

| 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 | | |
| 1.1.4 | Strategic Preparation | Establish baseline of ICS | IT asset inventory; | EXTERNAL | Acquire IT asset inventory | Entries to ICS asset inventory with IT components; | |
| 1.1.5 | Strategic Preparation | Establish baseline of ICS | IT components attributes; | 1.1.3; EXTERNAL | 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; | Identify supported and undocumented technology systems (modern/proprietary systems) | 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 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 | Strategic Preparation | Establish baseline of ICS | Field devices, actuators and sensors (were applicable) configuration; | 1.1.10; 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/capabilities 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; | Analyze fields protocol | pattern/bytes of protocol; | [4] |
| 1.3.4 | Strategic Preparation | Determining known and unknown data types (data model) | Engineering workstation files; | 1.1.15; | Analyze project filetype | content of specific filetype; | |
| 1.3.5 | Strategic Preparation | Determining known and unknown data types (data model) | Stored configuration files; | 1.1.16; | | | |
| 1.3.6 | Strategic Preparation | Determining known and unknown data types (data model) | Network components cofigurations; | 1.1.19; | Analyze configurationfiles | specific content of configurations; | |
| 1.3.6 | Strategic Preparation | Determining known and unknown data types (data model) | field devices content; | 1.1.1; 1.2.4; | Analyze firmware files | firmware; | [5] |
| 1.3.7 | Strategic Preparation | Determining known and unknown data types (data model) | Stored control logic files; Location of data sources; | 1.1.18; 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; 1.3.3; 1.3.4; 1.3.5; 1.3.6; 1.3.7; | 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 capabilities in architecture; | [1] |
| 1.4.2 | Strategic Preparation | Assesment of forensic capabilities | field devices; | 1.1.1; | Identify devices interfaces | existing interfaces to retrieve forensic data; | |
| 1.4.3 | Strategic Preparation | Assesment of forensic capabilities | Assets; data sources; | 1.1.10; 1.2.4; | Identify software interfaces | existing software interface to retrieve forensic data; | |
| 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 capabilities 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); | |
| 1.5.4 | Strategic Preparation | determination of required capacities | established implementation view (IIRA compliant); | 1.5.3; | Calculation of data volumes | Required storage capacities; | [3] |
| 1.6.1 | Strategic Preparation | Generation of tool catalog | data sources; software interfaces; hardware interfaces; | 1.2.5; 1.4.3; 1.4.4; 1.4.5; | Assign existing tools | Specific tools for data retrieval and processing; | [6] |
| 1.6.2 | 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; | |
| 1.6.3 | Strategic Preparation | Generation of tool catalog | Required tools to be developed | 1.6.2; | implement missing/required tools | coverage of missing capabilities/tools; | |
| 1.7.2 | Strategic Preparation | implementation of forensic capabilities | Required storage capacities | 1.5.4; | implement data capacities/storage | availability of storage capacities; | |
| 1.7.3 | 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] |
| 1.7.4 | Strategic Preparation | implementation of forensic capabilities | Specific tools for data retrieval and processing; | 1.6.3; | Asses forensic compliance of tools | Required adaption of tools; | |
| 1.7.5 | Strategic Preparation | implementation of forensic capabilities | 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; | |
| 1.7.6 | Strategic Preparation | implementation of forensic capabilities | legal requirements; | EXTERNAL; | generate (legal) templates for checklists/questionnaires etc.. | document templates for operational preparation; | |
| 1.7.8 | Strategic Preparation | implementation of forensic capabilities | established implementation view; | 1.5.3; | implement all forensic measures | implemented forensic capabilities; | [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 | Assesment of system impact | 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 | Assesment of system impact | tool catalog; potential relevant data and their data sources; | 1.7.5; 2.2.1; | Filter tools catalog for relevant data/data sources | suitable tools for data acquisition; | |
