IODEF extension for Reporting Cyber-Physical System Incidents

draft-murillo-mile-cps-00

Martin J. Murillo
mmurillo@nd.edu
IETF 90, MILE
Toronto, Canada

Cyber-Physical Systems

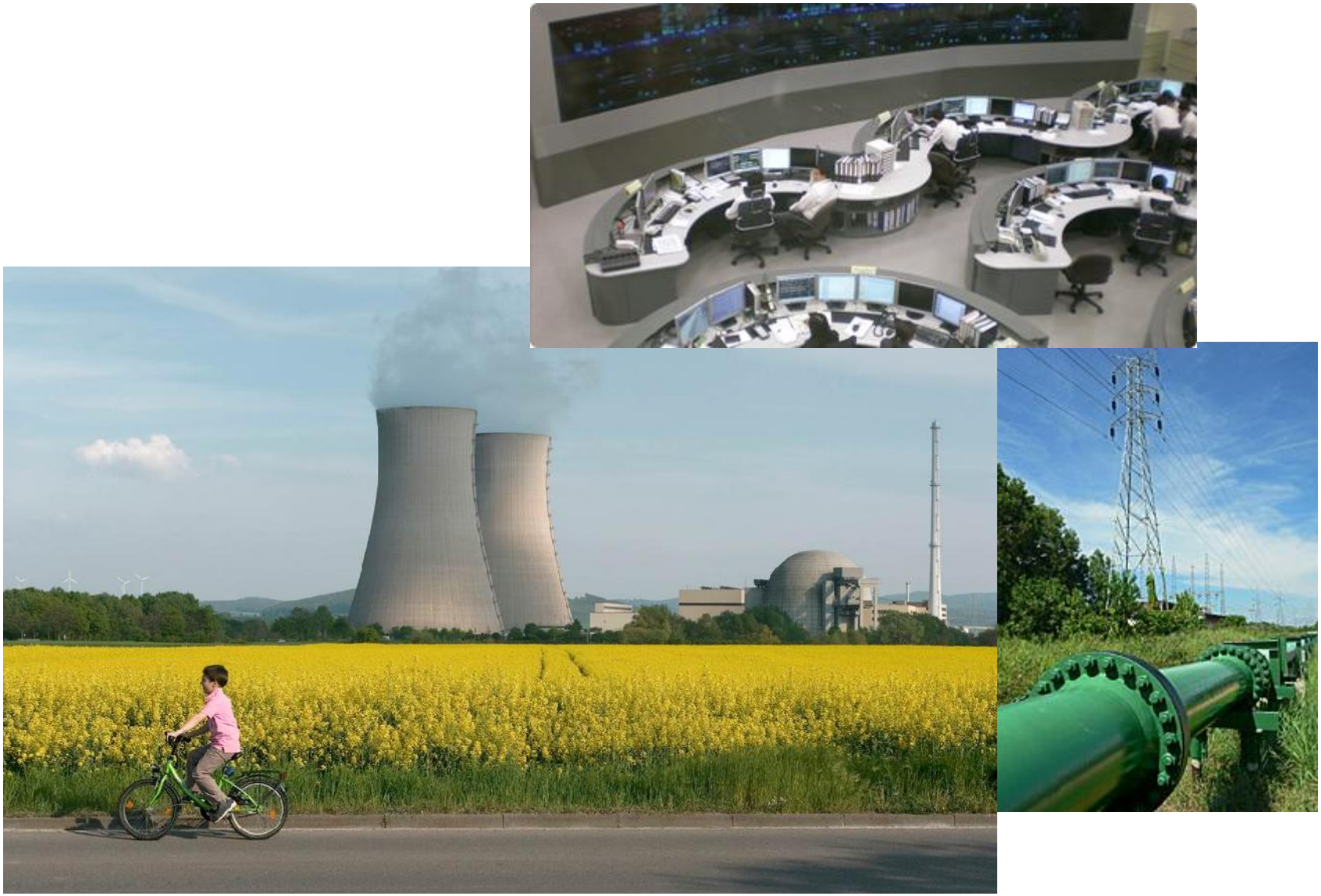
Cyber-Physical Systems are computer- or microprocessor- or microcontroller-based systems that monitor and control physical processes .

