Index	Activity	Task	Input	Output-Of Index	Function	Output	References
1.1.1	Strategic Preparation	Establish baseline of ICS	Available information of devices;	EXTERNAL	Identify field devices	Table/Entry with attributes [Serial number, manufacturer, modules, (I/O) ports, location, connections, MAC, Interfaces];	[1]
1.1.2	Strategic Preparation	Establish baseline of ICS	Available information of Actuators/Sensors;	EXTERNAL	Identify actuators and sensors	Table with attributes [Serial number, manufacturer, modules, (I/O) ports, location, connected field devices];	[1]
1.1.3	Strategic Preparation	Establish baseline of ICS	Available information of industrial PC/OS;	EXTERNAL	Identify industrial IT components	Entries to ICS asset inventory with IT components;	
1.1.4	Strategic Preparation	Establish baseline of ICS	Entries to ICS asset inventory with IT components; IT components attributes:	EXTERNAL	Add to IT asset inventory	IT asset inventory with adapted IT components;	
1.1.5	Strategic Preparation	Establish baseline of ICS	IT asset inventory with adapted IT components;	EXTERNAL; 1.1.5;	Identify adaptions of IT components (OS) for industrial environment	Adaptions/Differences of IT components for industrial environment;	[1]
1.1.6	Strategic Preparation	Establish baseline of ICS	Available information of network components;	EXTERNAL	Identify network components	Entries with network components in asset inventory;	[1]
1.1.7	Strategic Preparation	Establish baseline of ICS	See Output-Of Index	1.1.1; 1.1.2; 1.1.4; 1.1.5;	Identify old or unsupported systems (legacy systems)	Functionality [Effecting Audit/Logging]; Forensics Compliant; Reference materials available;	[1]
1.1.8	Strategic Preparation	Establish baseline of ICS	See Output-Of Index	1.1.1; 1.1.2; 1.1.4; 1.1.5;		Functionality [Effecting Audit/Logging]; Forensics Compliant; Reference Materials Available;	[1]
1.1.9	Strategic Preparation	Establish baseline of ICS	Available information of field bus components;	EXTERNAL	Identify supported and undocumented technology systems (modern/proprietary systems)  Identify field bus components	Entries with field bus components in asset inventory;	[1]
1.1.10	Strategic Preparation	Establish baseline of ICS	See Output-Of Index	1.1.1; 1.1.2; 1.1.4; 1.1.5;	Generate asset inventory	Final searchable asset inventory with all components and their attributes;	[1]
1.1.11	Strategic Preparation	Establish baseline of ICS	Connections of assets;	1.1.1; 1.1.2; 1.1.6; 1.1.10;	Identify internal and external connections	Connections to and from partner or peer locations; Access to mechanisms used by the vendor to support control systems technology; Access to mechanisms used by contractors to support control systems environments; Actual relationships between cyber resources and real-world operations; The pervasiveness of effective cyber security policies governing control systems operations; Information exchange mechanisms within the supply chain; Used protocols;	[1]
1.1.12	Strategic Preparation	Establish baseline of ICS	Asset inventory; Internal and external connections;	1.1.9; 1.1.10;	Determine architecture	Known vulnerabilities; Available security and safety mechanisms; Connections; All available components;	[1]
1.1.13	Strategic Preparation	Establish baseline of ICS	Asset inventory; Internal and external connections; Architecture;	1.1.9; 1.1.11;	Identify attack paths	Networkconnections required visibility on;	[1]
1.1.14	Strategic Preparation	Establish baseline of ICS	Asset inventory; Internal and external connections; Architecture; Attack paths;	1.1.10; 1.1.11; 1.1.13;	Generate threat model	Locations/Assets required visibility on;	
1.1.15	Strategic Preparation	Establish baseline of ICS	Engineering workstation files;	EXTERNAL	Store Project files	Secure and forensic compliant files for further retrieval;	[2]
1.1.16		Establish baseline of ICS	Field devices, actuators and sensors (were applicable)	1.1.10;	Store hardware configuration	Cocure and forencie compliant storage of original configurations	[2]
1.1.10	Strategic Preparation	Establish baseline of ics	configuration;	1.1.15;	Store hardware configuration	Secure and forensic compliant storage of original configuration;	[2]
1.1.17	Strategic Preparation	Establish baseline of ICS	Wiring diagrams of field device/bus with actutors and sensors;	1.1.1; 1.1.2; 1.1.10; 1.1.15;	Store Wiring diagrams	Secure and forensic compliant storage of intended files;	[2]
1.1.18	Strategic Preparation	Establish baseline of ICS	Field devices;	1.1.1; 1.1.10; 1.1.15;	Store control logic programs	Secure and forensic compliant storage of intended control logic;	[2]
1.1.19	Strategic Preparation	Establish baseline of ICS	Network components cofigurations;	1.1.6; 1.1.10; 1.1.15;	Store network configuration	Secure and forensic compliant storage of intended network configurations;	[2]
1.2.1	Strategic Preparation	Identification of data sources	All (IT) components; All Assets with storage capabilities; Architecture;	1.1.10; 1.1.12;	Identify all databases	available databases and their specific data;	[1]
1.2.2	Strategic Preparation	Identification of data sources	field devices;	1.1.1;	Identify data storages of components	field components with storage functions/capabiltiles and their data;	[1]
1.2.3	Strategic Preparation	Identification of data sources	Asset inventory;	1.7.8;	Locate external storage media	Available external storage media and devices;	[3]
1.2.4	Strategic Preparation	Identification of data sources	available data sources;	1.1.1; 1.1.10; 1.2.1; 1.2.2;	Locate data sources	Location of data source within architecture;	
1.3.1	Strategic Preparation	Determining known and unknown data types (data model)	data sources;	1.2.5;	Analyze data source content	data types and evidence;	
1.3.2		Determining known and unknown data types (data model)	Connections to and from partner or peer locations;	1.1.11; 1.1.12;	Identify used protocols	used protocols in architecture;	[4]
1.3.3	Strategic Preparation	Determining known and unknown data types (data model)	Identified protocols of devices;	EXTERNAL; 1.1.1; 1.3.2;	nienny useu protocol  Analyze fields protocol	pattern/bytes of protocol;	[4]
1.3.4	Strategic Preparation	Determining known and unknown data types (data model)	Engineering workstation files;	1.3.2;	Analyze fields protocol  Analyze project filetypes	content of specific filetypes;	
1.3.5	Strategic Preparation	Determining known and unknown data types (data model)	Storaged configuration files;	1.1.16;		specific content of configurations;	
1.3.6	Strategic Preparation	Determining known and unknown data types (data model)	Network components cofigurations; field devices content;	1.1.19; 1.1.1; 1.2.4;	Analyze configurationfiles  Analyze firmware files	specific content or comigurations; firmware;	[5]
1.3.7	Strategic Preparation	Determining known and unknown data types (data model)	Stored control logic files;	1.1.18;		control logic :	
1.3./	Strategic Preparation	Determining known and unknown data types (data model)	Location of data sources;	1.1.19;	Analyze control logic files	control logic;	

1.3.8	Strategic Preparation	Determining known and unknown data types (data model)	All data sources content;	1.1.14; 1.1.15; 1.1.16; 1.1.17; 1.1.18; 1.2.1; 1.2.2; 1.2.3; 1.2.4; 1.3.1; 1.3.2; 1.3.2; 1.3.3; 1.3.4; 1.3.5; 1.3.6; 1.3.6;	add available data types to the data model	available data (types) in ICS with forensic value/adapted data model;	
1.4.1	Strategic Preparation	Assesment of forensic capabilities	Assets;	1.1.10;	Identify logging capabilities	Existing logging capabilties in archtiecture;	[1]
1.4.2	Strategic Preparation	Assesment of forensic capabilities	field devices;	1.1.1:	Identify devices interfaces	existing interfaces to retrieve forensic data;	
			Assets:	1.1.10;	in the state of th		
1.4.3	Strategic Preparation	Assesment of forensic capabilities	data sources:	1.2.4:	Identify software interfaces	existing software interface to retrieve forensic data;	4
1.4.4	Strategic Preparation	Assesment of forensic capabilities	Location of data source within architecture; Existing logging capabilities in architecture; existing interfaces to retrieve forensic data; existing software interface to retrieve forensic data; live capabilities to retrieve forensic data; post mortem capabilities to retrieve forensic data;	1.2.4; 1.4.1; 1.4.2; 1.4.3;	check existing ways to access data live in the ICS in conjunction with data model	live capabilities to retrieve forensic data;	
1.4.5	Strategic Preparation	Assesment of forensic capabilities	Location of data source within architecture; Existing logging capabilities in architecture; existing interfaces to retrieve forensic data; existing software interface to retrieve forensic data; live capabilities to retrieve forensic data; post mortem capabilities to retrieve forensic data;	1.2.4; 1.4.1; 1.4.2; 1.4.3;	check existing ways to access data post mortem in the ICS in conjunction with data model	post mortem capabilites to retrieve forensic data;	
1.4.6	Strategic Preparation	Assesment of forensic capabilities	Location of data source within architecture; Existing logging capabilities in architecture; existing interfaces to retrieve forensic data; existing software interface to retrieve forensic data; live capabilities to retrieve forensic data; post mortem capabilities to retrieve forensic data;	1.4.1; 1.4.2; 1.4.3; 1.4.4; 1.4.5; 1.4.6;	Check compliance of forensic capabilities	required measures for compliance;	
1.5.1	Strategic Preparation	Determination of forensic measures	Existing forensic capabilities; Data model;	1.4.1; 1.4.2; 1.4.3; 1.4.4; 1.4.5; 1.4.6; EXTERNAL;	Identify required forensic capabilities	required forensic capabilities;	
1.5.2	Strategic Preparation	Determination of forensic measures	required measures for compliance; required forensic capabilities;	1.4.6; 1.5.1; EXTERNAL;	Set measures or functions for protection goals measures	functions for protection goals/compliance of forensic capabilities or functions;	
1.5.3	Strategic Preparation	Determination of forensic measures	required forensic capabilities;	1.5.1;	add implementation (view) to selected functions	established implementation view (IIRA compliant);	4
1.6.1	Strategic Preparation	Determination of required capacities	established implementation view (IIRA compliant);	1.5.3;	Calculation of data volumes	Required storage capacities;	[3]
1.7.1	Strategic Preparation	Generation of tool catalog	data sources; software interfaces; hardware interfaces;	1.2.5; 1.4.3; 1.4.4; 1.4.4; 1.4.5;	Assign existing tools	Specific tools for data retrieval and processing:	[6]
