Industrial Cybersecurity Knowledge Survey Results Analysis

Sean McBride, Carl Shuett, Sami ElMurr, Heidi Cook

Table of Contents

Table of Contents

Table of Contents

Introduction

Recognizing a lack of widely accepted curricular guidance for industrial cybersecurity, Idaho State University, and Idaho National Laboratory set out to identify the knowledge an industrial cybersecurity professional would need that he or she would not get from a traditional information technology, computer science, or cybersecurity program of study.

In January 2020 Idaho State University (ISU) and a group of 14 industrial cybersecurity subject matter experts from the Idaho National Laboratory (INL) engaged in a nominal group technique session to create a list of industrial control systems and industrial cybersecurity knowledge topics. The results of that session formed a strawman curricular guidance document.

The INL, ISU, and the International Society of Automation (ISA), sought to refine and improve the strawman curricular document through an online survey administered to a broader group of practitioners and experts.

The online survey was administered between November 2021 and March 2022. It was advertised primarily through presentations made to the Industrial Cybersecurity Workforce Development Community of Practice (ICSCOP), and the International Society of Automation Global Cybersecurity Alliance (ISA GCA).

The survey included a total of 363 possible inputs (some inputs were only displayed if the respondent answered in a certain way) divided into three sections:

- Respondent Background – 19 possible inputs
- Foundational Industrial Control Systems Knowledge – 205 possible inputs
- Industrial Cybersecurity Knowledge – 139 possible inputs

As seen in the table below, the survey had 170 total respondents, 96 of which (56%) answered at least one question in Section II. We refer to this group of respondents as "Contributors." They spent an average of 49 minutes on the survey.

Respondents	**Number**
Total	170
Contributors (answered at least one question in Section II)	96
Section II Finishers	70
Section III Finishers	65
Writers (provided textual input)	58

The remainder of this document provides basic analysis of the responses provided by Contributors.

Table of Contents

Section I – Contributor Background

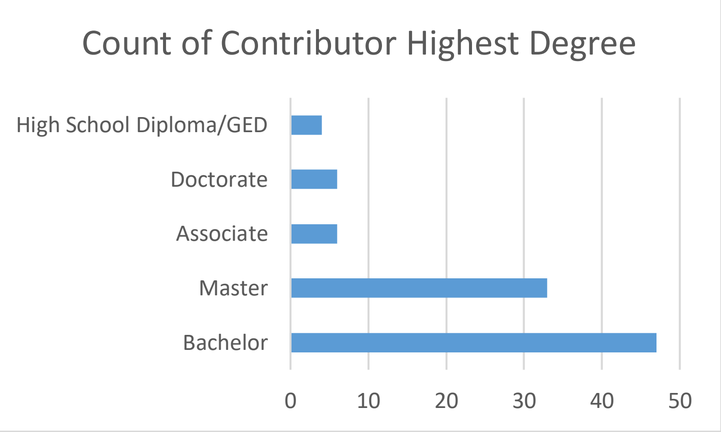
Analysis by Sami ElMurr of NNN, Heidi Cook of the International Society of Automation, and Sean McBride of Idaho State University and Idaho National Laboratory.

The original spreadsheets for this analysis can be found here.

Question I-1

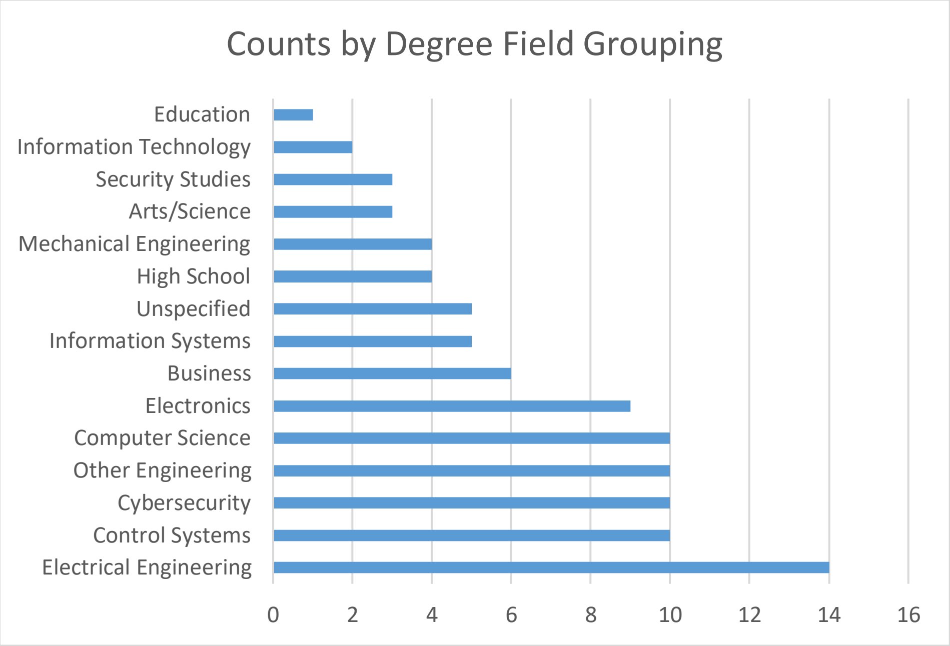
Question I-1 asked respondents to identify their highest formal degree. Nearly half of the contributors selected Bachelor, and about one third selected Master.

Highest Degree	Count of I-1/8	Percent
Bachelor	47	49%
Master	33	34%
Associate	6	6%
Doctorate	6	6%
High School Diploma/GED	4	4%
Grand Total	**96**	**100%**



Question I-2

Question I-2 asked respondents to name the field of their highest degree. Contributor responses were grouped into 15 distinct categories.



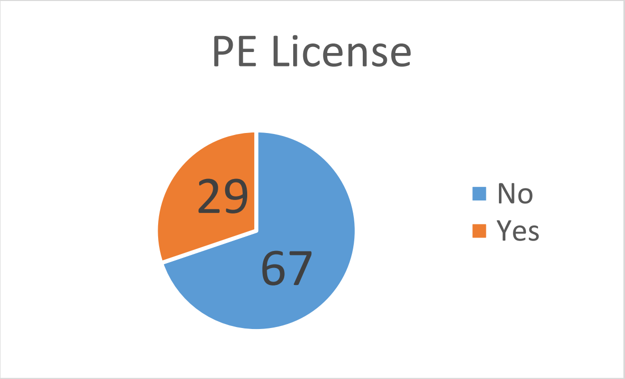
Row Labels	Count of Degree Grouping	Percent
Electrical Engineering	14	14.58%
Control Systems	10	10.42%
Cybersecurity	10	10.42%
Other Engineering	10	10.42%
Computer Science	10	10.42%
Electronics	9	9.38%
Business	6	6.25%
Information Systems	5	5.21%
Unspecified	5	5.21%
High School	4	4.17%
Mechanical Engineering	4	4.17%
Arts/Science	3	3.13%
Security Studies	3	3.13%
Information Technology	2	2.08%
Education	1	1.04%
Grand Total	**96**	**100.00%**

Table of Contents

Question I-3

Question I-3 asked respondents whether they held a professional engineer (PE) license. Those who did were asked to identify their field of specialty (if any).

PE License?	Count
No	67
Yes	29
Grand Total	**96**



Of those indicating they had a PE license, nearly 79 percent indicated they specialized in control systems

PE Specialty by Responses	Count	Percent of Respondents
Control Systems	23	79.31%
Electrical	10	34.48%
Industrial	6	20.69%
Other	5	17.24%
Mechanical	4	13.79%
Chemical	3	10.34%
Civil	1	3.45%

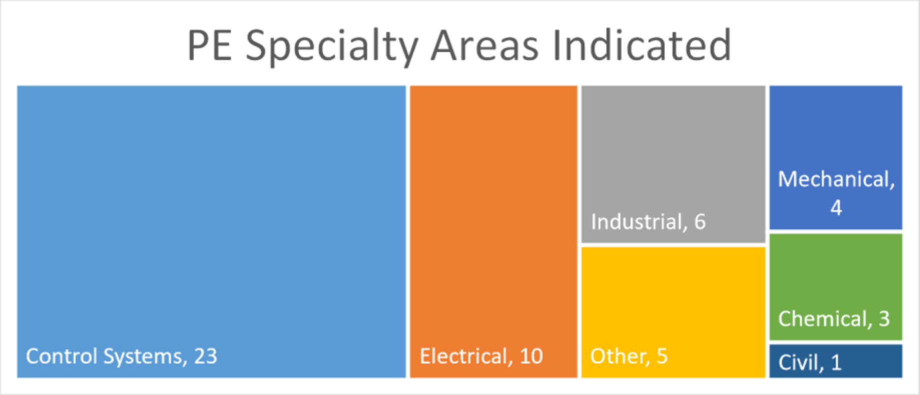
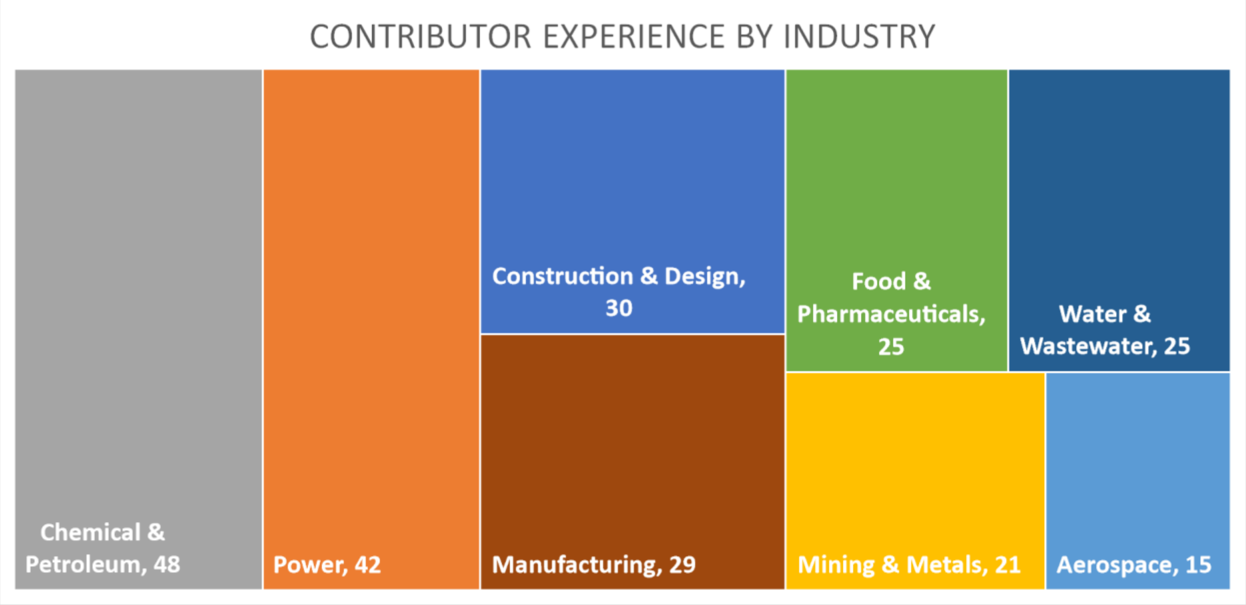


Table of Contents

Question I-4

Questions I-4 asked students to describe their professional experience in various industries. The industries roughly match the International Society of Automation division areas. Fifty percent of contributors reported experience in Chemical & Petroleum industry. Forty-four percent reported experience in the Power industry.

Industry	Count	Percent of Contributors
Aerospace	15	16%
Power	42	44%
Chemical & Petroleum	48	50%
Mining & Metals	21	22%
Construction & Design	30	31%
Food & Pharmaceuticals	25	26%
Water & Wastewater	25	26%
Manufacturing	29	30%



Question I-5

Questions I-5 asked respondents to describe the number of years spent in ICS organization roles. Respondents had spent a cumulative total of 543 years working for asset owners, and 532 years for ICS integration providers.

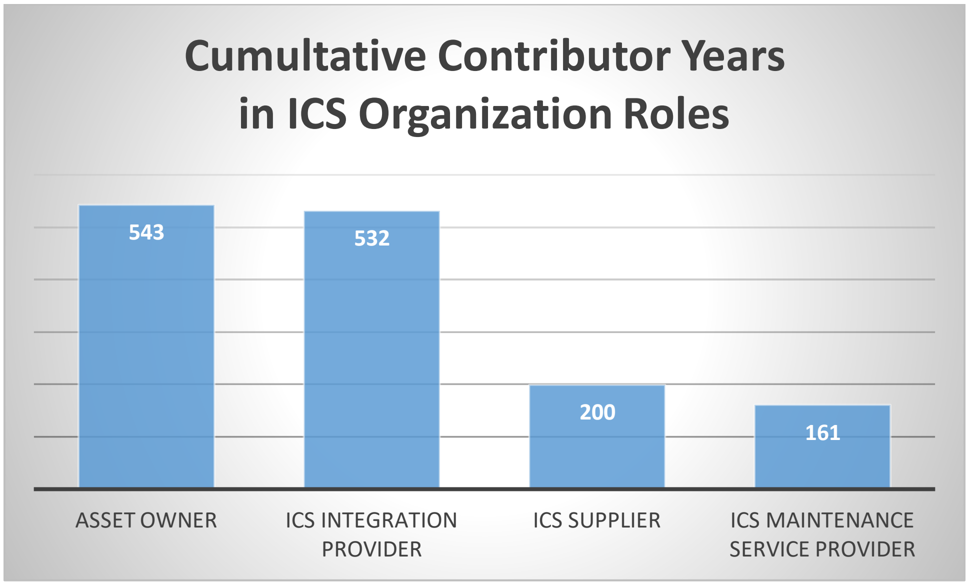
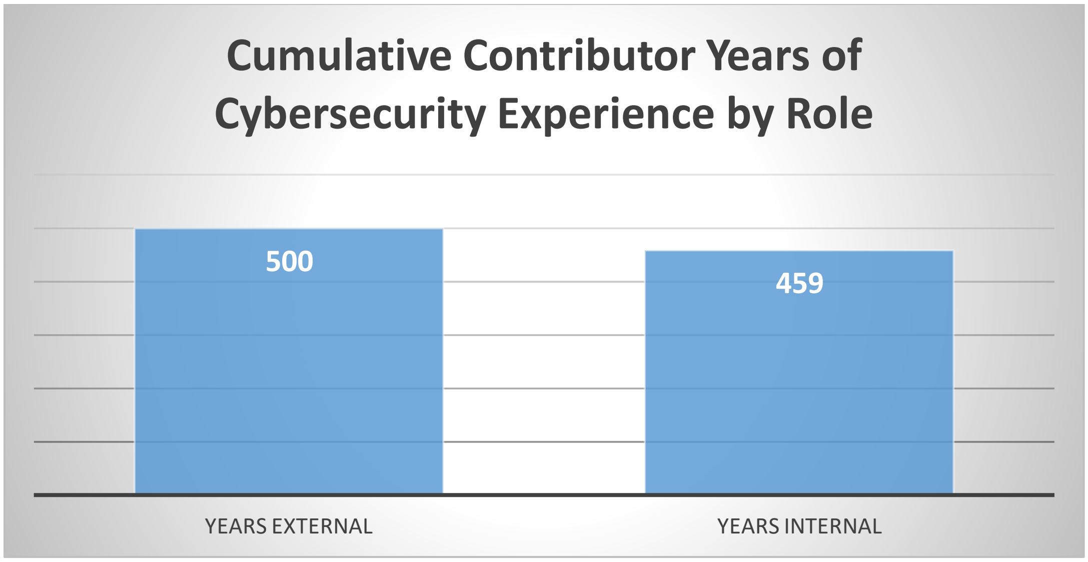


Table of Contents

Question I-6
Question I-6 asked respondents to characterize the years they had spent working in the cybersecurity field. Contributors reported a cumulative total of 959 years in cybersecurity. These years were broken down by 1) Internal vs external role; 2) employer type; and 3) Control systems vs IT focus.

Contributors reported a nearly even distribution of experience working in internal vs external service provider roles.



Contributors reported vastly more experience working in for-profit organizations than for government, non-profit, or academia.

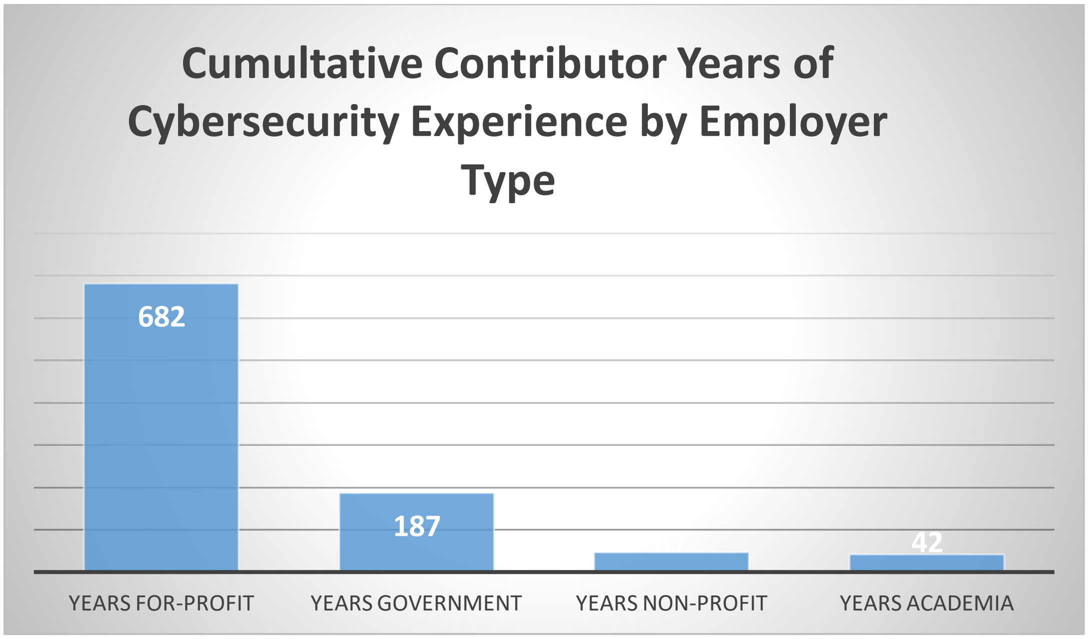


Table of Contents

Contributors also reported nearly three times as many years working on industrial control systems cybersecurity than IT cybersecurity.

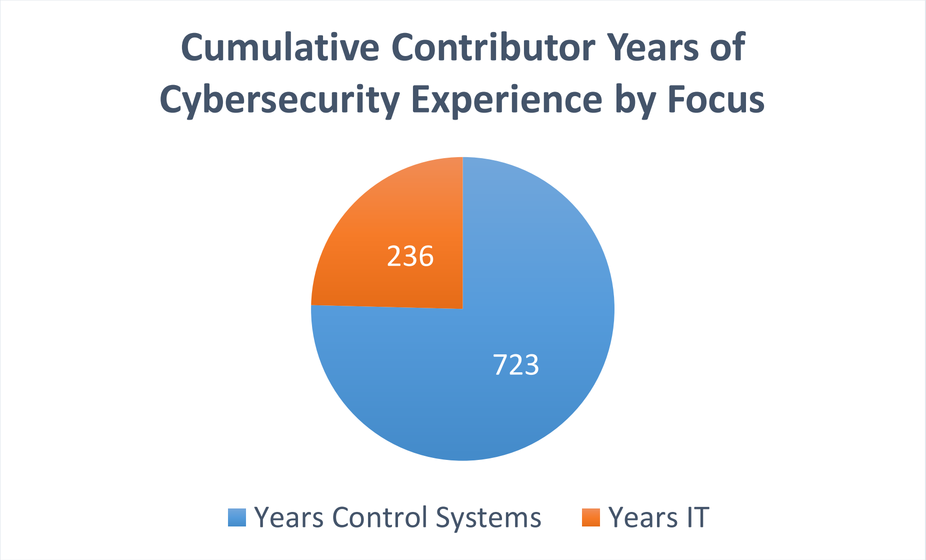
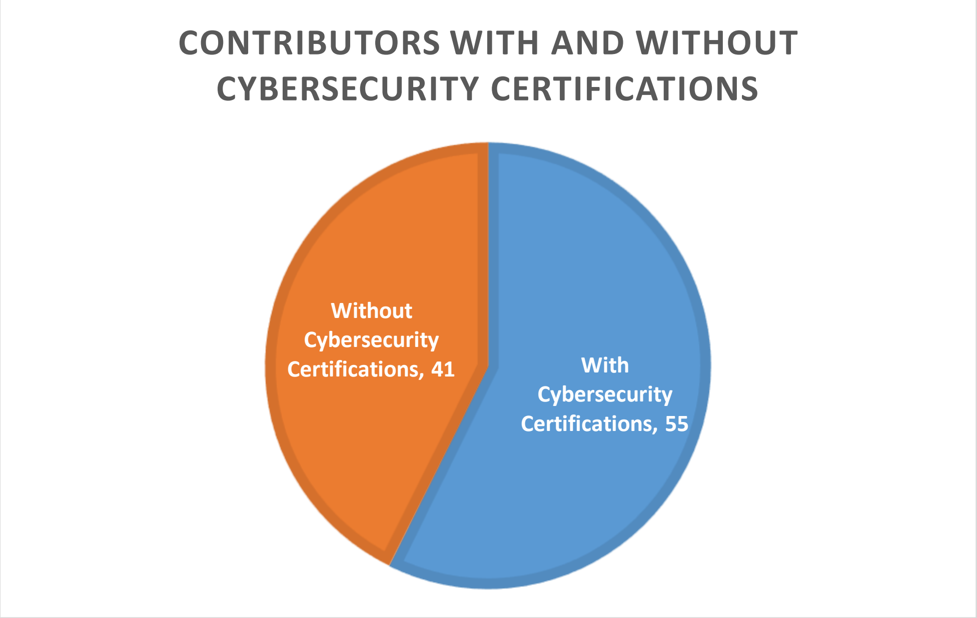


Table of Contents

Question I-7
Question I-7 asked respondents to identify the cybersecurity, industrial cybersecurity, and industrial automation certifications they held.

Fifty-five Contributors listed cybersecurity or industrial cybersecurity certifications, 41 did not



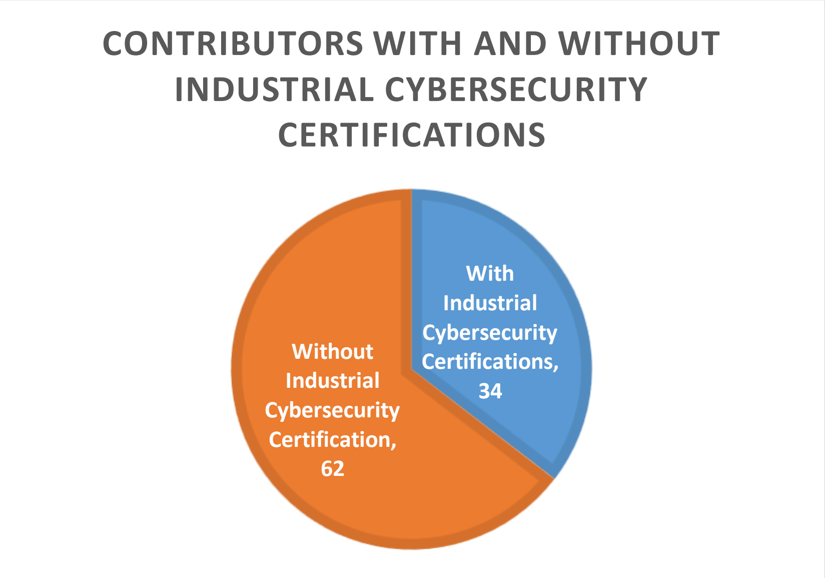
Contributors reported 132 total cybersecurity and industrial cybersecurity certifications. The Certified Information Systems Security Professional (CISSP) and Global Industrial Cyber Security Professional (GICSP) were the most commonly held credentials.

Cert	Count
CISSP	23
GICSP	19
Security+	17
62443 Fundamentals Specialist	13
62443 Risk Assessment Specialist	8
62443 Design Specialist	6
62443 Maintenance Specialist	6
ISO27001	4
CCNA-Security	3
CISA	3
GRID	3
ISACA CISM	3
SABSA	3
SSCP	2
CCSP	2

Table of Contents

CEH	2
CAP	1
CCISO	1
CCSK	1
CFSP	1
CHFI	1
CompTIA CASP	1
Cyber Defense Focus Certification	1
CySA+	1
Digital Forensics Focus Certification	1
ESCA	1
GCIP	1
ISACA CDPSE	1
Offensive Operations Focus Certification	1
OSCP	1
TUV Cysec Specialist	1
Total Cybersecurity Certifications Reported	**132**

Thirty-four of the 96 contributors reported holding industrial cybersecurity certifications.



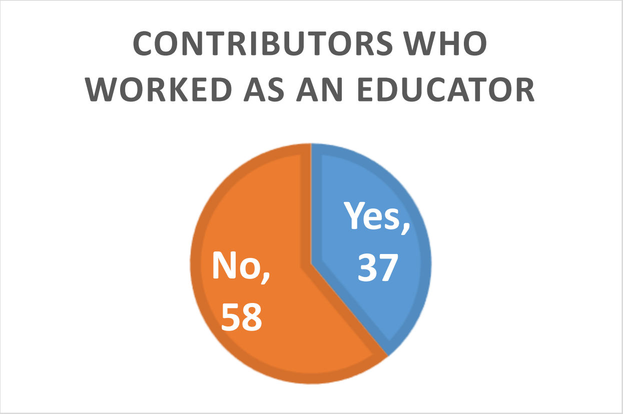
Twelve of the 96 Contributors reported holding non-cybersecurity industrial automation certifications.

Category	Count
Contributors with non-cybersecurity Industrial Automation Certs	12
Contributors without non-cybersecurity Industrial Automation Certs	84

Table of Contents

Question I-8

Question I-8 asked respondents to describe their experience working as an educator.
37 of the 95 Contributors who responded to this question had not worked as an educator.



Contributors reported a cumulative total of 13 years teaching cybersecurity. They reported that 8.8 of those years were dedicated to teaching industrial cybersecurity.

Total years teaching IT cybersecurity	Total years teaching industrial cybersecurity	Total years teaching other cybersecurity
1.7625	8.8125	2.875

Section II – Foundational Industrial Control Systems Knowledge

Analysis by Sean McBride of Idaho National Laboratory and Idaho State University.

Original spreadsheets for this analysis can be found here.