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.

Other names for Cyber-Physical Systems

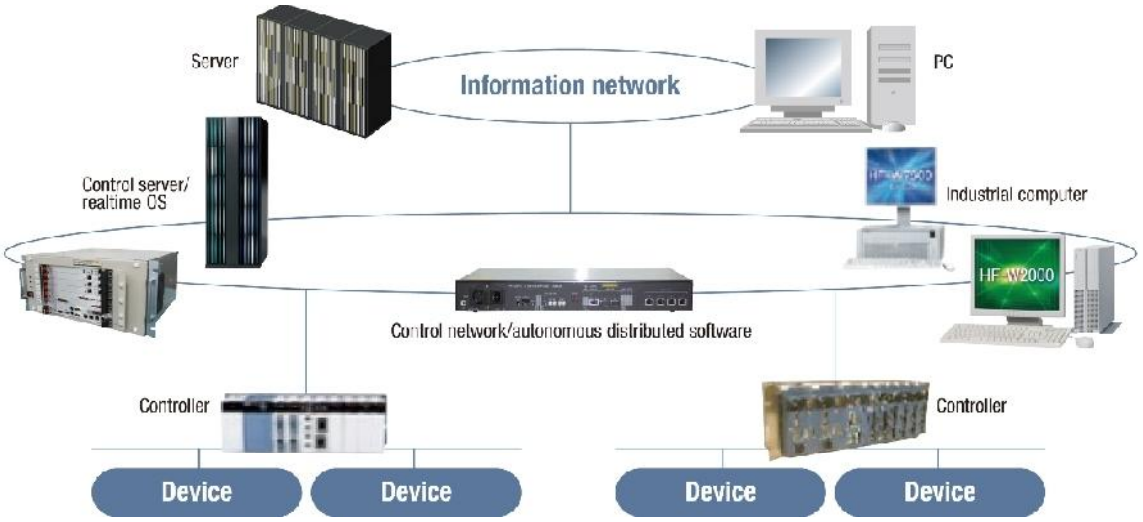
- **Cyber-physical infrastructure**
- **Industry control systems**
- **Automated control systems**
- **Critical system infrastructure**
- **Cyber-Physical Systems (CPS),**
- **Operational Technology Systems,**
- **Control Systems**