1.7.2	Strategic Preparation	Generation of tool catalog	Specific tools for data retrieval and processing	1.2.5; 1.6.1;	Identify gaps or missing tools in tool assignment	Required tools to be developed;	1 1
1.7.3	Strategic Preparation	Generation of tool catalog	Required tools to be developed	1.6.2;	implement missing/required tools	coverage of missing capabilities/tools;	
1.8.1	Strategic Preparation	implementation of forensic capabilities	Required storage capacities	1.5.4;	implement data capacities/storage	availability of storage capacities;	
1.8.2	Strategic Preparation	implementation of forensic capabilities	Specific tools for data retrieval and processing;	1.6.1; 1.6.2;	build forensic tool kit	forensic tool kit ready for use;	[7]
1.8.3	Strategic Preparation	implementation of forensic capabilities	Specific tools for data retrieval and processing;	1.6.2;	Asses forensic compliance of tools	Required adaption of tools;	_
1.8.4	Strategic Preparation	implementation of forensic capabilities	Specific tools for data retrieval and processing,  Specific tools for data retrieval or processing;  forensic tool kit ready for use:	1.6.1; 1.7.3:	build tool catalog	finished tool catalog;	
1.8.5	Strategic Preparation	implementation of forensic capabilities	legal requirements;	EXTERNAL;	generate (legal) templates for checkists/questionaires etc	document templates for operational preparation;	
1.8.6	Strategic Preparation	implementation of forensic capabilities	established implementation view;	1.5.3;	implement all forensic measures	implemented forensic capabilties;	[1]
2.1.1	Operational preparation	Identification of related assets (and data sources)	Available information of incident (IP of IDS alert, serial number  Etc.);  Asset inventory;	EXTERNAL; 1.1.10;	retrieve from asset inventory	Affected assets;	[±]
2.1.2	Operational preparation	Identification of related assets (and data sources)	Affected assets;	2.1.1:	Identify data sources	related data sources of affected assets;	[3]
2.2.1	Operational preparation	Preselect potential relevant data	related data sources of affected assets;	2.1.2;	Identify data (types)	potential data required for evidence;	[3]
2.2.1	Operational preparation	Preselect potential relevant data	potential data required for evidence;	2.2.1;	Select relevant data	data to be acquired;	[3]
2.3.1	Operational preparation	Impact on system assessment	function catalog; potential relevant data and their data sources;	1.5.2; 2.2.1;	Filter functions catalog for relevant data/data sources	suitable functions for data acquisition;	
2.3.2	Operational preparation	Impact on system assessment	tool catalog;	1.7.5;		suitable tools for data acquisition:	
2.3.2	Operational preparation	Impact on system assessment	potential relevant data and their data sources; suitable functions for data acquisition;	2.2.1;	Filter tools catalog for relevant data/data sources		-
2.3.3	Operational preparation	impact on system assessment	report of predicted system impact of data acquisition; Estimated duration of shutdown;	2.3.2;	summarize impacts of suitable functions and tools;	report of predicted system impact of data acquisition;  Costs of a shutdown;	4
2.4.1	Operational preparation	live vs postmortem decision	Estimated duration of shutdown; Replacesystems availability;	EXTERNAL;	Determine business issues	Costs or a snutrown;  Lost evidence due to impossible post mortem acquisition;  Impact on ICS productivity;	

1.5   Communication   No. operation   No. op					EVTERNAL			
14.5   Septiment personne   Company of the Compan	2.4.2	Operational preparation	live vs postmortem decision	Impact on ICS productivity;	EXTERNAL; 1.7.6;	Determine legal issues	legal documents and clearances;	[8]
10	2.4.3	Operational preparation	live vs postmortem decision	available information of current productivity;	EXTERNAL;		productivity status of the ICS;	
1-15   Control regions   The symmetry of the control of the cont	2.4.4	Operational preparation	live vs postmortem decision			Control of the state of the sta	post mortem only or not	
1.00   1.00						Determine it shutdown occured or plant is already impaired		
1-2-	2.4.5	Operational preparation	live vs postmortem decision			Determine non-live retrieval data	potential evidence only post mortem retrievable;	
1-32   Common or processor   Common or pro								
1.5   General (Information Company)	2.4.6	Operational preparation	live vs postmortem decision				decision to shut down ICS/post mortem or live;	
1.52   According properties   Content for the first own set and	2.5.1	Operational preparation	setup of order to retrieve data				volatility of potential data required to be acquired:	[9]
Section of the companion   Contract Review of the section of the companion   Contract Review of the contract   Contract Review of the contract   Contract Review of the contract Revi		Operational preparation						[3]
1.								
11	2.6.1	Operational preparation	Create list with data sources and tools for data retrieval				list of data to be acquired with specific tools;	
1.1   1.2				potential data required for evidence;	2.2.1;	assign tools for data retrieval		
Accordance   1.1.00				list of data to be acquired with specific tools;	2.6.1;			
13.2   District Operation	3.1.1	Data acquisition	Locate data sources				location of data sources with data to be acquired;	
1.1.						lookup data souzrce of potential data to acquired;		
1.1.1	3.2.1	Data acquisition	Collect physical storage media			collect external physical storages	physical data storage components;	[3]
13.3   100 constitute   100 control data   100 control   11.6   100 control   100 co						create forensic compliant dupliciation		
3.3.2   Consequence	0.0.0							
1.12   1.12						capture I/O		[10]
1.3.4   Cite sequence of cites   Control of cites	3.3.3	Data acquisition	Live retrieval of data			Translate and store events in audit log file	forensic compliant logs;	
3.3.4   Dist registering   Dis								
13.1   13.1   13.2	2 2 4	Data acquisition	Live retrieval of data	stored data by implemented forencie canabilities	1.7.8;			
1.15   Data aquatation   Description of data   Effected field complete;   1.3.1   Agent former from descriptions   2.3.2   Agent former for descriptions   2.3.2   Agent former for descriptions   2.3.3   Agent former form	5.5.4	Data acquisition	Live retrieval of data	stored data by implemented forensic capabilities;				
13.16   Data sepaction   Data information of design   Data information   Da						retrieve from databases		
1370 Des arquitibles   Les retinoued datas   Controller defence   11.12   Controller defence   12.12   Controller defence   12.13   Controller defence   13.14   Controller defence   13.15	3.3.5	Data acquisition	Live retrieval of data	affected field controller;			actual firmware of device;	
13.18 Dies appellen 13.19 Dies appellen 13.19 Dies appellen 13.10			Live retrieval of data	·				[2]
3.3.8 One aquietice   Uveretrieved data   depress infection   1.3.7;   Determine dispersation   depress infection   1.3.3.1   1.3.3.2   1.3.3.3.2   1.3.3.3.3.3   1.3.3.3.3.3   1.3.3.3.3.3.3.3.3.3.3.3.3.3.3.3.3.3.3.3						·		
13.0   Data aquisition   Use retrieved of data   request to affected device   1.2.5   August Variable content data   Vasibable content data   Vasibable content data   Page   Vasibable cont								
Jack Dea aquantion (Jack Interferent) of data report or effected devices (122)								[2]
3.3.12   Data association   Use retrieval of data   request to effected device;   12.2;   Association   Use retrieval of data   request to effected device;   2.3.2;   Association   Use retrieval of data   request to effected device;   13.2;   Association   Post content noticeal   device device;   13.2;   Association   Post content noticeal   device device;   3.4.3;   Post association   Post content noticeal   device device;   3.4.3;   Post association   Post content noticeal   device device;   3.4.3;   Post association   Post content noticeal   request   device device;   3.4.3;   Post association   Post content noticeal   request;   12.2;   Association   Post content noticeal   Post conte								
3.12   Data exposition   Deventioned of data   progressing whose legs   1.22   Acquire device diagnostics and Cog				request to affected device;				
August control agreement of the appetition   Post montem retired disabase;   1.1.0.   Post montem retired disabase;   1.2.1   Post appetition   Post montem retired   Post mon	22.12	Data a serviciti	the extense of data		122			[44]
3.1.1 Data acquisition Post monten retrieval device bostlow.  3.2.1 Data acquisition Post monten retrieval feeting for feeting feeting.  3.2.1 Data acquisition Post monten retrieval retrieval feeting.  3.2.1 Data acquisition Post monten retrieval request.  3.2.2 Data acquisition Post monten retrieval request.  3.2.3 Data acquisition Post monten retrieval request.  3.2.3 Data acquisition Post monten retrieval request.  3.2.4 Data acquisition Post monten retrieval request.  3.2.5 Data acquisition Post monten retrieval request.  3.2.6 Data acquisition Post monten retrieval request.  3.2.7 Data acquisition Post monten retrieval retrieval request.  3.2.8 Data acquisition Post monten retrieval retrieval retrieval retrieval retrieval retrieval retrieval retrieval period retrieval peri	3.3.12	Data acquisition	Live retrieval of data		1.2.2;	Acquire device diagnostics and Logs	errros and events;	[11]
1.4.3 Data acquisition Post morter retiroal effective device; 3.4.5; Place device in included manipulation of traffic; 1.3.5 Agricultural retiroal in flower retiroal		Data acquisition		device location;		remove field controller from network		[12]
3.4.4 Data acquisition Post mortem retrieval register; 1.2.1 Acquire PC agricultion Code Agriculture (Post of Agriculture) Post mortem retrieval register; 1.2.1 Acquire PC agriculture) Post mortem retrieval register; 1.2.1 Acquire formare late acquire formare of device; 1.2.1 Acquire formare late acquire formare of device; 1.2.1 Acquire formare late; 1.2.2 Acquire formare formare formare late; 1.2.2 Acquire formare formare formare formare formare formare formare formare for		Data acquisition						
3.6.5 Data acquisition Post mortem retrieval request; 1.2.2 Acquire PEC. Meta Data media dat of affected PEC.  3.6.8 Data acquisition Post mortem retrieval request; 1.2.2 Acquire PEC. Meta Data (process) and fuge error and function retrieval request.  3.6.1 Data acquisition Post mortem retrieval retrieval device; 3.4.1 Benutly interfaces available interface types; 3.5.1 Data acquisition Post mortem retrieval persistent memory components; 3.6.5 Read persistent memory components; 3.6.5	3.4.4	Data acquisition	Post mortem retrieval		1.2.2;	Acquire PLC application Code	Application code of affected field controller;	