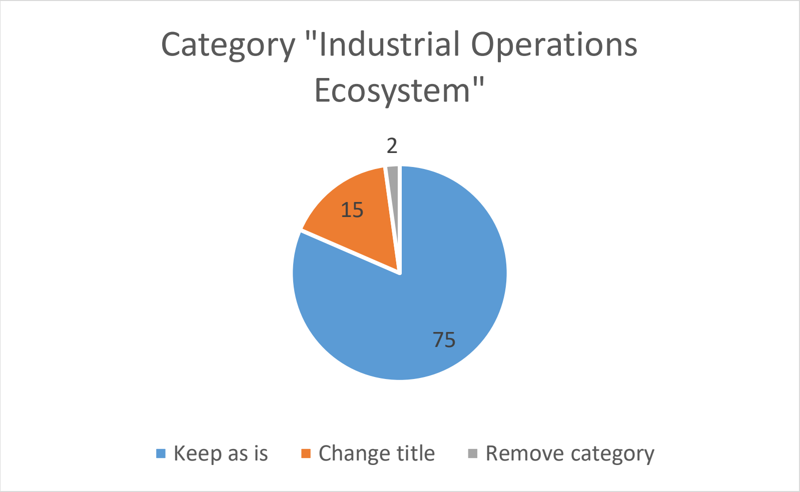
Question II-2

Question II-2 dealt with five proposed ICS knowledge categories:

- Industrial Operations Ecosystem
- Instrumentation and Control
- Equipment Under Control
- Industrial Communications
- Safety

For each category title, recommend whether to: keep as is, change, or remove entirely.
If you recommend to change the title, you will be asked to suggest a new title in a follow-up question.
If you recommend to remove the title, you will be asked to enter a brief explanation.

II-2_1 Industrial Operations Ecosystem



Response	Count	Percent
Keep as is	75	81.5%
Change title	15	16.3%
Remove category	2	2.2%
Total	92	100.0%

Suggestions for "Change title"

Respondent ID	Response content
R_2YX5Hjj1Z8JitHY	Industrial Operations and the Enterprise: the risks

Table of Contents

R_26hX0Es8WVUZ3i0	Industrial Operations Administration
R_3esDNNOgJnH5tM1	
R_3lMl6Hi3p0cr1K4	Industrial Control Systems Environments
R_1rGFDHuFhnB2AQB	The definition is too broad. You have included people and engineering designs as synonamous. . Our profession and this subset of the automation profession want to play a game of very precise language but then wants large public acceptance. The two can't work together. I think this catagory needs to be split into the People (profession, organizations, certifications, etc) part and the products the people create (Designs, specifications, etc))
R_2WHW03nONpmCTMk	Control System Administration and Interfacing
R_vZYehSwKucwaIcF	Business and industrial operations ecosystem
R_3MQjCEJ5fsIuCBG	Industrial Operations/Process
R_1eUD8SM0184KR6B	
R_1C7kv6fnDsy5HUO	Industrial Operations, Projects & Environment
R_1ozQprcw4UVW9AU	NA
R_pbAInmS3zy7lwhb	Documentation and Lifecycle Management
R_21onh8CfZn5Ywhn	Industrial Automation Security governance and compliance management.
R_1NDgRhbaLUQhIEx	Operational Technology Management
R_2aRo3qs2LIv8otL	

Reasoning for “Remove”

R_1HduUVDzYT3QuFp	Not specific enough
R_3nTrmSy2ZCbkjrb	

Analysis

Reviewing the responses for “Industrial Operations Ecosystem” shows several concerns with the diversity of the category.

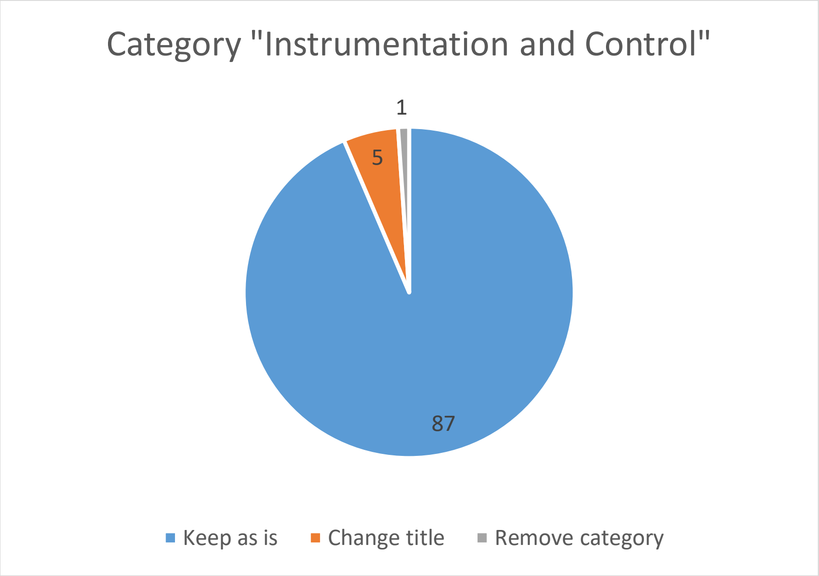
There seems to be concern with both the category (industrial operations) and the descriptor (ecosystem).

- Six suggestions included the term “industrial”
- Three included the phrase “industrial operations”
- “Industrial automation” was included once
- “Operational technology” was included once
- Two included “environment” – seemingly in preference over “ecosystem”
- Three included “management”
- “Business”, “interfacing”, and “enterprise” were also advanced once each.

Table of Contents

Table of Contents

II-2_2 Instrumentation and Control



Response	**Count**	**Percent**
Keep as is	87	93.5%
Change title	5	5.4%
Remove category	1	1.1%
Total	93	100.0%

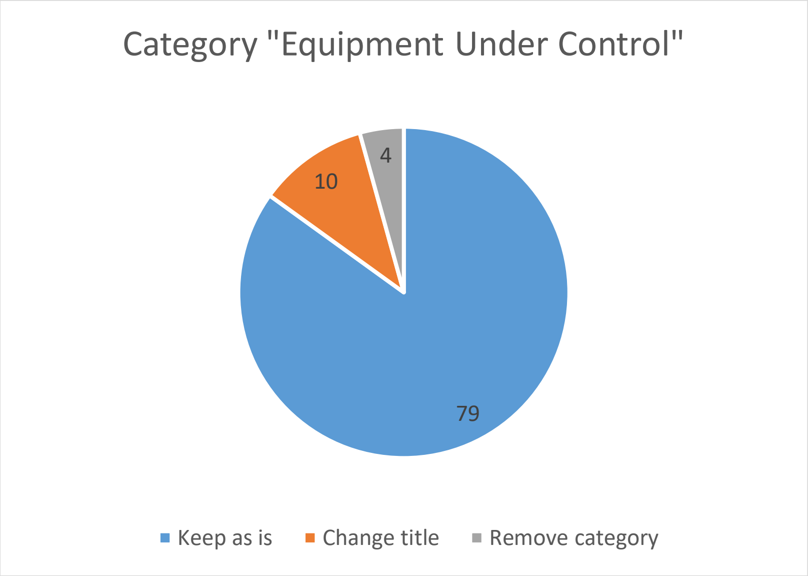
Suggestions for "Change title"

Respondent ID	**Response content**
R_1rGFDHuFhnB2AQB	Follow the INCOSE definitions of Systems.
R_21onh8CfZn5Ywhn	Industrial Automation and Control Systems
R_VJBb9QiRZiR3xC1	SCADA, Instrumentation & Control
R_10UDV2BKZ2prJG2	Split into two: (1) Computer Science of Embedded Systems and (2) Instrumentation and Control
R_UfkYybej4RRfKRH	Industrial Automation and Control System

Reasoning for "Remove category"

R_3esDNNOgJnH5tM1

II-2_3 Equipment Under Control



Response	Count	Percent
Keep as is	79	84.9%
Change title	10	10.8%
Remove category	4	4.3%
Total	93	100.0%

Suggestions for “Change title”

Respondent ID	Response content
R_26hX0Es8WVUZ3i0	Not a change, but I'd move VFDs into the same catagory as controllers
R_3MQjCEJ5fsIuCBG	Equipment and Machinery
R_1eUD8SM0184KR6B	
R_pbAInmS3zy7lwhb	End Devices
R_2aRo3qs2LIv8otL	
R_2Su9412OXG578E9	Equipment Functional Control
R_z2mjyxCfek8q3lv	Assets under control
R_3EaM9vGMjuCCcuf	
R_UfkYybej4RRfKRH	Process under control
R_3CAZq03xeRuPvRk	

Reasoning for “Remove”

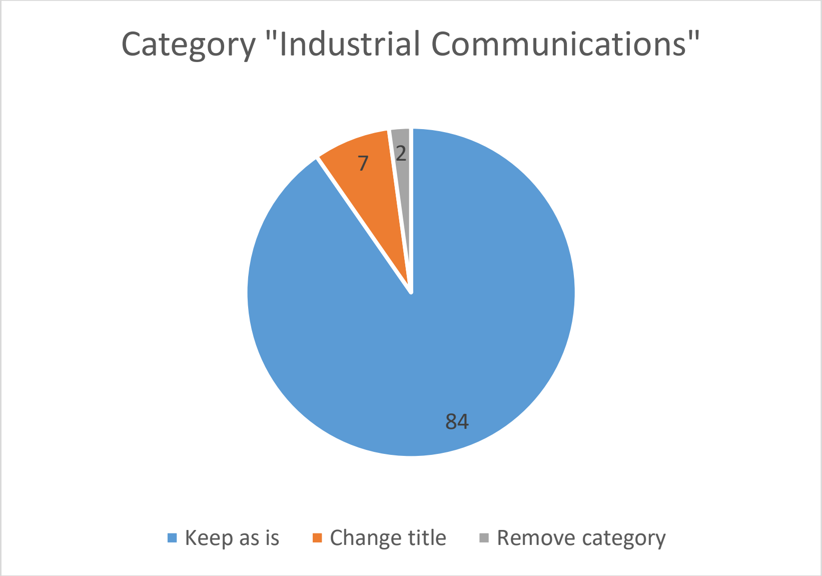
R_3esDNNOgJnH5tM1	
R_1rGFDHuFhnB2AQB	The definition is flawed. Are you controlling the Pump or controlling the VFD which controls the Pump. It can't be both.

Table of Contents

	Again, we have definitions for this already. Let's use them. It should be called the Process.
R_2AX45Pxy89BCTuf	This should be incorporated between the Communications and Instrumentation and Control catagory, for a more total look at communication methodology and machine control, respectively.
R_3nTrmSy2ZCbkjrb	

Table of Contents

II-2_4 Industrial Communications



Response	**Count**	**Percent**
Keep as is	84	90.3%
Change title	7	7.5%
Remove category	2	2.2%
Total	93	100.0%

Suggestions for “Change title”

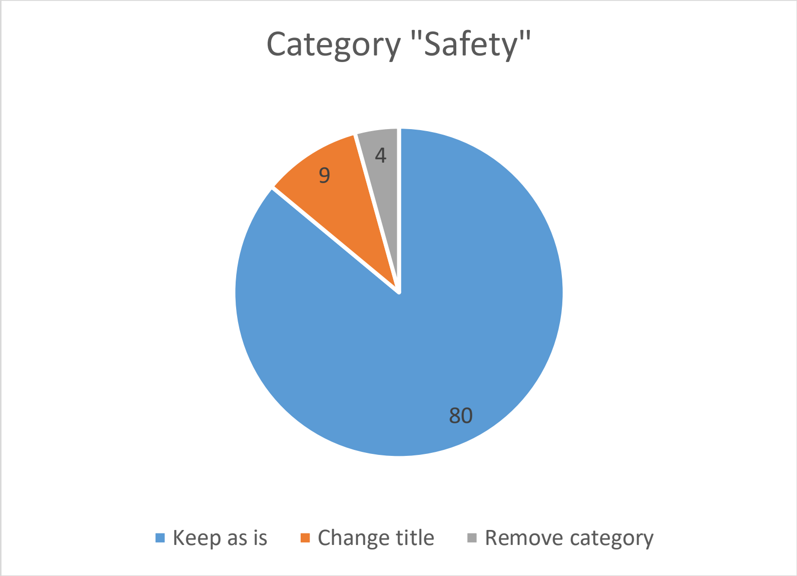
R_3esDNNOgJnH5tM1	
R_1rGFDHuFhnB2AQB	need to drop this concept of Industrial. What does that mean anyway? THis should adopt the accetped terms of Operational Tech Communications. Or just plain Communications as what "ICS" platform is not using ethernet which is not a solely industrial communication protocol. Let's stop trying to be different than IT and accept that we need to partner with them and move our protocols into a general Communications.
R_3MQjCEJ5fsIuCBG	Industrial Protocols and Communications
R_1ozQprcw4UVW9AU	NA
R_21onh8CfZn5Ywhn	Networking and communications for IACS.
R_3EaM9vGMjuCCcuf	
R_UfkYybej4RRfKRH	IACS Network

Reasoning for “Remove”

R_1HduUVDzYT3QuFp	IoT is blending into industrial
R_3nTrmSy2ZCbkjrb	

Table of Contents

II-2_5 Safety



Response	**Count**	**Percent**
Keep as is	80	86.0%
Change title	9	9.7%
Remove category	4	4.3%
Total	93	100.0%

Suggestions for “Change title”

R_2YX5Hjj1Z8JitHY	Safety: Secured, why it is not "IT"
R_1rGFDHuFhnB2AQB	This is too broad. Safety Instrumented System is just a system with more complex instruments and controllers. Why is it in its own catagory over just being a subset in Control and Instrumentation? You can't group Personell Safety (OSHA) in with equipment safety (pressure relief valves) they are two very different skills sets. And what of Envirnomental Safety? Again, you are very precise in other language and then you try to paint this giant brush stroke in a catch all category. Separate it into it individual sub category or lump put them into the areas previously listed.
R_vZYehSwKucwalcF	? something a bit less generic that makes one think about safety as a lifecycle criteria rather than an individual
R_1ozQprcw4UVW9AU	Critical loops/systems
R_1NDgRhbaLUQhIEx	keep title, but description is missing Functional Safety
R_2YsHBQvCLvWLRjo	Need to further define if this is equipment / process / physical / life safety. Its not descriptive enough on the specific focus of the category
R_XTVNiQSzyaZNSzn	Safety fine, would add Functional Safety (ISA84, IEC 61508/61511 field)

Reasoning for “Remove”

Table of Contents

R_3esDNNOgJnH5tM1	
R_pbAInmS3zy7lwhb	It seems less relevant and dilutes the focus for this particular discussion
R_XzBpdAcbe7EVaa5	
R_3nTrmSy2ZCbkjrb	

Table of Contents

II-2 Overall

	Response		
Category	*Keep as is*	*Change title*	*Remove*
Instrumentation and Control	87	5	1
Industrial Communications	84	7	2
Safety	80	9	4
Equipment Under Control	79	10	4
Industrial Operations Ecosystem	75	15	2

Looking across the categories, “Instrumentation and Control” was most chosen for “Keep as is”, while “Industrial Operations Ecosystem” was least chosen.

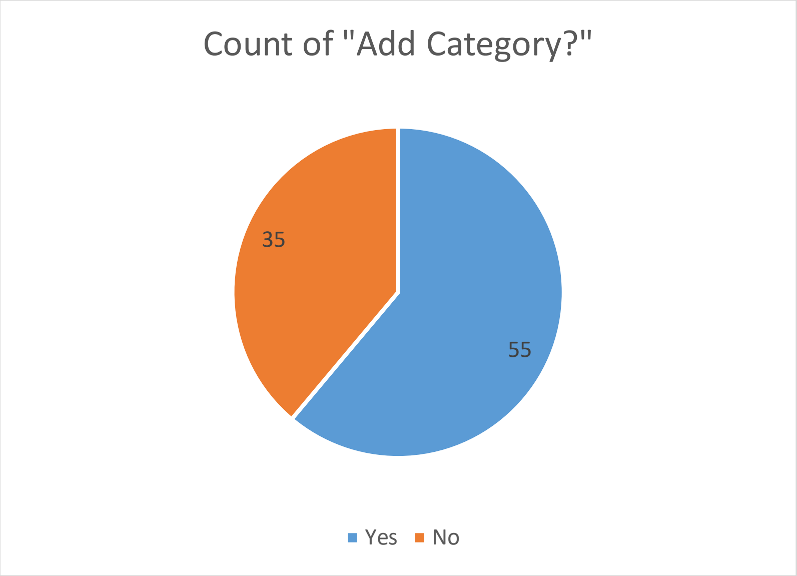
“Safety” and “Equipment Under Control” were equally most chosen for “Remove”.

Question II-3

Question II-3 dealt with adding additional categories

II-3

“Would you recommend adding additional categories of Foundational ICS knowledge to which traditional IT, computer science, or cybersecurity students/professionals are not normally exposed?”



Response	Count	Percent
Yes	55	61.1%
No	35	38.9%
Total	90	100.0%

II-3a Suggested Category to Add

R_2YX5Hjj1Z8JitHY	Control Systems theory and practice, Control System Risk, Control System Functions, Instrumentation theory, Control system roles
R_2YsHBQvCLvWLRjo	integration with IT, cloud and edge technologies, risk management,
R_1l72Afnm6478fXP	Operational Availability
R_26hX0Es8WVUZ3i0	Move the procedures from Safety into the Ecosystem topic.
R_2Squ4P2NtTznJ4a	Cyber-Physical Systems
R_RqVMBWhBtfTdYrf	PLC secure coding practices
R_38nm6wLeA6p5nLb	IIoT
R_3lMl6Hi3p0cr1K4	
R_2Su9412OXG578E9	Configuration Management
R_1BxKzD0XM4g0jcZ	Access.
R_336XnflxyqB4ir6	Nist Framework Experience
R_3kMMhb0mj6S80wG	OT Security Operations Center (SOC)

Table of Contents

R_1HduUVDzYT3QuFp	Industrial Data Communication
R_1rGFDHuFhnB2AQB	Environmental Safety, Personnel Safety,
R_1Cyk2xvhANWeilI	
R_2WHW03nONpmCTMk	Remote Connections and Cloud Cybersecurity
R_3njf722UBVndAP8	Maintenance
R_XTVNiQSzyaZNSzn	
R_3eqX8pib0BYlC2z	Cybersecurity for power systems
R_28HRVFlTwpY1Y9m	Physics for the Cybersecurity Professional, Compare and Contrast Perdue Reference and OSI Models and Why, A 2-3 Course block on Basic Industrial Equipment Used across Commerical, Institutional, Heavy Industries, Marine/Transportation and Energy Industry Sectors, What is a Data Diode and Where Can It Be Ineffectively or Effectively Applied - and why, At each course in the A.S. or B.S. curriculum include some form of discussion about cybersecurity as an orientation to - or facet of - the "quality" of their technical/technology education
R_3CZvA7p1ny9D7Su	Hardware Reverse Engineering
R_3MQjCEJ5fsIuCBG	Industrial Control Systems
R_41siJvbhXtEUFmp	Secure Coding practice
R_1n87BSaF6YgOCbm	Risk management frameworks
R_3R9FXVwJeSQbdCH	Cybersecurity in operations is physic risk
R_Qh4JJ9Sl3FTmiWZ	Wireless communication (cell phones 5g), emergency management systems/services (what if these were hacked),
R_1NksqgCl7Akb5rm	
R_274qf7ZvI8Uo4YW	Something around mechanical engineering controls that a person who is less familiar with engineering in the physical work would benefit from.
R_3L11jmMH3DJ4ha8	Informal ICS Exposure, i.e. HMI user or maintenance technician.
R_x65cwLz09tf5P0Z	
R_3PHz5Hw4MGOxWNK	Communications, Networking
R_12l0CIht5vgY902	Use of AI in Cybersecurity
R_3CISd6mModucet0	Industrial Automation and Control Systems
R_1eqr6le0DY5qvYg	Understand Industries constraints, Adaptation to Industrial world
R_1C7kv6fnDsy5HUO	Professional Ethics
R_2y7OAWWVwHpdUnP	Industrial Safety, Process Control Theory
R_3Pc1V6PF3wO56q2	
R_1JLVvwwpCaXn84N	Control Systems Cybersecurity
R_3EKGwQYaHhLTi4H	Software Design and Integration from the purview of Industrial Cybersecurity
R_3EaM9vGMjuCCcuf	Risk Analysis
R_2AX45Pxy89BCTuf	Industrial Communications Systems
R_XzBpdAcbe7EVaa5	
R_1PT2NuDukXD5IH3	Industrial IT, Web Security
R_2uOoUsoZNgrVOVi	Running a production facility with control systems
R_10UDV2BKZ2prJG2	Computer Science of Embedded Systems

Table of Contents

R_1ozQprcw4UVW9AU
R_1MPQ2QhyNfNcAV3
R_21onh8CfZn5Ywhn
R_241sHjNVIdRaCW1
R_1JUYV5E3P6NzgbE
R_UfkYybej4RRfKRH
R_1NDgRhbaLUQhIEx
R_2aRo3qs2LIv8otL
R_2ebeSEVBFoDIHDj
R_31LwtZXJfcVIB8C

Of the 55 respondents who chose “Yes” add a category, 38 suggested a new category name.

A review of the suggestions shows that it is a challenge to identify what should be a category versus what should fit into a category.

Responses that deal specifically with cybersecurity appear to have not recognized that section III of the survey would deal with those items.

The review also indicates that respondents could have approached the question assuming that the student already had an IT background or already had an industrial operations background. The survey intended to ask the question from the perspective of a student who lacked the industrial operations background.

Responses may also indicate that terms that are commonly used in a traditional cybersecurity course have different implications in and industrial environment.

Several of the responses could reasonable be grouped into a category called “Integration with IT” or similar

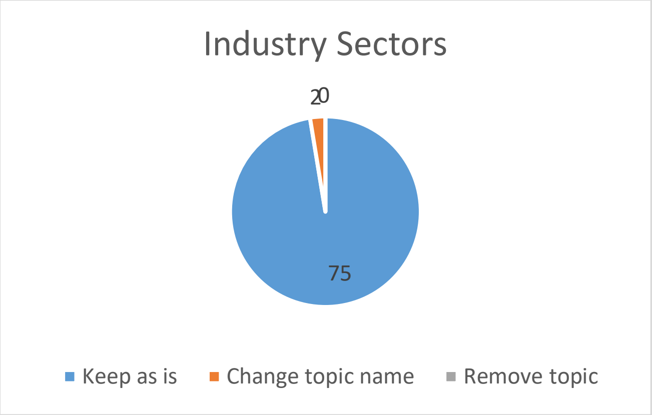
Table of Contents

Question II-5 to II-6 Topics in "Industrial Operations Ecosystem"

Questions II-5, and II-6 deal with the topics of the proposed category "Industrial Operations Ecosystem", which are: industry sectors, professional roles and responsibilities in industrial environments, organizational roles, facilities, engineering diagrams, process types, industrial life-cycles

II-5_1 Industry Sectors

Question II-5_1 asked participants whether to Keep as is, Change, or Remove the topic "Industry Sectors". If participants chose "Change" they were asked to provide a suggestion. If they chose "Remove" they were asked to explain why.



Response	Count	Percent
Keep as is	75	97.4%
Change topic name	2	2.6%
Remove	0	0.0%
Total	77	100.0%

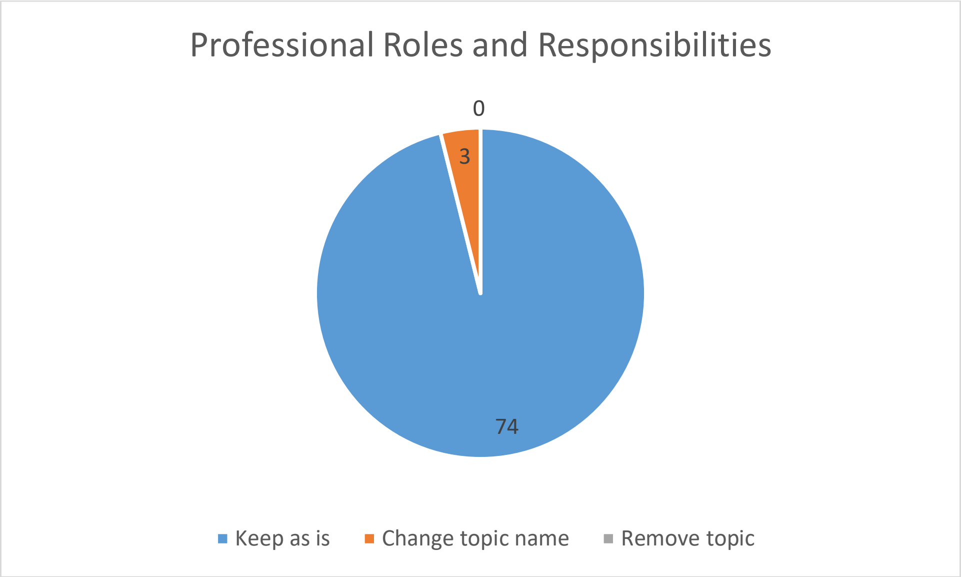
Suggestions for "Change"

R_1rGFDHuFhnB2AQB	Why is this relevant today?
R_12l0CIht5vgY902	industry fields

Table of Contents

II-5_2 Professional Roles and Responsibilities

Question II-5_2 asked participants whether to Keep as is, Change, or Remove the topic “Professional Roles and Responsibilities”. If participants chose “Change” they were asked to provide a suggestion. If they chose “Remove” they were asked to explain why.



Response	Count	Percent
Keep as is	74	96.1%
Change topic name	3	3.9%
Remove	0	0.0%
Total	77	100.0%

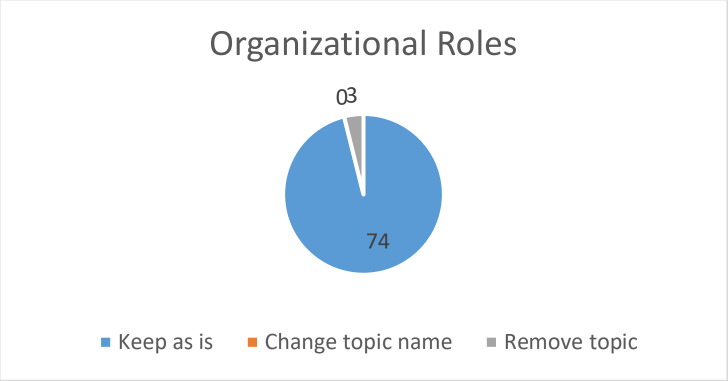
Suggestions for “Change topic name”

R_1rGFDHuFhnB2AQB	Professional roles and Responsibilities. remove industrial environments
R_12l0CIht5vgY902	Organizational roles and responsibilities
R_1C7kv6fnDsy5HUO	Professional Ethics & Obligations(should be separate)

Table of Contents

II-5_3 Organizational Roles

Question II-5_3 asked participants whether to Keep as is, Change, or Remove the topic “Organizational Roles”. If participants chose “Change” they were asked to provide a suggestion. If they chose “Remove” they were asked to explain why.