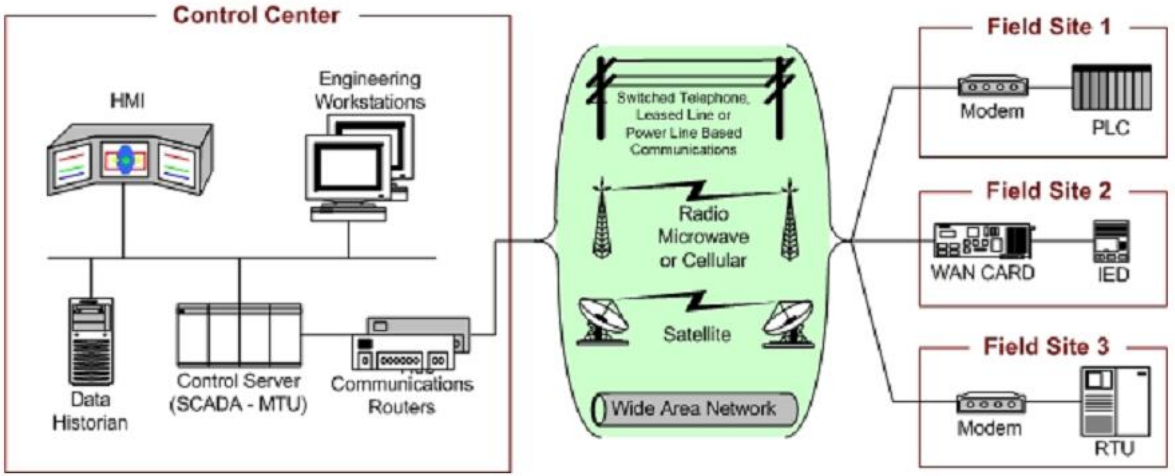
Cyber-Physical Infrastructure



Sources: nist.gov, enisa.europa.eu, toshiba.co.jp,

Cyber-Physical Infrastructure

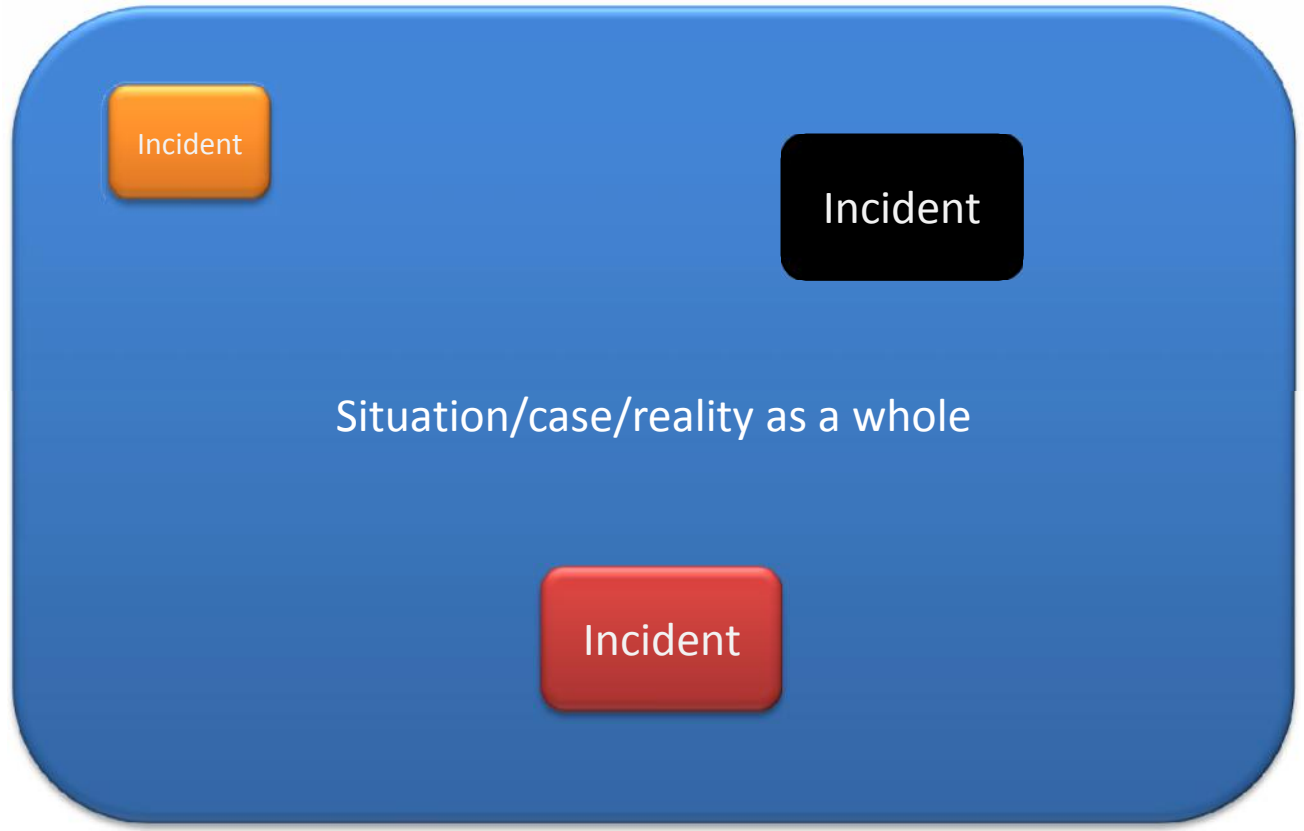




Examples of CPS incidents

- IT system misbehavior or 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 (alarms not reporting to the central computer; devices (pumps, etc) not running when they should; others)
- The disruption of control systems operation due to the blocking of the flow of information through corporate or control networks
- A loss of communication between the central computer and various stations (pumping)
- 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
- 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

An incident is a glimpse of the overall situation, which might change across time and space