| 2.3.3 | Operational preparation | Assesment of system impact | suitable functions for data acquisition; report of predicted system impact of data acquisition; | 2.3.1; 2.3.2; | summarize impacts of suitable functions and tools; | report of predicted system impact of data acquisition; | |
| 2.4.1 | Operational preparation | live vs postmortem decision | Estimated duration of shutdown; Replacesystems availability; | EXTERNAL; | Determine business issues | Costs of a shutdown; Lost evidence due to impossible post mortem acquisition; Impact on ICS productivity; | |

| | | | | | | | |
|--------|-------------------------|--|--|---|---|---|------|
| 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] |
| 2.4.3 | | | available information of current productivity; | EXTERNAL; | determine production status of ICS | productivity status of the ICS; | |
| 2.4.4 | Operational preparation | live vs postmortem decision | legal issues; productivity status of the ICS; | 2.4.2; 2.4.3; | Determine if shutdown occurred or plant is already impaired | post mortem only or not | |
| 2.4.5 | Operational preparation | live vs postmortem decision | potential relevant data and their data sources; tools catalog; | 2.2.1; 2.3.2; | Determine non-live retrieval data | potential evidence only post mortem retrievable; | |
| 2.4.6 | Operational preparation | live vs postmortem decision | potential evidence only post mortem retrievable; Impact on ICS productivity; productivity status of the ICS; | 2.4.1; 2.4.3; 2.4.5; | consider and sum up | decision to shut down ICS/post mortem or live; | |
| 2.5.1 | Operational preparation | setup of order to retrieve data | data required to be acquired; | 2.2.1; | Asses volatility of data | volatility of potential data required to be acquired; | [9] |
| 2.5.2 | Operational preparation | setup of order to retrieve data | volatility of potential data required to be acquired; | 2.5.1; | Prioritize data | order of data to be acquired; | [3] |
| 2.6.1 | Operational preparation | Create list with data sources and tools for data retrieval | suitable tools for data acquisition; decision for post mortem or live retrievable; potential data required for evidence; | 2.3.2; 2.4.6; 2.2.1; | assign tools for data retrieval | list of data to be acquired with specific tools; | |
| 3.1.1 | Data acquisition | Locate data sources | list of data to be acquired with specific tools; ICS architecture; asset inventory; | 2.6.1; EXTERNAL; 1.1.10; | lookup data source of potential data to be acquired; | location of data sources with data to be acquired; | |
| 3.2.1 | Data acquisition | Collect physical storage media | asset inventory; location of data sources with data to be acquired; | 1.1.10; 3.1.1; | collect external physical storages | physical data storage components; | [3] |
| 3.2.2 | Data acquisition | Collect physical storage media | physical data storage components; | 3.2.1; | create forensic compliant duplication | forensic processable image; | [3] |
| 3.3.1 | Data acquisition | Live retrieval of data | traffic tap data; | 1.7.8; | capture traffic | traffic captures; | [10] |
| 3.3.2 | Data acquisition | Live retrieval of data | I/O tap data; | 1.7.8; | capture I/O | I/O values captures; | [10] |
| 3.3.3 | Data acquisition | Live retrieval of data | traffic captures; I/O values captures; | 3.3.1; 3.3.2; | Translate and store events in audit log file | forensic compliant logs; | |
| 3.3.4 | Data acquisition | Live retrieval of data | stored data by implemented forensic capabilities; | 1.7.8; | retrieve from databases | forensic compliant logs; I/O values captures; traffic captures; project files; diagnosis files; | |
| 3.3.5 | Data acquisition | Live retrieval of data | affected field controller; | 1.1.1; 2.1.1; | Acquire firmware live | actual firmware of device; | |
| 3.3.6 | Data acquisition | Live retrieval of data | request; | 1.2.2; | Acquire Controller Status | controller status; | [2] |
| 3.3.7 | Data acquisition | Live retrieval of data | visible status indicator of device; | 1.1.1; | Determine controller modus status | status (RUN, STOP, MAINT, ERROR..) | [2] |
| 3.3.8 | Data acquisition | Live retrieval of data | display status/messages; | 3.3.7; | Determine display status | diagnosis indicator; | [2] |
| 3.3.9 | Data acquisition | Live retrieval of data | request to affected device; | 1.2.2; | Acquire Variable content data | Variable content data of affected field controller; | [11] |