Reasoning for “Remove topic”

R_1rGFDHuFhnB2AQB	it belongs in the group above
R_3MQjCEJ5fsIuCBG	This could be included in the previous category (Profesional Roles)
R_2AX45Pxy89BCTuf	It seems redundant when you already have a topic for Professional Roles and Responsibility

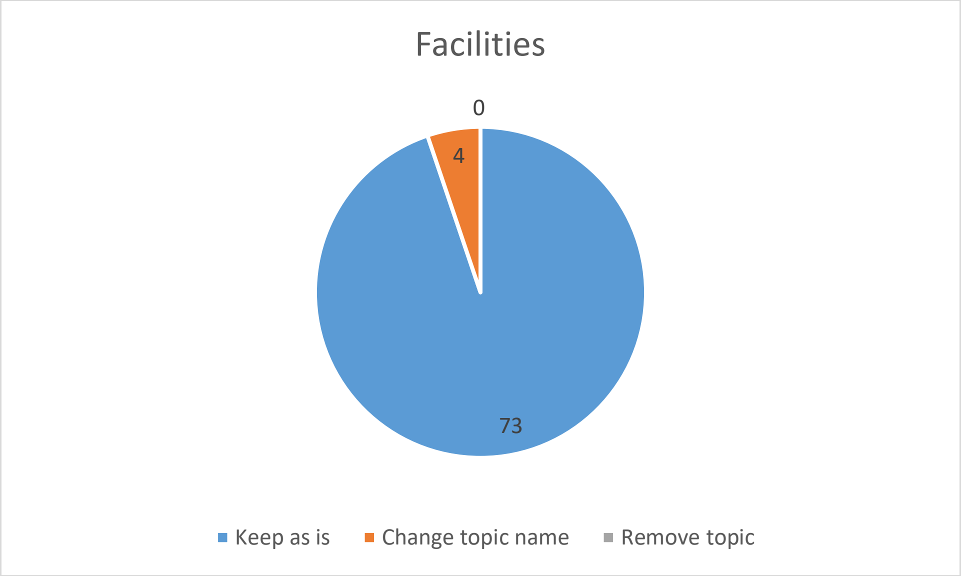
Table of Contents

II-5_4 Facilities

Question II-5_4 asked participants whether to Keep as is, Change, or Remove the topic “Facilities”. If participants chose “Change” they were asked to provide a suggestion. If they chose “Remove” they were asked to explain why.

Note Question II-4_7 was numbered incorrectly. It should have been II-4_4. So, it does correspond to II-5_4 (they are both Facilities) even though the numbering does not match. The fact that II-4_7 was numbered incorrectly means that the following numbering holds

II-4_7 corresponds to II-5_4
II-4_4 corresponds to II-5_5
II-4_5 corresponds to II-5_6
II-4_6 corresponds to II-5_7



Response	Count	Percent
Keep as is	73	94.8%
Change topic name	4	5.2%
Remove topic	0	0.0%
Total	77	100.0%

Suggestions for “Change topic name”

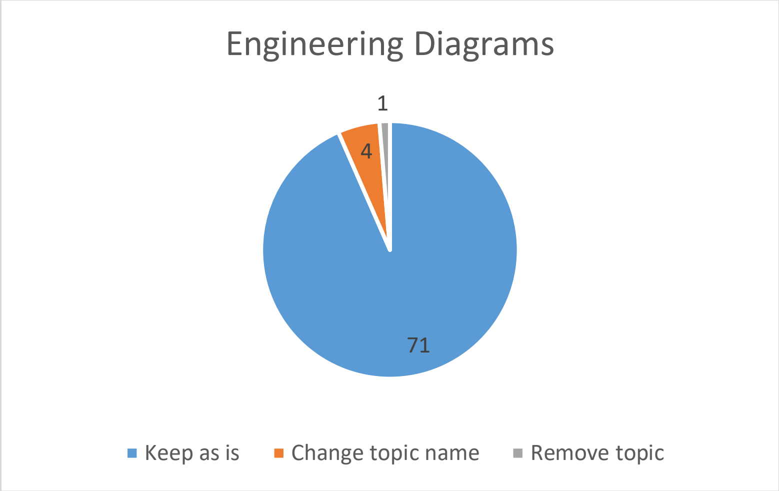
R_1rGFDHuFhnB2AQB	I don't know what this means.
R_2WHW03nONpmCTMk	Control System Architecture
R_27a3HBRQ60cNEsj	Facility Types
R_12l0CIht5vgY902	Types of facilities

Table of Contents

II-5_5 Engineering Diagrams

Question II-5_5 asked participants whether to Keep as is, Change, or Remove the topic “Engineering Diagrams”. If participants chose “Change” they were asked to provide a suggestion. If they chose “Remove” they were asked to explain why.

Note The fact that II-4_7 was numbered incorrectly means that II-4_4 corresponds to II-5_5



Response	Count	Percent
Keep as is	71	93.4%
Change topic name	4	5.3%
Remove topic	1	1.3%
Total	76	100.0%

Suggestions for “Change topic name”

R_1n87BSaF6YgOCbm	Engineering and project document files
R_12l0CIht5vgY902	Engineering Drawings
R_3EKGwQYaHhLTi4H	
R_2AX45Pxy89BCTuf	Professional Engineering Communications

Reasoning for “Remove topic”

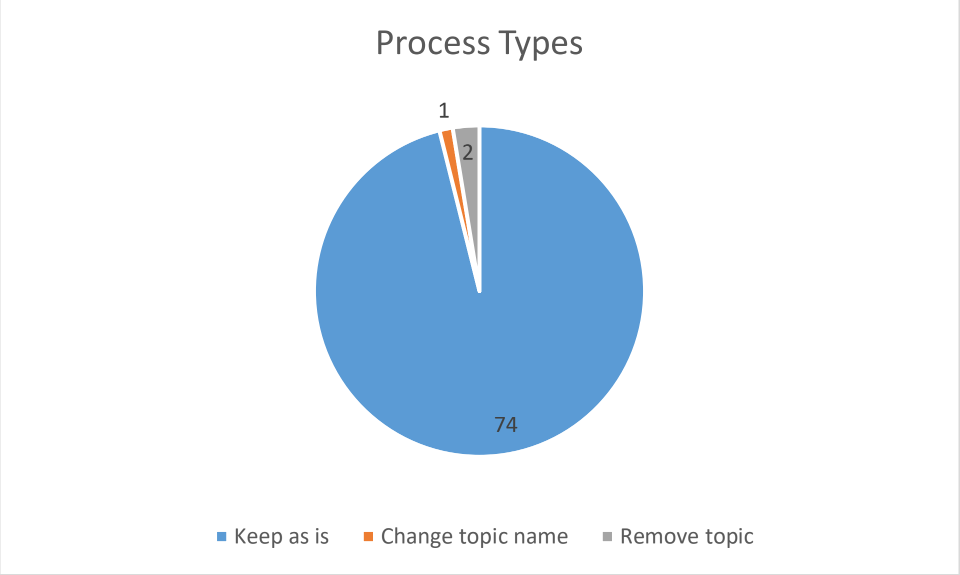
R_1rGFDHuFhnB2AQB	not part of an ecosystem. part of the control system.

Table of Contents

II-5_6 Process Types

Question II-5_6 asked participants whether to Keep as is, Change, or Remove the topic “Process Types”. If participants chose “Change” they were asked to provide a suggestion. If they chose “Remove” they were asked to explain why.

Note The fact that II-4_7 was numbered incorrectly means that II-4_5 corresponds to II-5_6.



Response	Count	Percent
Keep as is	74	96.1%
Change topic name	1	1.3%
Remove topic	2	2.6%
Total	77	100.0%

Suggestions for “Change topic name”

R_2WHW03nONpmCTMk	Continuous and Discrete Industrial Processes

Reasoning for “Remove topic”

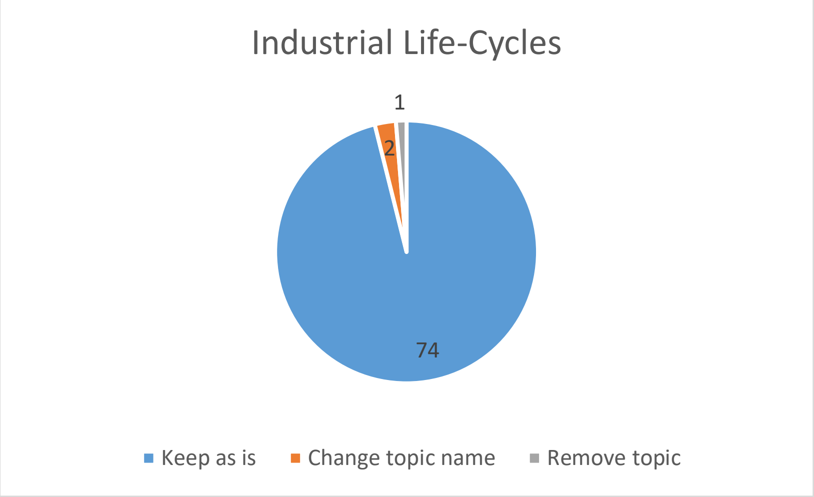
R_1rGFDHuFhnB2AQB	not part of the "ecosystem"
R_3NId6QsP1huq1WV	I think Industrial Sectors is good enough and we don't need to dig into process types.

Table of Contents

II-5_7 Industrial Life-cycles

Question II-5_7 asked participants whether to Keep as is, Change, or Remove the topic “Industrial life-cycles”. If participants chose “Change” they were asked to provide a suggestion. If they chose “Remove” they were asked to explain why.

Note The fact that II-4_7 was numbered incorrectly means that II-4_6 corresponds to II-5_7.



Response	Count	Percent
Keep as is	74	96.1%
Change topic name	2	2.6%
Remove topic	1	1.3%
Total	77	100.0%

Suggestions for “Change topic name”

R_12l0CIht5vgY902	-
R_3EKGwQYaHhLTi4H	

No answers provided

Reasoning for “Remove topic”

R_1rGFDHuFhnB2AQB	not part of the "ecosystem"

Table of Contents

II-5 Topics in Industrial Operations Ecosystem Overall

Topic	Response *Keep as is*	*Change topic name*	*Remove topic*
Industry Sectors	75	2	0
Professional Roles and Responsibilities	74	3	0
Organizational Roles	74	0	3
Process Types	74	2	2
Industrial Life-Cycles	74	2	1
Facilities	73	4	0
Engineering Diagrams	71	4	1

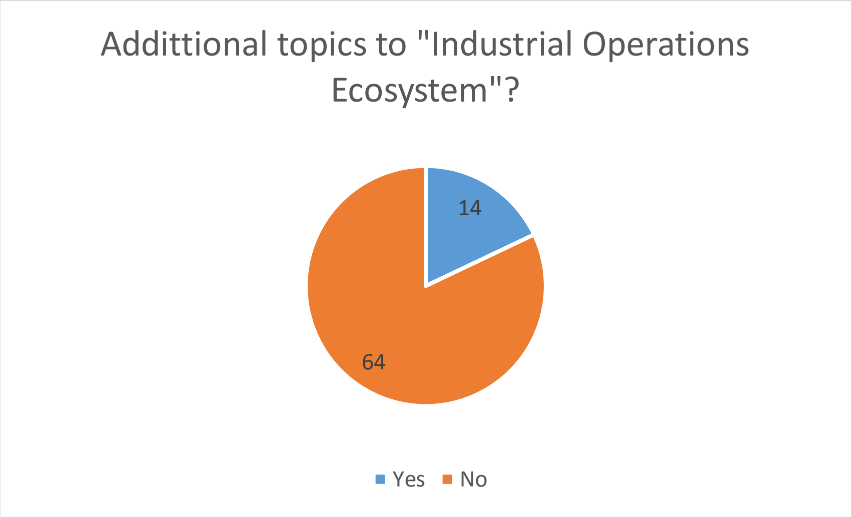
Industry Sectors received the most responses for “Keep as is”. Organizational Roles received the most responses for “Remove topic” – three. Facilities and Engineering Diagrams tied for most responses for “Change topic name” – four each.

The limited “remove topic responses” indicates that the topics are quite sound.

A comparison of the relevance responses with the change responses shows that while industry sectors had the lowest relevance rating, no one suggested removing it.

II-6 Additional topics in “Industrial Operations Ecosystem” Category

Question II-6 asked whether additional topics should be added to the category Industrial Operations Ecosystem



Response	Count	Percent
Yes	14	17.9%
No	64	82.1%
Total	78	100.0%

If participants chose “Yes”, they were prompted to suggest additional topics.
Suggested topics:

ResponseId	II-6a
R_2YX5Hjj1Z8JitHY	Control System Manufacturer: Following Required Security Practices
R_3lMl6Hi3p0cr1K4	
R_336XnflxyqB4ir6	ICS Purposed Cybersecurity Tooling
R_3kMMhb0mj6S80wG	Communication diagrams
R_1HduUVDzYT3QuFp	cloud
R_1rGFDHuFhnB2AQB	it depends on how the rest of this shakes out.
R_XTVNiQSzyaZNSzn	Process Dynamics
R_28HRVFlTwpY1Y9m	Subordinate facilities (e.g. Substations which may or may not have a structure in it), Primary Equipment as a Facility (e.g. ships/boats/trains/aircraft/mining trucks/drones-robotics/spacecraft/etc.),
R_27a3HBRQ60cNEsj	IT/OT Collaboration
R_1C7kv6fnDsy5HUO	Captial Project (Lifecycles)
R_3Pc1V6PF3wO56q2	Threat Landscape
R_3EaM9vGMjuCCcuf	Risk
R_2AX45Pxy89BCTuf	Shared Knowledge in Cyberspace, Shared Resources of Cyber Security

Table of Contents

R_1ozQprcw4UVW9AU

Many of the responses dealt with cybersecurity topics – which were addressed in Section III. We need to make sure to review each of these suggestions in the light of Section III.

Three of the suggestions dealt with the depth of the proposed topics: capital project, subordinate facilities, and process dynamics

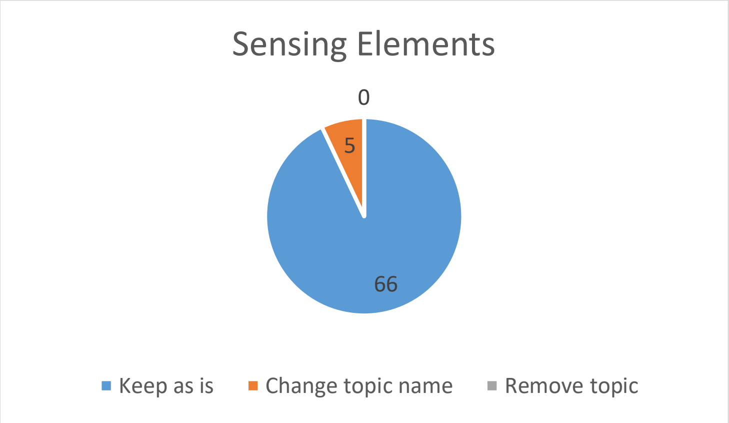
Two suggestions deal with relations between IT and OT: IT/OT collaboration and Shared knowledge and resources. Cloud and communications diagrams might have common elements.

Table of Contents

Question II-8 to II-9 Topics in Instrumentation and Control
Question II-8 dealt with proposed topics for the proposed category "Instrumentation and Control", which are: Sensing elements, Control devices, Programmable control devices, Control paradigms, Programming methods, Process variables, Data acquisition, Supervisory control, Alarms, Engineering laptops/workstations, Process data historians, Operator interfaces, Control system software

II-8_1 Sensing elements

Question II-8_1 asked participants whether to Keep as is, Change, or Remove the topic "Sensing elements". If participants chose "Change" they were asked to provide a suggestion. If they chose "Remove" they were asked to explain why.



Response	Count	Percent
Keep as is	66	93.0%
Change topic name	5	7.0%
Remove topic	0	0.0%
Total	71	100.0%

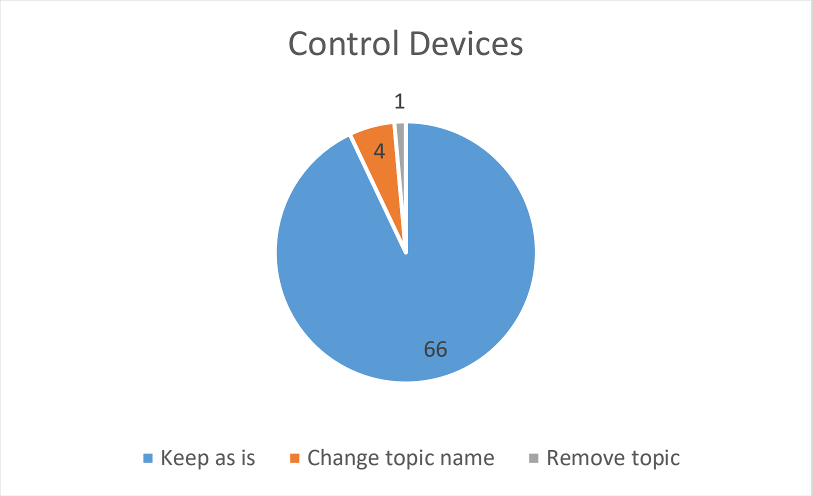
Suggestions for "change"

R_2YX5Hjj1Z8JitHY	Sensing Elements, Instrumentation and the physics
R_3lMl6Hi3p0cr1K4	Control Sensors
R_1rGFDHuFhnB2AQB	Follow our standardized naming conventions of a control system. Primary Element
R_VJBb9QiRZiR3xC1	Analog Sensing elements
R_2AX45Pxy89BCTuf	Primary Control Elements

Table of Contents

II-8_2 Control devices

Question II-8_2 asked participants whether to Keep as is, Change, or Remove the topic “Control devices”. If participants chose “Change” they were asked to provide a suggestion. If they chose “Remove” they were asked to explain why.



Response	Count	Percent
Keep as is	66	93.0%
Change topic name	4	5.6%
Remove topic	1	1.4%
Total	71	100.0%

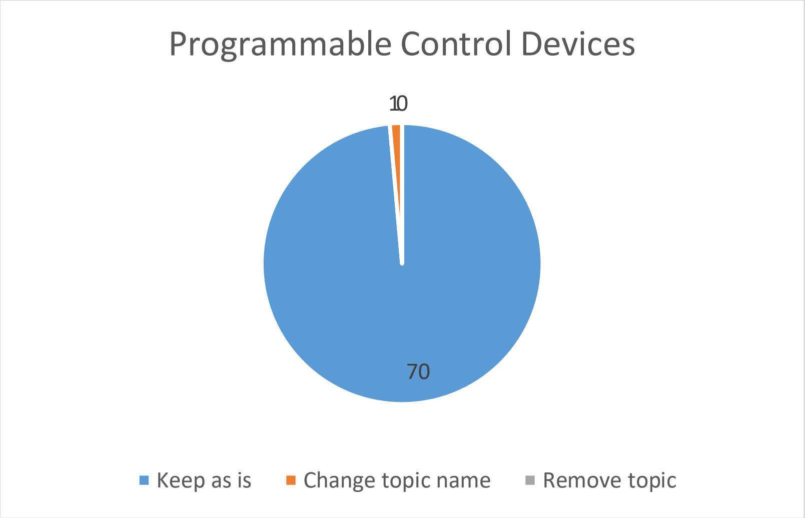
Suggestions for “Change”

R_2YX5Hjj1Z8JitHY	Control Devices and "finite element" theory
R_2YsHBQvCLvWLRjo	Final Controlled Devices
R_1rGFDHuFhnB2AQB	Follow our standardized naming conventions of a control system. Control Element
R_2AX45Pxy89BCTuf	Final Control Elements

Table of Contents

II-8_3 Programmable control devices

Question II-8_3 asked participants whether to Keep as is, Change, or Remove the topic “Programmable control devices”. If participants chose “Change” they were asked to provide a suggestion. If they chose “Remove” they were asked to explain why.



Response	Count	Percent
Keep as is	70	98.6%
Change topic name	1	1.4%
Remove topic	0	0.0%
Total	71	100.0%

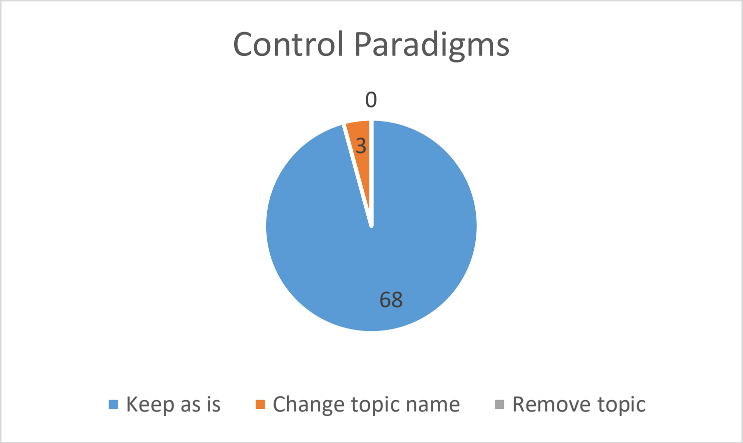
Suggestions for “Change”

R_1rGFDHuFhnB2AQB	Controller

Table of Contents

II-8_4 Control paradigms

Question II-8_4 asked participants whether to Keep as is, Change, or Remove the topic “Control paradigms”. If participants chose “Change” they were asked to provide a suggestion. If they chose “Remove” they were asked to explain why.



Response	Count	Percent
Keep as is	68	95.8%
Change topic name	3	4.2%
Remove topic	0	0.0%
Total	71	100.0%

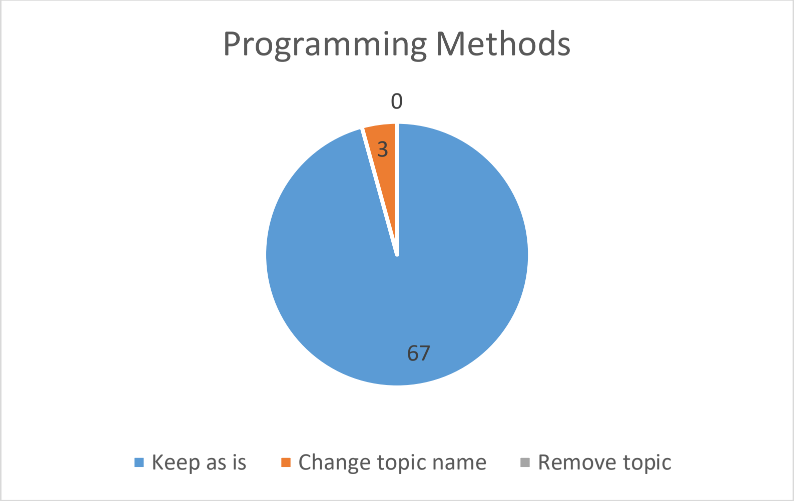
Suggestions for “Change”

R_1rGFDHuFhnB2AQB	what is this? the Algorithm, the narrative? i don't know what you are trying to define here.
R_2WHW03nONpmCTMk	Control Application and Algorithms
R_1C7kv6fnDsy5HUO	That depends what you mean by this.

Table of Contents

II-8_5 Programming methods

Question II-8_5 asked participants whether to Keep as is, Change, or Remove the topic “Programming methods”. If participants chose “Change” they were asked to provide a suggestion. If they chose “Remove” they were asked to explain why.



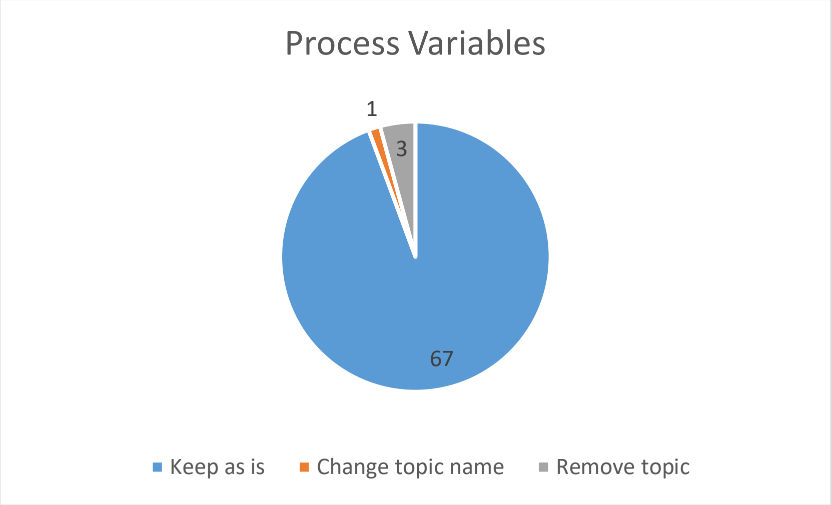
Response	Count	Percent
Keep as is	67	95.7%
Change topic name	3	4.3%
Remove topic	0	0.0%
Total	70	100.0%

Suggestions for “change”

R_2YX5Hjj1Z8JitHY	Programming Methods and ISO/IEC61131
R_1rGFDHuFhnB2AQB	again, what is this? Ladder Logic, SFC??? Or the software development lifecycle?
R_2WHW03nONpmCTMk	Programming Languages

II-8_6 Process variables

Question II-8_6 asked participants whether to Keep as is, Change, or Remove the topic “Process variables”. If participants chose “Change” they were asked to provide a suggestion. If they chose “Remove” they were asked to explain why.



Response	Count	Percent
Keep as is	67	94.4%
Change topic name	1	1.4%
Remove topic	3	4.2%
Total	71	100.0%

Suggestions for “change”

R_XzBpdAcbe7EVaa5	Security

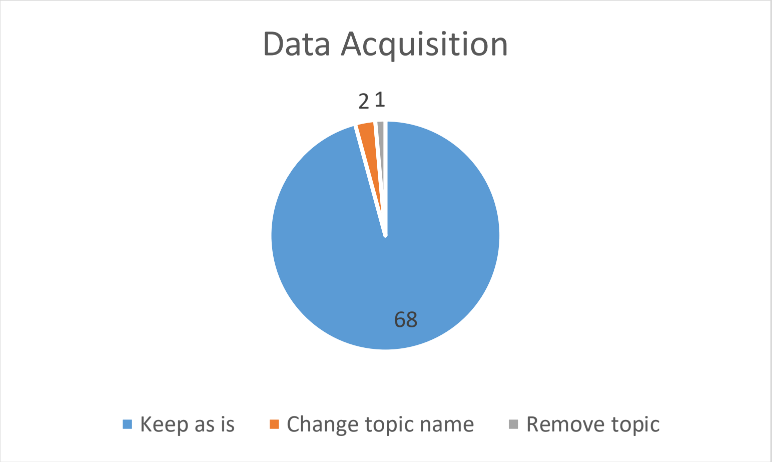
Reasoning for “remove”

R_1rGFDHuFhnB2AQB	this is falls under the Primary element
R_2WHW03nONpmCTMk	In cybersecurity it is not necessary to understand process variables, it is important to focus on the infrastructure.
R_1C7kv6fnDsy5HUO	Probably adequately covered under sensing subject area.

Table of Contents

II-8_7 Data acquisition

Question II-8_7 asked participants whether to Keep as is, Change, or Remove the topic “Data acquisition”. If participants chose “Change” they were asked to provide a suggestion. If they chose “Remove” they were asked to explain why.



