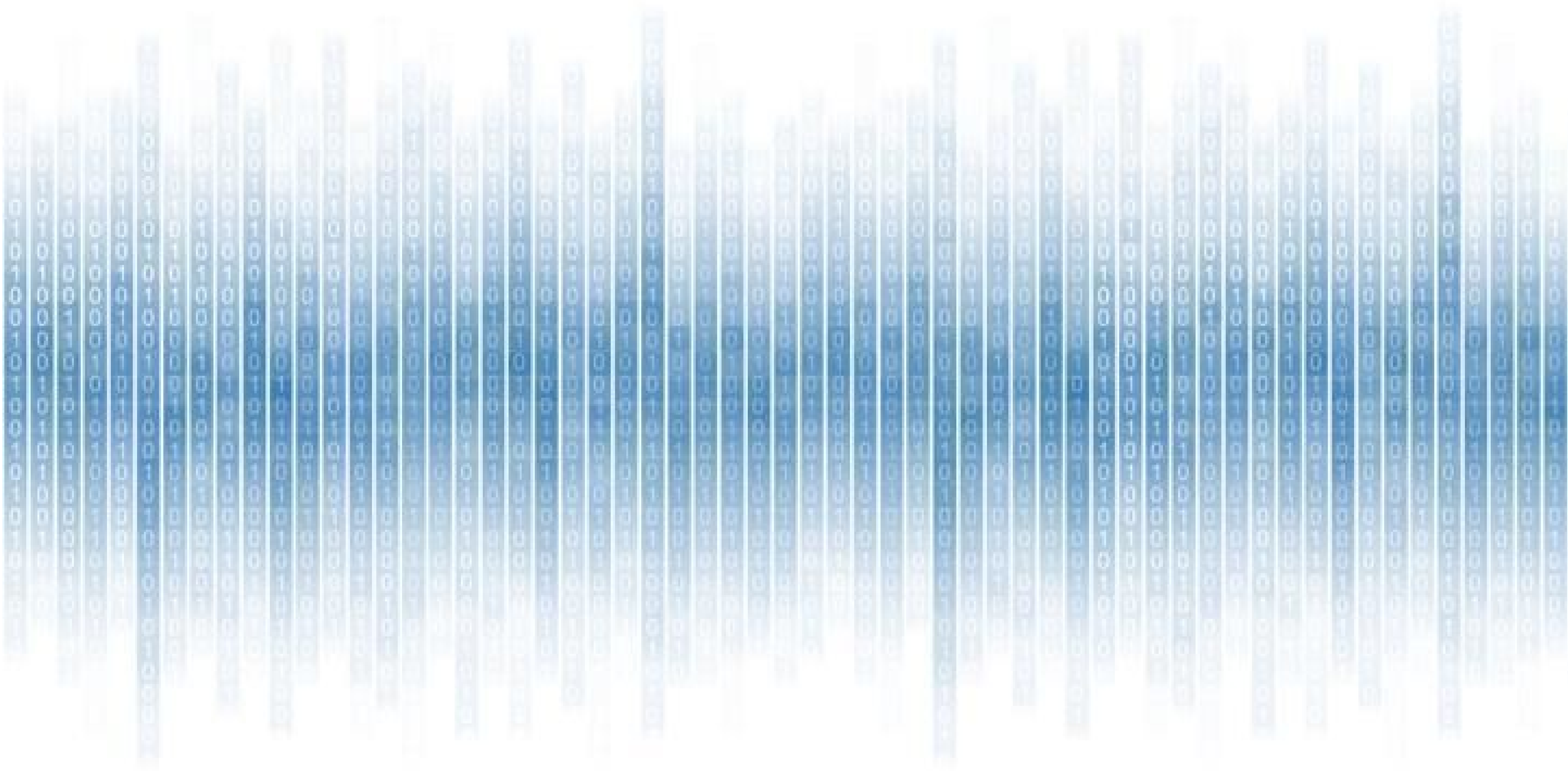

CSA ICS Security Working Group

Charter

August 2018

WORKING GROUP EXECUTIVE OVERVIEW

Working Group Scope and Responsibilities

Working Group Membership

Working Group Structure

Co-Chairs

Committees

Sub-Work Groups

Alignments with Outside Groups

Operations

Advisory

Research Lifecycle

Peer Review

Communications Methods

Infrastructure & Resource Requirements

Work Group Conference Calls and In-person Meetings

Decision-making Procedures

Deliverables/Activities

Duration

Charter Revision History

WORKING GROUP EXECUTIVE OVERVIEW

Mission Statement: To help organizations secure industrial networks, endpoints, and controllers in production sites from new or emerging cybersecurity risks.

As industrial control systems (ICS) advance to Industrial Internet of Things (IIoT), ICS are connecting to the cloud, and at the same time the risk of cyber-attacks is increasing more than ever before. Since 2010, advanced cyber attacks on cyber-physical systems have occurred (e.g., Stuxnet, Havex, BlackEnergy, Industroyer, Triton). On the other hand, while asset owners understand cyber risks to connect ICS to external networks including cloud, there are challenges to mitigate cyber risks due to system specification differences between information systems and ICS.

The ICS Security Working Group aims to develop security recommendations that asset owners and Industrial Automation vendors can leverage globally to protect industrial networks, endpoints, and controllers from new or emerging cybersecurity risks.

The ICS Security Working Group will create the following research artifacts:

1. ICS Cyber Security Management – Digitalization trends in production sites, need for implementing measures to curb security risks, challenges of risk mitigation in ICS, practices to build up security enhancement activities, governance
2. Practical security controls of ICS security – Security controls related to network separation, industrial network monitoring, access control, portable media device management, system vulnerability management, threat management, incident handling, ICS / cloud / IOT integration security, etc.

CSA initiatives that may be relevant for this work will be referenced in this work. Furthermore, alignment to global standards can be achieved through the CSA International Standardization Council.