| 3.3.10 | Data acquisition | Live retrieval of data | request to affected device; | 1.2.2; | Acquire PLC application Code | application code of affected field controller; | [11] |
| 3.3.11 | Data acquisition | Live retrieval of data | request to affected device; | 1.2.2; | Acquire PLC Meta-Data | meta data of affected PLC; | [11] |
| 3.3.12 | Data acquisition | Live retrieval of data | request to affected device; projecting software logs; related database; | 1.2.2; | Acquire device diagnostics and Logs | errors and events; | [11] |
| 3.4.1 | Data acquisition | Post mortem retrieval | device location; | 1.1.10; | remove field controller from network | disassembled field controller; | [12] |
| 3.4.2 | Data acquisition | Post mortem retrieval | retrieved device; | 3.4.1; | Place device in isolated network | MIM-excluded manipulation of traffic; | |
| 3.4.3 | Data acquisition | Post mortem retrieval | request; | 1.2.2; | Acquire Variable content data | Variable content data of affected field controller; | |
| 3.4.4 | Data acquisition | Post mortem retrieval | request; | 1.2.2; | Acquire PLC application Code | Application code of affected field controller; | |
| 3.4.5 | Data acquisition | Post mortem retrieval | request; | 1.2.2; | Acquire PLC Meta-Data | meta data of affected PLC; | |
| 3.4.6 | Data acquisition | Post mortem retrieval | request; | 1.2.2; | Acquire Device Diagnostics and Logs | errors and hints; | |
| 3.4.7 | Data acquisition | Post mortem retrieval | request; | 1.2.2; | Acquire firmware live | actual firmware of device; | |
| 3.4.8 | Data acquisition | Post mortem retrieval | retrieved device; | 3.4.1; | Identify interfaces | available interface types; | |
| 3.4.9 | Data acquisition | Post mortem retrieval | persistent memory component; | 3.4.9; | Read persistent memory components | raw memory binary; | |
| 3.5.1 | Data acquisition | Retrieval of IT forensic data | common forensic database; | 1.7.8; | Retrieve data acquired by IT forensic process | IT components forensic data; | |
| 3.6.1 | Data acquisition | Acquire witness report | trigger; related personnel; status of the field devices; | EXTERNAL; EXTERNAL; | Identify potential witnesses | personel for further questioning; | [13] |
| 3.6.2 | Data acquisition | Acquire witness report | questionnaire templates; personell for further questioning; | 1.7.6; 3.6.1; | Questioning potential witnesses | filled questionnaires; | |
| 4.1.1 | Examination | Assign acquired data to the data model | OT components forensic data; | 3.2.1; 3.2.2; 3.3.1; 3.3.2; 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; 3.4.3; 3.4.4; 3.4.5; 3.4.6; 3.4.7; 3.4.8; 3.4.9; | Assign collected OT data to data model | all available OT forensic data structured/filled data model with available data; | |

| | | | | | | | |
|--------|-------------|--|--|------------------------------|---|--|-----|
| 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; | |
| 4.2.1 | Examination | Selection of appropriate tools | all available OT forensic data structured; all available IT forensic data structured; data model; | 4.1.1; 4.1.2; 1.3.8; | Asses format/aggregation level of acquired data | extractable data/further artefacts contained in acquired data (types); | |
| 4.2.2 | Examination | Selection of appropriate tools | all available OT forensic data structured/filled data model with available data; all available IT forensic data structured/filled data model with available data; extractable data/further artefacts contained in acquired data; | 4.1.1; 4.1.2; 4.2.1; | Asses available data | missing data or gaps in filled data model; | |
| 4.2.3 | Examination | Selection of appropriate tools | tool catalog; extractable data (types)/further artefacts contained in acquired data; | 1.7.5; 4.2.1; | Choose tools to search extractable data types | tools to search specific data types; | [3] |
| 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; raw memory binary; | 3.3.1; 3.4.9; | Search for control logic including variables | bytes position containing control logic and variables; | |
| 4.3.7 | Examination | Identification of artefacts/evidence | traffic captures; | 3.3.1; | Search for updates | bytes position containing updates; | |
| 4.3.8 | Examination | Identification of artefacts/evidence | traffic captures; bytes position containing updates; raw memory binary; | 3.3.1; 4.3.7; | Search for configurations; | bytes position containing configurations; | |
| 4.3.9 | Examination | Identification of artefacts/evidence | traffic captures; raw memory binary; | 3.3.1; 4.3.7; | Search for misc or unidentified data types | bytes position with misc or unknown data types; | |