Response	Count	Percent
Keep as is	68	95.8%
Change topic name	2	2.8%
Remove topic	1	1.4%
Total	71	100.0%

Suggestions for “change”

R_1rGFDHuFhnB2AQB	This topic should cover Data from Acquistion at the primary element to storage in the historion.
R_XzBpdAcbe7EVaa5	Architecture

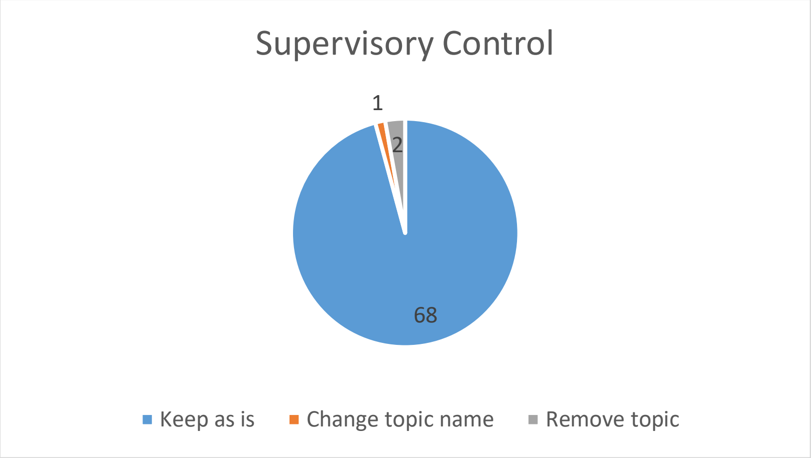
Reasoning for “remove”

R_2AX45Pxy89BCTuf	SCADA systems are an accepted title in industrial space. This should be merged into the Supervisor Control title

Table of Contents

II-8_8 Supervisory control

Question II-8_8 asked participants whether to Keep as is, Change, or Remove the topic “Supervisory control”. If participants chose “Change” they were asked to provide a suggestion. If they chose “Remove” they were asked to explain why.



Response	Count	Percent
Keep as is	68	95.8%
Change topic name	1	1.4%
Remove topic	2	2.8%
Total	71	100.0%

Suggestions for “change”

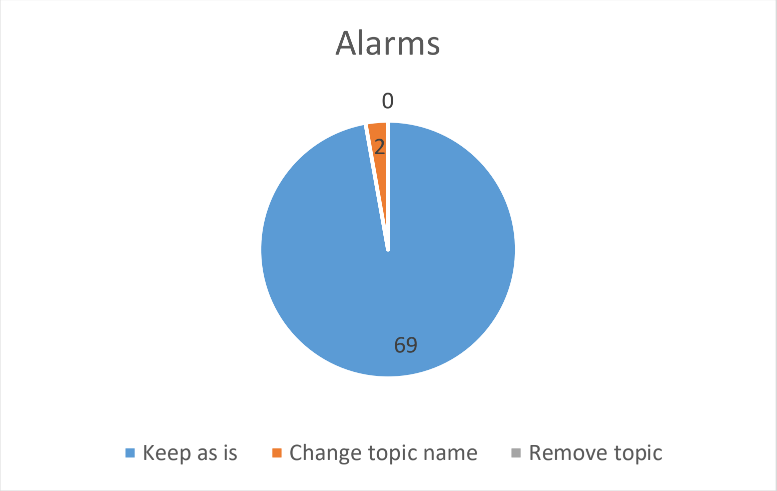
R_2AX45Pxy89BCTuf	After merging the Data Acquisition title into this, the title should be changed to "Supervisory Control and Data Acquisition Systems". It should also, briefly, touch on data collection systems.

Reasoning for “remove”

R_1rGFDHuFhnB2AQB	SCADA is an obsolete term and needs to stop be propagated by our profession. It's just control.
R_2WHW03nONpmCTMk	What is the difference between supervisory control (a.k.a. monitoring) and data acquisition?

II-8_9 Alarms

Question II-8_9 asked participants whether to Keep as is, Change, or Remove the topic “Alarms”. If participants chose “Change” they were asked to provide a suggestion. If they chose “Remove” they were asked to explain why.



Response	Count	Percent
Keep as is	69	97.2%
Change topic name	2	2.8%
Remove topic	0	0.0%
Total	71	100.0%

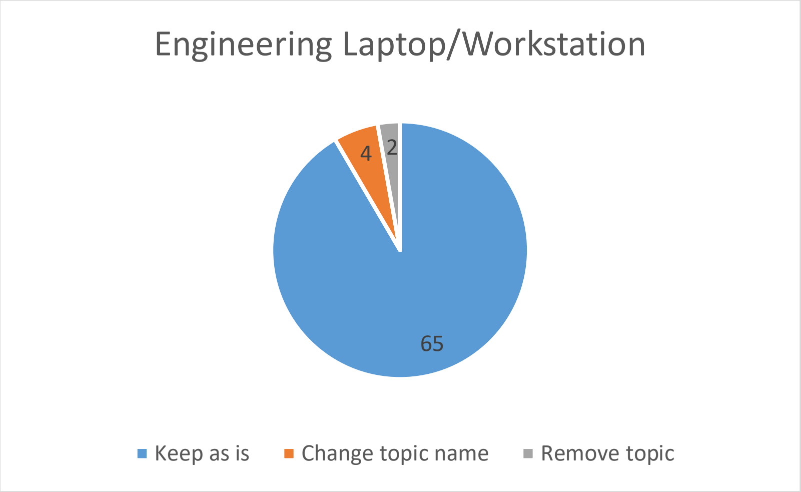
Suggestions for “change”

R_2YsHBQvCLvWLRjo	Alarm Management
R_1rGFDHuFhnB2AQB	Again, this is too broad.

Table of Contents

II-8_10 Engineering laptops/workstations

Question II-8_10 asked participants whether to Keep as is, Change, or Remove the topic “Engineering laptops/workstations”. If participants chose “Change” they were asked to provide a suggestion. If they chose “Remove” they were asked to explain why.



Response	Count	Percent
Keep as is	65	91.5%
Change topic name	4	5.6%
Remove topic	2	2.8%
Total	71	100.0%

Suggestions for “change”

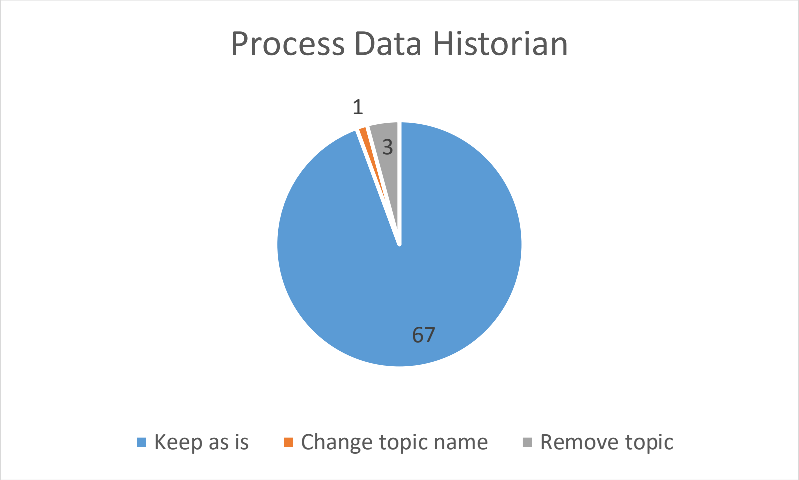
R_2YsHBQvCLvWLRjo	ICS Engineering & Maintenance Subsystems
R_1rGFDHuFhnB2AQB	this is all workstations. laptop, desktop, operator, engineer, user.
R_2WHW03nONpmCTMk	Control System Servers and Workstations
R_vZYehSwKucwalcF	Engineering laptops/workstations/transient devices

Reasoning for “remove”

R_1kNOtjKCfiKSTDZ	Shold be included in the category 'Programmable nd Control devices'
R_1C7kv6fnDsy5HUO	although important to secure it's not a huge subject area

II-8_11 Process data historians

Question II-8_11 asked participants whether to Keep as is, Change, or Remove the topic “Process data historians”. If participants chose “Change” they were asked to provide a suggestion. If they chose “Remove” they were asked to explain why.



Response	Count	Percent
Keep as is	67	94.4%
Change topic name	1	1.4%
Remove topic	3	4.2%
Total	71	100.0%

Suggestions for “change”

R_ekst6dSTefw2r85	Process data historians, MES, etc

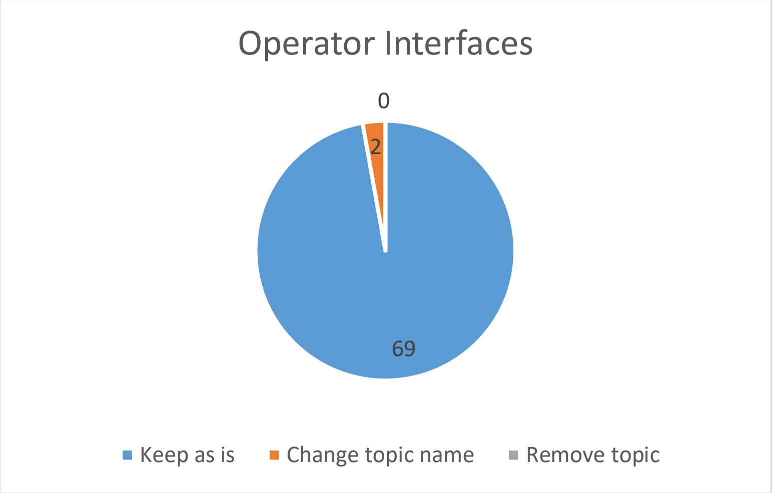
Reasoning for “remove”

R_1rGFDHuFhnB2AQB	part of data acquisition and storage
R_2WHW03nONpmCTMk	What is the difference between historians and data acquisition?
R_1C7kv6fnDsy5HUO	too much emphasis on one aspect of integrated architecture

Table of Contents

II-8_12 Operator interfaces

Question II-8_12 asked participants whether to Keep as is, Change, or Remove the topic “Operator interfaces”. If participants chose “Change” they were asked to provide a suggestion. If they chose “Remove” they were asked to explain why.



Response	Count	Percent
Keep as is	69	97.2%
Change topic name	2	2.8%
Remove topic	0	0.0%
Total	71	100.0%

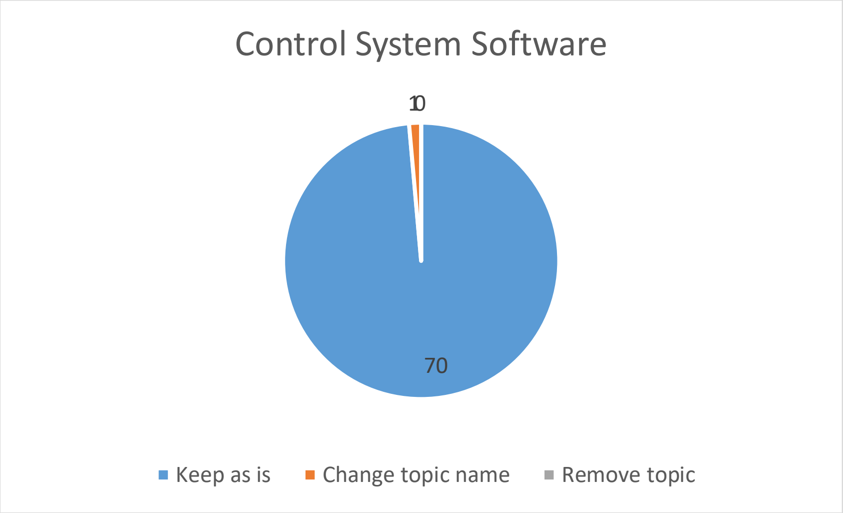
Suggestions for “change”

R_1rGFDHuFhnB2AQB	User Inteface. Doesn't matter who it is. if someone is looking at it, they are making decisions.
R_2WHW03nONpmCTMk	Control System Interfaces and Third Party Systems Integration

Table of Contents

II-8_13 Control system software

Question II-8_13 asked participants whether to Keep as is, Change, or Remove the topic “Control system software”. If participants chose “Change” they were asked to provide a suggestion. If they chose “Remove” they were asked to explain why.



Response	Count	Percent
Keep as is	70	98.6%
Change topic name	1	1.4%
Remove topic	0	0.0%
Total	71	100.0%

Suggestions for “change”

R_1rGFDHuFhnB2AQB	what is this? the programming software or the program itself?

Table of Contents

II-8 Topics in “Instrumentation and Control” overall

	Response		
Topic	*Keep as is*	*Change topic name*	*Remove topic*
Programmable control devices	70	1	0
Control system software	70	1	0
Alarms	69	2	0
Operator interfaces	69	2	0
Control paradigms	68	3	0
Data acquisition	68	2	1
Supervisory control	68	1	2
Programming methods	67	3	0
Process variables	67	1	3
Process data historian	67	1	3
Sensing elements	66	5	0
Control devices	66	4	1
Engineering laptop/workstation	65	4	2

Programmable control devices and Control system software received the most responses for “Keep as is”. “Control devices” received the fewest for “Keep as is”.

Sensing elements received the most responses for “Change topic name”, though no one suggested removing it.

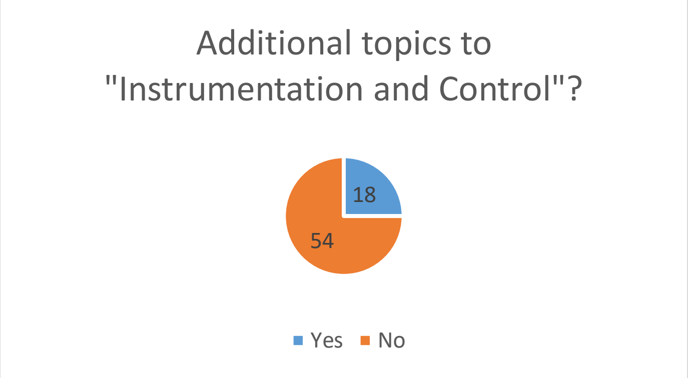
Process variables and Process data historian received the most responses for “Remove topic”, with three each. The low number of “Remove” responses indicates the soundness of the concepts.

A comparison between the two shows that Process variables was the most poorly regarded.

Table of Contents

II-9 Additional topics in “Instrumentation and Control” Category

Question II-9 asked whether additional topics should be added to the category Industrial Operations Ecosystem



Response	Count	Percent
Yes	18	25.0%
No	54	75.0%
Total	72	100.0%

If participants chose “Yes”, they were prompted to suggest additional topics.
Suggested topics:

R_2YX5Hjj1Z8JitHY	Unique aspects of protecting Control System functions
R_2YsHBQvCLvWLRjo	ICS Networking, System Architecture
R_1I72Afnm6478fXP	Networks and Protective Devices
R_26hX0Es8WVUZ3i0	VFD, IEDs
R_2Squ4P2NtTznJ4a	Modelling, analytics, real-time on-line models / digital twins
R_RqVMBWhBtfTdYrf	PLC secure coding practices
R_1BxKzD0XM4g0jcZ	Access is probably covered in one of other sections but passwords and access.
R_3kMMhb0mj6S80wG	Process Systems (Servers that run production)
R_1rGFDHuFhnB2AQB	i don't have the time to think about it now.
R_5c0uAAMSNWyojMB	Controller Architectures, Volatile/Non-Volatile Memory Types
R_3njf722UBVndAP8	Network/Communication Equipment
R_XTVNiQSzyaZNSzn	Analysis of failure modes, rates, history, consequences
R_vZYehSwKucwalcF	ICS software maintenance, ICS hardware maintenance
R_28HRVFlTwpY1Y9m	Machine Learning (ML), Physical Security Equipment (cameras; locks- esp.-smart locks; buried-slit coax sensors; etc.)
R_3MQjCEJ5fsIuCBG	SMART instrumentation
R_27a3HBRQ60cNEsj	Remote Monitoring, RTU, IED, Secure Remote Access, Industrial Cloud Services, Edge Processing
R_VJBb9QiRZiR3xC1	Intelligent Sensing Elements
R_2AX45Pxy89BCTuf	Wireless Control Systems Security

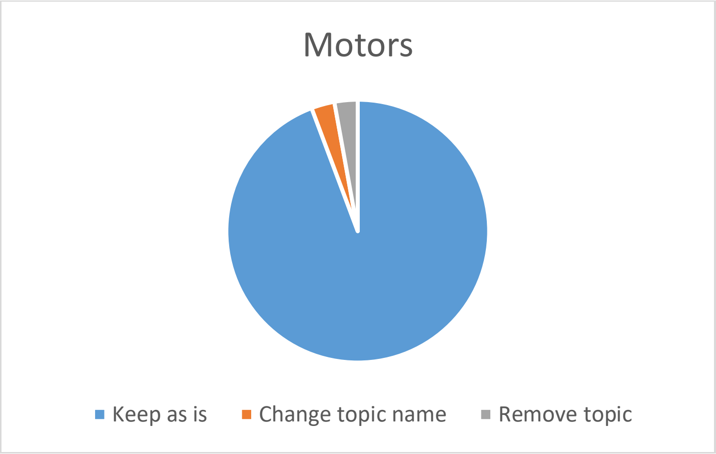
Table of Contents

Question II-11 to II-12 Topics in Equipment Under Control

This section dealt with the topics proposed under the category “Equipment Under Control”, which are: Motors, Pumps, Valves, Relays, Generators, Transformers, Breakers, Variable Frequency Drives.

II-11_1 Motors

Question II-11_1 asked participants whether to Keep as is, Change, or Remove the topic “Motors”. If participants chose “Change” they were asked to provide a suggestion. If they chose “Remove” they were asked to explain why.



Response	Count	Percent
Keep as is	66	94.3%
Change topic name	2	2.9%
Remove topic	2	2.9%
Total	70	100.0%

Suggestions for “change”

R_2YsHBQvCLvWLRjo	motors and pumps should be integrated into one topic. A pump requires a motor to drive it
R_28HRVFlTwpY1Y9m	Smart Motors and Motor Controllers

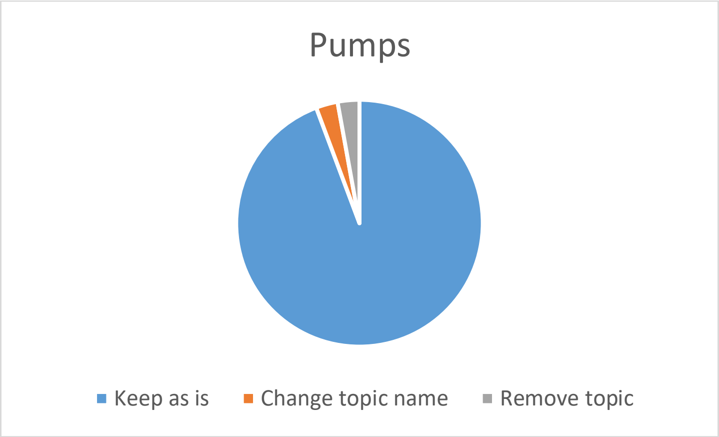
Reasoning for “remove”

R_2WHW03nONpmCTMk	Irrelevant to cybersecurity.
R_2AX45Pxy89BCTuf	When looking at "Motors" as a topic in Cyber Security, the only thing ther would be to look at is the during and after effects of an attack.

Table of Contents

II-11_2 Pumps

Question II-11_2 asked participants whether to Keep as is, Change, or Remove the topic “Pumps”. If participants chose “Change” they were asked to provide a suggestion. If they chose “Remove” they were asked to explain why.



Response	Count	Percent
Keep as is	66	94.3%
Change topic name	2	2.9%
Remove topic	2	2.9%
Total	70	100.0%

Suggestions for “change”

R_2YsHBQvCLvWLRjo	combine motors and pumps - see my response above
R_28HRVFlTwpY1Y9m	Smart Pumps and Pump Controllers

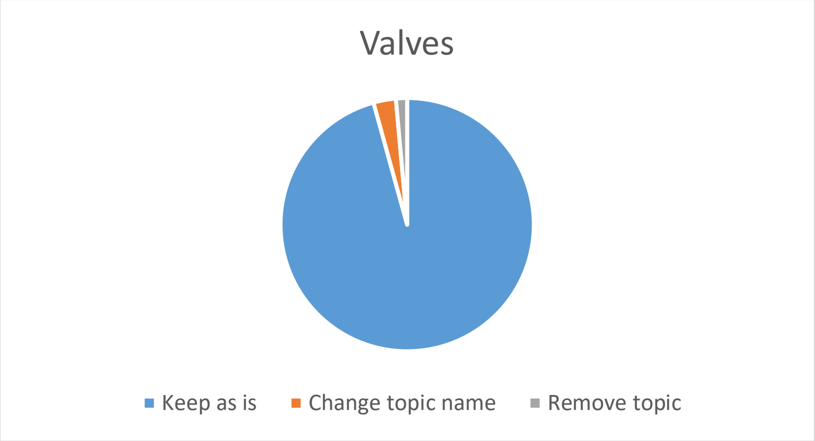
Reasoning for “Remove”

R_2WHW03nONpmCTMk	Irrelevant to cybersecurity, what moves the pump is the motor at the end of the day.
R_2AX45Pxy89BCTuf	When looking at "Pumps" as a topic in Cyber Security, the only thing to evaluate would be the effects during and after an attacj

Table of Contents

II-11_3 Valves

Question II-11_3 asked participants whether to Keep as is, Change, or Remove the topic “Valves”. If participants chose “Change” they were asked to provide a suggestion. If they chose “Remove” they were asked to explain why.



Response	Count	Percent
Keep as is	67	95.7%
Change topic name	2	2.9%
Remove topic	1	1.4%
Total	70	100.0%

Suggestions for “change”

R_28HRVFlTwpY1Y9m	Intelligent, Communicating Valves and other Flow Control
R_2AX45Pxy89BCTuf	Final Control Elements

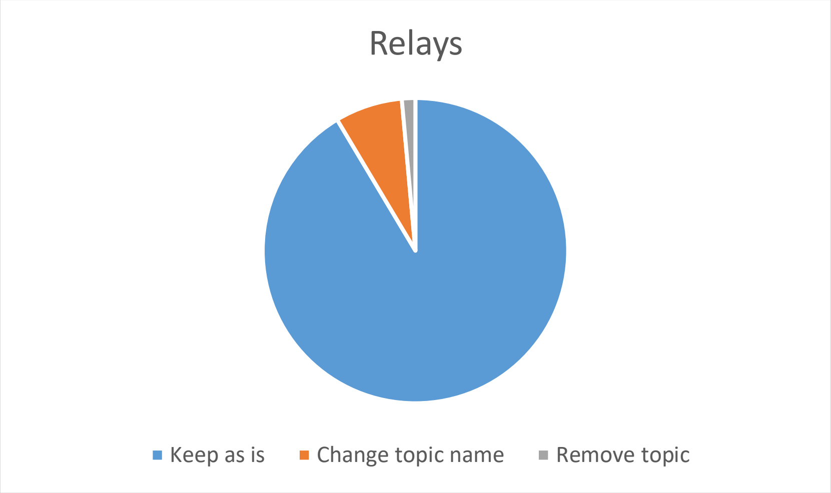
Reasoning for “remove”

R_2WHW03nONpmCTMk	Irrelevant. A valve is controlled by a positioner for that matter.

Table of Contents

II-11_4 Relays

Question II-11_4 asked participants whether to Keep as is, Change, or Remove the topic “Relays”. If participants chose “Change” they were asked to provide a suggestion. If they chose “Remove” they were asked to explain why.



Response	Count	Percent
Keep as is	64	91.4%
Change topic name	5	7.1%
Remove topic	1	1.4%
Total	70	100.0%

Suggestions for “change”

R_2YsHBQvCLvWLRjo	Protective Relaying and Switchgear
R_26hX0Es8WVUZ3i0	Mecanical Relays (Differentiate from Smart IEDs/Power System Relays)
R_vZYehSwKucwalcF	Intermediate Devices (because relays aren't the terminal equipment being controlled)
R_28HRVFlTwpY1Y9m	Communicating and Protective Relays
R_2AX45Pxy89BCTuf	Smart Relays

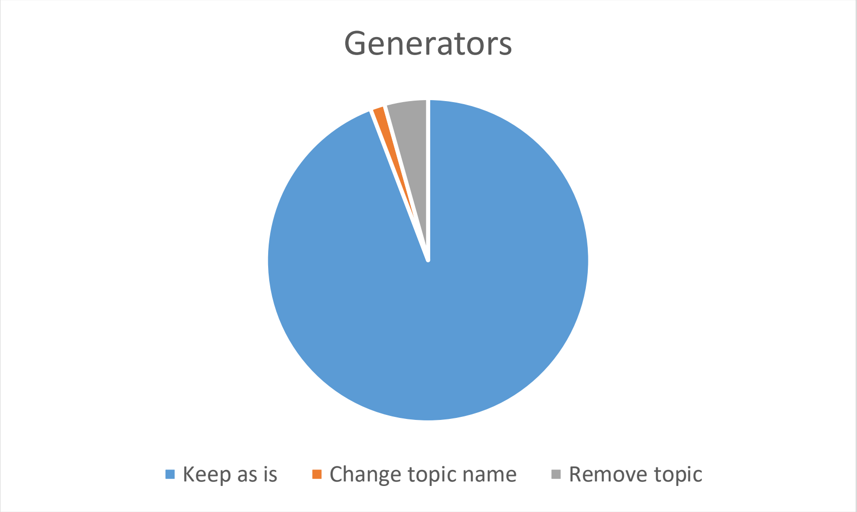
Reasoning for “remove”

R_2WHW03nONpmCTMk	Irrelevant if this is a regular pure electrical relay, such as an interposing relay. If referring to an IED then this is considered part of the ICS infrastructure.

Table of Contents

II-11_5 Generators

Question II-11_5 asked participants whether to Keep as is, Change, or Remove the topic “Generators”. If participants chose “Change” they were asked to provide a suggestion. If they chose “Remove” they were asked to explain why.