3.47 Data acquisition Post morters entrieval request; 2.27 Acquire immazer live acquired morters retrieval refreshed edice; 3.41; Bestiviseffaces substitution Post morters retrieval persistent memory components in the post morter retrieval persistent memory components in the post morters and persistent memory components in the post morters and persistent memory components in the post memory components in the po	3.4.5	Data acquisition	Post mortem retrieval		1.2.2;	Acquire PLC Meta-Data	meta data of affected PLC;	
3.4.5 Data acquisition Post mortem retrieval retrieval persistent memory components (3.4.5) Read persistent memory components (3.4.5) Retrieve data acquirition (3.4.5) Retrieve d								
3.5.1 Data acquisition Retrieval off in forestic data common forensic databases.  1.7.8 Retrieve data acquired by IT forensic process IT components forensic data;  1.8.1 Part acquisition Acquire witness report rigidest personel; status of the field device;  1.1.5 PETRINA; POTERNA;	3.4.8	Data acquisition	Post mortem retrieval	retrieved device;	3.4.1;	Identify interfaces	available interface types;	
Acquire witness report rigger related personel; status of the field devices; status of the field device								
Data acquisition   Acquire witness report   Components forensic data;   Components f	3.5.1	Data acquisition	Retrieval of 11 forensic data			Retrieve data acquired by 11 forensic process	11 components forensic data;	
3.6.2 Data acquisition Acquire witness report questioning:  3.6.1 Questioning potential witnesses  3.6.2 Data acquisition Acquire witness report questioning:  3.6.2 Questioning potential witnesses  3.6.1 Questioning potential witnesses  3.2.1 3.3.2 3.3.1 3.3.3 3.3.3 3.3.3 3.3.3 3.3.3 3.3.3 3.3.3 3.3.3 3.3.3 3.3.3 3.3 3.3.3 3.3.3 3.3.3 3.3.3 3.3.3 3.3.3 3.3.3 3.3.3 3.3.3 3.3.3 3.3 3.3.3 3.3.3 3.3.3 3.3.3 3.3.3 3.3.3 3.3.3 3.3.3 3.3.3 3.3.3 3.3 3.3.3 3.3.3 3.3.3 3.3.3 3.3.3 3.3.3 3.3.3 3.3.3 3.3.3 3.3.3 3.3 3.3.3 3.3.3 3.3.3 3.3.3 3.3.3 3.3.3 3.3.3 3.3.3 3.3.3 3.3.3 3.3 3.3.3 3.3.3 3.3.3 3.3.3 3.3.3 3.3.3 3.3.3 3.3.3 3.3.3 3.3.3 3.3 3.3.3 3.3.3 3.3.3 3.3.3 3.3.3 3.3.3 3.3.3 3.3.3 3.3.3 3.3.3 3.3 3.3.3 3.3.3 3.3.3 3.3.3 3.3.3 3.3.3 3.3.3 3.3.3 3.3.3 3.3.3 3.3 3.3.3 3.3.3 3.3.3 3.3.3 3.3.3 3.3.3 3.3.3 3	261	Data acquisition	Acquira witness report			Identify notantial witnesses	personal for further questioning	[12]
3.6.2 Data acquicition  Acquire witness report  Questionaire templates; personell for further questioning:  3.6.1; 3.2.1; 3.2.2; 3.3.1; 3.3.4; 3.3.5; 3.3.6; 3.3.7; 3.3.8; 3.3.9; 4.1.1  Examination  Assign acquired data to the data model  OT components forensic data; 3.3.1; 3	3.0.1	Data acquisition	Acquire witness report			identity potential witnesses	personer for further questioning;	[15]
3.6.2 Data acquisition Acquire witness report Questioning:    Substitute					176:			
Assign acquired data to the data model   OT components forensic data;   3.2.1;   3.2.2;   3.3.3;   3.3.6;   3.3.6;   3.3.6;   3.3.6;   3.3.6;   3.3.6;   3.3.7;   3.3.8;   3.3.1;   3	3.6.2	Data acquisition	Acquire witness report				filled questionaires;	
4.1.1 Examination Assign acquired data to the data model OT components forensic data;  3.2.2; 3.3.3; 3.3.4; 3.3.5; 3.3.6; 3.3.7; 3.3.8; 3.3.9; 3.3.10; 3.3.11; 3.3.12; 3.4.1; 3.4.2; 3.4.4; 3.4.5; 3.4.4; 3.4.5; 3.4.6; 3.4.7; 3.4.8;				personell for further questioning;		Questioning potential witnesses		
4.1.1 Examination Assign acquired data to the data model OT components forensic data;  4.1.1 Examination Assign acquired data to the data model OT components forensic data;  3.3.1; 3.3.1; 3.3.1; 3.3.1; 3.3.1; 3.3.1; 3.3.1; 3.3.1; 3.4.1; 3.4.2; 3.4.3; 3.4.4; 3.4.5; 3.4.6; 3.4.6; 3.4.7; 3.4.8;								
3.3.2; 3.3.3; 3.3.4; 3.3.5; 3.3.6; 3.3.7; 3.3.8; 3.3.9;  4.1.1 Examination Assign acquired data to the data model OT components forensic data;  3.3.10; 3.3.11; 3.3.12; 3.4.1; 3.4.2; 3.4.4; 3.4.5; 3.4.6; 3.4.6; 3.4.7; 3.4.8;								
4.1.1 Examination Assign acquired data to the data model OT components forensic data;  3.3.6; 3.3.7; 3.3.8; 3.3.9; 3.3.10; 3.3.11; 3.3.12; 3.4.1; 3.4.2; 3.4.3; 3.4.4; 3.4.5; 3.4.6; 3.4.7; 3.4.8;					3.3.2;			
4.1.1 Examination Assign acquired data to the data model OT components forensic data;  3.3.6; 3.3.7; 3.3.8; 3.3.9; 3.3.10; 3.3.11; 3.3.12; 3.4.1; 3.4.2; 3.4.3; 3.4.4; 3.4.5; 3.4.6; 3.4.7; 3.4.8;					3.3.3;			
4.1.1 Examination Assign acquired data to the data model OT components forensic data;  3.3.6; 3.3.7; 3.3.8; 3.3.9; 3.3.10; 3.3.11; 3.3.12; 3.4.1; 3.4.2; 3.4.3; 3.4.4; 3.4.5; 3.4.6; 3.4.7; 3.4.8;								
4.1.1 Examination Assign acquired data to the data model OT components forensic data;  3.3.7; 3.3.8; 3.3.9; 3.3.10; 3.3.11; 3.3.12; 3.4.1; 3.4.2; 3.4.3; 3.4.4; 3.4.5; 3.4.6; 3.4.7; 3.4.8;								
4.1.1 Examination Assign acquired data to the data model OT components forensic data;  3.3.8; 3.3.9; 3.3.10; 3.3.11; 3.3.12; 3.4.1; 3.4.2; 3.4.3; 3.4.4; 3.4.5; 3.4.6; 3.4.7; 3.4.8;								
4.1.1 Examination Assign acquired data to the data model OT components forensic data;  3.3.10; 3.3.11; 3.3.12; 3.4.1; 3.4.2; 3.4.3; 3.4.4; 3.4.5; 3.4.6; 3.4.7; 3.4.8;								
3.3.11; 3.3.12; 3.4.1; 3.4.2; 3.4.3; 3.4.4; 3.4.5; 3.4.6; 3.4.6; 3.4.7; 3.4.8;	411	Evamination	Assign acquired data to the data model	OT components forencis data:		Assign collected OT data to data model	all available OT forencic data structured filled data model with available data	
3.3.12; 3.4.1; 3.4.2; 3.4.3; 3.4.4; 3.4.5; 3.4.6; 3.4.7; 3.4.8;	4.1.1	Examination	Assign acquired data to the data model	Or components forensic data;		Assign conected of data to data model	an available O1 Toterisic data structured/filled data model with available data;	
3.4.2; 3.4.3; 3.4.4; 3.4.5; 3.4.6; 3.4.7; 3.4.8;					3.3.12;			
3.4.3; 3.4.4; 3.4.5; 3.4.6; 3.4.7; 3.4.8;								
3.4.4; 3.4.5; 3.4.6; 3.4.7; 3.4.8;								
3.4.5; 3.4.6; 3.4.7; 3.4.8;								
3.4.7; 3.4.8;					3.4.5;			
3.4.8;								
					3.4.9;			

4.1.2	Examination	Assign acquired data to the data model	IT components forensic data:	3.5.1:	Assign collected IT data to data model	all available IT forensic data structured/filled data model with available data:	
4.2.2	Examination	7 SJight dequired data to the data model	all available OT forensic data structured;	4.1.1;	rising it concected it data to data mode.	an dranable in foreigne data stratedy linea data model with available data,	
4.2.1	Examination	Selection of appropriate tools	all available IT forensic data structured;	4.1.2;		extractable data/further artefacts contained in acquired data (types);	
			data model;	1.3.8;	Asses format/aggregation level of acquired data	(7,1-7)	
			all available OT forensic data structured/filled data model with				
			an available OT forensic data structured/filled data model with	4.1.1;			
4.2.2	Examination	Selection of appropriate tools	all available IT forensic data structured/filled data model with	4.1.1,	Asses available data	missing data or gaps in filled data model;	
4.2.2	Examination	Selection of appropriate tools	available 11 foreitsic data structured/filled data filloder with	4.2.1;	Asses available data	missing data of gaps in filled data filoder,	
			extractable data/further artefacts contained in acquired data;	4.2.1,			
			tool catalog;	1.7.5;			
4.2.3	Examination	Selection of appropriate tools	extractable data (types)/further artefacts contained in acquired	4.2.1;		tools to search specific data types;	[3]
			data;		Choose tools to search extractable data types		
4.3.1	Examination	Identification of artefacts/evidence	traffic captures;	3.3.1;	Search for connections/requests	connections within acquired data;	
4.3.2	Examination	Identification of artefacts/evidence	traffic captures;	3.3.1;	Search for uploads/downloads	uploads/downloads within traffic captures;	
4.3.3	Examination	Identification of artefacts/evidence	uploads/downloads within traffic captures;	4.3.2;	Identify uploaded/downloaded data	bytes position containing payload;	
4.3.4	Examination	Identification of artefacts/evidence	traffic captures;	3.3.1;	Search for commands	bytes position containing commands;	
4.3.5	Examination	Identification of artefacts/evidence	traffic captures;	3.3.1;	Search for read/write	bytes position containing read/write operations;	
4.3.6	Examination	Identification of artefacts/evidence	traffic captures;	3.3.1;		bytes position containing control logic and variables;	
			raw memory binary;	3.4.9;	Search for control logic including variables	,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	
4.3.7	Examination	Identification of artefacts/evidence	traffic captures;	3.3.1;	County for any debag	bytes position containing updates;	
			4		Search for updates		
4.3.8	Examination	Identification of artefacts/evidence	traffic captures; bytes position containing updates;	3.3.1;		bytes position containing configurations;	
4.5.8	examination	identification of arteracts/evidence	raw memory binary;	4.3.7;	Search for configurations;	bytes position containing configurations;	
			traffic captures;	3.3.1;	Search for configurations;		
4.3.9	Examination	Identification of artefacts/evidence	raw memory binary;	4.3.7;	Search for misc or unidentified data types	bytes position with misc or unknown data types;	
			tool catalog;	·	Search for thisc or unidentified data types		
4.4.1	Examination	Extraction of further data types and artefacts	extractable data (types)/further artefacts contained in acquired	1.7.5;		tools to extract specific data types;	[3]
4.4.1	Examination	Extraction of further data types and arteracts	data;	4.2.1;	Choose tools to extract extractable data types	tools to extract specific data types,	[3]
4.4.2	Examination	Extraction of further data types and artefacts	connections within acquired data;	4.3.1;	Extract connection data	connection details (IP etc.) with timestamp;	
4.4.2	Examination	Extraction of further data types and artefacts	traffic captures;		Extract connection data	connection details (if etc.) With diffestants,	
			bytes position containing updates;	3.3.1;			
4.4.3	Examination	Extraction of further data types and artefacts	bytes position containing payload;	4.3.7;		uploaded/downloaded payload with timestamp;	
			-,,,	4.3.3;	Extract upload/download data		
			traffic captures;	3.3.1;	,		
4.4.4	Examination	Extraction of further data types and artefacts	bytes position containing read/write operations;	4.3.5;	Extract read/write operations	single read/write operations with registers and timestamps;	
			traffic captures;	3.3.1;			