| 4.4.1 | Examination | Extraction of further data types and artefacts | tool catalog; extractable data (types)/further artefacts contained in acquired data; | 1.7.5; 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; | |
| 4.4.3 | Examination | Extraction of further data types and artefacts | traffic captures; bytes position containing updates; bytes position containing payload; | 3.3.1; 4.3.7; 4.3.3; | Extract upload/download data | uploaded/downloaded payload with timestamp; | |
| 4.4.4 | Examination | Extraction of further data types and artefacts | traffic captures; bytes position containing read/write operations; | 3.3.1; 4.3.5; | Extract read/write operations | single read/write operations with registers and timestamps; | |
| 4.4.5 | Examination | Extraction of further data types and artefacts | traffic captures; | 3.3.1; | Extract commands | single commands to devices with timestamp; | |
| 4.4.6 | Examination | Extraction of further data types and artefacts | bytes position containing containing commands; | 4.3.4; | Extract reported I/O status; | by protocol reported I/O values with timestamp; | |
| 4.4.7 | Examination | Extraction of further data types and artefacts | traffic captures; | 3.3.1; | Extract I/O values | specific I/O values with timestamp from I/O tap; | |
| 4.4.8 | Examination | Extraction of further data types and artefacts | I/O values captures; | 3.3.2; | | | |
| 4.4.8 | Examination | Extraction of further data types and artefacts | traffic captures; | 3.3.1; | Extract control logic with variables | control logic binary; | |
| 4.4.9 | Examination | Extraction of further data types and artefacts | raw bytes containing payload with timestamp; bytes position containing control logic with variables; | 4.4.3; 4.3.8; | | | |
| 4.4.9 | Examination | Extraction of further data types and artefacts | traffic captures; | 3.3.1; | Extract configuration data | configuration files; | |
| 4.4.10 | Examination | Extraction of further data types and artefacts | bytes position containing configuration data; | 4.3.8; | | | |
| 4.4.10 | Examination | Extraction of further data types and artefacts | traffic captures; | 3.3.1; | Extract firmware | firmware binary; | |
| 4.4.11 | Examination | Extraction of further data types and artefacts | bytes position containing configuration data; raw memory binary; | 4.3.8; 3.4.10; | | | |
| 4.4.11 | Examination | Extraction of further data types and artefacts | traffic captures; | 3.3.1; | Extract control logic | control logic binary; | |
| 4.4.12 | Examination | Extraction of further data types and artefacts | raw memory binary; | 3.4.10; | | | |
| 4.4.12 | Examination | Extraction of further data types and artefacts | bytes position containing configuration data; raw memory binary; | 4.3.8; 3.4.10; | Extract configurations | configuration binary; | |
| 4.4.13 | Examination | Extraction of further data types and artefacts | traffic captures; | 3.3.1; | | | |
| 4.4.13 | Examination | Extraction of further data types and artefacts | bytes position with misc or unknown data; raw memory binary; | 4.3.9; 3.4.10; | Extract misc or unknown data | misc or unknown data; | |
| 4.4.14 | Examination | Extraction of further data types and artefacts | firmware binary; | 4.4.10; | | | |
| 4.4.14 | Examination | Extraction of further data types and artefacts | configuration binary; raw memory binary; | 4.4.12; 3.4.9; | extract file types; | available filetypes; | |
| 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 | |
| 4.5.3 | Examination | Translation into right kind of format | extracted I/O values; PLC control logic; I/O captures; | 4.4.6; 4.5.2; 4.4.7; | Assign I/O to variables | variable content data with timestamp; | |
| 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 read/write operations | send or received read/write operations with specific data and timestamp; | |
| 4.5.6 | Examination | Translation into right kind of format | control logic binary; configuration binary; memory binary parts; | 4.4.8; 4.4.12; 4.4.14; | parse raw data to filetypes | all available filetypes; | |
| 4.5.7 | Examination | Translation into right kind of format | filled questionnaires; | 3.6.2; | parse answers to computer analysable answers | computer analyzable facts/events with timestamp of witness report; | |

| | | | | | | | |
|-------|-------------|--|--|---|--|--|------|