Response	Count	Percent
Keep as is	65	94.2%
Change topic name	1	1.4%
Remove topic	3	4.3%
Total	69	100.0%

Suggestions for “change”

R_2YsHBQvCLvWLRjo	combine generators / transformers / breakers into Electrical Generation & Substations

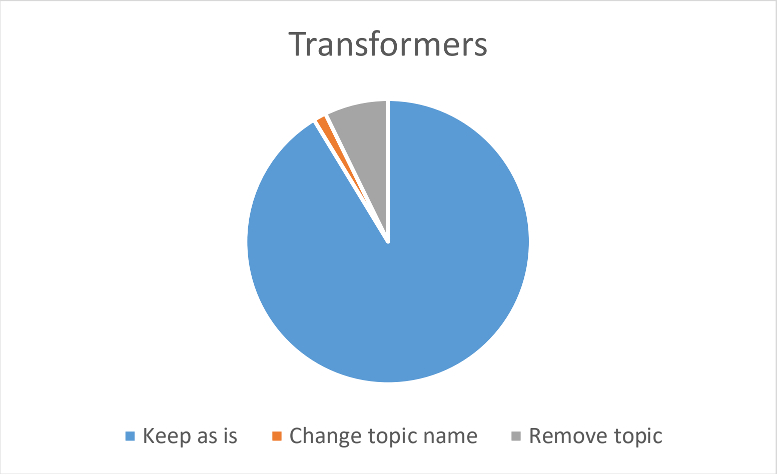
Reasoning for “remove”

R_1rGFDHuFhnB2AQB	this is a backup device in most cases, not something we control. Unless you are in the power generation
R_2WHW03nONpmCTMk	Irrelevant for cybersecurity to know how generators work and they are controlled.
R_vZYehSwKucwaIcF	Toe electric power specific, and also an aggregation of lower level systems

Table of Contents

II-11_6 Transformers

Question II-11_6 asked participants whether to Keep as is, Change, or Remove the topic “Transformers”. If participants chose “Change” they were asked to provide a suggestion. If they chose “Remove” they were asked to explain why.



Response	Count	Percent
Keep as is	63	91.3%
Change topic name	1	1.4%
Remove topic	5	7.2%
Total	69	100.0%

Suggestions for “change”

R_2YsHBQvCLvWLRjo	combine generators / transformers / breakers into Electrical Generation & Substations

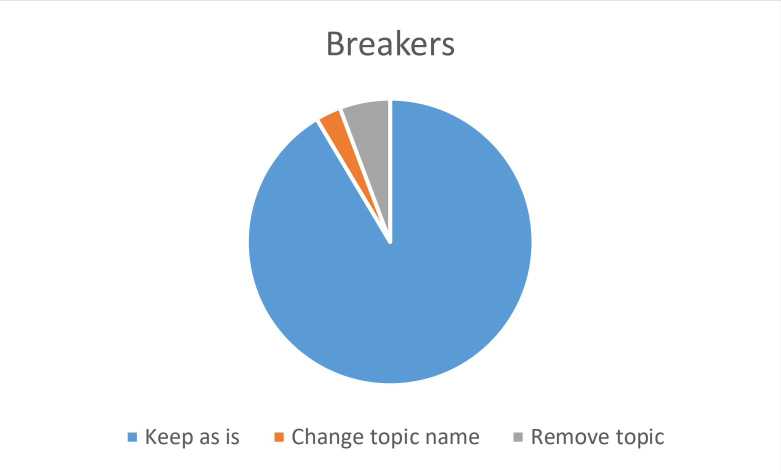
Reasoning for “remove”

R_1HduUVDzYT3QuFp	No ethernet
R_1rGFDHuFhnB2AQB	how do you control a transformer? Again too specific
R_2WHW03nONpmCTMk	Irrelevant, what matters is to protect the IEDs of the transformers
R_vZYehSwKucwaIcF	Too electric power specific, and the actual controllable parts are not the core part of the transformer and also exist elsewhere on this list (i.e. motors and pumps)
R_2AX45Pxy89BCTuf	When evaluating "Transformers" as a topic in Cyber Security, the only thing to look at is during and after effects of an attack

Table of Contents

II-11_7 Breakers

Question II-11_7 asked participants whether to Keep as is, Change, or Remove the topic “Breakers”. If participants chose “Change” they were asked to provide a suggestion. If they chose “Remove” they were asked to explain why.



Response	Count	Percent
Keep as is	64	91.4%
Change topic name	2	2.9%
Remove topic	4	5.7%
Total	70	100.0%

Suggestions for “change”

R_2YsHBQvCLvWLRjo	combine generators / transformers / breakers into Electrical Generation & Substations
R_28HRVFlTwpY1Y9m	Circuit Breakers, Intelligent/Smart Switches and Smart Circuit Protections

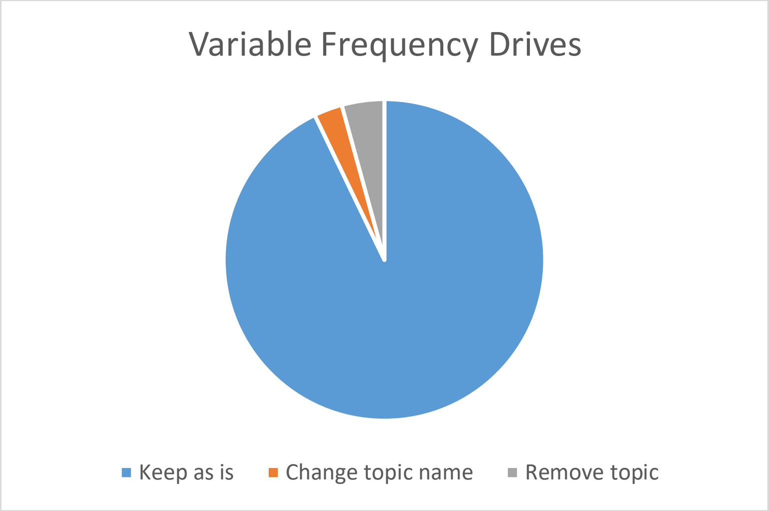
Reasoning for “remove”

R_1rGFDHuFhnB2AQB	safety device, not a control device. again too specific
R_2WHW03nONpmCTMk	Irrelevant. What matters are the IEDs.
R_vZYehSwKucwalcF	Too electric power specific here, include in the Facilities and Safety parts for the other aspects
R_2AX45Pxy89BCTuf	When evaluating "Breakers" as a topic in Cyber Security, the only thing to evaluate is during and after effects

Table of Contents

II-11_8

Question II-11_8 asked participants whether to Keep as is, Change, or Remove the topic “Variable Frequency Drives”. If participants chose “Change” they were asked to provide a suggestion. If they chose “Remove” they were asked to explain why.



Response	Count	Percent
Keep as is	65	92.9%
Change topic name	2	2.9%
Remove topic	3	4.3%
Total	70	100.0%

Suggestions for “change”

R_28HRVFlTwpY1Y9m	Adjustable Speed Motor Controllers (which includes Soft-Starters and similar controllers)
R_30ucmUIOod5Mkl0	Adjustable Speed Drive

Reasoning for “remove”

R_26hX0Es8WVUZ3i0	Belongs with Controls vs motors
R_1rGFDHuFhnB2AQB	this is a final control element. It controls a pump or motor. By itself, it does nothing.
R_2WHW03nONpmCTMk	Irrelevant to the cybersecurity discipline.

Table of Contents

II-10 Topics in “Equipment Under Control” overall

	Response		
Topic	*Keep as is*	*Change topic name*	*Remove topic*
Valves	67	2	1
Motors	66	2	2
Pumps	66	2	2
Variable frequency drives	65	2	3
Generators	65	1	3
Relays	64	5	1
Breakers	64	2	4
Transformers	63	1	5

While motors and pumps received the lowest average relevancy scores, it was Breakers and Transformers that received the greatest number of responses for “Remove topic”, with 4 and 5 selections each.

Table of Contents

II-12 Additional topics in Equipment Under Control

If participants chose “yes” they were prompted to suggest additional topics.
Additional topics:

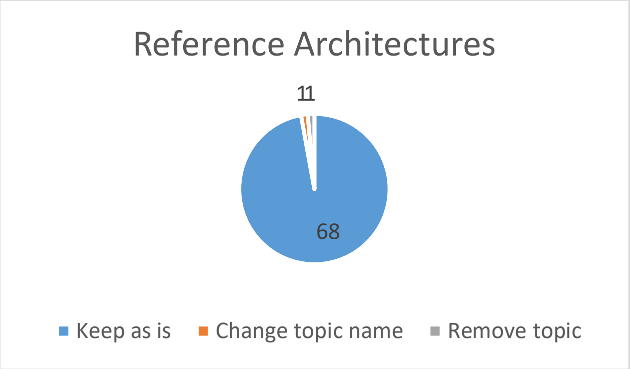
R_2YX5Hjj1Z8JitHY	Safety Components and Safety Systems; Programmable Devices from the PLC to the sensor
R_8ugyg2V7BXUQEr7	compressors
R_2YsHBQvCLvWLRjo	process / pressure vessels, boilers, turbines, robotics, discrete automation
R_RqVMBWhBtfTdYrf	Meters, Valves, robotics
R_2Su9412OXG578E9	Process Heating & Cooling, Hi Speed rotating equipment, HVAC,
R_1HduUVDzYT3QuFp	Process Analyzers, Smart Calibration devices
R_1rGFDHuFhnB2AQB	no time
R_XTVNiQSzyaZNSzn	Piping (hydraulics, dynamics)
R_vZYehSwKucwaIcF	Actuators
R_28HRVFlTwpY1Y9m	Automated Medical/Surgical/Systems/Machines and Instrumentation, Boilers & boiler controls, Automated Ingress & Egress Controls,
R_3MQjCEJ5fsIuCBG	Types of actuators (Hydrauilic, Pneumatic and Electric)
R_0chS1EeHbRXgJ7X	
R_Qh4JJ9Sl3FTmiWZ	Safety valves, safety over rides, safety switches, upper and lower limit switches
R_27a3HBRQ60cNEsj	Safety Related, Protective Relays (Need to differentiate between simple relays and IEDs), Packaged Systems (Skids), Air Handling Units (AHU)
R_x65cwLz09tf5P0Z	Engines
R_3PHz5Hw4MGOxWNK	
R_1eqr6le0DY5qvYg	Robots, conveyor belt
R_XzBpdAcbe7EVaa5	Inside threats, malicious actors privacy

Table of Contents

Question II-14 to II-15 Topics in Industrial Communications
This section dealt with topics proposed under the Category "Industrial Communications". These are: Reference architectures, Industrial communications protocols, Transmitter signals, Fieldbuses.

II-14_1 Reference architectures

Question II-14_1 asked participants whether to Keep as is, Change, or Remove the topic "Reference Architectures". If participants chose "Change" they were asked to provide a suggestion. If they chose "Remove" they were asked to explain why.



Response	Count	Percent
Keep as is	68	97.1%
Change topic name	1	1.4%
Remove topic	1	1.4%
Total	70	100.0%

Suggestions for "change"

R_3EKGwQYaHhLTi4H	Reference Network Topology

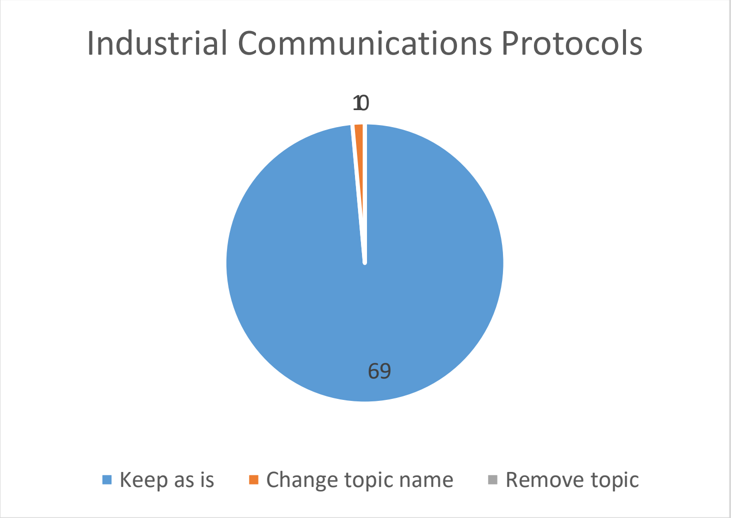
Reasoning for "remove"

R_3lMl6Hi3p0cr1K4	No context

Table of Contents

II-14_2 Industrial Communications Protocols

Question II-14_2 asked participants whether to Keep as is, Change, or Remove the topic “Industrial Communications Protocols”. If participants chose “Change” they were asked to provide a suggestion. If they chose “Remove” they were asked to explain why.



Response	Count	Percent
Keep as is	69	98.6%
Change topic name	1	1.4%
Remove topic	0	0.0%
Total	70	100.0%

Suggestions for “change”

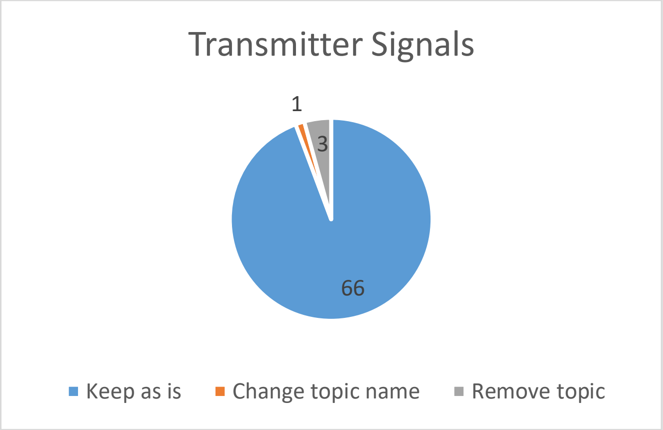
R_1rGFDHuFhnB2AQB	remove Industrial

Reasoning for “remove”
None.

Table of Contents

II-14_3 Transmitter signals

Question II-14_3 asked participants whether to Keep as is, Change, or Remove the topic “Transmitter Signals”. If participants chose “Change” they were asked to provide a suggestion. If they chose “Remove” they were asked to explain why.



Response	Count	Percent
Keep as is	66	94.3%
Change topic name	1	1.4%
Remove topic	3	4.3%
Total	70	100.0%

Suggestions for “change”

R_26hX0Es8WVUZ3i0	Transmitter Types

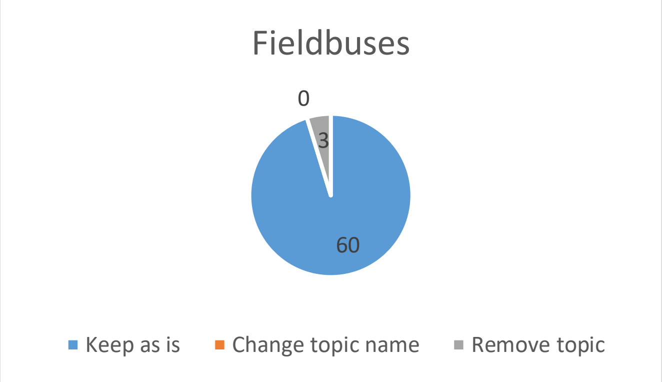
Reasoning for “remove”

R_1rGFDHuFhnB2AQB	the way a transmitter gets its signal to a controller is just a protocol. why does it have its own topic. If you keep this, then you need a whole lot more.
R_2WHW03nONpmCTMk	The signal is either a 4-20mA or a fieldbus no need to separate them. And if it's a fieldbus then it's an industrial communication protocol
R_1C7kv6fnDsy5HUO	Probably can be covered under sensing subject

Table of Contents

II-14_4 Fieldbuses

Question II-14_4 asked participants whether to Keep as is, Change, or Remove the topic “Fieldbuses”. If participants chose “Change” they were asked to provide a suggestion. If they chose “Remove” they were asked to explain why.



Response	Count	Percent
Keep as is	60	95.2%
Change topic name	0	0.0%
Remove topic	3	4.8%
Total	63	100.0%

Suggestions for “change”
None.

Reasoning for “remove”

R_2Su9412OXG578E9
R_1rGFDHuFhnB2AQB
R_2WHW03nONpmCTMk
The reasoning for these was left blank.

Table of Contents

II-14 Topics in Industrial Communications Overall

	Response		
Topic	*Keep as is*	*Change topic name*	*Remove topic*
Industrial Communication Protocols	69	1	0
Reference Architectures	68	1	1
Transmitter Signals	66	1	3
Fieldbuses	60	0	3

No respondents thought that Industrial Communications Protocols should be removed. Three thought that Fieldbuses should be removed.

Table of Contents

II-15 Additional topics in Industrial Communications

If participants chose “yes” they were prompted to suggest additional topics.
Additional topics:

R_1QbTAYJzAas8vNF	mobile devices: calibrators and configuration devices
R_1MPQ2QhyNfNcAV3	Networking technologies, fundamentals of network segmentation
R_21onh8CfZn5Ywhn	Wireless (Fieldbus), Wireless (Bluetooth), WIreless (Wi-Fi), Wireless (Mesh, LTE, 5G, Other)
R_1n2c6fNrttesqpg	Statefull packet inspection
R_241sHjNVIdRaCW1	Cloud and security architectures
R_1JUYV5E3P6NzgbE	
R_UfkYybej4RRfKRH	deployment techniques, switch management,
R_1NDgRhbaLUQhIEx	depends on how these changes are incorporated
R_2Pe7wD3ySp315F0	Networked Communications, Interface Specifications / Interface Control Documents, Software Block Diagrams, Boundary Diagrams, Ports/Protocols Matrix
R_2ZQ4pInrnKrcZiM	Communications media and devices
R_2aRo3qs2LIv8otL	Data Diodes (what they are, are not, and when and how to use them), GPS & Navigation systems-how they can be compromised and results of being compromised, Ultra-sonic and motion detection systems/subsystems/devices, 5G connection/communication and M2M control capabilities, Legacy Trunking-Radio & Packet Switching Computer Systems,
R_2ebeSEVBFoDIHDj	Effects of Latency * discussion around throughput and bandwidth availability in Industrial applications
R_31LwtZXJfcVIB8C	Alarms
R_3nTrmSy2ZCbkjrb	Safety Related
R_3CAZq03xeRuPvRk	Security

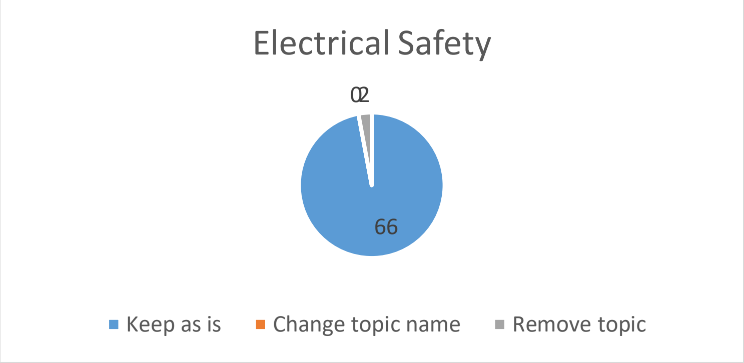
Table of Contents

Question II-17 to II-18 Topics in Safety

This question dealt with topics proposed in the Safety category, which are: Electrical safety, Personal protective equipment, Safety/Hazards assessment, Safety Instrumented Functions, Lock-out tag-out, Safe work procedures, Common failure modes.

II-17_1 Electrical Safety

Question II-17_1 asked participants whether to Keep as is, Change, or Remove the topic "Electrical Safety". If participants chose "Change" they were asked to provide a suggestion. If they chose "Remove" they were asked to explain why.



Response	Count	Percent
Keep as is	66	97.1%
Change topic name	0	0.0%
Remove topic	2	2.9%
Total	68	100.0%

Suggestions for "change"

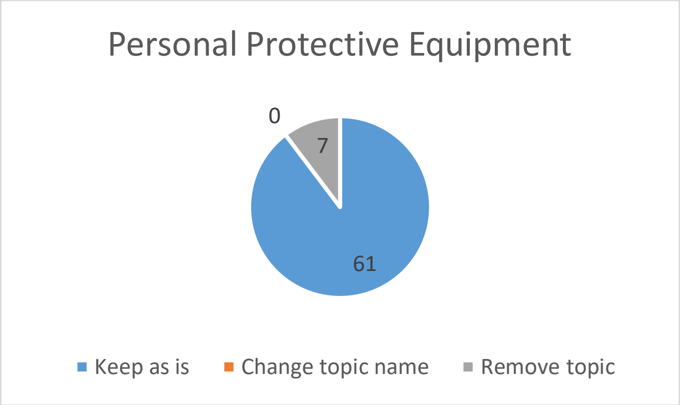
None.

Reasoning for "remove"

R_2Su9412OXG578E9	this topic is governed by the specific equipment owner and varies greatly, better handled by employer
R_1rGFDHuFhnB2AQB	This is its own category and Cyber is a subset of Electrical Safety. I don't see it the other way around.

II-17_2 Personal Protective Equipment

Question II-17_2 asked participants whether to Keep as is, Change, or Remove the topic “Personal Protective Equipment”. If participants chose “Change” they were asked to provide a suggestion. If they chose “Remove” they were asked to explain why.



Response	Count	Percent
Keep as is	61	89.7%
Change topic name	0	0.0%
Remove topic	7	10.3%
Total	68	100.0%

Suggestions for “change”

None

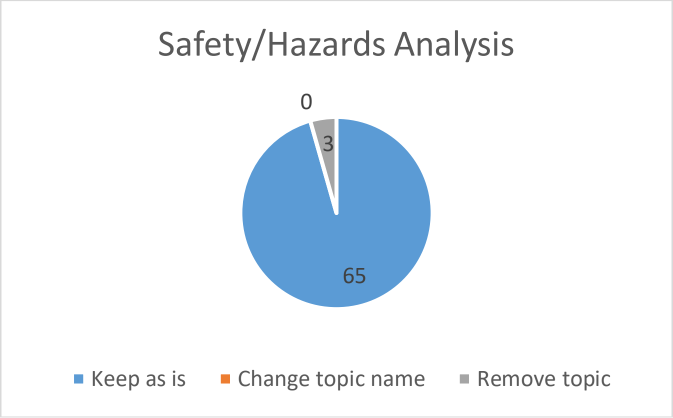
Reasoning for “remove”

R_2YsHBQvCLvWLRjo	PPE is a final element of safety that is performed if no other method of removing the hazard can be deployed. It may be referenced in a general sense but not applicable to cybersecurity as a specific topic
R_2Su9412OXG578E9	this topic is governed by the specific equipment owner and varies greatly, better handled by employer
R_yQjIaqY7oRRQQNP	Shouldn't be part of the Operational Technology Network
R_1rGFDHuFhnB2AQB	People wearing safety glasses is not a concern of Cyber.
R_3NId6QsP1huq1WV	Seems wholly unrelated to cybersecurity.
R_1C7kv6fnDsy5HUO	largely irrelevant and basics could be covered under another area
R_1JLVvwwpCaXn84N	Relates more towards workplace safety and less on the technical aspects of cybersecurity.

Table of Contents

II-17_3 Safety/Hazards Analysis

Question II-17_3 asked participants whether to Keep as is, Change, or Remove the topic “Safety/Hazards Analysis”. If participants chose “Change” they were asked to provide a suggestion. If they chose “Remove” they were asked to explain why.



Response	Count	Percent
Keep as is	65	95.6%
Change topic name	0	0.0%
Remove topic	3	4.4%
Total	68	100.0%

Suggestions for “Change”:
None

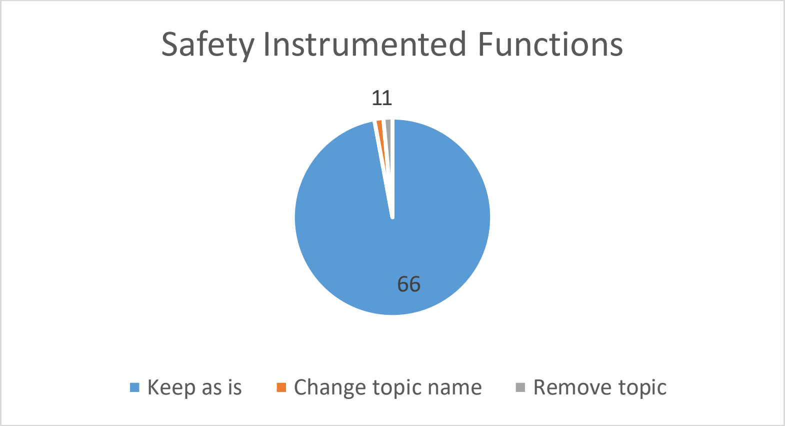
Reasoning for “Remove”:

R_1rGFDHuFhnB2AQB	Cyber belongs in the Assessment. The assessment is not part of Cyber.
R_2WHW03nONpmCTMk	A cybersecurity hazards assessment it's unnecessary. The only thing necessary is the architecture of the ICS.
R_1JLVvwwpCaXn84N	Relates more towards workplace safety and less on the technical aspects of cybersecurity.

Table of Contents

II-17_4 Safety Instrumented Functions

Question II-17_4 asked participants whether to Keep as is, Change, or Remove the topic “Safety Instrumented Functions”. If participants chose “Change” they were asked to provide a suggestion. If they chose “Remove” they were asked to explain why.



Response	Count	Percent
Keep as is	66	97.1%
Change topic name	1	1.5%
Remove topic	1	1.5%
Total	68	100.0%

Suggestions for “Change”:

R_1C7kv6fnDsy5HUO	Functional Safety (SIF is a process/IEC61511 industry term)

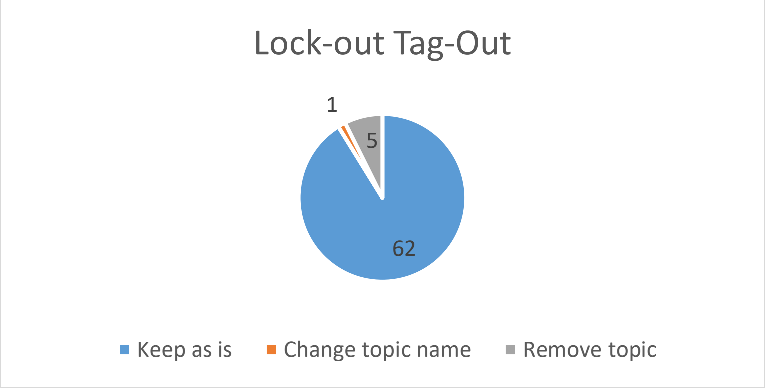
Reasoning for “Remove”:

R_1rGFDHuFhnB2AQB	belongs in Control Systems.

Table of Contents

II-17_5 Lock-out Tag-out

Question II-17_5 asked participants whether to Keep as is, Change, or Remove the topic “Lock-out Tag-out”. If participants chose “Change” they were asked to provide a suggestion. If they chose “Remove” they were asked to explain why.



Response	Count	Percent
Keep as is	62	91.2%
Change topic name	1	1.5%
Remove topic	5	7.4%
Total	68	100.0%

Suggestions for “Change”:

R_2YsHBQvCLvWLRjo	Integrate Lock-out / Tag-out with safe work procedures

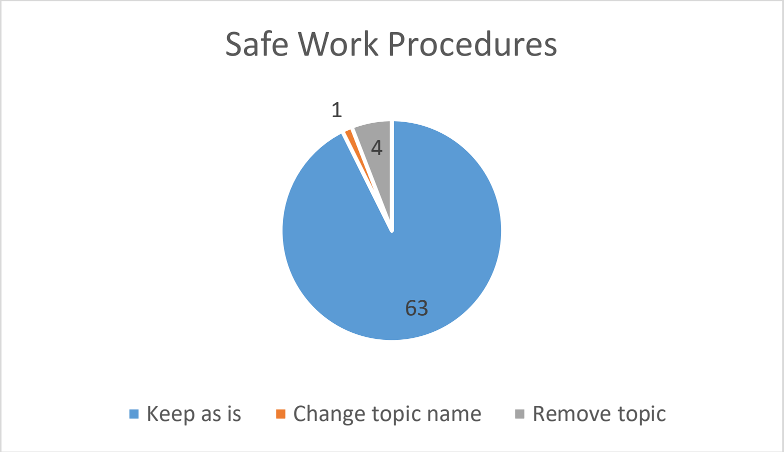
Reasoning for “Remove”:

R_2Su9412OXG578E9	this topic is governed by the specific equipment owner and varies greatly, better handled by employer
R_yQjIaqY7oRRQQNP	I'm only aware of manual systems, none that would be compromised through cyber mthods
R_1rGFDHuFhnB2AQB	not part of Cyber
R_3NId6QsP1huq1WV	If we are talking physical LOTO, then not as related.
R_1JLVvwwpCaXn84N	Tribal jargon. It's not clear to me what that means. I would at least suggest renaming it.