4.4.5	Examination	Extraction of further data types and artefacts	bytes position containing containing commands;	4.3.4;	Extract commands	single commands to devices with timestamp;	
4.4.6	Examination	Extraction of further data types and artefacts	traffic captures;	3.3.1;	Extract reported I/O status;	by protocol reported I/O values with timestamp;	
4.4.7	Examination	Extraction of further data types and artefacts	I/O values captures;	3.3.2;	Extract I/O values	specific I/O values with timestamp from I/O tap;	
			traffic captures;	3.3.1;			
4.4.8	Examination	Extraction of further data types and artefacts	raw bytes containing payload with timestamp;	4.4.3;		control logic binary;	
			bytes position containing control logic with variables;	4.3.8;	Extract control logic with variables		
4.4.9	Examination	Extraction of further data types and artefacts	traffic captures;	3.3.1;		configuration files;	
4.4.5	Examination	Extraction of further data types and arteracts	bytes position containing configuration data;	4.3.8;	Extract configuration data	configuration files,	
			traffic captures;	3.3.1;			
4.4.10	Examination	Extraction of further data types and artefacts	bytes position containing configuration data;	4.3.8;		firmware binary;	
			raw memory binary;	3.4.10;	Extract firmware		
4.4.11	Examination	Extraction of further data types and artefacts	traffic captures;	3.3.1;		control logic binary;	
4.4.11	ZAGITITI GUOTI	Extraction of further data types and artefacts	raw memory binary;	3.4.10;	Extract control logic	control logic billary,	
			traffic captures;	3.3.1;			
4.4.12	Examination	Extraction of further data types and artefacts	bytes position containing configuration data;	4.3.8;		configuration binary;	
			raw memory binary;	3.4.10;	Extract configurations		
			traffic captures;	3.3.1;			
4.4.13	Examination	Extraction of further data types and artefacts	bytes position with misc or unknown data;	4.3.9;		misc or unknown data;	
			raw memory binary;	3.4.10;	Extract misc or unknown data		
			firmware binary;	4.4.10;			
4.4.14	Examination	Extraction of further data types and artefacts	configuration binary;	4.4.12;		available filetypes;	
454		T 10 11 11 11 11	raw memory binary;	3.4.9;	extract file types;	1/0 1 21 22 12	
4.5.1	Examination	Translation into right kind of format	specific I/O values with timestamp;	4.4.7;	convert/parse bytes to human readable I/O values	I/O values with units and timestamp	
4.5.2	Examination	Translation into right kind of format	control logic binary;	4.4.11;	convert/parse bytes to human readable control logic	According IEC 31131-3 filetype	1
452	Fii	Toursdaying into sinht bind of forms:	extracted I/O values;	4.4.6;			
4.5.3	Examination	Translation into right kind of format	PLC control logic;	4.5.2;	Assiss 1/O Associables	variable content data with timestamp;	
			I/O captures;	4.4.7;	Assign I/O to variables		
4.5.4	Examination	Translation into right kind of format	single commands to devices with timestamp;	4.4.5;	convert/parse bytes to human readable commands	send commands with specific data and timestamp; received commands with specific data and timestamp;	
4.5.5	Examination	Translation into right kind of format	single read/write operations with registers and timestamps;	4.4.4;	convert/parse bytes to human readable commands  convert/parse bytes to human readable read/write operations	send or received read/write operations with specific data and timestamp;	<b>+</b>
4.3.3	EXAMINIBUON	rransiation into right kind of format	single read/write operations with registers and timestamps; control logic binary;	4.4.4;	convert/parse bytes to number readable read/write operations	send of received read/write operations with specific data and timestamp;	<b>+</b>
4.5.6	Examination	Translation into right kind of format	control logic binary; configuration binary;	4.4.8; 4.4.12;		all available filetypes;	
4.5.0	cxammation	Translation into right kind or format	memory binary parts;	4.4.12;	parse raw data to filetypes	an available metypes,	
4.5.7	Examination	Translation into right kind of format	filled questionaires;	3.6.2;	parse raw data to metypes  parse answers to computer analysable answers	computer analyzable facts/events with timestamp of witness report;	
				3.0.2,	parse answers to computer analysable answers		

				4.4.2;			
				4.4.3;			
				4.4.4;			
				4.4.5;			
				4.4.6;			
				4.4.7;			
				4.4.8;			
				4.4.9;			
				4.4.10;			
4.6.1	Examination	Assigning extracted evidence to data model	all extracted artefacts;	4.4.11;		structurized overview of available and missing evidence (filled data model);	
4.0.1	Examination	753gmig extracted evidence to data model	an extracted arteracts,	4.4.12;		Strategical overview of available and missing evidence (mica data modely,	
				4.4.13;			
				4.4.14;			
				4.5.1;			
				4.5.2;			
				4.5.3;			
				4.5.4;			
				4.5.5;			
				4.5.6;	Assigning all extracted data and filetypes to data model		
			specific I/O values with timestamp;	4.4.7;			
			variable content data;	4.5.3;			
5.1.1	Analysis	Identify potential coherences				events impacting I/O and vice versa;	[14]
			by protocol reported I/O values;	4.4.6;			
			event logs;	3.3.3;	Correlation of events with I/O status;		
5.1.2	Analysis	Identify potential coherences	connections/requests;	4.4.2;		related events and connections/request;	[15]
3.1.2	Allalysis	identity potential concrences	event logs;	3.3.3.;	Correlation of events and connections;	related events and connections/request,	[17]
			answers;	4.5.7;			
5.1.3	Analysis	Identify potential coherences	events;	3.3.3;		further related events;	
			I/O data with timestamp;	4.5.1;	Correlate witness reports with artefacts;		
			I/O data with timestamp;				
5.1.4	Analysis	Identify potential coherences	send or received read/write operations with specific data and	4.5.1;		related impact of variable commands to I/O;	
3.1.4	7 11 11 7 31 3	identity potential concrences	timestamp;	4.5.5;	Correlate I/O data with register operations	related impact of variable community to 1/0/	
			tillestamp,	4.4.2;	Correlate 1/O data with register operations		
				4.4.3;			
				4.4.4;			
				4.4.5;			
				4.4.6;			
5.1.5	Analysis	433. 453;	all extracted artefacts timestamps:	4.4.7;		chronological colationships between artefacts /	[3]
3.1.3	Alialysis		chronological relationships between artefacts/events;	[5]			
				4.5.3:			
				4.5.4;			
				4.5.5;			
		/ I					
				4.5.6;			
				4.5.7;	Correlate timestamp of artefacts		
				4.4.2;			
				4.4.3;			
				4.4.4;			
				4.4.5;			
				4.4.6;			
				4.4.7;			
5.1.6	Analysis	Analysis Identify potential coherences	all extracted artefacts timestamps;	4.5.1;		events with impact on components;	[3]
				4.5.3;			
				4.5.4;			
				4.5.5;			
				4.5.5; 4.5.6;			
				4.5.6; 4.5.7;	Identify startistical above		
				4.5.7;	Identify stastistical changes		
				4.4.2;			
				4.4.3;			
				4.4.4;			
				4.4.5;			
				4.4.6;			
5.1.7	Annibusia	Identify and add to be a second	all as to a to disable to the bigger and a	4.4.7;		and and an artist and a staff at a	(2)
5.1.7	Analysis	Identify potential coherences	all extracted artefacts timestamps;	4.5.1;		related events and artefacts;	[3]
				4.5.3;			
				4.5.4;			
				4.5.5;			
				4.5.6;			
					Markit annual		
				4.5.7;	Identify patterns		
			send/received commands;	4.5.4;			
5.1.8	Analysis	Identify potential coherences	computer analyzable facts/events with timestamp of witness			executed commands;	
	,		report;	5.1.4;			
			chronological relationships between artefacts/events;	3.1.4,	Correlate commands with artefacts		
			send/received commands;	4.5.4;			
			executed commands;				
5.2.1	Analysis	Identify inconsistencies	send or received read/write operations;	5.1.8;		Related authorized register commands with events;	
	.,	,	computer analyzable facts/events with timestamp of witness	4.5.5;			
			report;	4.5.7;	Compare input with read/write operations		
			connections/requests;	4.4.2;	compare input maneau/ write operations		
5.2.2	Analysis	Identify inconsistencies	uploaded/downloaded payload with timestamp;	4.4.2;	Compare connection/requests with up-/downloads	suspicious connections/requests with timestamp;	I
			upidaded/downloaded payload with timestamp;	4.4.5;	compare connection/requests with up-/downloads		

				4.4.2;			
				4.4.3;			
				4.4.4;			
				4.4.5;			
				4.4.6;			
				4.4.7;			
				4.5.1;			
5.2.4	Analysis	Identify inconsistencies	all extracted data with timestamps;	4.5.3;		suspicious events/artefacts with timestamp;	
3.2.4	Analysis	identity inconsistencies	all extracted data with timestamps,	4.5.4;		suspicious events/arteracts with timestamp,	
				4.5.5;			
				4.5.6;			
				4.5.7;			
				5.1.7;			
				5.1.8;			
				5.2.1;			
				5.2.2;	Identify anomalies		
5.2.5	Analysis	Identify inconsistencies	control logic binary;	4.4.11;	transform control logic binary to logical formulas	mathematical model representing behavior;	
					transform control logic binary to logical formulas		
5.2.6	Analysis	Identify inconsistencies	inloop data;	EXTERNAL;	Monitor payload behavior	generated I/O data of inloop simulator;	
				5.2.6			
5.2.7	Analysis	Identify inconsistencies	I/O data of inloop simulator;	5.2.6;	Create model of intended behvaior	mathematical model representing behavior;	
5.2.8	Analysis	Identify inconsistencies	generated I/O data of inloop simulator;	5.2.6;		unintended control logic behavior;	[16]
3.2.0	7.11017313	identity inconsistences	mathemtical model representing behavior;	5.2.5;	Compare model intended behavior with actual model	diminentate control logic benditory	[20]
5.2.9	Analysis	Identify inconsistancies	I/O values with timestamp (I/O tap);	4.4.6;		discrepancies between reported and actual I/O states;	[17]
5.2.9	Analysis	Identify inconsistencies	by protocol reported I/O values;	4.4.7;	Compare protocol information with I/O status	uiscrepancies between reported and actual I/O States;	[1/]
				1.1.1;			
				1.1.2;			
				1.1.3;			
			entify inconsistencies baseline data;	1.1.4;			
				1.1.5;			
				1.1.6;			
				1.1.7;			
		Identify inconsistencies				(unauthorized) changes of ICS with timestamp;	
				1.1.8;			
				1.1.9;			
5.2.10	Analysis			1.1.10;			
				1.1.11;			
				1.1.12;			
				1.1.13;			
				1.1.14;			
				1.1.15;			
				1.1.16;			
				1.1.17;			
				1.1.17,			
				1.1.19;	Compare baseline data with artefacts		
5.3.1	Analysis	Finalize Evidence	list acquired datas data sources;	2.6.1;		overview of used data sources and their data;	
			filled data model;	4.7.1;	Summarize distinct datasources into common timeline		
