response to the incident and limit its‘ initial impact
5. Demonstrate management of incident response using key components of ICS4ICS
6. Present ICS4ICS structure and showcase key components of the program
7. Work on Remediation and Resolution of incident

Threat/Hazard: Cyber Security Incident impacting Industrial Control System, HVAC

Planning P

Initiating Incident Response

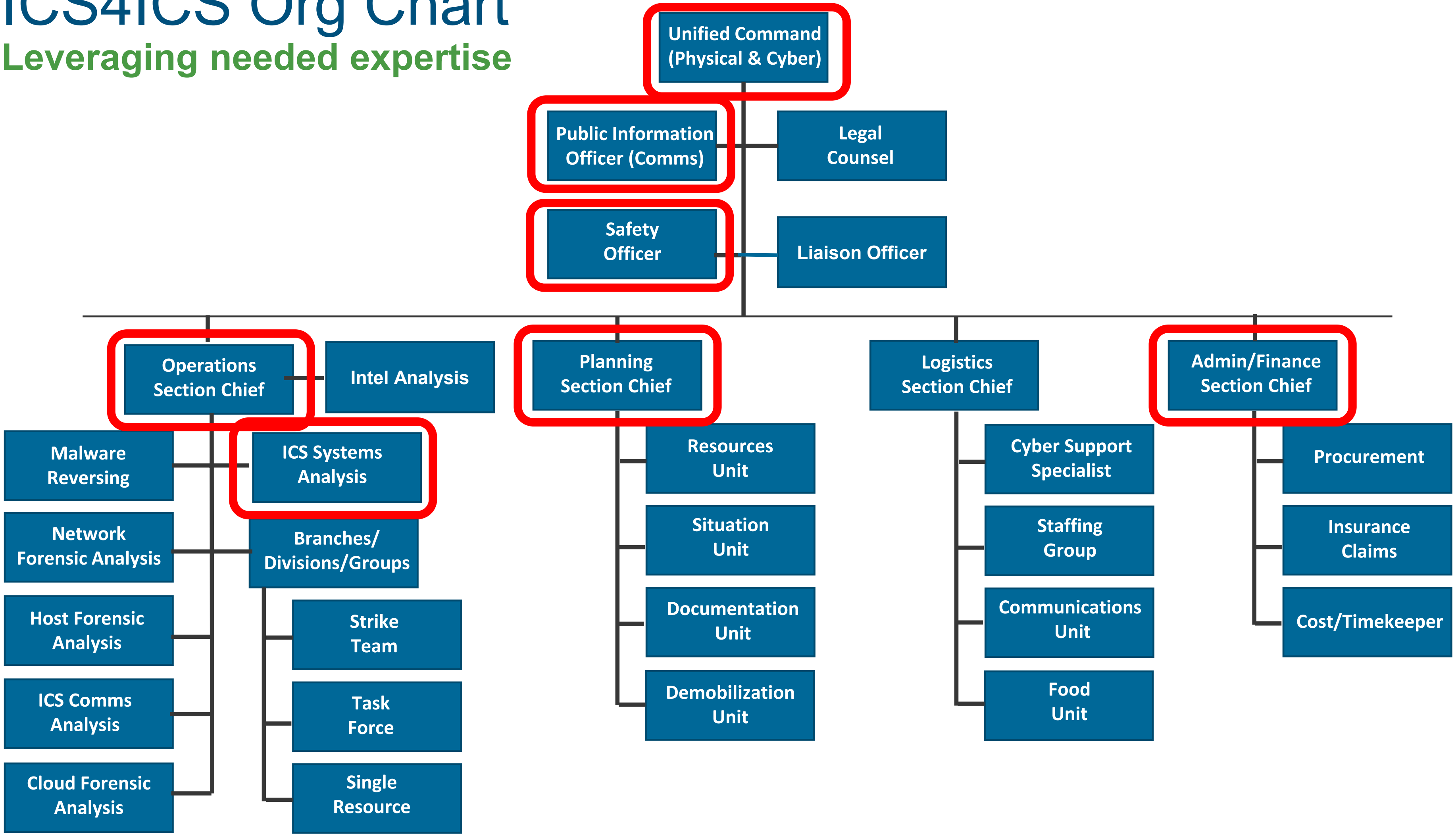


Initial Response & Assessment

- The company leadership previously designated an Incident Commander with the authority to declare an incident.