Differences between IT systems and Industrial Control Systems

	IT system	Industrial Control System
Performance Requirements	•Non-real-time •Response must be consistent •High throughput is demanded •High delay and jitter maybe acceptable	•Real-time •Response is time-critical •Modest throughput is acceptable •High delay and/or jitter is a serious concern
Availability Requirements	•Responses such as rebooting are acceptable •Availability deficiencies can often be tolerated, depending on the system's operational requirements	•Responses such as rebooting may not be acceptable because of process availability requirements •Outages must be planned and scheduled days/weeks in advance. High availability requires exhaustive pre-deployment testing
Risk Management Requirements	•Data confidentiality and integrity is paramount •Fault tolerance is less important – momentary downtime is not a major risk •Major risk impact is delay of business operations	•Human safety is paramount, followed by protection of the process •Fault tolerance is essential, even momentary downtime is not acceptable •Major risk impact is regulatory non-compliance, loss of life, equipment, or production
Architecture Security Focus	•Primary focus is protecting the IT assets, and the information stored on or transmitted among these assets. •Central server may require more protection	•Primary goal is to protect edge clients (e.g., field devices such as process controllers) •Protection of central server is still important
Unintended Consequences	•Security solutions are designed around typical IT systems	•Security tools must be tested to ensure that they do not compromise normal ICS operation
Time-Critical Interaction	•Less critical emergency interaction •Tightly restricted access control can be implemented to the degree necessary	•Response to human and other emergency interaction is critical •Access to ICS should be strictly controlled, yet not hamper human-machine interaction
System Operation	•Systems are designed for use with typical operating systems •Upgrades are straightforward with the availability of automated deployment tools	•Differing and custom operating systems often without security capabilities •Software changes must be carefully made, usually by software vendors, because of the specialized control algorithms and perhaps modified hardware and software involved

	IT system	Industrial Control System
Resource Constraints	•Systems are specified with enough resources to support the addition of third-party applications such as security solutions	•Systems are designed to support the intended industrial process, with minimal memory and computing resources to support the addition of security technology
Communications	•Standard communications protocols •Primarily wired networks with some localized wireless capabilities •Typical IT networking practices	•Many proprietary and standard communication protocols •Several types of communications media used including dedicated wire and wireless (radio and satellite) •Networks are complex and sometimes require the expertise of control engineers
Change Management	•Software changes are applied in a timely fashion in the presence of good security policy and procedures. The procedures are often automated.	•Software changes must be thoroughly tested and deployed incrementally throughout a system to ensure that the integrity of the control system is maintained. ICS outages often must be planned and scheduled days/weeks in advance
Managed Support	•Allow for diversified support styles	•Service support is usually via a single vendor
Component Lifetime	•Lifetime on the order of 3-5 years	•Lifetime on the order of 15-20 years
Access to Components	•Components are usually local and easy to access	•Components can be isolated, remote, and require extensive physical effort to gain access to them