5.3.2	Analysis	Finalize Evidence	suspicious events/artefacts withe timetamp;	5.2.4;	assign all events to timelines	summarized timeline with all related events and their impact;	
5.3.3	Analysis	Finalize Evidence	connections/requests;	4.4.2;	Create network map	actual connections and devices in ICS;	
3.3.3	Allalysis	rinalize evidence			Create network map	actual connections and devices in ics,	
				5.1.1;			
				5.1.2;			
				5.1.3;			
				5.1.4;			
				5.1.5;			
				5.1.6;			
				5.1.7;			
504		6. 0. 6.1		5.1.8;			
5.3.4	Analysis	Finalize Evidence	all vizualizable artefacts;	5.2.1;		Clear summarization of evidence and its information value;	
				5.2.2;			
				5.2.4;			
				5.2.5;			
				5.2.6;			
				5.2.7;			
				5.2.8;			
				5.2.9;			
				5.2.10;	Visualize evidence		
				J.Z.10,	visualize evidence		

				5.1.1;			
				5.1.2;			
				5.1.3;			
				5.1.4;			
				5.1.5;			
				5.1.6;			
				5.1.7;			
				5.1.8;			
				5.2.1;			
5.4.1	Analysis	Create Hypothesis/Reconstruct incident	all gained evidence in analysis;	5.2.2;	Assign new data to data model	structurized overview of available and missing evidence;	
				5.2.4;			
				5.2.5;			
				5.2.6;			
				5.2.7;			
				5.2.8;			
				5.2.9;			
				5.2.10;			
				5.3.4;			
			structurized overview of available and missing evidence;	5.4.1;			
5.4.2	Analysis	Create Hypothesis/Reconstruct incident				incident trace;	
	<u> </u>	H	Clear summarization of evidence and its information value;	5.3.4;	create incident trace		
			incident trace;	5.4.2;			
5.4.3	Analysis	Create Hypothesis/Reconstruct incident	actuators/sensors;	1.1.1;		Impacts on ICS with related components;	
			ICS components;	1.1.2;	Note actions and their impact		
5.4.4	Analysis	Create Hypothesis/Reconstruct incident	structurized overview of available and missing evidence;	5.4.1;	Relate evidence to events	related evidence leading to incident;	
	.,	, , , , , , , , , , , , , , , , , , , ,	and the same of th	5.1.1;			
				5.1.2;			
				5.1.3;			
				5.1.4;			
				5.1.5;			
				5.1.6;			
	Analysis			5.1.7;			
		Reconsidertaion of further data (types) to retrieve		5.1.8;			
				5.2.1;			
5.5.1			all gained evidence in analysis;	5.2.2;		unseen assets and data sources;	
				5.2.4;			
				5.2.5;			
				5.2.6;			
				5.2.6; 5.2.7;			
				5.2.6; 5.2.7; 5.2.8;			
				5.2.6; 5.2.7; 5.2.8; 5.2.9;			
				5.2.6; 5.2.7; 5.2.8; 5.2.9; 5.2.10;	Eliteraries uncon humalistate delan		
				5.2.6; 5.2.7; 5.2.8; 5.2.9; 5.2.10; 5.3.4;	Filter prior unseen/unselected data		
5.5.2	Analysis	Reconsidertaion of further data (types) to retrieve	unseen assets and data sources;	5.2.6; 5.2.7; 5.2.8; 5.2.9; 5.2.10; 5.3.4; 5.5.1;	add new asset and data sources to list	assets and data sources to acquire data;	
5.5.3	Analysis	Reconsidertaion of further data (types) to retrieve	assets and data sources to acquire data;	5.2.6; 5.2.7; 5.2.8; 5.2.9; 5.2.10; 5.3.4; 5.5.1; 5.5.2;	add new asset and data sources to list begin next iteration at operational preparation task X.Y	Index of next activity and task;	[3]
			assets and data sources to acquire data; timestamp of performed functions and results;	5.2.6; 5.2.7; 5.2.8; 5.2.9; 5.2.10; 5.3.4; 5.5.1; 5.5.2; N/A	add new asset and data sources to list		[3]
5.5.3	Analysis	Reconsidertaion of further data (types) to retrieve	assets and data sources to acquire data; timestamp of performed functions and results; tools to search specific data types;	5.2.6; 5.2.7; 5.2.8; 5.2.9; 5.2.10; 5.3.4; 5.5.1; 5.5.2; N/A	add new asset and data sources to list begin next iteration at operational preparation task X.Y	Index of next activity and task;	[3]
5.5.3	Analysis	Reconsidertaion of further data (types) to retrieve	assets and data sources to acquire data; timestamp of performed functions and results;	5.2.6; 5.2.7; 5.2.8; 5.2.9; 5.2.10; 5.3.4; 5.5.1; 5.5.2; N/A 2.6.1; 4.2.3;	add new asset and data sources to list begin next iteration at operational preparation task X.Y	Index of next activity and task;	[3]
5.5.3 6.1.1	Analysis Reporting	Reconsidertaion of further data (types) to retrieve Generate History Report	assets and data sources to acquire data; timestamp of performed functions and results; tools to search specific data types; tools to extract specific data types;	5.2.6; 5.2.7; 5.2.8; 5.2.9; 5.2.10; 5.3.4; 5.5.1; 5.5.2; N/A	add new asset and data sources to list begin next iteration at operational preparation task X.Y Note all actions taken	Index of next activity and task; timeline of forensic investigation actions;	
5.5.3 6.1.1 6.1.2	Analysis Reporting Reporting	Reconsidertaion of further data (types) to retrieve Generate History Report Generate History Report	assets and data sources to acquire data; timestamp of performed functions and results; tools to search specific data types; tools to extract specific data types; list of data to be acquired with specific tools;	5.2.6; 5.2.7; 5.2.8; 5.2.9; 5.2.10; 5.3.4; 5.5.1; 5.5.2; N/A 2.6.1; 4.2.3; 4.4.1;	add new asset and data sources to list begin next iteration at operational preparation task X.Y Note all actions taken Note all tools used	index of next activity and task: timeline of forensic investigation actions; all used tools and processed data;	[3]
5.5.3 6.1.1 6.1.2	Analysis Reporting Reporting Reporting	Reconsidertaion of further data (types) to retrieve Generate History Report Generate History Report Generate History Report	assets and data sources to acquire data; timestamp of performed functions and results; tools to search specific data types; tools to extract specific data types; list of data to be acquired with specific tools; list of data to be acquired with specific tools;	5.2.6; 5.2.7; 5.2.8; 5.2.9; 5.2.10; 5.3.4; 5.5.1; 5.5.2; N/A 2.6.1; 4.2.3; 4.4.1;	add new asset and data sources to list begin next iteration at operational preparation task X.Y  Note all actions taken  Note all tools used  Note used data (sources)	index of next activity and task; timeline of forensic investigation actions;  all used tools and processed data;  all affected and relevant data sources;	[3]
5.5.3 6.1.1 6.1.2	Analysis Reporting Reporting	Reconsidertaion of further data (types) to retrieve Generate History Report Generate History Report	assets and data sources to acquire data; timestamp of performed functions and results; tools to search specific data types; tools to extract specific data types; list of data to be acquired with specific tools; list of data to be acquired with specific tools; timeline of forensic investigation actions;	5.2.6; 5.2.7; 5.2.8; 5.2.9; 5.2.10; 5.3.4; 5.5.1; 5.5.2; N/A 2.6.1; 4.2.3; 4.4.1; 4.4.1; 6.1.1;	add new asset and data sources to list begin next iteration at operational preparation task X.Y Note all actions taken Note all tools used	index of next activity and task: timeline of forensic investigation actions; all used tools and processed data;	[3]
5.5.3 6.1.1 6.1.2	Analysis Reporting Reporting Reporting	Reconsidertaion of further data (types) to retrieve Generate History Report Generate History Report Generate History Report	assets and data sources to acquire data; timestamp of performed functions and results; tools to search specific data types; tools to extract specific data types; list of data to be acquired with specific tools; list of data to be acquired with specific tools; timeline of forensic investigation actions; legal actions taken;	5.2.6; 5.2.7; 5.2.8; 5.2.9; 5.2.10; 5.3.4; 5.5.1; 5.5.2; N/A 2.6.1; 4.2.3; 4.4.1;	add new asset and data sources to list begin next iteration at operational preparation task X.Y  Note all actions taken  Note all tools used  Note used data (sources)	index of next activity and task; timeline of forensic investigation actions;  all used tools and processed data;  all affected and relevant data sources;	[3]
5.5.3 6.1.1 6.1.2 6.1.3 6.1.4	Analysis Reporting Reporting Reporting Reporting	Reconsidertation of further data (types) to retrieve Generate History Report Generate History Report Generate History Report Generate History Report	assets and data sources to acquire data; timestamp of performed functions and results; tools to search specific data types; tools to extract specific data types; list of data to be acquired with specific tools; list of data to be acquired with specific tools; timeline of forensic investigation actions; legal actions taken; protection goals status of final artefacts (filled data model);	5.2.6; 5.2.7; 5.2.8; 5.2.9; 5.2.10; 5.3.4; 5.5.1; 5.5.2; N/A 2.6.1; 4.2.3; 4.4.1; 4.4.1; N/A	add new asset and data sources to list begin next iteration at operational preparation task X.Y  Note all actions taken  Note all tools used  Note used data (sources)	index of next activity and task: timeline of forensic investigation actions; all used tools and processed data; all affected and relevant data sources; Authorized manipulation of ICS components;	[3]
5.5.3 6.1.1 6.1.2	Analysis Reporting Reporting Reporting	Reconsidertaion of further data (types) to retrieve Generate History Report Generate History Report Generate History Report	assets and data sources to acquire data; timestamp of performed functions and results; tools to search specific data types; tools to extract specific data types; list of data to be acquired with specific tools; list of data to be acquired with specific tools; timeline of forensic investigation actions; legal actions taken;	5.2.6; 5.2.7; 5.2.8; 5.2.9; 5.2.10; 5.3.4; 5.5.1; 5.5.2; N/A 2.6.1; 4.2.3; 4.4.1; 4.4.1; N/A 4.7.1;	add new asset and data sources to list begin next iteration at operational preparation task X.Y Note all actions taken  Note all tools used Note used data (sources) Note manipulations taken on systems	index of next activity and task; timeline of forensic investigation actions;  all used tools and processed data;  all affected and relevant data sources;	[3]
5.5.3 6.1.1 6.1.2 6.1.3 6.1.4	Analysis Reporting Reporting Reporting Reporting Reporting Reporting	Reconsidertaion of further data (types) to retrieve Generate History Report	assets and data sources to acquire data; timestamp of performed functions and results; tools to search specific data types; tools to extract specific data types; list of data to be acquired with specific tools; list of data to be acquired with specific tools; timeline of forensic investigation actions; legal actions taken; protection goals status of final artefacts (filled data model); forensic compilant requirements;	5.2.6; 5.2.7; 5.2.8; 5.2.9; 5.2.10; 5.3.4; 5.5.1; 5.5.2; N/A 2.6.1; 4.2.3; 4.4.1; 4.4.1; 6.1.1; N/A 4.7.1; EXTERNAL	add new asset and data sources to list begin next iteration at operational preparation task X.Y  Note all actions taken  Note all tools used  Note used data (sources)  Note manipulations taken on systems  Asses compliance with protection goals (measures)	Index of next activity and task: timeline of forensic investigation actions; all used tools and processed data; all affected and relevant data sources; Authorized manipulation of ICS components; forensic compliance of final evidence;	[3]