Table of Contents

II-17_6 Safe work procedures

Question II-17_6 asked participants whether to Keep as is, Change, or Remove the topic “Safe Work Procedures”. If participants chose “Change” they were asked to provide a suggestion. If they chose “Remove” they were asked to explain why.



Response	Count	Percent
Keep as is	63	92.6%
Change topic name	1	1.5%
Remove topic	4	5.9%
Total	68	100.0%

Suggestions for “Change”:

R_2YsHBQvCLvWLRjo	Integrate Lock-out / Tag-out with safe work procedures

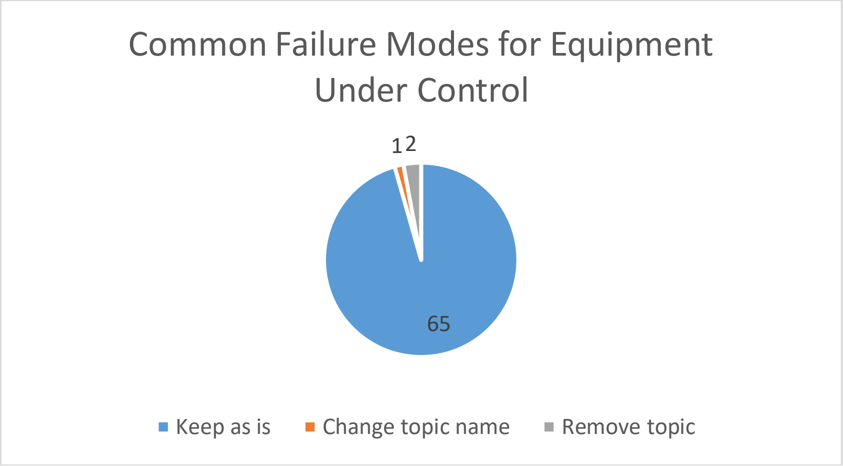
Reasoning for “Remove”:

R_2Su9412OXG578E9	this topic is governed by the specific equipment owner and varies greatly, better handled by employer
R_1rGFDHuFhnB2AQB	not part of Cyber. the procedure needs to include cyber if it is relevant.
R_3MQjCEJ5fsIuCBG	This can be merged with LOTO
R_1JLVvwwpCaXn84N	Applies more towards incident response.

Table of Contents

II-17_7 Common Failure Modes for Equipment Under Control

Question II-17_7 asked participants whether to Keep as is, Change, or Remove the topic “Common Failure Modes for Equipment Under Control”. If participants chose “Change” they were asked to provide a suggestion. If they chose “Remove” they were asked to explain why.



Response	Count	Percent
Keep as is	65	95.6%
Change topic name	1	1.5%
Remove topic	2	2.9%
Total	68	100.0%

Suggestions for “Change”:

R_1rGFDHuFhnB2AQB	depends on if you change the category

Reasoning for “Remove”:

R_vZYehSwKucwaIcF	Keep it but put it somewhere other than Safety, it seems unlike the other choices
R_1C7kv6fnDsy5HUO	could easily be covered under SIF/functional safety

Table of Contents

II-17 Topics in Safety Overall

Topic	**Response** *Keep as is*	*Change topic name*	*Remove topic*
Safety Instrumented Functions	66	1	1
Electrical Safety	66	0	2
Safety/Hazards Assessment	65	0	3
Common Failure Modes for Equipment Under Control	65	1	2
Safe Work Procedures	63	1	4
Lock-out Tag-out	62	1	5
Personal Protective Equipment	61	0	7

Of the suggested topics in the Safety category, one respondent suggested removing “Safety Instrumented Functions”. Seven respondents suggested removing “Personal Protective Equipment”.

Table of Contents

II-18 Additional topics in Safety

R_2YX5Hjj1Z8JitHY	The unique aspects of securing safety function
R_2YsHBQvCLvWLRjo	process safety, physical security
R_26hX0Es8WVUZ3i0	
R_RqVMBWhBtfTdYrf	CCE, CyberPHA, Threat and Attack Modeling, Consequence Red Teaming
R_3lMl6Hi3p0cr1K4	Environmental Awareness
R_2Su9412OXG578E9	life safety systems
R_1rGFDHuFhnB2AQB	this whole topic is flawed.
R_XTVNiQSzyaZNSzn	Pneumatic systems, hydraulic systems, other energy storage systems
R_ekst6dSTefw2r85	Process safety, safety in design, risk assessment
R_vZYehSwKucwaIcF	Chemical safety, Machine safety, Pressurized systems safety (if you're going to have electrical safety then probably should have all of them)
R_28HRVFlTwpY1Y9m	How to detect/determine/diagnose a Safety System intrusion/remote control/failure,
R_3CZvA7p1ny9D7Su	Hardware vs. Software Safety Controls
R_3MQjCEJ5fsIuCBG	Control overrides and logic forcing
R_27a3HBRQ60cNEsj	Safety Protocols and Standards

Table of Contents

Question II-19

Question II-19 asked respondents “Please list the topics that you recommend should be in the new Foundational ICS Knowledge category (or categories) you suggested. Provide the list in the format of Category1: topic1, topic2, topic3, ...”

R_2Su9412OXG578E9	Configuration Management: backup/archive, device configurations, change management practices, auditing
R_2WHW03nONpmCTMk	Industrial Communication Networks: Design and Engineering, Network Management, Network Access Control and Security. Windows Domain: Domain Group Policies, Domain Users and Computer Group Management.
R_1HduUVDzYT3QuFp	Logical Segmentation
R_1rGFDHuFhnB2AQB	not enough time or space here.
R_3R9FXVwJeSQbdCH	Remote control outside plant
R_3EaM9vGMjuCCcuf	Risk
R_1BxKzD0XM4g0jcZ	Safety PLCs
R_RqVMBWhBtfTdYrf	Secure PLC coding practices, consequence red teaming, cyberPHA, threat and attack modeling and CCE
R_2AX45Pxy89BCTuf	Security: creating secure industrial communications, Securing CIP (common industrial protocol), Securing programmable controls from industrial ethernet,
R_3eqX8pib0BYlC2z	software defined networks, communication determinism
R_3kMMhb0mj6S80wG	Topic 1 - support and maintenance Topic 2- Shop Floor Architecture standards Topic 3 - Lifecycle management Topic 4- backup
R_3PHz5Hw4MGOxWNK	topic 4
R_1eqr6le0DY5qvYg	Understand Industries constraints: business continuity, business disruption consequences, process availability; Adaptation to Industrial world: difference between IT world and Industrial world, security topics

Table of Contents

Section III – Industrial Control Systems Knowledge

Analysis by Carl Schuett of QED Solutions

For each chart, the original spreadsheet is included as a linked object.

Section III asked respondents to help determine a reasonable foundational set of knowledge needed to secure control systems – to which traditional IT, computer science, or cybersecurity students/professionals are not normally exposed.

Knowledge categories were broken down into four general categories:

- Regulation and Guidance
- Common Weaknesses
- Events and Incidents
- Defensive Technologies and Approaches

This section summarizes narrative responses provided by the respondents. Provided answers were assessed for incorporation into the ICS Cybersecurity Workforce Framework based on the judgement of the assessment team and the weighting of the respondent's experience. All recorded responses include the survey identifier. Blank responses were filtered from the results.

Table of Contents

Question III-2 Industrial Cybersecurity Categories
The initial set of narrative questions covered the four primary categories. Respondents were asked if they would suggest a change to each category or suggest that categories removal.

Question III-2_1 Regulation and Guidance

For Regulations and Guidance, a total of 68 respondents completed the question. As shown in Figure 1, 67 respondents selected "Keep as is" and one survey respondent suggested a title change. No respondents suggested that the category be removed. The change suggestion is:

Respondent ID	Response Content
R_1HduUVDzYT3QuFp	Regulations, Industry Alliances, Guidance, Frameworks and Standards

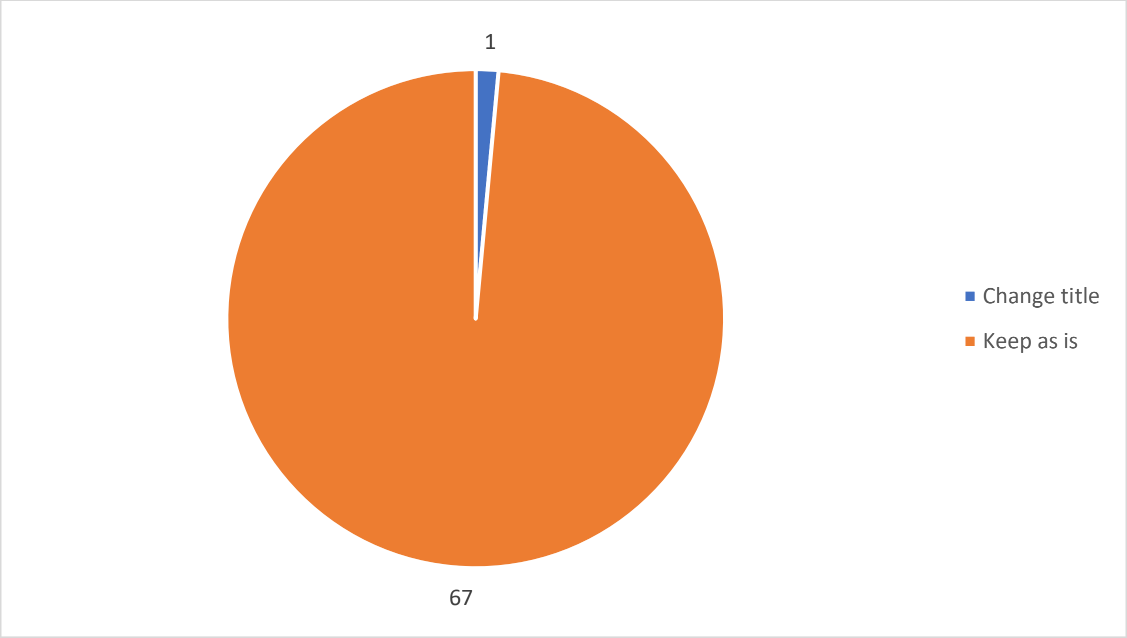


Figure 1 - Regulations and Guidance Recommendations

Row Labels	Regulations and Guidance Category Suggestions
Change title	1
Keep as is	67
Grand Total	**68**

III-2_2 Common Weaknesses

For Common Weaknesses, a total of 68 respondents completed the question. As shown in Figure 2, 65 respondents selected “keep as is” and three respondents suggested a change to the category name. No respondents suggested that the category be removed. The change suggestions were as follows:

Respondent ID	Response Content
R_2YX5Hjj1Z8JitHY	Common Weaknesses and CVE's
R_28HRVFlTwpY1Y9m	Historical Understanding of Vulnerabilities/What We Know/Suspect/Don't Know & Reporting Requirements & Need For Transparency
R_2WHW03nONpmCTMk	Common Vulnerabilities

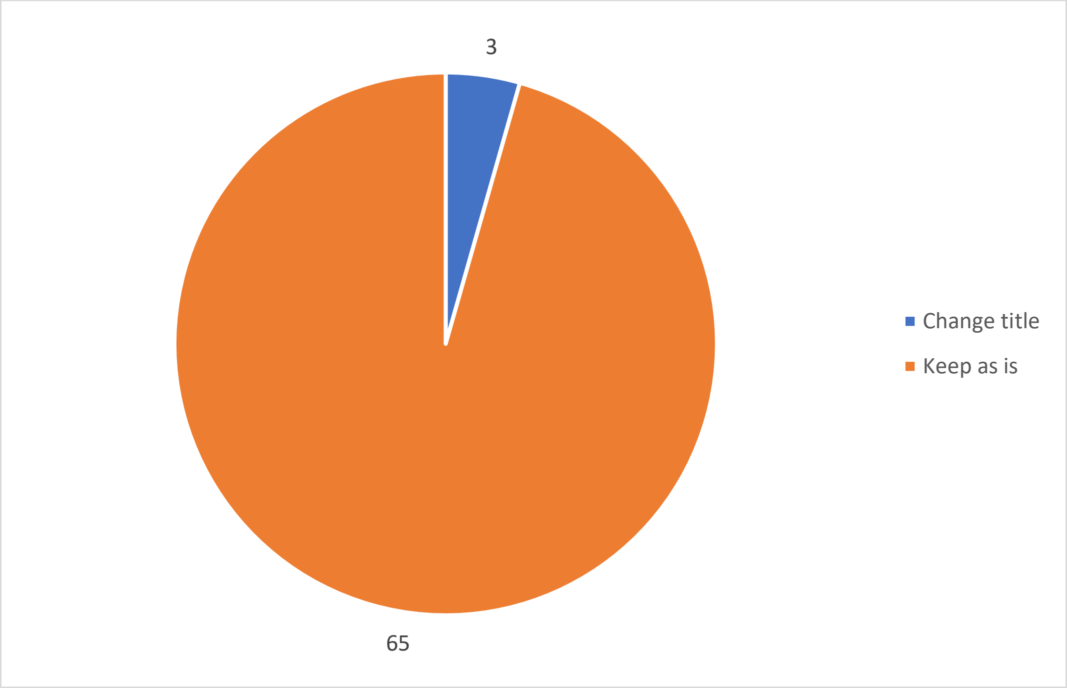


Figure 2 - Common Weaknesses Recommendations

Row Labels	Common Weaknesses Category Suggestions
Change title	3
Keep as is	65
Grand Total	**68**

Table of Contents

III-2_3 Events and Incidents

For Events and Incidents, a total of 68 survey respondents answered the question. As shown in Figure 3, 68 respondents selected “keep as is” and two respondents suggested a title change. No respondents suggested that the category be removed. The change suggestions were as follows:

Respondent ID	Response Content
R_2YX5Hjj1Z8JitHY	CVE's, Events and Incidents
R_28HRVFlTwpY1Y9m	A Catalog of Significant Cybersecurity Events/Ramifications/Lessons Learned & Industry Adjustments Taken

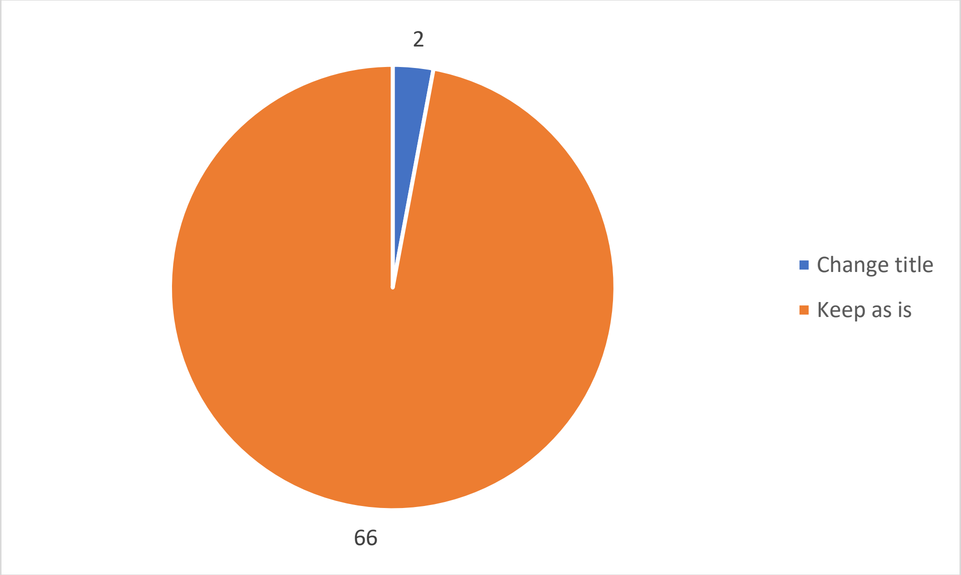


Figure 3 - Events and Incidents Recommendations

Row Labels	Events and Incidents Category Suggestions
Change title	2
Keep as is	66
Grand Total	**68**

III-2_4 Defensive Technologies and Approaches

For Defensive Technologies and Approaches, a total of 68 respondents provided a response. As shown in Figure 4, 66 respondents selected “Keep as is” and two respondents suggested a change to the category name. No respondents suggested that the category be removed. The change suggestions were as follows:

Respondent ID	Response Content
R_2Su9412OXG578E9	Defensive technologies and Risk Informed Deployment
R_2WHW03nONpmCTMk	ICS Hardening and Monitoring

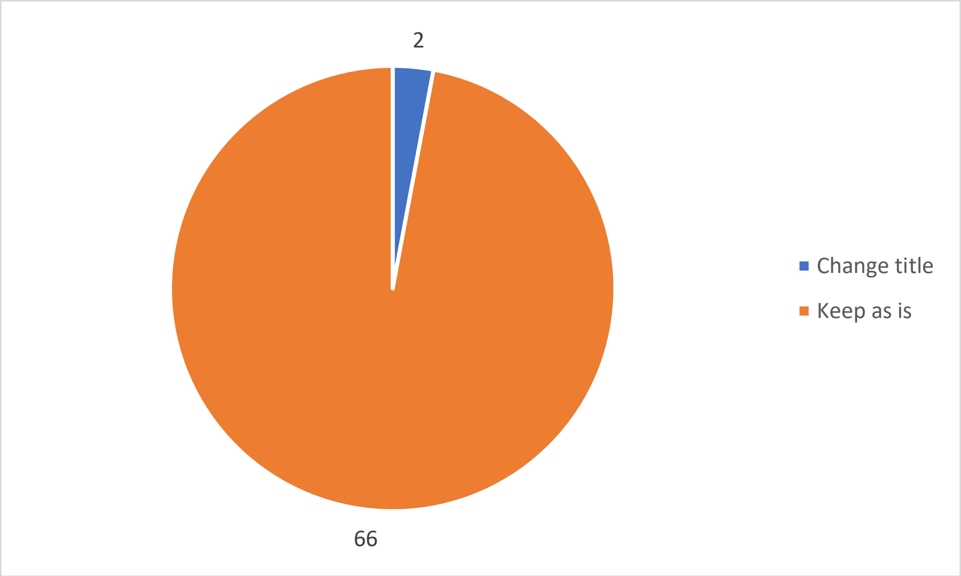


Figure 4 - Defensive Technologies Recommendations

Row Labels	Defensive Technologies - Category Suggestions
Change title	2
Keep as is	66
Grand Total	**68**

III-3 Additional Categories

Respondents were also asked to suggest additional core categories. 14 respondents suggested a total of 23 additional categories.

Respondent ID	**Response Content**
R_2YX5Hjj1Z8JitHY	Additions based upon survey results showing deficiencies
R_2YsHBQvCLvWLRjo	Historical and legacy aspects of ICS
R_2YsHBQvCLvWLRjo	Security Risk Management
R_2YsHBQvCLvWLRjo	Security vs Compliance
R_2YsHBQvCLvWLRjo	ICS Security Tools
R_XTVNiQSzyaZNSzn	Continual update
R_2Squ4P2NtTznJ4a	Quantitative Risk Assessments/Metrics
R_RqVMBWhBtfTdYrf	Secure Design and Integration
R_RqVMBWhBtfTdYrf	Secure PLC Coding Practices
R_3EaM9vGMjuCCcuf	Risk
R_2Su9412OXG578E9	Procurement Strategies
R_2AX45Pxy89BCTuf`	Futureproofing ICS
R_3kMMhb0mj6S80wG	Password and credentials
R_3kMMhb0mj6S80wG	Change control
R_3kMMhb0mj6S80wG	Lifecycle management
R_3kMMhb0mj6S80wG	Remote access and support
R_3kMMhb0mj6S80wG	Configuration management
R_3kMMhb0mj6S80wG	Backups
R_28HRVFlTwpY1Y9m	The Aurora Test/Experiment/Demonstration & What/Where/Why & How It Was Done
R_28HRVFlTwpY1Y9m	Nexus of Cybersecurity in Commercial/Industrial/Institutional/Transportation & Healthcare
R_1HduUVDzYT3QuFp	Production Loss
R_1rGFDHuFhnB2AQB	feels like we are missing something here but can't put my finger on it at this time.
R_Qh4JJ9Sl3FTmiWZ	Nuclear

The data analysis teams grouped the responses into the following high level categories which could be used as additional categories based on the feedback from the COP. Responses that fall into the “Other” category were recorded for completeness, but were not used in the development of categories. The responses were grouped by the data analysis team as follows:

- Risk
    - Security Risk Management (R_2YsHBQvCLvWLRjo)
    - Quantitative Risk Assessments/Metrics (R_2Squ4P2NtTznJ4a)
    - Risk (R_3EaM9vGMjuCCcuf)
- Procurement and Configuration Control
    - Procurement Strategies (R_2Su9412OXG578E9)
    - Futureproofing ICS (R_2AX45Pxy89BCTuf)
    - Change control (R_3kMMhb0mj6S80wG)
    - Lifecycle management (R_3kMMhb0mj6S80wG)
    - Configuration management (R_3kMMhb0mj6S80wG)
    - Continual update (R_XTVNiQSzyaZNSzn)

    - Backups (R_3kMMhb0mj6S80wG)
- Security and Compliance
    - Security vs Compliance (R_2YsHBQvCLvWLRjo)
    - ICS Security Tools (R_2YsHBQvCLvWLRjo)
    - Secure Design and Integration (R_RqVMBWhBtfTdYrf)
    - Secure PLC Coding Practices (R_RqVMBWhBtfTdYrf)
    - Password and credentials (R_3kMMhb0mj6S80wG)
    - Remote access and support (R_3kMMhb0mj6S80wG)
- History and Context
    - Historical and legacy aspects of ICS (R_2YsHBQvCLvWLRjo)
    - The Aurora Test/Experiment/Demonstration & What/Where/Why & How It Was Done (R_28HRVFlTwpY1Y9m)
    - Nexus of Cybersecurity in Commercial/Industrial/Institutional/Transportation & Healthcare (R_28HRVFlTwpY1Y9m)
    - Nuclear (R_Qh4JJ9Sl3FTmiWZ)
- Production Control
    - Production Loss (R_1HduUVDzYT3QuFp)
- Other
    - Additions based upon survey results showing deficiencies (R_2YX5Hjj1Z8JitHY)
    - feels like we are missing something here but can't put my finger on it at this time. (R_1rGFDHuFhnB2AQB)

III-5 Regulation and Guidance

This section expands on the Regulations and Guidance knowledge area. The Regulations and Guidance questions asked respondents to rank the importance of specific regulations that might be relevant to the knowledge area and should be included as a topic in a proposed cybersecurity framework. Respondents were asked to rank the importance of each specific regulation. Respondents also had the option to recommend a change to the title of the topic, or recommend removal of the topic.

Question III-5_1 ISA/IEC 62443

For ISA/IEC 624432, a total of 67 respondents provided a response. As shown in Figure 5, 65 respondents selected “Keep as is” and two respondents selected “Change topic name”. No respondents suggested that the topic be removed. The change suggestions is as follows:

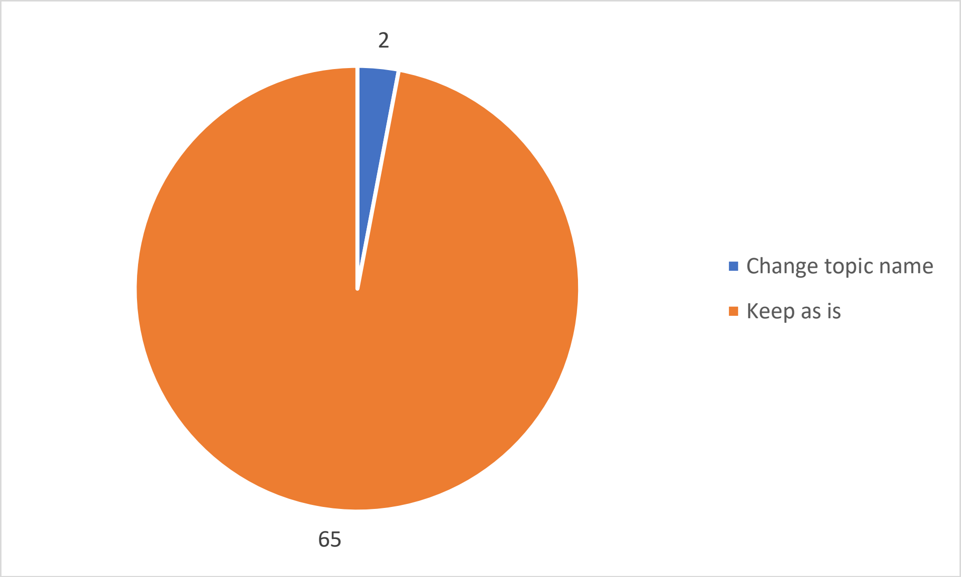


Figure 5 - ISA/IEC 62443 Suggestions

Row Labels	ISA/IEC 62443
Change topic name	2
Keep as is	65
Grand Total	**67**

Respondent ID	**Response Content**
R_3MQjCEJ5fsIuCBG	General Industry Standards

Respondent ID	**Response Content**
R_1rGFDHuFhnB2AQB	A little more context...let's not assume everyone knows what this is

III-5_2 Presidential Orders

For Presidential Orders, a total of 67 respondents provided a response. As shown in Figure 6, 61 respondents selected “Keep as is” and one respondent requested a change to the topic name. Five respondents requested that the topic be removed. The change suggestion is as follows:

Respondent ID	**Response Content**
R_3MQjCEJ5fsIuCBG	Governance, Compliance and Regulations

Justifications for removal are as follows:

Respondent ID	**Response Content**
R_2YsHBQvCLvWLRjo	This is a fleeting topic - the executive orders should be integrated within fundamental industry segment standards
R_RqVMBWhBtfTdYrf	only applies to government and rarely specific enough for ICS direct needs
R_1C7kv6fnDsy5HUO	Too US focused
R_1n87BSaF6YgOCbm	Do not have specific clarity
R_vZYehSwKucwalcF	Federal policy at the White House level is far removed from the plant floor and field sites; it may be interesting but not worth the opportunity cost in the curriculum

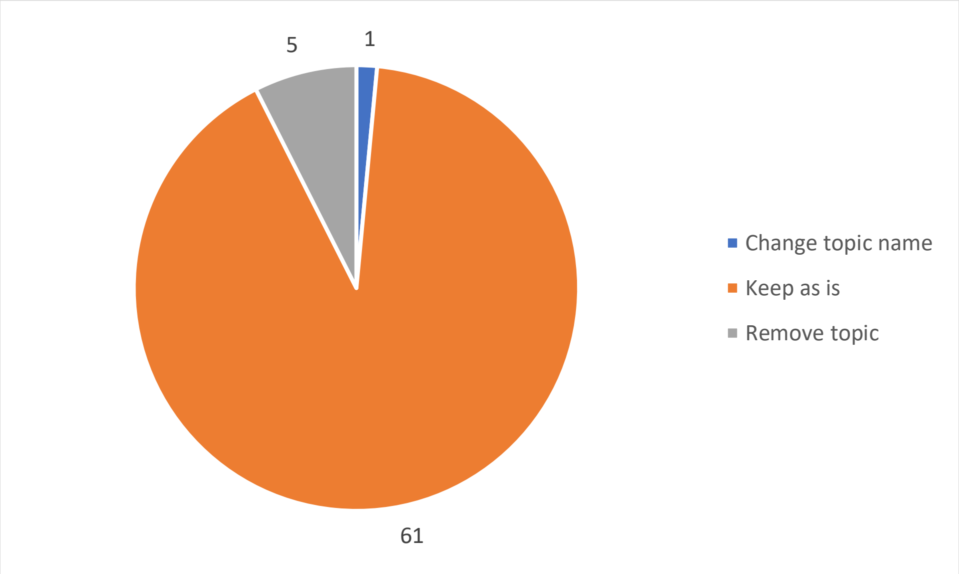


Figure 6 - Presidential Orders Recommendations

Row Labels	**Presidential Orders**
Change topic name	1
Keep as is	61
Remove topic	5
Grand Total	**67**

Table of Contents

III-5_3 NIST SP 800-82r2

For NIST SP 800-82r2, there were a total of 67 responses. As shown in Figure 7, 65 respondents selected “Keep as is” and two respondents requested a change to the topic name. No respondents suggested that the topic be removed. The change suggestion is as follows:

Respondent ID	Response Content
R_vZYehSwKucwaIcF	Voluntary recommendations and guidelines e.g. NIST SP 800-82r2

One respondent answered “same” (R_1rGFDHuFhnB2AQB) in their response. The data analysis team assumes that this was a correction to the request to change the topic name. No further clarification was provided.