ICS4ICS Org Chart

Leveraging needed expertise



Unified Command (Physical & Cyber)

Public Information Officer (Comms)

Legal Counsel

Safety Officer

Liaison Officer

Operations Section Chief

Intel Analysis

Malware Reversing

ICS Systems Analysis

Network Forensic Analysis

Branches/ Divisions/Groups

Host Forensic Analysis

Strike Team

ICS Comms Analysis

Task Force

Cloud Forensic Analysis

Single Resource

Planning Section Chief

Resources Unit

Situation Unit

Documentation Unit

Demobilization Unit

Logistics Section Chief

Cyber Support Specialist

Staffing Group

Communications Unit

Food Unit

Admin/Finance Section Chief

Procurement

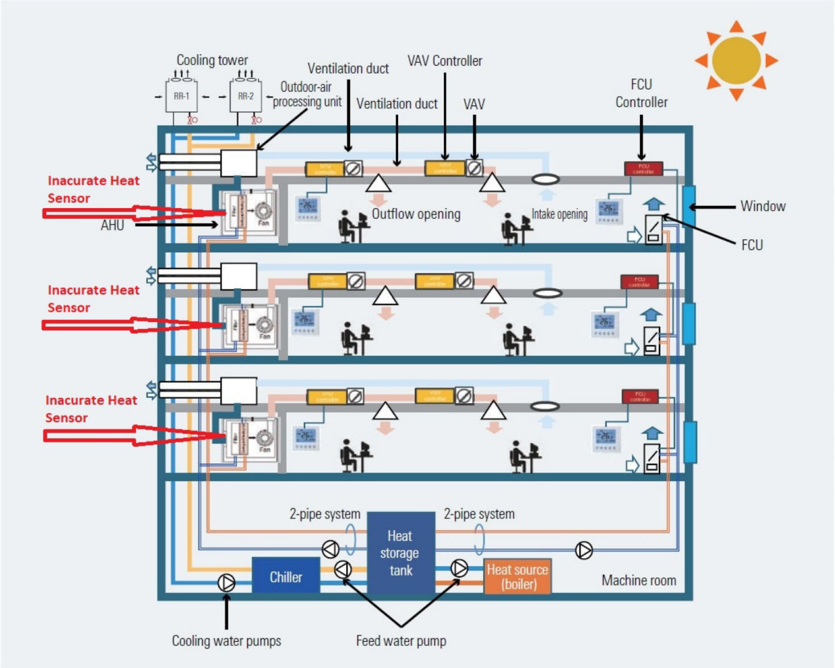
Insurance Claims

Cost/Timekeeper

INCIDENT BRIEFING (ICS 201)

1. Incident Name: ICS4ICS WORKSHOP	**2. Incident Number:** N/A	**3. Date/Time Initiated:** Date: 01/24/2022 Time: 2:30 PM

4. Map/Sketch (include sketch, showing the total area of operations, the incident site/area, impacted and threatened areas, overflight results, trajectories, impacted shorelines, or other graphics depicting situational status and resource assignment):



5. Situation Summary and Health and Safety Briefing (for briefings or transfer of command): Recognize potential incident Health and Safety Hazards and develop necessary measures (remove hazard, provide personal protective equipment, warn people of the hazard) to protect responders from those hazards.

As of 1/23/2022, 9:35 hrs am, the temperature in the offices began to rise. Building Maintenance were unable to resolve the situation and HVAC Vendor was contacted.

HVAC personnel arrived on 1/24/2022 at 10:00 am and determined that the HVAC systems has been compromised with malware. The vendor has not been able to contain or eradicate the malware and has no solutions to restored the HVAC system.

At 10:15 am, ICS Analyst - HVAC Technical Analyst Coordinator contacts the Computer Incident Response Team (CIRT) to report that malware has been detected in the HVAC systems supporting the building, the data center, and other Industrial Control Systems in the building.

Based on the escalation procedures, CIRT Manager declares an incident and initiates ICS4ICS.