5.5.3 6.1.1 6.1.2 6.1.3 6.1.4	Analysis Reporting Reporting Reporting Reporting	Reconsidertation of further data (types) to retrieve Generate History Report Generate History Report Generate History Report Generate History Report	assets and data sources to acquire data; timestamp of performed functions and results; tools to search specific data types; tools to extract specific data types; list of data to be acquired with specific tools; list of data to be acquired with specific tools; timeline of forensic investigation actions; legal actions taken; protection goals status of final artefacts (filled data model);	5.2.6; 5.2.7; 5.2.8; 5.2.9; 5.2.10; 5.3.4; 5.5.1; 5.5.2; N/A 2.6.1; 4.2.3; 4.4.1; 4.4.1; N/A 4.7.1;	add new asset and data sources to list begin next iteration at operational preparation task X.Y Note all actions taken  Note all tools used Note used data (sources) Note manipulations taken on systems	index of next activity and task: timeline of forensic investigation actions; all used tools and processed data; all affected and relevant data sources; Authorized manipulation of ICS components;	[3]
5.5.3 6.1.1 6.1.2 6.1.3 6.1.4	Analysis Reporting Reporting Reporting Reporting Reporting Reporting	Reconsidertaion of further data (types) to retrieve Generate History Report	assets and data sources to acquire data; timestamp of performed functions and results; tools to search specific data types; tools to extract specific data types; list of data to be acquired with specific tools; list of data to be acquired with specific tools; timeline of forensic investigation actions; legal actions taken; protection goals status of final artefacts (filled data model); forensic compliant requirements;	5.2.6; 5.2.7; 5.2.8; 5.2.9; 5.2.10; 5.3.4; 5.5.1; 5.5.2; N/A 2.6.1; 4.2.3; 4.4.1; 4.4.1; 6.1.1; N/A 4.7.1; EXTERNAL	add new asset and data sources to list begin next iteration at operational preparation task X.Y  Note all actions taken  Note all tools used  Note used data (sources)  Note manipulations taken on systems  Asses compliance with protection goals (measures)	Index of next activity and task: timeline of forensic investigation actions; all used tools and processed data; all affected and relevant data sources; Authorized manipulation of ICS components; forensic compliance of final evidence;	[3]
5.5.3 6.1.1 6.1.2 6.1.3 6.1.4	Analysis Reporting Reporting Reporting Reporting Reporting Reporting	Reconsidertaion of further data (types) to retrieve Generate History Report	assets and data sources to acquire data; timestamp of performed functions and results; tools to search specific data types; tools to extract specific data types; list of data to be acquired with specific tools; list of data to be acquired with specific tools; timeline of forensic investigation actions; legal actions taken; protection goals status of final artefacts (filled data model); forensic compilant requirements;  forensic compilant requirements; related events and incident trace;	5.2.6; 5.2.7; 5.2.8; 5.2.9; 5.2.10; 5.3.4; 5.5.1; 5.5.2; N/A 2.6.1; 4.2.3; 4.4.1; 4.4.1; N/A 4.7.1; EXTERNAL 6.1.6;	add new asset and data sources to list begin next iteration at operational preparation task X.Y  Note all actions taken  Note all tools used  Note used data (sources)  Note manipulations taken on systems  Asses compliance with protection goals (measures)	Index of next activity and task: timeline of forensic investigation actions; all used tools and processed data; all affected and relevant data sources; Authorized manipulation of ICS components; forensic compliance of final evidence;	[3]
5.5.3 6.1.1 6.1.2 6.1.3 6.1.4 6.1.6	Analysis Reporting Reporting Reporting Reporting Reporting Reporting Reporting	Reconsidertation of further data (types) to retrieve Generate History Report	assets and data sources to acquire data; timestamp of performed functions and results; tools to search specific data types; tools to extract specific data types; list of data to be acquired with specific tools; list of data to be acquired with specific tools; timeline of forensic investigation actions; legal actions taken; protection goals status of final artefacts (filled data model); forensic compliant requirements;  forensic compliant end evidence; related events and incident trace; Impacts on ICS with related components;	5.2.6; 5.2.7; 5.2.8; 5.2.9; 5.2.10; 5.3.4; 5.5.1; 5.5.2; N/A 2.6.1; 4.4.1; 4.4.1; N/A 4.7.1; EXTERNAL 6.1.6;	add new asset and data sources to list begin next iteration at operational preparation task X.Y  Note all actions taken  Note all tools used  Note used data (sources)  Note manipulations taken on systems  Asses compliance with protection goals (measures)	index of next activity and task; timeline of forensic investigation actions; all used tools and processed data; all affected and relevant data sources; Authorized manipulation of ICS components; forensic compliance of final evidence; significance of use of the evidence;	[3] [3] [3]
5.5.3 6.1.1 6.1.2 6.1.3 6.1.4	Analysis Reporting Reporting Reporting Reporting Reporting Reporting	Reconsidertaion of further data (types) to retrieve Generate History Report	assets and data sources to acquire data; timestamp of performed functions and results; tools to search specific data types; tools to extract specific data types; list of data to be acquired with specific tools; list of data to be acquired with specific tools; timeline of forensic investigation actions; legal actions taken; protection goals status of final artefacts (filled data model); forensic compliant requirements;  forensic compliant requirements; related events and incident trace; Impacts on ICS with related components; related evidence leading to incident;	5.2.6; 5.2.7; 5.2.8; 5.2.9; 5.2.10; 5.3.4; 5.5.1; 5.5.2; N/A 2.6.1; 4.2.3; 4.4.1; 4.4.1; 6.1.1; N/A 4.7.1; EXTERNAL 6.1.6;	add new asset and data sources to list begin next iteration at operational preparation task X.Y  Note all actions taken  Note all tools used  Note used data (sources)  Note manipulations taken on systems  Asses compliance with protection goals (measures)	Index of next activity and task: timeline of forensic investigation actions; all used tools and processed data; all affected and relevant data sources; Authorized manipulation of ICS components; forensic compliance of final evidence;	[3]
5.5.3 6.1.1 6.1.2 6.1.3 6.1.4 6.1.6	Analysis Reporting Reporting Reporting Reporting Reporting Reporting Reporting	Reconsidertation of further data (types) to retrieve Generate History Report	assets and data sources to acquire data; timestamp of performed functions and results; tools to search specific data types; tools to extract specific data types; list of data to be acquired with specific tools; list of data to be acquired with specific tools; timeline of forensic investigation actions; legal actions taken; protection goals status of final artefacts (filled data model); forensic compliant requirements;  forensic compliant end evidence; related events and incident trace; Impacts on ICS with related components;	5.2.6; 5.2.7; 5.2.8; 5.2.9; 5.2.10; 5.3.4; 5.5.1; 5.5.2; N/A 2.6.1; 4.4.1; 4.4.1; N/A 4.7.1; EXTERNAL 6.1.6;	add new asset and data sources to list begin next iteration at operational preparation task X.Y  Note all actions taken  Note all tools used  Note used data (sources)  Note manipulations taken on systems  Asses compliance with protection goals (measures)	index of next activity and task; timeline of forensic investigation actions; all used tools and processed data; all affected and relevant data sources; Authorized manipulation of ICS components; forensic compliance of final evidence; significance of use of the evidence;	[3] [3] [3]
5.5.3 6.1.1 6.1.2 6.1.3 6.1.4 6.1.6	Analysis Reporting Reporting Reporting Reporting Reporting Reporting Reporting	Reconsidertation of further data (types) to retrieve Generate History Report	assets and data sources to acquire data; timestamp of performed functions and results; tools to search specific data types; tools to extract specific data types; list of data to be acquired with specific tools; list of data to be acquired with specific tools; timeline of forensic investigation actions; legal actions taken; protection goals status of final artefacts (filled data model); forensic compliant requirements;  forensic compliant requirements; related events and incident trace; Impacts on ICS with related components; related evidence leading to incident;	5.2.6; 5.2.7; 5.2.8; 5.2.9; 5.2.10; 5.3.4; 5.5.1; 5.5.2; N/A 2.6.1; 4.2.3; 4.4.1; 4.4.1; 6.1.1; N/A 4.7.1; EXTERNAL 6.1.6;	add new asset and data sources to list begin next iteration at operational preparation task X.Y Note all actions taken  Note all tools used  Note used data (sources) Note manipulations taken on systems  Asses compliance with protection goals (measures) Note compliance of evidence in report	index of next activity and task; timeline of forensic investigation actions; all used tools and processed data; all affected and relevant data sources; Authorized manipulation of ICS components; forensic compliance of final evidence; significance of use of the evidence;	[3] [3] [3]
5.5.3 6.1.1 6.1.2 6.1.3 6.1.4 6.1.6	Analysis Reporting Reporting Reporting Reporting Reporting Reporting Reporting	Reconsidertation of further data (types) to retrieve Generate History Report	assets and data sources to acquire data; timestamp of performed functions and results; tools to search specific data types; tools to extract specific data types; list of data to be acquired with specific tools; list of data to be acquired with specific tools; timeline of forensic investigation actions; legal actions taken; protection goals status of final artefacts (filled data model); forensic compliant requirements;  forensic compliant end evidence; related events and incident trace; Impacts on ICS with related components; related evidence leading to incident; Clear summarization of evidence and its information value; summarized timeline with all related events and their impact;	5.2.6; 5.2.7; 5.2.8; 5.2.9; 5.2.10; 5.3.4; 5.5.1; 5.5.2; N/A 2.6.1; 4.4.1; 6.1.1; N/A 4.7.1; EXTERNAL 6.1.6; 5.4.2; 5.4.3; 5.4.4;	add new asset and data sources to list begin next iteration at operational preparation task X.Y  Note all actions taken  Note all tools used  Note used data (sources)  Note manipulations taken on systems  Asses compliance with protection goals (measures)	index of next activity and task; timeline of forensic investigation actions; all used tools and processed data; all affected and relevant data sources; Authorized manipulation of ICS components; forensic compliance of final evidence; significance of use of the evidence;	[3] [3] [3]