Working Group Scope and Responsibilities

The CSA ICS Security Working Group will be the primary decision-making body relative to the reference architecture and the defined deliverables. A majority of the members will make decisions.

The scope for the ICS Security working group includes, but is not limited to:

- Develop more situational awareness for asset owners and Industrial Automation vendors
- Enlightenment of C-level
- Business and system use cases of ICS connected to cloud

- Cyber-attack trends of ICS
- Cyber Security Risk Analysis based on Use Cases
- Analysis of ICS challenges – Awareness, Organization and Process, Knowledge, Technology
- Industry specific standard, regulations, and risk will be developed

WORKING GROUP MEMBERSHIP

The working group is co-chaired by Tadashi Onodera in CSA Japan Chapter.

Principal attendees will be designated representatives from an entity and any alternative to be designated by each principal.

The chair may appoint others as necessary to assure the effective execution of the defined work.

Other individuals may be invited to attend meetings by the principals as deemed necessary to provide inputs to topics under discussion.

Working Group Structure

Co-chair

The working group will be led by co-chair in addition to the selected leadership. The co-chair will assist with the leadership responsibility of the working group. The co-chair may appoint others as necessary to assist in the effective execution of the defined research.

Committees

The working group may designate and organize subcommittees to aid in research with the initiatives about the subject matter of the working group.

Sub-Work Groups

Ad hoc sub-workgroups comprising subject matter experts may be formed to plan or execute any related outreach, awareness or research opportunities. Such sub-working groups shall report directly to the main working group.

ALIGNMENTS WITH OUTSIDE GROUPS

The working group may also choose to allow resource sharing between ICS and cybersecurity communities focused on ICS and other CSA working groups to assist in the timely completion of projects, programs and other activities needed to support/enable the working group's defined body of work, on-demand basis. The working group will share research and standards that align with other CSA Working Groups, advisory groups, and industry partners (i.e., SDOs, gov).