Source: NIST

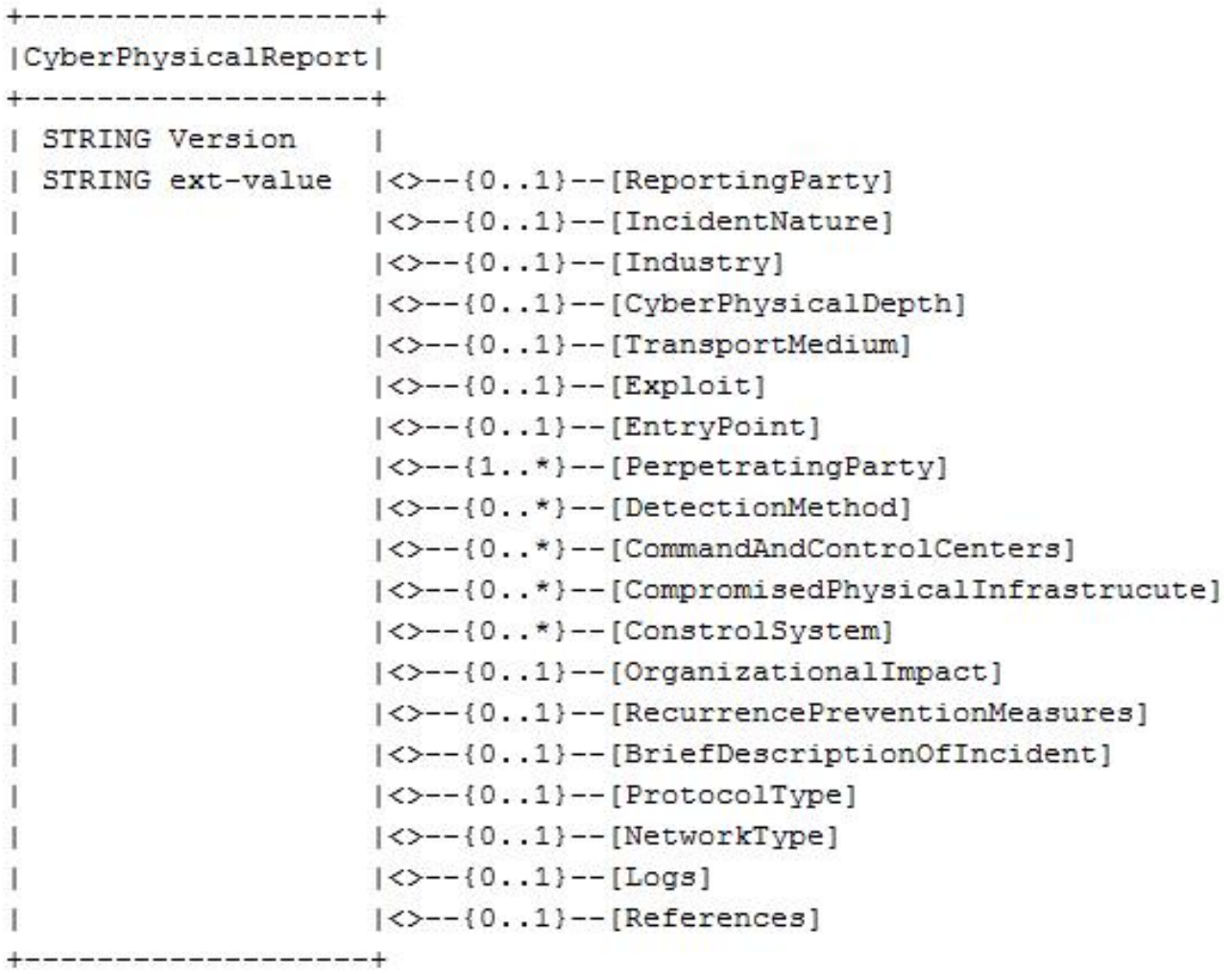
Why an extension is needed

- There does not exist a global, machine friendly approach for reporting incidents that happen in physical systems.
- These systems are proliferating in all spheres
- These systems are gradually becoming more interconnected
- Legacy systems do not have proper cybersecurity protection
- The exists highly-skilled individuals and motivations;
- Some 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)
- 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.

