

IODEF extension for Reporting Cyber-Physical System Incidents

draft-murillo-mile-cps-00

Martin J. Murillo

IETF 89, London, UK.

Why an extension is needed

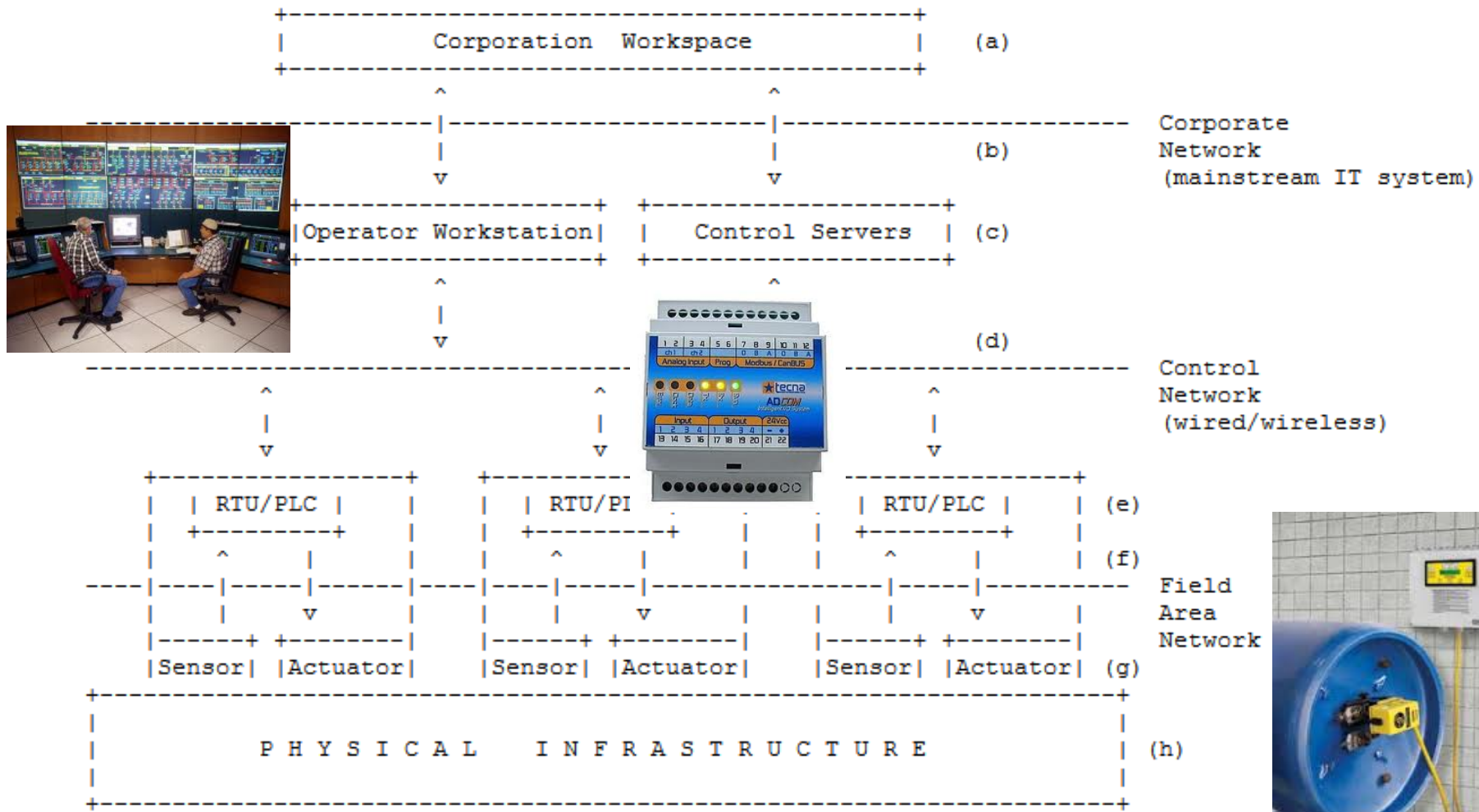
- There does not exist a global, machine friendly approach for reporting incidents that happen in physical systems that are controlled by software and hardware systems (nuclear reactor, electric grid, rail transportation systems, etc)
- These systems are gradually becoming more interconnected; legacy systems do not have proper cybersecurity protection; there exists highly-skilled individuals and motivations; some of these systems are generally considered critical; attacks to CPS systems are a natural extension of IT cyber-attacks; the emergence of the Internet of Things (IOT); and these attacks can be carried out remotely and quite inexpensively
- IETF is a leading global standards organization whose work in the field would benefit an area that needs urgent attention.