5.5.3 6.1.1 6.1.2 6.1.3 6.1.4 6.1.6	Analysis Reporting Reporting Reporting Reporting Reporting Reporting Reporting	Reconsidertation of further data (types) to retrieve Generate History Report	assets and data sources to acquire data; timestamp of performed functions and results; tools to search specific data types; tools to extract specific data types; its of data to be acquired with specific tools; list of data to be acquired with specific tools; timeline of forensic investigation actions; legal actions taken; protection goals status of final artefacts (filled data model); forensic compliant requirements;  forensic compliant requirements; related events and incident trace; Impacts on ICS with related components; related evidence leading to incident; Clear summarization of evidence and its information value; summarized timeline with all related events and their impact; Legal requirements;	5.2.6; 5.2.7; 5.2.8; 5.2.9; 5.2.10; 5.3.4; 5.5.1; 5.5.2; N/A 2.6.1; 4.2.3; 4.4.1; 4.4.1; 6.1.1; N/A 4.7.1; EXTERNAL 6.1.6;	add new asset and data sources to list begin next iteration at operational preparation task X.Y Note all actions taken  Note all tools used  Note used data (sources) Note manipulations taken on systems  Asses compliance with protection goals (measures) Note compliance of evidence in report	index of next activity and task; timeline of forensic investigation actions; all used tools and processed data; all affected and relevant data sources; Authorized manipulation of ICS components; forensic compliance of final evidence; significance of use of the evidence;	[3] [3] [3]
5.5.3 6.1.1 6.1.2 6.1.3 6.1.4 6.1.6	Analysis Reporting Reporting Reporting Reporting Reporting Reporting Reporting	Reconsidertation of further data (types) to retrieve Generate History Report	assets and data sources to acquire data; timestamp of performed functions and results; tools to search specific data types; tools to extract specific data types; list of data to be acquired with specific tools; list of data to be acquired with specific tools; timeline of forensic investigation actions; legal actions taken; protection goals status of final artefacts (filled data model); forensic compliant requirements;  forensic compliant end evidence; related events and incident trace; Impacts on ICS with related components; related evidence leading to incident; Clear summarization of evidence and its information value; summarized timeline with all related events and their impact;	5.2.6; 5.2.7; 5.2.8; 5.2.9; 5.2.10; 5.3.4; 5.5.1; 5.5.2; N/A 2.6.1; 4.4.1; 6.1.1; N/A 4.7.1; EXTERNAL 6.1.6; 5.4.2; 5.4.3; 5.4.4;	add new asset and data sources to list begin next iteration at operational preparation task X.Y Note all actions taken  Note all tools used  Note used data (sources) Note manipulations taken on systems  Asses compliance with protection goals (measures) Note compliance of evidence in report	index of next activity and task; timeline of forensic investigation actions; all used tools and processed data; all affected and relevant data sources; Authorized manipulation of ICS components; forensic compliance of final evidence; significance of use of the evidence;	[3] [3] [3]
6.1.2 6.1.3 6.1.4 6.1.6 6.1.7	Analysis Reporting Reporting Reporting Reporting Reporting Reporting Reporting Reporting Reporting	Reconsideration of further data (types) to retrieve Generate History Report	assets and data sources to acquire data; timestamp of performed functions and results; tools to search specific data types; tools to extract specific data types; its of data to be acquired with specific tools; list of data to be acquired with specific tools; timeline of forensic investigation actions; legal actions taken; protection goals status of final artefacts (filled data model); forensic compliant requirements;  forensic compliant requirements; related events and incident trace; Impacts on ICS with related components; related evidence leading to incident; Clear summarization of evidence and its information value; summarized timeline with all related events and their impact; Legal requirements;	5.2.6; 5.2.7; 5.2.8; 5.2.9; 5.2.10; 5.3.4; 5.5.1; 5.5.2; N/A 2.6.1; 4.2.3; 4.4.1; 6.1.1; N/A 4.7.1; EXTERNAL 6.1.6; 5.4.2; 5.4.3; 5.4.4;	add new asset and data sources to list begin next iteration at operational preparation task X.Y Note all actions taken  Note all tools used  Note used data (sources) Note manipulations taken on systems  Asses compliance with protection goals (measures) Note compliance of evidence in report	Index of next activity and task: timeline of forensic investigation actions; all used tools and processed data; all affected and relevant data sources; Authorized manipulation of iCS components; forensic compliance of final evidence; significance of use of the evidence; Clear summarization of evidence and its information value;	[3] [3] [3] [3]
5.5.3 6.1.1 6.1.2 6.1.3 6.1.4 6.1.6	Analysis Reporting Reporting Reporting Reporting Reporting Reporting Reporting	Reconsidertation of further data (types) to retrieve Generate History Report	assets and data sources to acquire data; timestamp of performed functions and results; tools to search specific data types; tools to textract specific data types; its of data to be acquired with specific tools; list of data to be acquired with specific tools; timeline of forensic investigation actions; legal actions taken; protection goals status of final artefacts (filled data model); forensic compliant requirements;  forensic compliance of final evidence; related events and incident trace; Impacts on ICS with related components; related evidence leading to incident; Clear summarization of evidence and its information value; summarized timeline with all related events and their impact; Clear summarization of evidence and its information value; final evidence; Clear summarization of evidence and its information value; final evidence;	5.2.6; 5.2.7; 5.2.8; 5.2.9; 5.2.10; 5.3.4; 5.5.1; 5.5.2; N/A 2.6.1; 4.2.3; 4.4.1; N/A 4.7.1; EXTERNAL 6.1.6; 5.4.2; 5.4.4;	add new asset and data sources to list begin next iteration at operational preparation task X.Y Note all actions taken  Note all tools used  Note used data (sources) Note manipulations taken on systems  Asses compliance with protection goals (measures) Note compliance of evidence in report	index of next activity and task; timeline of forensic investigation actions; all used tools and processed data; all affected and relevant data sources; Authorized manipulation of ICS components; forensic compliance of final evidence; significance of use of the evidence;	[3] [3] [3]
6.1.2 6.1.3 6.1.4 6.1.6 6.1.7	Analysis Reporting Reporting Reporting Reporting Reporting Reporting Reporting Reporting Reporting	Reconsideration of further data (types) to retrieve Generate History Report	assets and data sources to acquire data; timestamp of performed functions and results; tools to search specific data types; tools to extract specific data types; its of data to be acquired with specific tools; list of data to be acquired with specific tools; timeline of forensic investigation actions; legal actions taken; protection goals status of final artefacts (filled data model); forensic compliant requirements;  forensic compliant requirements;  related events and incident trace; Impacts on ICS with related components; related evience leading to incident; Clear summarization of evidence and its information value; summarized timeline with all related events and their impact;  Legal requirements; Clear summarization of evidence and its information value; final evidence; timeline of forensic investigation;	5.2.6; 5.2.7; 5.2.8; 5.2.9; 5.2.10; 5.3.4; 5.5.1; 5.5.2; N/A 2.6.1; 4.2.3; 4.4.1; 6.1.1; N/A 4.7.1; EXTERNAL 6.1.6; 5.4.2; 5.4.4; 5.4.4;	add new asset and data sources to list begin next iteration at operational preparation task X.Y Note all actions taken  Note all tools used  Note used data (sources) Note manipulations taken on systems  Asses compliance with protection goals (measures) Note compliance of evidence in report	Index of next activity and task: timeline of forensic investigation actions; all used tools and processed data; all affected and relevant data sources; Authorized manipulation of iCS components; forensic compliance of final evidence; significance of use of the evidence; Clear summarization of evidence and its information value;	[3] [3] [3] [3]
6.1.2 6.1.3 6.1.4 6.1.6 6.1.7	Analysis Reporting Reporting Reporting Reporting Reporting Reporting Reporting Reporting Reporting	Reconsideration of further data (types) to retrieve Generate History Report	assets and data sources to acquire data; timestamp of performed functions and results; tools to search specific data types; tools to extract specific data types; its of data to be acquired with specific tools; list of data to be acquired with specific tools; timeline of forensic investigation actions; legal actions taken; protection goals status of final artefacts (filled data model); forensic compliant requirements;  forensic compliant requirements;  related events and incident trace; impacts on ICS with related components; related evidence leading to incident; Clear summarization of evidence and its information value; summarized timeline with all related events and their impact; Legal requirements; Clear summarization of evidence and its information value; final evidence; timeline of forensic investigation; all affected and relevant data sources;	5.2.6; 5.2.7; 5.2.8; 5.2.9; 5.2.10; 5.3.4; 5.5.1; 5.5.2; N/A 2.6.1; 4.2.3; 4.4.1; N/A 4.7.1; EXTERNAL 6.1.6; 5.4.2; 5.4.3; 5.4.4;	add new asset and data sources to list begin next iteration at operational preparation task X.Y  Note all actions taken  Note used data (sources)  Note used data (sources)  Note manipulations taken on systems  Asses compliance with protection goals (measures)  Note compliance of evidence in report	Index of next activity and task: timeline of forensic investigation actions; all used tools and processed data; all affected and relevant data sources; Authorized manipulation of iCS components; forensic compliance of final evidence; significance of use of the evidence; Clear summarization of evidence and its information value;	[3] [3] [3] [3]