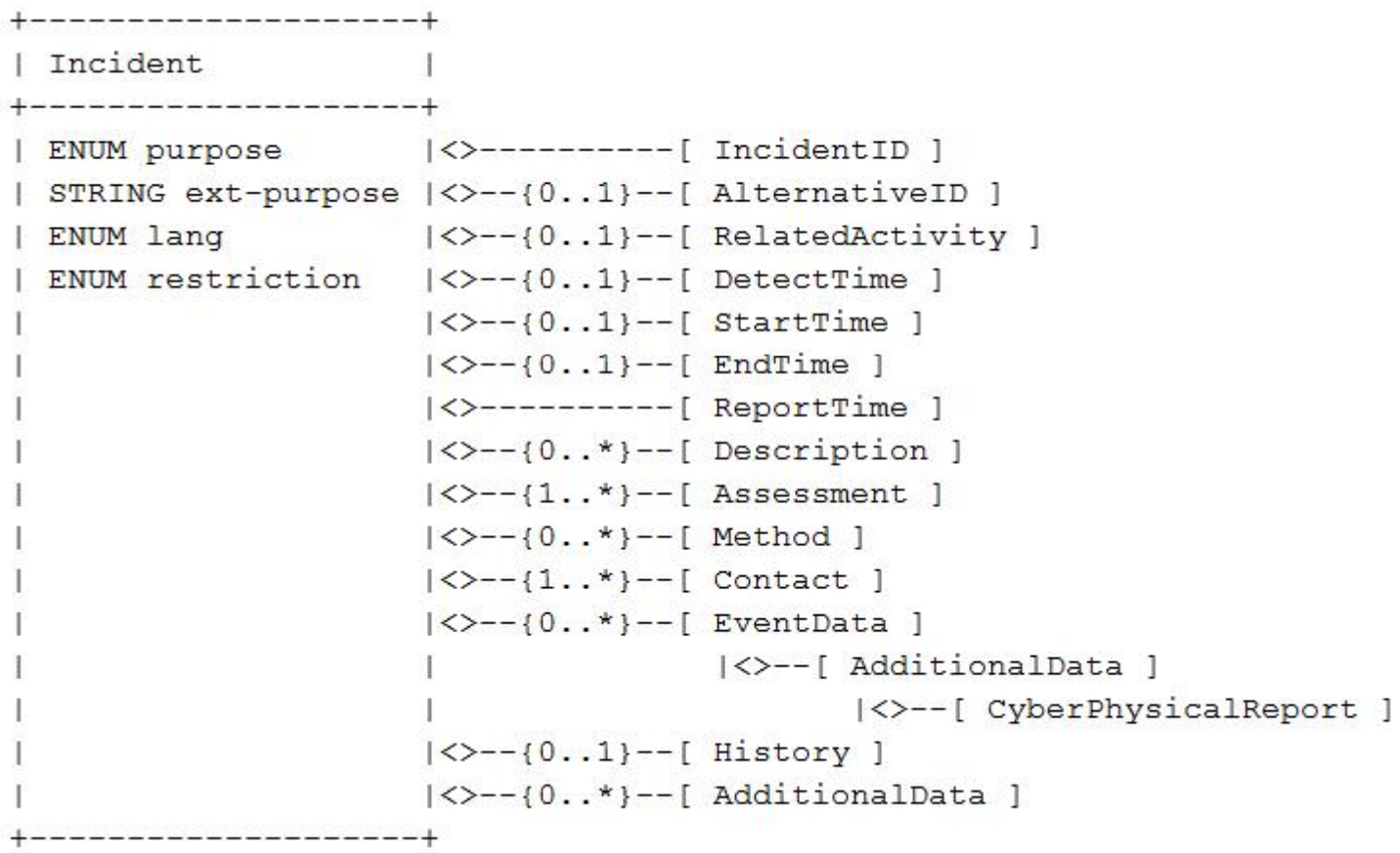
Generic CPS system

```
          +----------------------------------------------+
          |           Corporation  Workspace              |   (a)
          +----------------------------------------------+
                     ^                        ^
---------------------|------------------------|------------------------  Corporate
                     |                        |                    (b)   Network
                     v                        v                          (mainstream IT system)
           +---------------------+  +---------------------+
           |Operator Workstation|  |   Control Servers   |  (c)
           +---------------------+  +---------------------+
                     ^                        ^
                     |
                     v                                             (d)
--------------------------------------      -------------------------  Control
        ^                      ^                     ^                 Network
        |                      |                     |                 (wired/wireless)
        v                      v                     v
   +-----------------+    +---------            -----------------+
   |  | RTU/PLC |     |    |  | RTU/PI           | RTU/PLC |      |  (e)
   |  +---------+     |    |  +---------+    |  |  +---------+   |
   |     ^      |     |    |     ^      |    |  |     ^      |   |  (f)
----|----|------|------|----|----|------|-----------------|-----|----------  Field
   |     |      v     |    |     |      v    |  |     |      v   |          Area
   |------+ +---------|    |------+ +---------|  |------+ +---------|      Network
   |Sensor| |Actuator|     |Sensor| |Actuator|   |Sensor| |Actuator|  (g)
+------------------------------------------------------------------+
|                                                                  |
|        P H Y S I C A L    I N F R A S T R U C T U R E            |  (h)
|                                                                  |
+------------------------------------------------------------------+
```