| 4.7.1 | Examination | Assigning extracted evidence to data model | all extracted artefacts; | 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; 4.4.11; 4.4.12; 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 | structured overview of available and missing evidence (filled data model); | |
| 5.1.1 | Analysis | Identify potential coherences | specific I/O values with timestamp; variable content data; by protocol reported I/O values; event logs; | 4.4.7; 4.5.3; 4.4.6; 3.3.3; | Correlation of events with I/O status; | events impacting I/O and vice versa; | [14] |
| 5.1.2 | Analysis | Identify potential coherences | connections/requests; event logs; | 4.4.2; 3.3.3; | Correlation of events and connections; | related events and connections/request; | [15] |
| 5.1.3 | Analysis | Identify potential coherences | answers; events; I/O data with timestamp; | 4.5.7; 3.3.3; 4.5.1; | Correlate witness reports with artefacts; | further related events; | |
| 5.1.4 | Analysis | Identify potential coherences | I/O data with timestamp; send or received read/write operations with specific data and timestamp; | 4.5.1; 4.5.5; | Correlate I/O data with register operations | related impact of variable commands to I/O; | |
| 5.1.5 | Analysis | Identify potential coherences | all extracted artefacts timestamps; | 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.4.6; 4.4.7; 4.5.1; 4.5.3; 4.5.4; 4.5.5; 4.5.6; 4.5.7; | Correlate timestamp of artefacts | chronological relationships between artefacts/events; | [3] |
| 5.1.6 | Analysis | Identify potential coherences | all extracted artefacts timestamps; | 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.4.6; 4.4.7; 4.5.1; 4.5.3; 4.5.4; 4.5.5; 4.5.6; 4.5.7; | Identify statistical changes | events with impact on components; | [3] |
| 5.1.7 | Analysis | Identify potential coherences | all extracted artefacts timestamps; | 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.4.6; 4.4.7; 4.5.1; 4.5.3; 4.5.4; 4.5.5; 4.5.6; 4.5.7; | Identify patterns | related events and artefacts; | [3] |
| 5.1.8 | Analysis | Identify potential coherences | send/received commands; computer analyzable facts/events with timestamp of witness report; chronological relationships between artefacts/events; | 4.5.4; 5.1.4; | Correlate commands with artefacts | executed commands; | |
| 5.2.1 | Analysis | Identify inconsistencies | send/received commands; executed commands; send or received read/write operations; computer analyzable facts/events with timestamp of witness report; | 4.5.4; 5.1.8; 4.5.5; 4.5.7; | Compare input with read/write operations | Related authorized register commands with events; | |
| 5.2.2 | Analysis | Identify inconsistencies | connections/requests; uploaded/downloaded payload with timestamp; | 4.4.2; 4.4.3; | Compare connection/requests with up-/downloads | suspicious connections/requests with timestamp; | |

| | | | | | | | |
|--------|----------|--------------------------|--|--|---|---|------|
| 5.2.4 | Analysis | Identify inconsistencies | all extracted data with timestamps; | 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.4.6; 4.4.7; 4.5.1; 4.5.3; 4.5.4; 4.5.5; 4.5.6; 4.5.7; 5.1.7; 5.1.8; 5.2.1; 5.2.2; | Identify anomalies | suspicious events/artefacts with timestamp; | |
| 5.2.5 | Analysis | Identify inconsistencies | control logic binary; | 4.4.11; | transform control logic binary to logical formulas | mathematical model representing behavior; | |
| 5.2.6 | Analysis | Identify inconsistencies | inloop data; | EXTERNAL; | Monitor payload behavior | generated I/O data of inloop simulator; | |
| 5.2.7 | Analysis | Identify inconsistencies | I/O data of inloop simulator; | 5.2.6; | Create model of intended behavior | mathematical model representing behavior; | |
| 5.2.8 | Analysis | Identify inconsistencies | generated I/O data of inloop simulator; mathematical model representing behavior; | 5.2.6; 5.2.5; | Compare model intended behavior with actual model | unintended control logic behavior; | [16] |
| 5.2.9 | Analysis | Identify inconsistencies | I/O values with timestamp (I/O tap); by protocol reported I/O values; | 4.4.6; 4.4.7; | Compare protocol information with I/O status | discrepancies between reported and actual I/O states; | [17] |
| 5.2.10 | Analysis | Identify inconsistencies | baseline data; | 1.1.1; 1.1.2; 1.1.3; 1.1.4; 1.1.5; 1.1.6; 1.1.7; 1.1.8; 1.1.9; 1.1.10; 1.1.11; 1.1.12; 1.1.13; 1.1.14; 1.1.15; 1.1.16; 1.1.17; 1.1.18; 1.1.19; | Compare baseline data with artefacts | (unauthorized) changes of ICS with timestamp; | |