6.1.2 6.1.3 6.1.4 6.1.6 6.1.7	Analysis Reporting Reporting Reporting Reporting Reporting Reporting Reporting Reporting Reporting	Reconsideration of further data (types) to retrieve Generate History Report	assets and data sources to acquire data; timestamp of performed functions and results; tools to search specific data types; tools to extract specific data types; list of data to be acquired with specific tools; list of data to be acquired with specific tools; timeline of forensic investigation actions; legal actions taken; protection goals status of final artefacts (filled data model); forensic compliant requirements;  forensic compliant requirements;  related events and incident trace; Impacts on ICS with related components; related evidence leading to incident; Clear summarization of evidence and its information value; summarized timeline with all related events and their impact;  Legal requirements; Clear summarization of evidence and its information value; final evidence; timeline of forensic investigation; all affected and relevant data sources; Authorized mainpluation of (SC components;	5.2.6; 5.2.7; 5.2.8; 5.2.9; 5.2.10; 5.3.4; 5.5.1; 5.5.2; N/A 2.6.1; 4.2.3; 4.4.1; 4.4.1; 6.1.1; N/A 4.7.1; EXTERNAL 6.1.6; 5.4.2; 5.4.3; 5.4.4; 6.1.8; 6.1.8; 6.1.3; 6.1.3; 6.1.3; 6.1.3; 6.1.1; 6.1.1;	add new asset and data sources to list begin next iteration at operational preparation task X.Y Note all actions taken  Note all tools used  Note used data (sources) Note manipulations taken on systems  Asses compliance with protection goals (measures) Note compliance of evidence in report	Index of next activity and task: timeline of forensic investigation actions; all used tools and processed data; all affected and relevant data sources; Authorized manipulation of iCS components; forensic compliance of final evidence; significance of use of the evidence; Clear summarization of evidence and its information value;	[3] [3] [3] [3]
5.5.3 6.1.1 6.1.2 6.1.3 6.1.4 6.1.6 6.1.7	Analysis Reporting Reporting Reporting Reporting Reporting Reporting Reporting Reporting Reporting	Reconsideration of further data (types) to retrieve Generate History Report	assets and data sources to acquire data; timestamp of performed functions and results; tools to search specific data types; tools to extract specific data types; its of data to be acquired with specific tools; list of data to be acquired with specific tools; timeline of forensic investigation actions; legal actions taken; protection goals status of final artefacts (filled data model); forensic compliance of final evidence; related events and incident trace; Impacts on ICS with related components; related evidence leading to incident; Clear summarization of evidence and its information value; summarized timeline with all related events and their impact; Legal requirements; Clear summarization of evidence and its information value; final evidence; timeline of forensic investigation; all affected and relevant data sources; Authorized manipulation of ICS components;	5.2.6; 5.2.7; 5.2.8; 5.2.9; 5.2.10; 5.3.4; 5.5.1; 5.5.2; N/A 2.6.1; 4.2.3; 4.4.1; 6.1.1; N/A 4.7.1; EXTERNAL 6.1.6; 5.4.2; 5.4.3; 5.4.4; 6.1.3; 6.1.1; 6.1.3; 6.1.3; 6.1.3; 6.1.3; 6.1.3;	add new asset and data sources to list begin next iteration at operational preparation task X.Y  Note all actions taken  Note used data (sources)  Note used data (sources)  Note manipulations taken on systems  Asses compliance with protection goals (measures)  Note compliance of evidence in report  Full incident and impact of events	Index of next activity and task: timeline of forensic investigation actions; all used tools and processed data; all affected and relevant data sources; Authorized manipulation of ICS components; forensic compliance of final evidence; significance of use of the evidence; Clear summarization of evidence and its information value; final evidence report;	[3] [3] [3] [3]
6.1.2 6.1.3 6.1.4 6.1.6 6.1.7	Analysis Reporting Reporting Reporting Reporting Reporting Reporting Reporting Reporting Reporting	Reconsideration of further data (types) to retrieve Generate History Report	assets and data sources to acquire data; timestamp of performed functions and results; tools to search specific data types; tools to extract specific data types; its of data to be acquired with specific tools; list of data to be acquired with specific tools; timeline of forensic investigation actions; legal actions taken; protection goals status of final artefacts (filled data model); forensic compliant requirements;  forensic compliant requirements; related events and incident trace; Impacts on ICS with related components; related evidence leading to incident; Clear summarization of evidence and its information value; summarized timeline with all related events and their impact; Legal requirements; Clear summarization of evidence and its information value; final evidence; timeline of forensic investigation; all affected and relevant data sources; Authorized manipulation of IcS components; target group roles; key objectives of target group roles;	5.2.6; 5.2.7; 5.2.8; 5.2.9; 5.2.10; 5.3.4; 5.5.1; 5.5.2; N/A 2.6.1; 4.4.1; 4.4.1; 6.1.1; N/A 4.7.1; EXTERNAL 6.1.6; 5.4.2; 5.4.4; 6.1.2; 6.1.3; 6.1.3; 6.1.2; 6.1.3; 6.1.2; 6.1.3; 6.1.2; 6.1.3; 6.1.2; 6.1.3; 6.1.2; 6.1.3; 6.1.2; 6.1.3; 6.1.2; 6.1.3; 6.1.2; 6.1.3; 6.1.2; 6.1.3; 6.1.2; 6.1.3; 6.1.2; 6.1.3; 6.1.2; 6.1.3;	add new asset and data sources to list begin next iteration at operational preparation task X.Y  Note all actions taken  Note used data (sources)  Note used data (sources)  Note manipulations taken on systems  Asses compliance with protection goals (measures)  Note compliance of evidence in report	Index of next activity and task: timeline of forensic investigation actions; all used tools and processed data; all affected and relevant data sources; Authorized manipulation of iCS components; forensic compliance of final evidence; significance of use of the evidence; Clear summarization of evidence and its information value;	[3] [3] [3] [3]
5.5.3 6.1.1 6.1.2 6.1.3 6.1.4 6.1.6 6.1.7	Analysis Reporting	Reconsideration of further data (types) to retrieve Generate History Report  Generate History Report  Generate History Report  Generate History Report  Generate History Report	assets and data sources to acquire data; timestamp of performed functions and results; tools to search specific data types; tools to extract specific data types; its of data to be acquired with specific tools; list of data to be acquired with specific tools; timeline of forensic investigation actions; legal actions taken; protection goals status of final artefacts (filled data model); forensic compliant requirements;  forensic compliant requirements;  related events and incident trace; Impacts on ICS with related components; related evidence leading to incident; Clear summarization of evidence and its information value; summarized timeline with all related events and their impact;  Legal requirements; Clear summarization of evidence and its information value; final evidence; timeline of forensic investigation; all affected and relevant data sources; Authorized manipulation of ICS components; target group requirements;	5.2.6; 5.2.7; 5.2.8; 5.2.9; 5.2.10; 5.3.4; 5.5.1; 5.5.2; N/A 2.6.1; 4.2.3; 4.4.1; 6.1.1; N/A 4.7.1; EXTERNAL 6.1.6; 5.4.2; 5.4.3; 5.4.4; 6.1.3; 6.1.3; 6.1.3; 6.1.3; 6.1.3; 6.1.3; 6.1.3; 6.1.3; 6.1.4; EXTERNAL; EXTERNAL; EXTERNAL; EXTERNAL; EXTERNAL; EXTERNAL; EXTERNAL; EXTERNAL;	add new asset and data sources to list begin next iteration at operational preparation task X.Y  Note all actions taken  Note all tools used  Note used data (sources)  Note manipulations taken on systems  Asses compliance with protection goals (measures)  Note compliance of evidence in report  Full incident and impact of events  Summarize  Asses target group requirements	Index of next activity and task:  timeline of forensic investigation actions;  all used tools and processed data;  all affected and relevant data sources; Authorized manipulation of ICS components;  forensic compliance of final evidence;  significance of use of the evidence;  Clear summarization of evidence and its information value;  final evidence report;  target group requirements;	[3] [3] [3] [3]
6.1.2 6.1.3 6.1.4 6.1.6 6.1.7	Analysis Reporting Reporting Reporting Reporting Reporting Reporting Reporting Reporting Reporting	Reconsideration of further data (types) to retrieve Generate History Report	assets and data sources to acquire data; timestamp of performed functions and results; tools to search specific data types; tools to extract specific data types; its of data to be acquired with specific tools; list of data to be acquired with specific tools; timeline of forensic investigation actions; legal actions taken; protection goals status of final artefacts (filled data model); forensic compliant requirements;  forensic compliant requirements; related events and incident trace; Impacts on ICS with related components; related evidence leading to incident; Clear summarization of evidence and its information value; summarized timeline with all related events and their impact; Legal requirements; Clear summarization of evidence and its information value; final evidence; timeline of forensic investigation; all affected and relevant data sources; Authorized manipulation of IcS components; target group roles; key objectives of target group roles;	5.2.6; 5.2.7; 5.2.8; 5.2.9; 5.2.10; 5.3.4; 5.5.1; 5.5.2; N/A 2.6.1; 4.4.1; 4.4.1; 6.1.1; N/A 4.7.1; EXTERNAL 6.1.6; 5.4.2; 5.4.4; 6.1.2; 6.1.3; 6.1.3; 6.1.2; 6.1.3; 6.1.2; 6.1.3; 6.1.2; 6.1.3; 6.1.2; 6.1.3; 6.1.2; 6.1.3; 6.1.2; 6.1.3; 6.1.2; 6.1.3; 6.1.2; 6.1.3; 6.1.2; 6.1.3; 6.1.2; 6.1.3; 6.1.2; 6.1.3; 6.1.2; 6.1.3;	add new asset and data sources to list begin next iteration at operational preparation task X.Y  Note all actions taken  Note used data (sources)  Note used data (sources)  Note manipulations taken on systems  Asses compliance with protection goals (measures)  Note compliance of evidence in report  Full incident and impact of events	Index of next activity and task: timeline of forensic investigation actions; all used tools and processed data; all affected and relevant data sources; Authorized manipulation of ICS components; forensic compliance of final evidence; significance of use of the evidence; Clear summarization of evidence and its information value; final evidence report;	[3] [3] [3] [3]