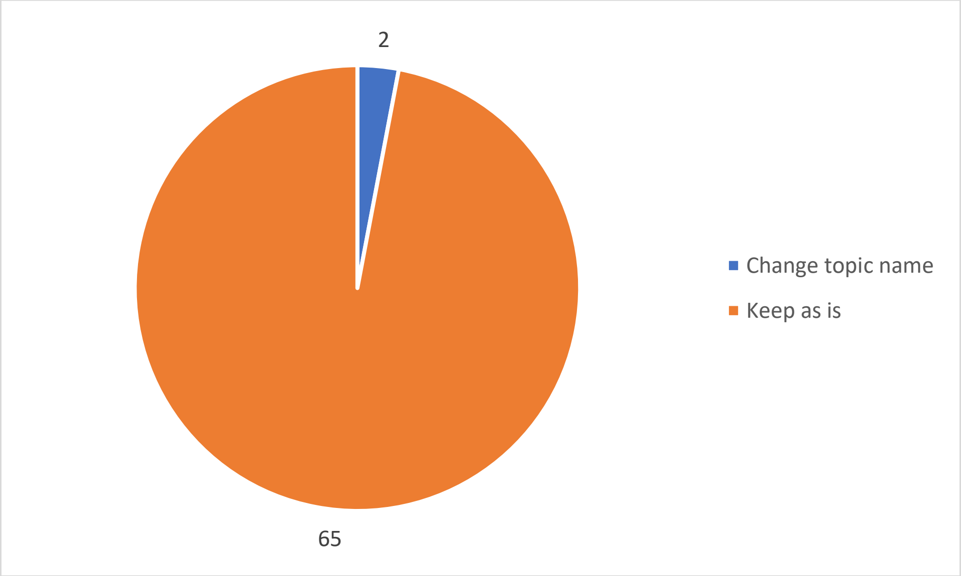


Figure 7 - NIST SP 800-82 Recommendations

Row Labels	NIST SP 800-82
Change topic name	2
Keep as is	65
Grand Total	**67**

III-5_4 NERC CIP

For NERC CIP, there were a total of 67 responses. As shown in Figure 8, 65 respondents selected “Keep as is” and two respondents requested a change to the topic name. No respondents suggested that the topic be removed. The change suggestion is as follows:

Respondent ID	**Response Content**
R_vZYehSwKucwaIcF	Mandatory standards e.g. NERC CIP

One respondent answered “same” (R_1rGFDHuFhnB2AQB) in their response. The data analysis team assumes that this was a correction to the request to change the topic name. No further clarification was provided.

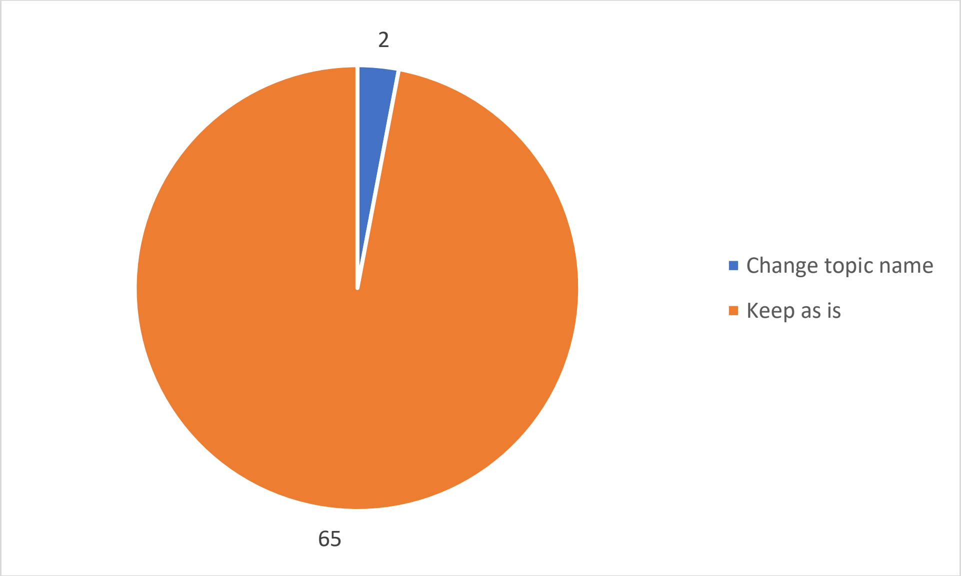


Figure 8 - NERC CIP Recommendations

Row Labels	**NERC CIP**
Change topic name	2
Keep as is	65
Grand Total	**67**

III-5_5 EU Cybersecurity Act

For EU Cybersecurity Act, there were a total of 67 responses. As shown in Figure 9, 64 respondents selected “Keep as is” and one respondent requested a change to the topic name. Two respondents suggested the topic be removed. The change suggestion is as follows:

Respondent ID	Response Content
R_3MQjCEJ5fsIuCBG	Merge with Governance, Compliance and Regulations

Justification for removals are as follows:

Respondent ID	Response Content
R_1C7kv6fnDsy5HUO	Too EU focused
R_yQjIaqY7oRRQNP	Not a US endorsed framework, and it does not specifically address Industrial Control environments.

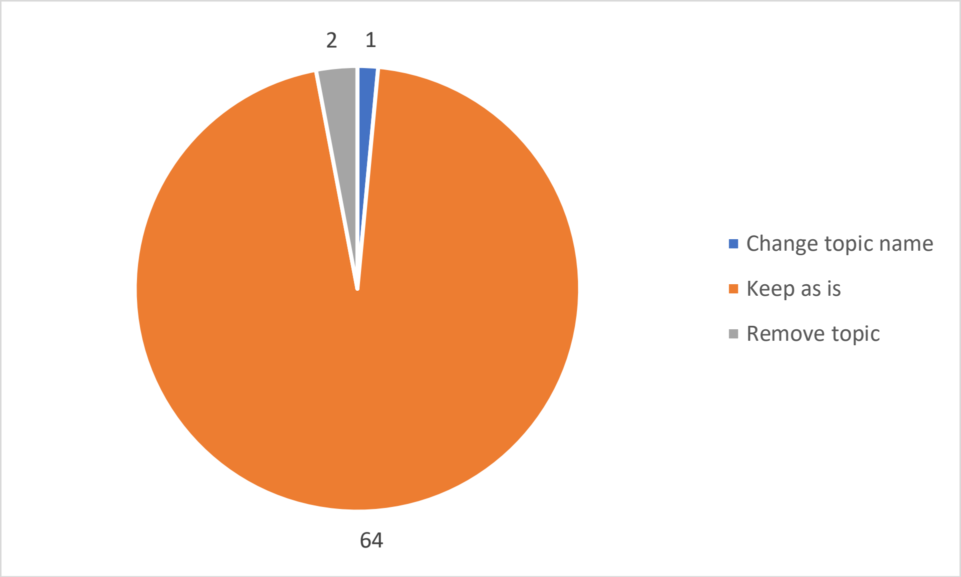


Figure 9 - EU Cybersecurity Act Recommendations

Row Labels	EU Cybersecurity Act
Change topic name	1
Keep as is	64
Remove topic	2
Grand Total	**67**

Table of Contents

III-6 Additional Topics for Regulations and Guidance

Respondents were also asked to suggest additional topics under the Regulations and Guidance knowledge area. Fourteen respondents suggested a total of twenty-three additional categories.

Respondent ID	Response Content
R_2YX5Hjj1Z8JitHY	Global / International Control Security Initiatives
R_27a3HBRQ60cNEsj	Sector Specific Guidance
R_26hX0Es8WVUZ3i0	Privacy Regulations
R_2Squ4P2NtTznJ4a	ISO 27000 (27001, 27002, 27005, 27019)
R_RqVMBWhBtfTdYrf	ISA84 security for safety systems
R_ekst6dSTefw2r85	AESCSF
R_1C7kv6fnDsy5HUO	Regulatory Frameworks
R_3MQjCEJ5fsIuCBG	Sector Specific Differences and Guidelines
R_2y7OAWWVwHpdUnP	NIST CSF
R_2y7OAWWVwHpdUnP	ISO 27019
R_2Su9412OXG578E9	common themes
R_2Su9412OXG578E9	10CFR73.54
R_2Su9412OXG578E9	FDA Cyber Guidelines
R_2Su9412OXG578E9	MHRA data Integrity
R_yQjIaqY7oRRQQNP	I would change the EU Cybersecurity Act to "Other Government requirement that are applicable"
R_1JLVvwwpCaXn84N	NDAA 1650
R_28HRVFlTwpY1Y9m	Adoption, Adherence, and Active Use of Standards in Your Company's Cybersecurity Mission, Organization
R_1rGFDHuFhnB2AQB	seems a bit limited.
R_Qh4JJ9Sl3FTmiWZ	CISA, blind trust

The data analysis team grouped the responses into the following topics. Responses that fall into the "Other" category were recorded for completeness, but were not used in the development of topics. The responses were grouped by the data analysis team as follows:

- ISO Standards
    - ISO 27000 (27001, 27002, 27005, 27019) (R_2Squ4P2NtTznJ4a)
    - ISO 27019 (R_2y7OAWWVwHpdUnP)
- Standards Bodies
    - ISA84 security for safety systems (R_RqVMBWhBtfTdYrf)
- Government Agencies
    - AESCSF (R_ekst6dSTefw2r85)
    - NIST CSF (R_2y7OAWWVwHpdUnP)
    - 10CFR73.54 (R_2Su9412OXG578E9)
    - MHRA data Integrity (R_2Su9412OXG578E9)
    - NDAA 1650 (R_1JLVvwwpCaXn84N)
- General
    - Adoption, Adherence, and Active Use of Standards in Your Company's Cybersecurity Mission, Organization (R_28HRVFlTwpY1Y9m)

  - I would change the EU Cybersecurity Act to "Other Government requirement that are applicable" (R_yQjIaqY7oRRQQNP)
  - Regulatory Frameworks (R_1C7kv6fnDsy5HUO)
  - Sector Specific Differences and Guidelines (R_3MQjCEJ5fsIuCBG)
  - Sector Specific Guidance (R_27a3HBRQ60cNEsj)
  - Privacy Regulations (GPDR, PCI, etc) (R_26hX0Es8WVUZ3i0)
  - Global / International Control Security Initiatives (R_2YX5Hjj1Z8JitHY)
  - FDA Cyber Guidelines (R_2Su9412OXG578E9)
- Other
  - CISA, blind trust (R_Qh4JJ9Sl3FTmiWZ)
  - seems a bit limited. (R_1rGFDHuFhnB2AQB)
  - common themes (R_2Su9412OXG578E9)

Table of Contents

III-7 Common Weaknesses

This section expands on the Common Weaknesses knowledge area. The Common Weaknesses questions asked respondents to rank the importance of specific common ICS vulnerabilities that might be relevant to the knowledge area and should be included as a topic in a proposed cybersecurity framework. Respondents were asked to rank the importance of each specific common weakness. Respondents also had the option to recommend a change to the title of the topic, or recommend removal of the topic.

III-7_1 Indefensible Network Architectures

For Indefensible Network Architectures, all 65 respondents suggested that the topic should be kept as currently documented.

III-7_2 Unauthenticated Protocols

For Unauthenticated Protocols, there were a total of 66 responses. As shown in Figure 10, 64 respondents selected “Keep as is and two respondents requested a change to the topic name. No respondents suggested that the topic be removed. The change suggestions are as follows:

Respondent ID	**Response Content**
R_8ugyg2V7BXUQEr7	Unauthenticated network protocols
R_vZYehSwKucwaIcF	Insecure and Unsecured Protocols

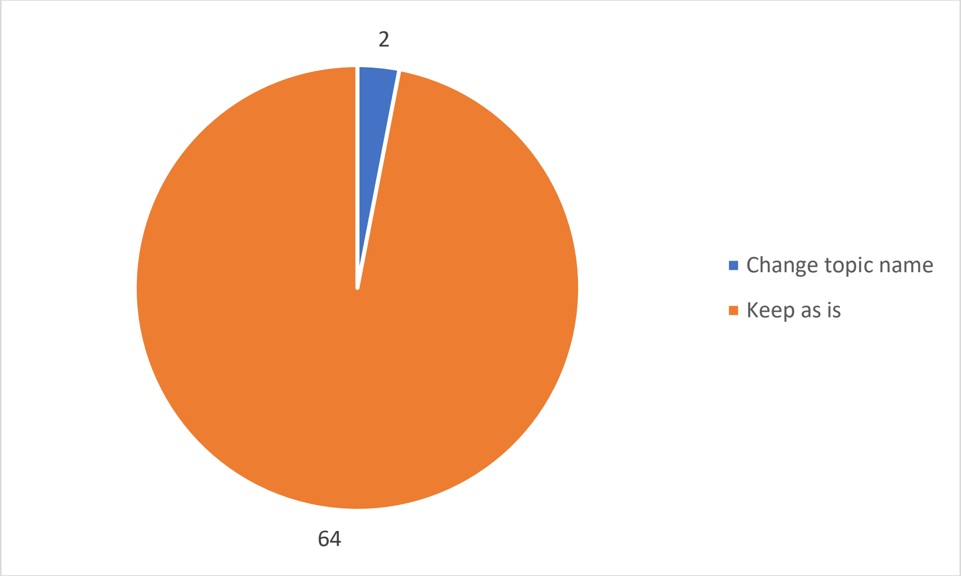


Figure 10 - Unauthenticated Protocols Recommendations

Row Labels	Unauthenticated Protocols
Change topic name	2
Keep as is	64
Grand Total	**66**

III-7_3 Unpatched and outdated systems

For Unpatched Systems, all 66 respondents suggested that the topic should be kept as currently documented.

Table of Contents

III-7_4 Lack of training

For Lack of Training, there were a total of 64 responses. As shown in Figure 11, 60 respondents selected "Keep as is", and two respondents requested a change to the topic name. One respondent suggested that the topic be removed. The change suggestions are as follows:

Respondent ID	**Response Content**
R_2YsHBQvCLvWLRjo	Security Training and Awareness
R_yQjIaqY7oRRQQNP	Lack of "Cybersecurity" training

The justification for removal is:

Respondent ID	**Response Content**
R_1C7kv6fnDsy5HUO	Small subject area could be covered elsewhere

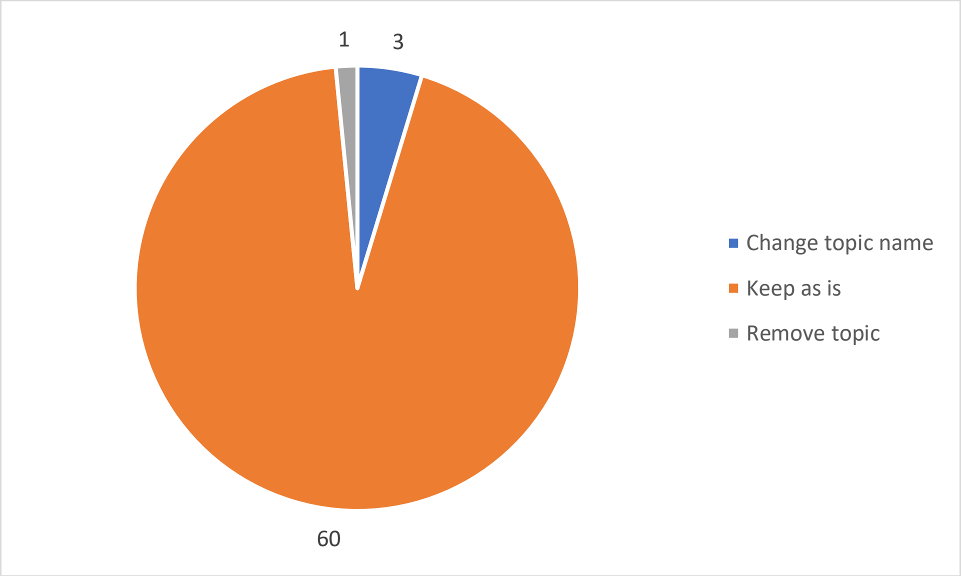


Figure 11 - Lack of Training Recommendations

Row Labels	**Lack of Training**
Change topic name	3
Keep as is	60
Remove topic	1
Grand Total	**64**

III-7_5 Transient devices

For Transient Devices, there were a total of 66 responses. As shown in Figure 12, 63 respondents selected “Keep as is” and three respondents requested a change to the topic name. No respondents suggested that the topic be removed. The change suggestions are as follows:

Respondent ID	**Response Content**
R_vZYehSwKucwaIcF	Poorly managed transient devices (as originally worded it's an asset not a weakness)
R_28HRVFlTwpY1Y9m	Transient Cyber Asset (TCA) as a function of NERC-CIP
R_2WHW03nONpmCTMk	Temporary Nodes

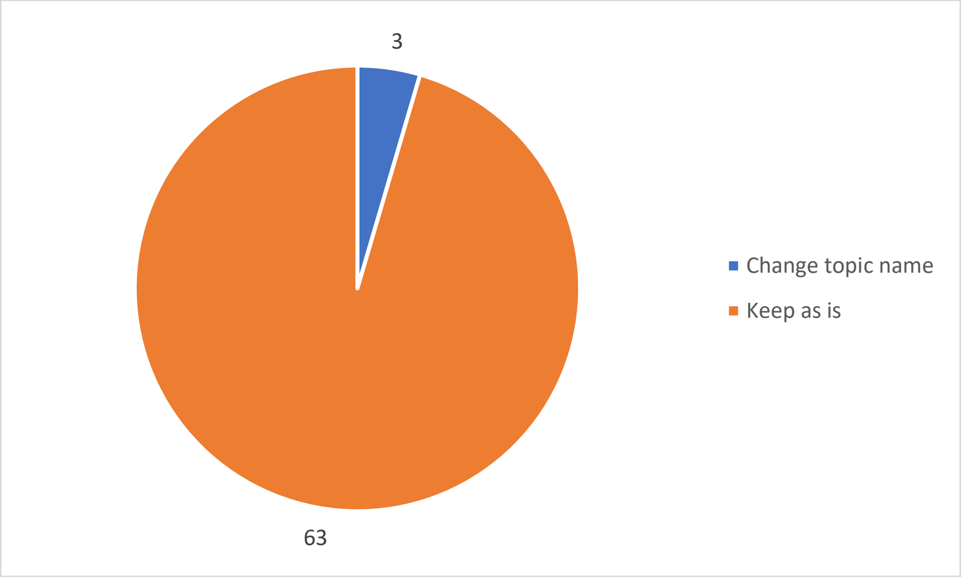


Figure 12 - Transient Devices Recommendations

Row Labels	**Transient Devices**
Change topic name	3
Keep as is	63
Grand Total	**66**

Table of Contents

III-7_6 Third Party Access

For Third Party Access, three respondents requested a change to the topic name. No respondents suggested that the topic be removed. The change suggestions are as follows:

Respondent ID	**Response Content**
R_3MQjCEJ5fsIuCBG	Required and optional access by third parties
R_vZYehSwKucwaIcF	Poorly managed third-party access (as originally worded it's an operational business process not a weakness)
R_2WHW03nONpmCTMk	External Access Control

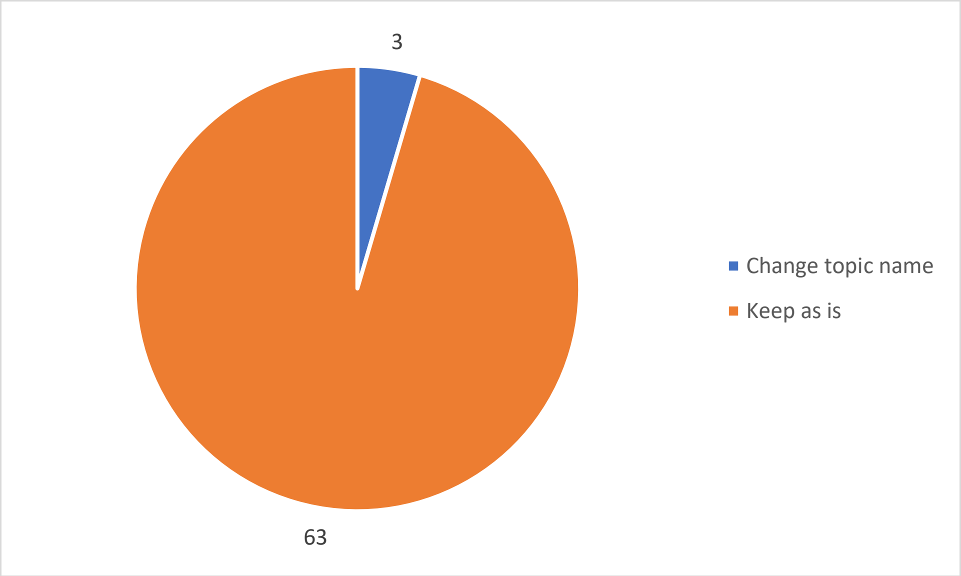


Figure 13 - Third Party Device Recommendations

Row Labels	**Third Party Devices**
Change topic name	3
Keep as is	63
Grand Total	**66**

Table of Contents

III-7_7 Supply Chain

For Supply Chain, there were a total of 65 responses. As shown in Figure 14, 60 respondents selected "Keep as is" andthree respondents requested a change to the topic name. Two respondents suggested that the topic be removed. The change suggestions are as follows:

Respondent ID	Response Content
R_2YsHBQvCLvWLRjo	Supply Chain Management Implications
R_1C7kv6fnDsy5HUO	Supply Chain
R_vZYehSwKucwaIcF	Lack of transparency in acquired software and hardware

The justification for removals are as follows:

Respondent ID	Response Content
R_2Su9412OXG578E9	merge with Procurement techniques category
R_2WHW03nONpmCTMk	Irrelevant for asset owners

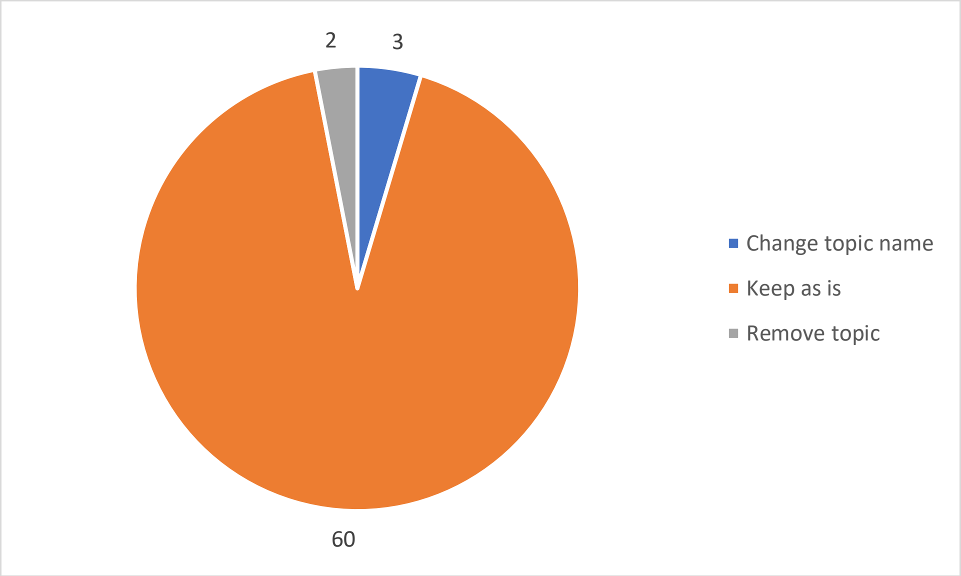


Figure 14 - Supply Chain Recommendations

Row Labels	Supply Chain
Change topic name	3
Keep as is	60
Remove topic	2
Grand Total	**65**

III-9 Additional topics for common weaknesses

Respondents were also asked to suggest additional topics under the Common Weaknesses knowledge area. Thirteen respondents suggested a total of twenty-five additional categories.