6. Prepared by: Name: I. M. Scribe Position/Title: Documentation Unit Lead Signature: I.M.Scribe

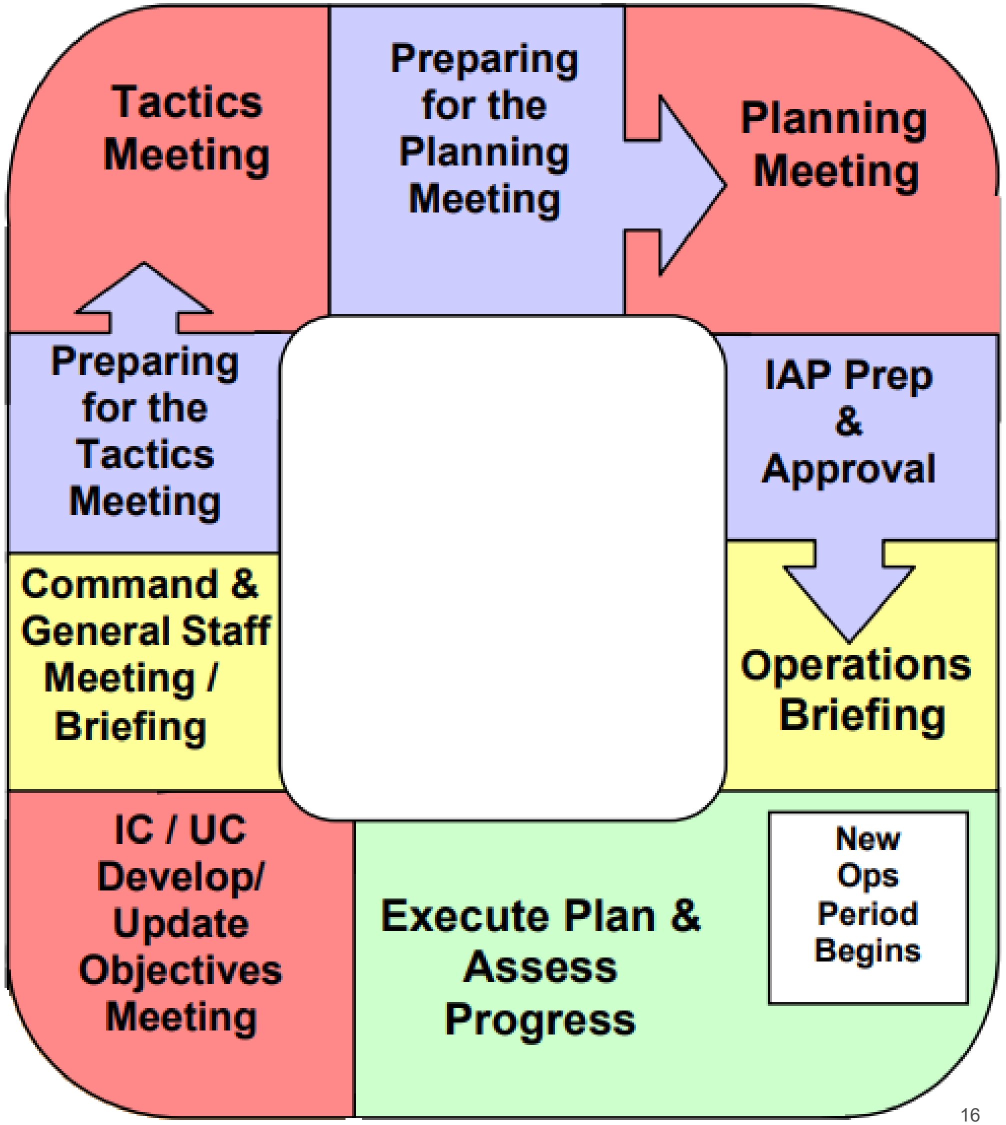
ICS 201, Page 1 Date/Time: 1/24/2022 3:00 pm

Incident Description

Planning P process

Repeating the Planning Cycle

- The Cycle is repeated multiple times to continue planning and working on response
  - Likely this will be repeated in 6-hour cycles
  - The next shift will also repeat the same cycle
- The ICS4ICS Team will have to be relieved by a 2nd shift ICS4ICS Team