| 5.3.1 | Analysis | Finalize Evidence | list acquired datas data sources; filled data model; | 2.6.1; 4.7.1; | Summarize distinct datasources into common timeline | overview of used data sources and their data; | |
| 5.3.2 | Analysis | Finalize Evidence | suspicious events/artefacts with timestamp; | 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; | |
| 5.3.4 | Analysis | Finalize Evidence | all vizualizable artefacts; | 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; 5.2.2; 5.2.4; 5.2.5; 5.2.6; 5.2.7; 5.2.8; 5.2.9; 5.2.10; | Visualize evidence | Clear summarization of evidence and its information value; | |

| | | | | | | | |
|-------|-----------|---|---|---|--|--|-----|
| 5.4.1 | Analysis | Create Hypothesis/Reconstruct incident | all gained evidence in analysis; | 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; 5.2.2; 5.2.4; 5.2.5; 5.2.6; 5.2.7; 5.2.8; 5.2.9; 5.2.10; 5.3.4; | Assign new data to data model | structured overview of available and missing evidence; | |
| 5.4.2 | Analysis | Create Hypothesis/Reconstruct incident | structured overview of available and missing evidence; Clear summarization of evidence and its information value; | 5.4.1; 5.3.4; | create incident trace | incident trace; | |
| 5.4.3 | Analysis | Create Hypothesis/Reconstruct incident | incident trace; actuators/sensors; ICS components; | 5.4.2; 1.1.1; 1.1.2; | Note actions and their impact | Impacts on ICS with related components; | |
| 5.4.4 | Analysis | Create Hypothesis/Reconstruct incident | structured overview of available and missing evidence; | 5.4.1; | Relate evidence to events | related evidence leading to incident; | |
| 5.5.1 | Analysis | Reconsideration of data (types) to retrieve | all gained evidence in analysis; | 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; 5.2.2; 5.2.4; 5.2.5; 5.2.6; 5.2.7; 5.2.8; 5.2.9; 5.2.10; 5.3.4; | Filter prior unseen/unselected data | unseen assets and data sources; | |
| 5.5.2 | Analysis | Reconsideration of data (types) to retrieve | unseen assets and data sources; | 5.5.1; | add new asset and data sources to list | assets and data sources to acquire data; | |
| 5.5.3 | Analysis | Reconsideration of data (types) to retrieve | assets and data sources to acquire data; | 5.5.2; | begin next iteration at operational preparation task X.Y | Index of next activity and task; | [3] |
| 6.1.1 | Reporting | Generate History Report | timestamp of performed functions and results; | N/A | Note all actions taken | timeline of forensic investigation actions; | |
| 6.1.2 | Reporting | Generate History Report | tools to search specific data types; tools to extract specific data types; list of data to be acquired with specific tools; | 2.6.1; 4.2.3; 4.4.1; | Note all tools used | all used tools and processed data; | [3] |
| 6.1.3 | Reporting | Generate History Report | list of data to be acquired with specific tools; | 4.4.1; | Note used data (sources) | all affected and relevant data sources; | [3] |
| 6.1.4 | Reporting | Generate History Report | timeline of forensic investigation actions; | 6.1.1; | Note manipulations taken on systems | Authorized manipulation of ICS components; | [3] |
| 6.1.6 | Reporting | Generate History Report | legal actions taken; protection goals status of final artefacts (filled data model); forensic compliant requirements; | N/A 4.7.1; EXTERNAL | Asses compliance with protection goals (measures) | forensic compliance of final evidence; | [3] |
| 6.1.7 | Reporting | Generate History Report | forensic compliance of final evidence; | 6.1.6; | Note compliance of evidence in report | significance of use of the evidence; | |
| 6.1.8 | Reporting | Generate History Report | 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; | 5.4.2; 5.4.3; 5.4.4; | Full incident and impact of events | Clear summarization of evidence and its information value; | [3] |
| 6.1.9 | Reporting | Generate History Report | 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; | EXTERNAL; 6.1.8; 6.1.2; 6.1.3; 6.1.1; 6.1.4; | Summarize | final evidence report; | [3] |
| 6.2.1 | Reporting | Generate target group report | target group roles; key objectives of target group roles; | EXTERNAL; EXTERNAL; | Asses target group requirements | target group requirements; | [3] |
| 6.2.2 | Reporting | Generate target group report | target group requirements; final evidence report; | EXTERNAL; 6.1.9; | Adapt history report target group requirements | forensic investigation report for target group; | [3] |