Respondent ID	**Response Content**
R_2YX5Hjj1Z8JitHY	Deterministic Protocols - why and when they are used,
R_5c0uAAMSNWyojMB	Lack of Signed Software
R_5c0uAAMSNWyojMB	Unauthenticated Logins
R_5c0uAAMSNWyojMB	Weak Software Integrity Mechanisms
R_27a3HBRQ60cNEsj	Weak Access Control
R_27a3HBRQ60cNEsj	No Least Privilege
R_27a3HBRQ60cNEsj	Lack of Monitoring (SIEM, IDS, IPS)
R_27a3HBRQ60cNEsj	Lack of OT Cybersecurity Program
R_2YsHBQvCLvWLRjo	OEM Limitations
R_2YsHBQvCLvWLRjo	ICS lifecycle impacts to security
R_VJBb9QiRZiR3xC1	System Backup (DR)
R_VJBb9QiRZiR3xC1	File Transfer
R_2Squ4P2NtTznJ4a	Sensor Integrity/calibration/alignment
R_RqVMBWhBtfTdYrf	Secure PLC Coding practices
R_2Su9412OXG578E9	Design Control
R_2AX45Pxy89BCTuf	Network perimeter security
R_yQjIaqY7oRRQQNP	Complacency, Lack of Business Resumption plans and testing,
R_vZYehSwKucwaIcF	Lack of budget and resources
R_vZYehSwKucwaIcF	Available but unused logging and forensics-friendly capabilities
R_vZYehSwKucwaIcF	Lack of available baseline data
R_3kMMhb0mj6S80wG	4th party risk
R_28HRVFlTwpY1Y9m	Vulnerabilities
R_28HRVFlTwpY1Y9m	Domain & Subdomain openings
R_28HRVFlTwpY1Y9m	horizontal/flat architectures
R_28HRVFlTwpY1Y9m	inept cybersecurity plan/methodologies/inadequate defenses

The data analysis team grouped the responses into the following topics. The responses were grouped by the data analysis team as follows:

- Signed Software
    - Lack of Signed Software (R_5c0uAAMSNWyojMB)
    - Weak Software Integrity Mechanisms (R_5c0uAAMSNWyojMB)
- Programmatic Vulnerabilities
    - Lack of OT Cybersecurity Program (R_27a3HBRQ60cNEsj)
    - Complacency, Lack of Business Resumption plans and testing, (R_yQjIaqY7oRRQQNP)
    - Inept cybersecurity plan/methodologies/inadequate defenses (R_28HRVFlTwpY1Y9m)
    - Lack of budget and resources (R_vZYehSwKucwaIcF)
- Unauthenticated or Weak Access
    - Unauthenticated Logins (R_5c0uAAMSNWyojMB)
    - Weak Access Control (R_27a3HBRQ60cNEsj)
- Poor System Design
    - Secure PLC Coding practices (R_RqVMBWhBtfTdYrf)
    - Design Control (R_2Su9412OXG578E9)

  - Horizontal/flat architectures (R_28HRVFlTwpY1Y9m)
  - Deterministic Protocols - why and when they are used, (R_2YX5Hjj1Z8JitHY)
  - No Least Privilege (R_27a3HBRQ60cNEsj)
  - Available but unused logging and forensics-friendly capabilities (R_vZYehSwKucwaIcF)
  - Lack of available baseline data (R_vZYehSwKucwaIcF)
  - Lack of Monitoring (SIEM, IDS, IPS) (R_27a3HBRQ60cNEsj)
  - File Transfer (R_VJBb9QiRZiR3xC1)
- Device Limitations
  - OEM Limitations (R_2YsHBQvCLvWLRjo)
  - Sensor Integrity/calibration/alignment (R_2Squ4P2NtTznJ4a)
- Configuration Management
  - ICS lifecycle impacts to security (R_2YsHBQvCLvWLRjo)
  - System Backup (DR) (R_VJBb9QiRZiR3xC1)
  - Domain & Subdomain openings (R_28HRVFlTwpY1Y9m)
  - 4th party risk (R_3kMMhb0mj6S80wG)
- Network perimeter security (R_2AX45Pxy89BCTuf)
- Vulnerabilities (R_28HRVFlTwpY1Y9m)

Table of Contents

Question III-10 Events and Incidents Category

This section expands on the Events and Incidents knowledge area. The Events and Incidents questions asked respondents to rank the importance of specific well known ICS focused cybersecurity incidents, both for demonstration purposes and malicious attacks, that might be relevant to the knowledge area and should be included as a topic in a proposed cybersecurity framework. Respondents were asked to rank the importance of each specific event or incident. Respondents also had the option to recommend a change to the title of the topic, or recommend removal of the topic.

The majority of respondents (61 of the total 64) selected “keep as is” for all events . Two respondents provided alternate titles for all events. The alternate titles are primarily expansions on the current title made for clarity.

The suggested title changes by respondent R_28HRVFlTwpY1Y9m are as follows:

Respondent ID	**Response Content**
R_28HRVFlTwpY1Y9m	DHS Aurora - Aurora Demonstration of codeless intrusion and impact to critical infrastructure
R_28HRVFlTwpY1Y9m	Stuxnet - Stuxnet Nation-State Cybersecurity Event That Damaged Equipment
R_28HRVFlTwpY1Y9m	Ukraine 2015 - Nation-State Cybersecurity Capture of Electrical Network in Ukraine in 2015
R_28HRVFlTwpY1Y9m	Ukraine 2016 - Nation-State 2016 Cybersecurity Re-Capture Due to Inadequate Recovery from 2015 Incident
R_28HRVFlTwpY1Y9m	Triton - Triton: Malware impact on an ICS Safety Instrumented Systems (SIS)
R_28HRVFlTwpY1Y9m	Taum Sauk Dam - Taum Sauk Dam Critical Infrastructure Failure Due to "Bad" Level Sensor Reporting
R_28HRVFlTwpY1Y9m	DC Metro Red Line - Critical Infrastructure Incident in Transportation that looked like a Cyber Incident
R_28HRVFlTwpY1Y9m	San Bruno - San Bruno Gas Pipeline incident - Pressure Sensor Failure
R_28HRVFlTwpY1Y9m	Colonial Pipeline - Colonial Pipeline - Voluntary Shutdown When a Company doesn't trust their Cybersecurity Defense Posture

The suggested title changes by respondent R_vZYehSwKucwaIcF are as follows:

Respondent ID	**Response Content**
R_vZYehSwKucwaIcF	DHS Aurora generator testing
R_vZYehSwKucwaIcF	Stuxnet Iranian centrifuge attack
R_vZYehSwKucwaIcF	2015 Ukraine electric distribution attacks
R_vZYehSwKucwaIcF	2016 Ukraine electric transmission attack
R_vZYehSwKucwaIcF	Triton/TRISIS refinery SIS attacks
R_vZYehSwKucwaIcF	Taum Sauk Dam failure
R_vZYehSwKucwaIcF	DC Metro Red Line crash
R_vZYehSwKucwaIcF	San Bruno gas pipeline failure
R_vZYehSwKucwaIcF	Colonial Pipeline IT ransomware attack

One respondent suggested removing three specific events with the following justifications(R_XTVNiQSzyaZNSzn):

Table of Contents

Respondent ID	Response Content
R_XTVNiQSzyaZNSzn	Taum Sauk Dam - Poor design, installation, not cyber related
R_XTVNiQSzyaZNSzn	DC Metro Red Line - Poor maintenance, not cyber related (could have provided attack)
R_XTVNiQSzyaZNSzn	San Bruno - Poor maintenance, documentation, not cyber related (offered attack surface)

Row Labels	DHS Aurora
Change topic name	2
Keep as is	61
Remove topic	1
Grand Total	**64**

Table of Contents

III-12 additional topics in events and incidents

Respondents were also asked to suggest additional topics under the Events and Incidents knowledge area. Seven respondents suggested specific events as listed below. Five additional respondents provided general suggestions about the organization and structure of the specific topics. The responses are as follows:

Respondent ID	**Response Content**
R_27a3HBRQ60cNEsj	NotPetya 2017 (global OT effects), Oldsmar/Ellsworth (shows long-term issue even after publicity)
R_3njf722UBVndAP8	Norsk Hydro
R_XTVNiQSzyaZNSzn	Ukraine NotPetya 2017 escalation from a taxation attack to shipping, pipeline, chocolate factory, server supplies
R_yQjIaqY7oRRQQNP	German Steel Mill Incident 2014
R_1JLVvwwpCaXn84N	2015 Jeep Hack, 2018 Ukraine Power Grid, 2021 Florida Wastewater Treatment Facility
R_Qh4JJ9Sl3FTmiWZ	SolarWinds-for the third party access and blind trust aspects
R_274qf7ZvI8Uo4YW	Oldsmar, FL
General Suggestions	
R_2YX5Hjj1Z8JitHY	Known Attacks: IT or Control System or both?
R_2YsHBQvCLvWLRjo	Internal vs External / Deliberate vs Accidental
R_RqVMBWhBtfTdYrf	Water, Maritime, Manufacturing
R_3MQjCEJ5fsIuCBG	Instead of individual attack names, categories (insecure remote access, insider threat etc.) for all categories
R_3kMMhb0mj6S80wG	OT Security Operations Center (SOC), Contingency and IR Plans

Table of Contents

III-13 Defensive Technologies Category

This section expands on the Defensive Technologies knowledge area. The Defensive Technologies questions asked respondents to rank the importance of ICS focused defensive technologies that might be relevant to the knowledge area and should be included as a topic in a proposed cybersecurity framework. Respondents were asked to rank the importance of each specific defensive technology. Respondents also had the option to recommend a change to the title of the topic, or recommend removal of the topic.

Table of Contents

III-13_1 Industrial Network Firewalls

For Industrial Network Firewalls, there were a total of 65 responses. As shown in Figure 15, 64 respondents selected “Keep as is” and one respondent suggested a topic name change. The change suggestion is as follows:

Respondent ID	Response Content
R_2YsHBQvCLvWLRjo	Industrial Networking Technologies

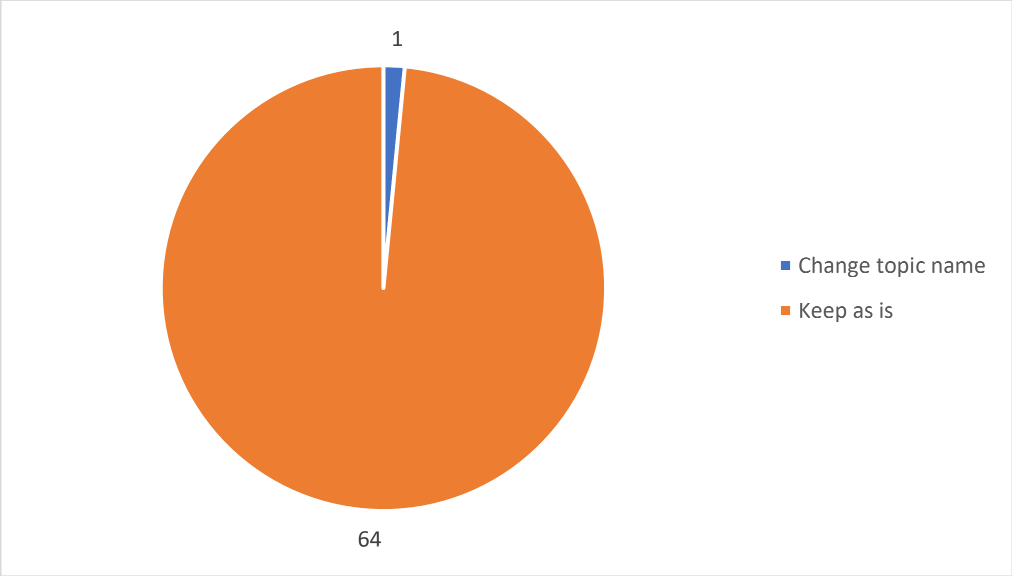


Figure 15 - Industrial Network Firewalls Recommendations

Row Labels	Count of Industrial network firewalls
Change topic name	1
Keep as is	64
Grand Total	**65**

Table of Contents

III-13_2 Data diodes

For Data Diodes, there were a total of 65 responses. As shown in Figure 16, 61 respondents selected "Keep as is" and one respondent suggested a topic name change. Three respondents suggested that the topic be removed. The change suggestion is as follows:

Respondent ID	Response Content
R_1eUD8SM0184KR6B	Specialty Firewall Appliances

Justifications for removals are as follows:

Respondent ID	Response Content
R_RqVMBWhBtfTdYrf	Limited useful use cases in bidirectional production environments and has not ability to inspect and filter ICS protocol commands being forwarded across diode
R_1rGFDHuFhnB2AQB	These are useless and cost prohibitive. They are the new "air gap" Why is this single technology called out as its own technology? Seems like influence from corprations
R_2WHW03nONpmCTMk	This should be combined with the Industrial Firewalls since the category is network traffic control

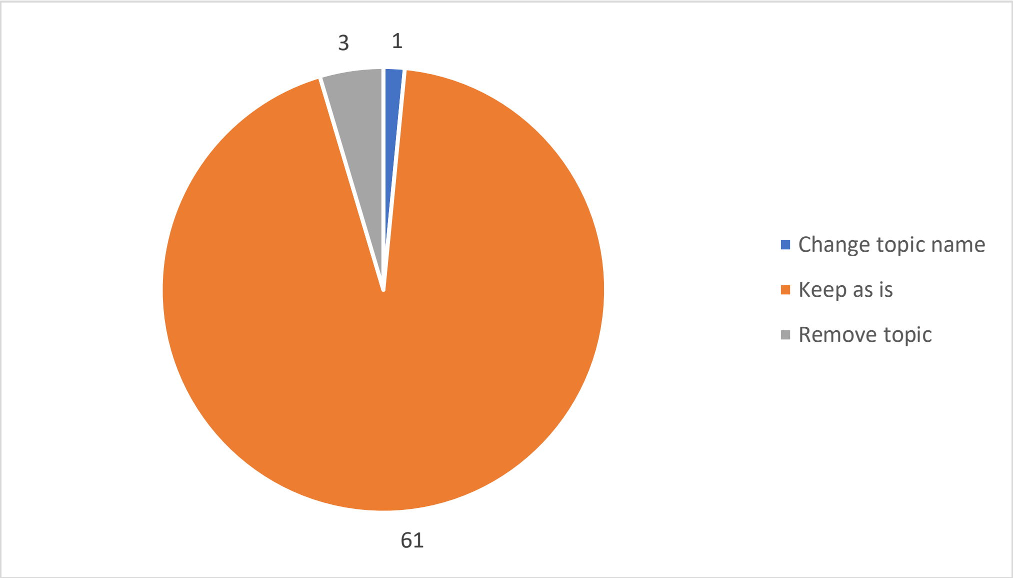


Figure 16 - Data Diodes Recommendations

Row Labels	Count of Data diodes
Change topic name	1
Keep as is	61
Remove topic	3
Grand Total	**65**

Table of Contents

III-13_3 Process data analysis

For Process Data Analysis, there were a total of 65 responses. As shown in Figure 17, 62 respondents selected "Keep as is" and two respondents suggested a topic name change. One respondent suggested that the topic be removed. The change suggestions are as follows:

Respondent ID	Response Content
R_VJBb9QiRZiR3xC1	Security Data Analysis
R_3MQjCEJ5fsIuCBG	Process Data Correlation and Analytics

The justification for removal is as follows:

Respondent ID	Response Content
R_2WHW03nONpmCTMk	Irrelevant for cybersecurity. Process and control engineers are monitoring the process 24/7

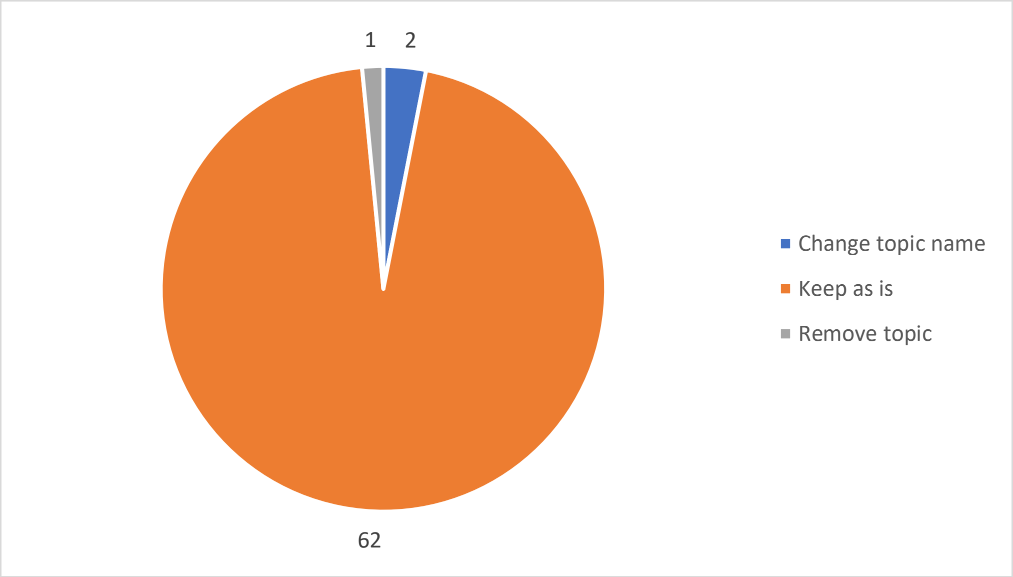


Figure 17 - Process Data Analysis Recommendations

Row Labels	**Count of Process data analysis**
Change topic name	2
Keep as is	62
Remove topic	1
Grand Total	**65**

III-13_4 ICS network monitoring

For ICS Network Monitoring, all 65 respondents suggested that the topic should be kept as documented.

Table of Contents

III-13_5 Cyber Informed engineering

For Cyber Informed Engineering, all 64 respondents suggested that the topic should be kept as documented.

Table of Contents

III-13_6 Process hazards assessment-based approaches

For Process Hazards and Assessment Based Approaches, there were a total of 64 responses. As shown in Figure 18, 63 respondents selected “Keep as is” and one respondent suggested that the topic be removed. The justification for removal is as follows:

Respondent ID	Response Content
R_2WHW03nONpmCTMk	Irrelevant for cybersecurity

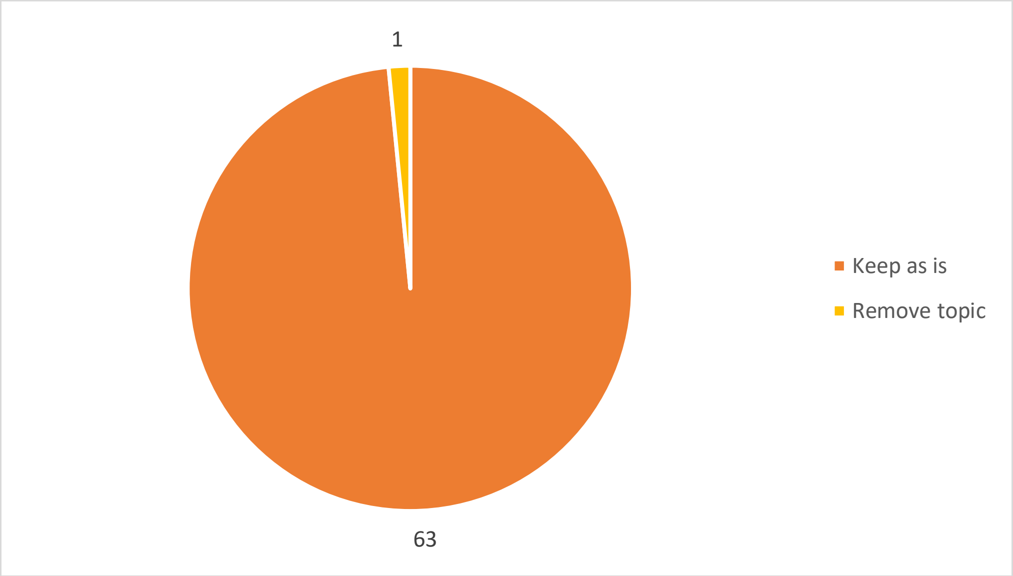


Figure 18 - Process Hazards and Assessment Based Approaches Recommendations

Row Labels	Count of Process hazards assessment-based approaches
Keep as is	63
Remove topic	1
Grand Total	**64**

Table of Contents

III-13_7 Cyber-physical fail-safes

For Cyber Physical Failsafes, there were a total of 64 responses. As shown in Figure 19, 61 respondents selected “Keep as is” and three respondents suggested that the topic be removed. The justification for removal is as follows:

Respondent ID	Response Content
R_1C7kv6fnDsy5HUO	Could be covered in other areas
R_3lMl6Hi3p0cr1K4	The term is confusing
R_2WHW03nONpmCTMk	There is no such thing as cyber-physical that hasn't been reviewed during a process hazard analysis.

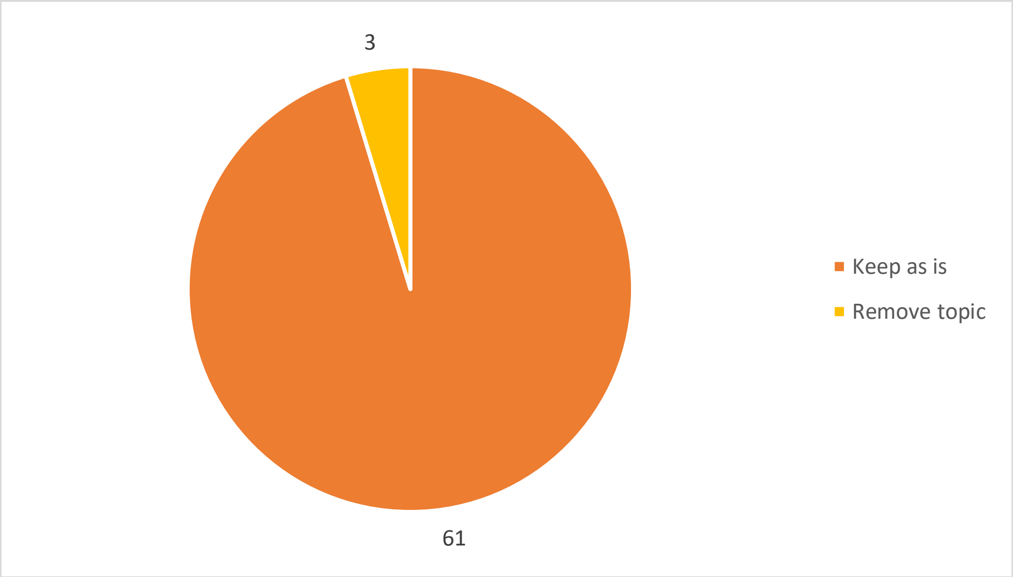


Figure 19 - Cyber Physical Failsafes Recommendations

Row Labels	Count of Cyber-physical fail-safes
Keep as is	61
Remove topic	3
Grand Total	**64**

III-13_8 Awareness and training for ICS-related personnel

For Awareness and training for ICS-related personnel, all 64 respondents suggested that the topic be kept as documented.

Table of Contents

III-15 Additional Defensive Technologies and Approaches

Respondents were also asked to suggest additional topics under the Defensive Technologies knowledge area. Nine respondents suggested a total of twenty additional categories.

Respondent ID	Response Content
R_2YX5Hjj1Z8JitHY	Failsafe vs fail secure: The RISK paradigm
R_5c0uAAMSNWyojMB	Code Signing
R_27a3HBRQ60cNEsj	Active Defense (IPS, Deception, Quarantine, Honeypots, etc.)
R_27a3HBRQ60cNEsj	Managed Services in OT/ICS
R_27a3HBRQ60cNEsj	Incident Response in OT/ICS
R_3lMl6Hi3p0cr1K4	PLC Secure Coding practices
R_3lMl6Hi3p0cr1K4	memory protection
R_RqVMBWhBtfTdYrf	BOM
R_3lMl6Hi3p0cr1K4	Audits
R_2Su9412OXG578E9	Defense-in-depth concept
R_2Su9412OXG578E9	end user awareness training
R_2Su9412OXG578E9	physical separation
R_2Su9412OXG578E9	functional segmentation
R_3kMMhb0mj6S80wG	Asset Management
R_3kMMhb0mj6S80wG	Configuration Management
R_3kMMhb0mj6S80wG	IoT protection
R_3kMMhb0mj6S80wG	Segmentation
R_3kMMhb0mj6S80wG	physical security
R_28HRVFlTwpY1Y9m	Methodologies for monitoring, detecting/alarming on devices/subsystems & operations of legacy systems with little to no cyber posture.
R_1rGFDHuFhnB2AQB	again, not enough time

The data analysis team grouped the responses into the following topics. Responses that fall into the "Other" category were recorded for completeness, but were not used in the development of topics. The responses were grouped by the data analysis team as follows:

- ICS Protection Processes
    - Audits (R_3lMl6Hi3p0cr1K4)
    - Incident Response in OT/ICS (R_27a3HBRQ60cNEsj)
    - Physical security (R_3kMMhb0mj6S80wG)
    - Methodologies for monitoring, detecting/alarming on devices/subsystems & operations of legacy systems with little to no cyber posture. (R_28HRVFlTwpY1Y9m)
- Asset Control
    - Asset Management (R_3kMMhb0mj6S80wG)
    - Configuration Management (R_3kMMhb0mj6S80wG)
- Device Level Protection
    - Failsafe vs fail secure: The RISK paradigm (R_2YX5Hjj1Z8JitHY)
    - Memory protection (R_3lMl6Hi3p0cr1K4)
- Training
    - End user awareness training (R_2Su9412OXG578E9)
- Secure-by-design Practices
    - Code Signing (R_5c0uAAMSNWyojMB)

Table of Contents

    - Functional segmentation (R_2Su9412OXG578E9)
    - Segmentation (R_3kMMhb0mj6S80wG)
    - Defense-in-depth concept (R_2Su9412OXG578E9)
    - Physical separation (R_2Su9412OXG578E9)
- Security Appliances
    - Active Defense (IPS, Deception, Quarantine, Honeypots, etc.) (R_27a3HBRQ60cNEsj)
    - PLC Secure Coding practices (R_3lMl6Hi3p0cr1K4)
    - Managed Services in OT/ICS (R_27a3HBRQ60cNEsj)
- Other
    - again, not enough time (R_1rGFDHuFhnB2AQB)
    - BOM (R_RqVMBWhBtfTdYrf)
    - IoT protection (R_3kMMhb0mj6S80w

Table of Contents

III-16 Additional Categories and Topics

This section captures new knowledge area categories and associated topics. Nine respondents provided answers to the survey question. Some responses could not be used to derive potential categories / topics and are organized under “Other”. The responses are as follows:

Additional ICS Cybersecurity Knowledge Areas (Suggestions from 9 respondents):

Respondent ID	**Response Content**
R_3njf722UBVndAP8	Asset Management
R_2YsHBQvCLvWLRjo	Security Log Collection: Aggregation / Monitoring / Analysis, Asset Detection and Inventory
R_RqVMBWhBtfTdYrf	PLC secure coding practices: memory protection, BOM
R_2Su9412OXG578E9	Procurement Techniques: requirements engineering, vendor audits, secure development environments, supply chain issues, hardware and software lifecycle planning, servicing issues
R_1BxKzD0XM4g0jcZ	Any of the smart devices, relays, sensors to cloud, safety.
R_3kMMhb0mj6S80wG	Topic 1 - Physical Security
R_28HRVFlTwpY1Y9m	Securing Legacy Systems With Little/No Cyber Posture
R_3PHz5Hw4MGOxWNK	topic1
R_3kMMhb0mj6S80wG	No

Table of Contents