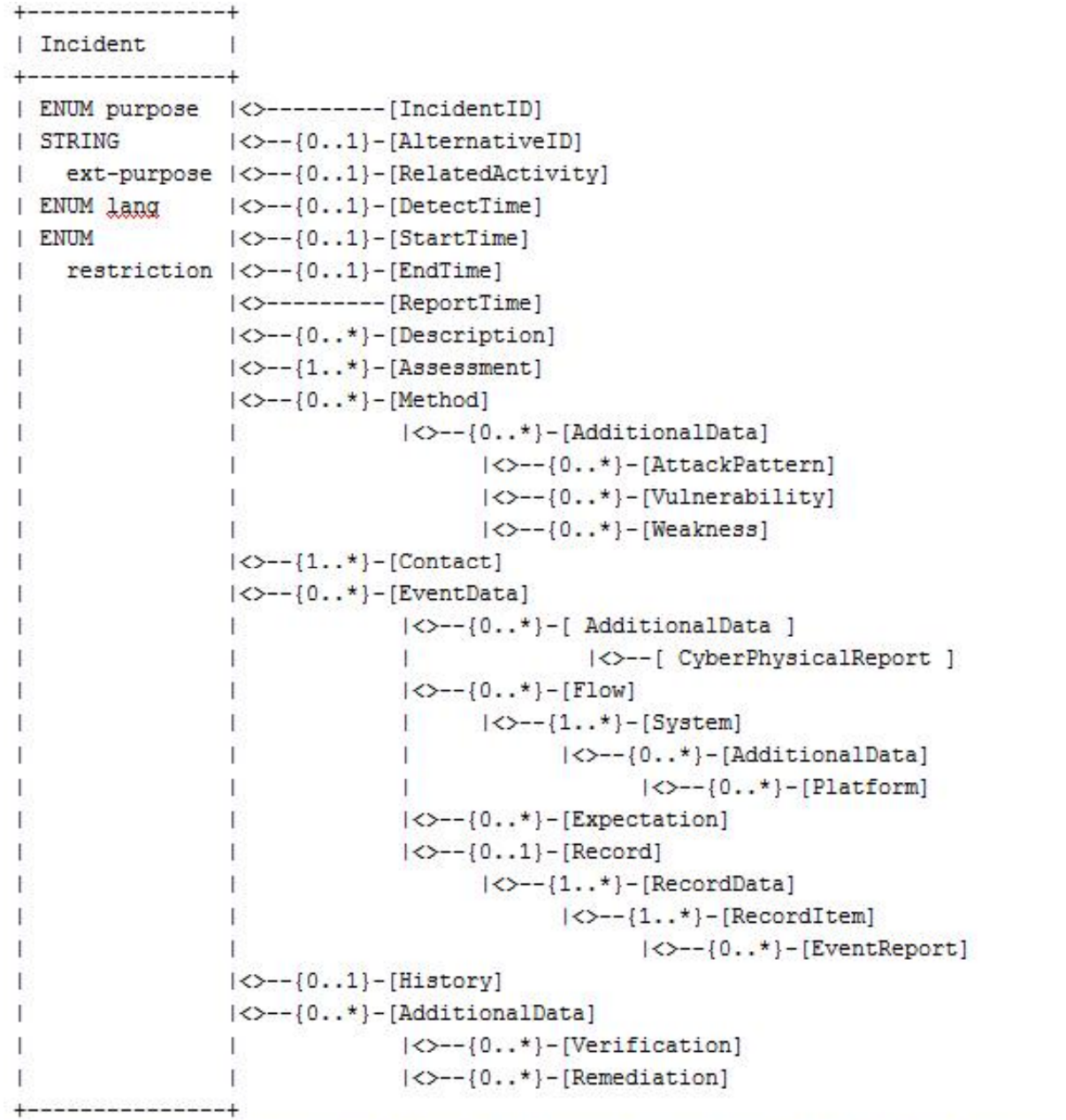
The CyberPhysicalReport Element



No reutilization of other extensions



Reutilization of other extensions



(ii) Utilization of IODEF-extension for structured cybersecurity information

Further work in the extension

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

Comments/Feedback