Cyber-Physical Systems

Cyber-Physical Systems are computer- or microprocessor- or microcontroller-based systems that monitor and control physical processes .

Example: Open/close reservoir locks, control rail system track system, control temperature/pressure in nuclear facilities, control flow of oil through pipelines, balance the distribution of electricity in (international) electric grids, etc.

Generic CPS system



Cyber-physical system incident

- IT system misbehavior
- Physical system misbehavior due to and IT system compromise
- Misbehavior of a physical system as noticed at the physical infrastructure level: explosion, flooding, pressure loss, and others
- Misconfiguration or degradation of control system performance, as noticed by an operator.
- The disruption of control systems operation due to the blocking of the flow of information through corporate or control networks
- Illegal or unauthorized changes made to alarm threshold levels, unauthorized commands issued to control equipment
- False information sent to control system operators or to corporate HQ
- The modification of control system software or configuration settings, producing unpredictable results
- Malicious software (e.g., virus, worm, Trojan horse) introduced into the system
- Recipes (i.e., the materials and directions for creating a product) or work instructions modified in order to bring about damage to products, equipment, or personnel

CyberPhysicalReport Report XML

```
+-----+
| Incident |
+-----+
| ENUM purpose |<>-----[ IncidentID ]
| STRING ext-purpose |<>--{0..1}--[ AlternativeID ]
| ENUM lang |<>--{0..1}--[ RelatedActivity ]
| ENUM restriction |<>--{0..1}--[ DetectTime ]
| |<>--{0..1}--[ StartTime ]
| |<>--{0..1}--[ EndTime ]
| |<>-----[ ReportTime ]
| |<>--{0..*}--[ Description ]
| |<>--{1..*}--[ Assessment ]
| |<>--{0..*}--[ Method ]
| |<>--{1..*}--[ Contact ]
| |<>--{0..*}--[ EventData ]
| | |<>--[ AdditionalData ]
| | |<>--[ CyberPhysicalReport ]
| |<>--{0..1}--[ History ]
| |<>--{0..*}--[ AdditionalData ]
+-----+
```

The CyberPhysicalReport Element

```
+-----+
|CyberPhysicalReport|
+-----+
| STRING Version      |<--{0..1}--[IncidentTitle]
| ENUM IncdntType    |<--{0..1}--[ReportingParty]
| STRING ext-value    |<--{0..1}--[ReportReliability]
|                    |<--{0..1}--[IncidentType]
|                    |<--{0..1}--[Industry]
|                    |<--{0..1}--[TargetSystems]
|                    |<--{0..1}--[CyberPhysicalDepth]
|                    |<--{0..1}--[TransportMedium]
|                    |<--{0..1}--[Exploit]
|                    |<--{0..1}--[EntryPoint]
|                    |<--{1..*}--[PerpetratingParty]
|                    |<--{0..*}--[DetectionMethod]
|                    |<--{0..*}--[CommandAndControlCenters]
|                    |<--{0..*}--[CompromisedPhysicalInfrastrucute]
|                    |<--{0..*}--[ConstrolSystem]
|                    |<--{0..1}--[OrganizationalImpact]
|                    |<--{0..1}--[RecurrencePreventionMeasures]
|                    |<--{0..1}--[BriefDescriptionOfIncident]
|                    |<--{0..1}--[ProtocolType]
|                    |<--{0..1}--[NetworkType]
|                    |<--{0..1}--[Logs]
|                    |<--{0..1}--[References]
+-----+
```

Figure 3: The CyberPhysicalReport Element

Further work in the extension

- **An XML Schema for the Extension**
- **An Example XML**
- **Case studies applied to different types of infrastructures/scenarios**
- **Revision of the CyberPhysicalReport Element/XML**
- **Others as needed**