OPERATIONS

Advisory

The CSA Subject Matter Expert (SME) Advisory Council, International Standardization Council (ISC), and CSA Executive Team will advise the CSA Working Group to ensure that the research under the working group is within the scope of the CSA and aligns with other industry partner research. The research will remain unique to the industry and refer to any redundant or replicated works.

Research Lifecycle

The CSA Working Group will follow the development of the CSA research lifecycle for all projects and initiatives:

https://downloads.cloudsecurityalliance.org/initiatives/general/CSA_Research_Lifecycle_FINAL.pdf

Peer Review

We will seek CSA's help in reaching out to peers for reviewing our charter, publications, and other documented activities of the working groups.

COMMUNICATIONS METHODS

Infrastructure & Resource Requirements

The working group will be composed of CSA volunteers; it will have co-chairs and/or committee(s). The working group will require standard project management, online workspace and technical writing assistance.

Work Group Conference Calls and In-person Meetings

The working group will hold conference calls no less than quarterly. Attendance or participation in the online workspace by the Principal or Alternate is required. The Alternate must have full authority to act on behalf of the Principal if the Principal is absent. In-person meetings will happen in a location to be determined.

DECISION-MAKING PROCEDURES

A. Definition of a majority

1. A majority shall consist of more than half of the members present and voting.
2. In computing a majority, members abstaining shall not be taken into account.
3. In case of a tie, a proposal or amendment shall be considered rejected.
4. For the purpose under this Charter, a "member present and voting" shall be a member voting "for" or "against" a proposal, including proxy representative.
5. Proxy where authority is delegated through a written statement or non-repudiated email should be declared and inspected for validity by the working group leadership before voting starts.

B. Abstentions of more than fifty percent

1. When the number of abstentions exceeds half the number of votes cast (for votes, plus against votes, plus abstention votes), consideration of the matter under discussion shall be postponed to a later meeting, at which time abstentions shall not be taken into further account.

C. Voting procedures

1) The voting procedures are as follows:
    a) By a show of hands as a general rule, unless a secret ballot has been requested; if at least two members, present and entitled to vote, so request before the beginning of the vote and if a secret ballot under b) has not been requested, or if the procedure under a) shows no clear majority;
    b) By a secret ballot, if at least five of the members present and entitled to vote so request before the beginning of the vote (online voting is applicable)
2) The Chair(s) shall, before commencing a vote, observe any request as to the manner in which the voting shall be conducted, and then shall formally announce the voting procedure to be applied and the issue to be submitted to the vote. The Chair(s) shall then declare the beginning of the vote and, when the vote has been taken, shall announce the results.
3) In the case of a secret ballot, the working group leadership shall at once take steps to ensure the secrecy of the vote.

DELIVERABLES/ACTIVITIES

Q1 2019
Publish guidance for ***ICS Cyber Security Management***. This includes consideration for overall ICS security.
Covering the following:

- Digitalization in production sites
- Specifics of ICS threat landscape
- Necessity for implementing measures to maintain ICS security
- Analysis of ICS challenges – Awareness, Organization and Process, Knowledge, Technology
- Practices to build up security enhancement activities
- Risk Management in ICS/OT environments
- Information on common regulatory frameworks
- Security for ICS safety systems

Q1 2020
Publish guidance for ***Practical security controls of ICS security****.* This includes consideration for best practice of implementing controls in production site.
Covering the following:

- Network separation
- Industrial network monitoring
- Device Authentication
- Access control
- Data Encryption
- Portable media device management
- System vulnerability management
- Threat management
- Incident handling
- Patch management
- Data Loss Prevention program
- Supply chain management
- Reference existing common standards/controls
- Develop standards/controls specific to cloud and IIOT connectivity (IIOT Analytics Hubs, etc.)

Q3 2020
Publish Engage in a charter review, and publish annual report for ICS security trends

DURATION

The working group will operate until Q2 2020 for its chartered deliverables, and at that time consider charter renewal.

Charter Revision History

Initial draft	May 2018
Open peer review	25 May – 25 June 2018
Charter finalized and released	7 August 2018