Tactics Meeting
Preparing for the Planning Meeting
Planning Meeting
Preparing for the Tactics Meeting
IAP Prep & Approval
Command & General Staff Meeting / Briefing
Operations Briefing
IC / UC Develop/ Update Objectives Meeting
Execute Plan & Assess Progress
New Ops Period Begins

After Action Review (AAR)

ICS4ICS: After Action

List the top three (3) strengths

- **NIMS/Incident Command System is widely used for most incidents (ALL-Hazards)**
  - Companies, Governments, and others can quickly apply NIMS/ICS to Cybersecurity incidents impacting Industrial Control Systems via ICS4ICS
- **ICS4ICS was built using standardized NIMS/ICS forms from FEMA**
  - The forms document decisions and activities of the incident which allows the next ICS4ICS shift to quickly assume their responsibilities when they arrive
  - Data enables look-back improvements, insurance and government reporting
- **ICS4ICS enables consistent and quick decision making**
  - Prevents paralysis that may occur without clear incident and decision processes
  - Ensures teams and team members are executing from the same set of decisions
  - Technical staff performs their work while leadership is making future decisions

ICS4ICS: After Action

List the top three (3) items requiring improvement

- Time is needed to get familiar with forms – present a summary list of the forms early in exercise
  - Provide an overview and explanation of the various forms
- Explain ICS4ICS is not a democracy – The Incident Commander is in charge!
  - Agreements are made, and issues resolved before meetings
- Describe roles that would normally be staffed in a real incident, as needed
  - Safety Officer has sub-team of Physical, Cyber, and Environmental experts
  - Liaison Officer(s) may be needed to interface with gov (DHS, FBI) / ISAC and others

ICS4ICS: After Action

Hot Wash Remarks/Comments

- Small companies may need help to use ICS4ICS
  - The exercise has been designed for Type 3 incidents – single company and single asset incidents, which will apply to small companies
  - The ICS4ICS Team will assist Industry Sectors to host exercises
    - This will address several smaller companies, like utility operators and others
- DOA is critical to be able to finance the incident response efforts
  - IC provides their Delegation of Authority or obtains more from executives
  - IC must be pre-authorized with DOA so work can begin immediately
- ICS4ICS processes, forms and other resources can be used for big or small incidents
  - The size of the ICS4ICS team will vary greatly based on the incident!

ICS4ICS: Credentials

Providing consistent organizational capabilities to execute ICS4ICS

- ICS4ICS credentials will ensure people are qualified for relevant ICS4ICS roles
- We are focused on credentialling these ICS4ICS roles initially:
  - Incident Commander (Unified Command)
  - Operations Section Chief
  - Planning Section Chief
  - Logistics Section Chief
  - Admin/Finance Section Chief
- We will add other key ICS4ICS roles
  - Malware and other IT roles
  - Public Information Officer, Liaison Officers, and other roles
- ICS4ICS is leveraging OneResponder and FEMA training for credentialling

ICS4ICS Future

Expanding ICS4ICS Capabilities

- Conduct ICS4ICS Exercises globally
  - Host ICS4ICS exercises globally to enable people to obtain credentials
- Offer ICS4ICS credentials and training globally
  - Grow the base of people with expertise in ICS4ICS
  - Manage credentialling with FEMA National Qualification System (OneResponder)
- Expand ICS4ICS processes and capabilities globally
  - Support more complex incidents: Type 2 - one-company, multi-assets/sites
  - Add Mutual Aid processes and templates for agreements and contracts

ICS4ICS and you

How can you get involved?

- Register for the ICS4ICS Newsletter
- Observe or Participate in an ICS4ICS exercise
- Host an ICS4ICS exercise at a public event or in your company
- Join an ICS4ICS team to help define the processes, training, etc.
- Consider presenting ICS4ICS at a future event

Contact us for more information

ICS4ICS – Useful links

Looking for more information?

- ICS4ICS website
- VIDEO – ICS4ICS overview
- VIDEO – ICS4ICS Exercise – Part 1
- VIDEO – ICS4ICS Exercise – Part 2

ICS4ICS

Incident Command System
for Industrial Control Systems

Matjaz Demsar
OT Cybersecurity expert
SIEMENS Professional Services
matjaz.demsar@siemens.com

dr Łukasz Kister
Global Product Cyber Security Expert
Corporate Technology Office
lukasz.kister@woodward.com