

PROTECTRAIL INTEROPERABILITY FRAMEWORK

The PROTECTRAIL Interoperability Framework has been adopted by the consortium members to facilitate the speed and ease of integrating new functions/capacities into an overall system of systems. The framework is based on open standards, and uses a very simple Event-Driven architecture based on Web Services.

For the High Probability Low Impact (HPLI) event Call for Demonstration, the PROTECTRAIL's Interoperability Framework base-level of integration will be used to quickly enable the various consumers (e.g. Security Operational Control Centre's, Crisis Management Systems and Passenger Information System) with the ability to receive events from the HPLI capacities. The base-level of integration into this framework requires that a HPLI capacity generates an Event. PROTECTRAIL use the Eventing Framework WS-BaseNotification and the Event-Format Common Alerting Protocol (CAP).

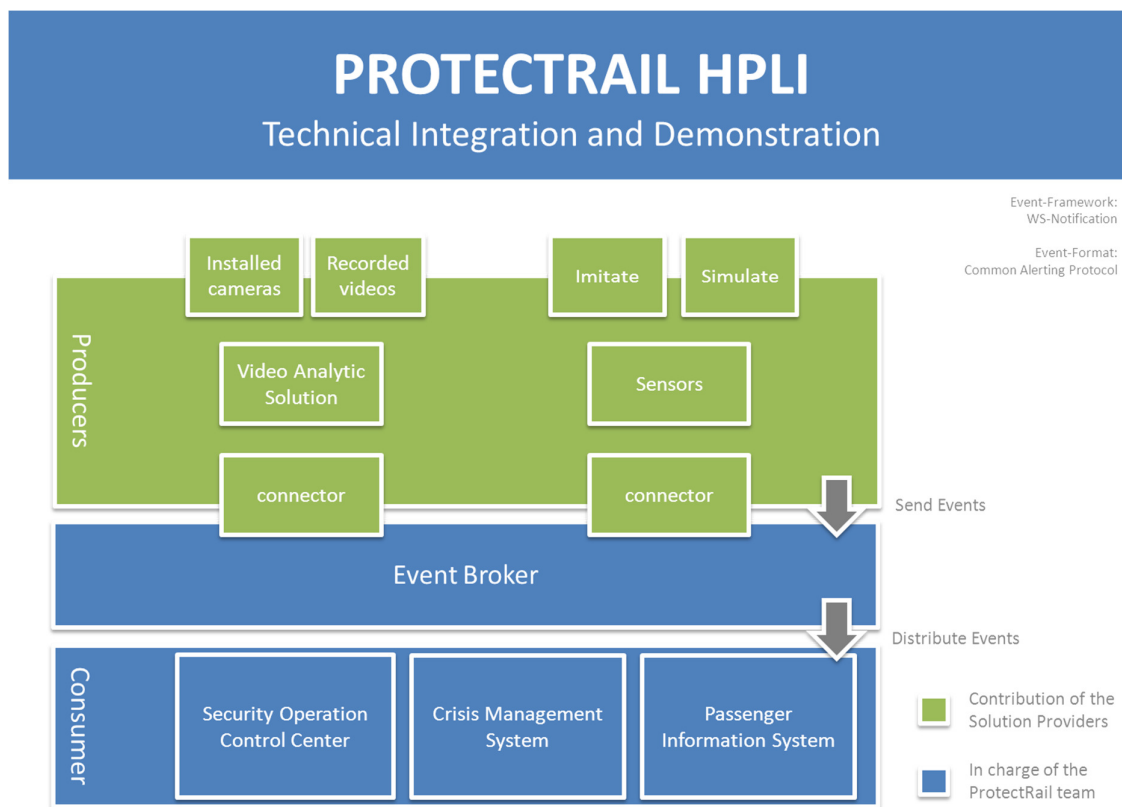


Figure 1 Event and SOA Based Interoperability Framework

At the PROTECTRAIL final event to be held in May 27th-28th 2014 in Paris, solution providers will demonstrate the integration into the PROTECTRAIL Interoperability Framework and also the performance of the solution in limited environment at the facilities of the UIC.

The video analytic solution / sensor solution will send an Event through a connector to the local installed Event Broker. The Event will need to specify a Topic, unique ID, GPS location, time. The Event Broker will dispatch the events to the consumers. The consumer will subscribe for a certain topic and will visualize the event.

The OASIS CAP standard defines key information of an alert such as: time, geolocation, event type, etc. The detailed structure of such a type of event is described below:

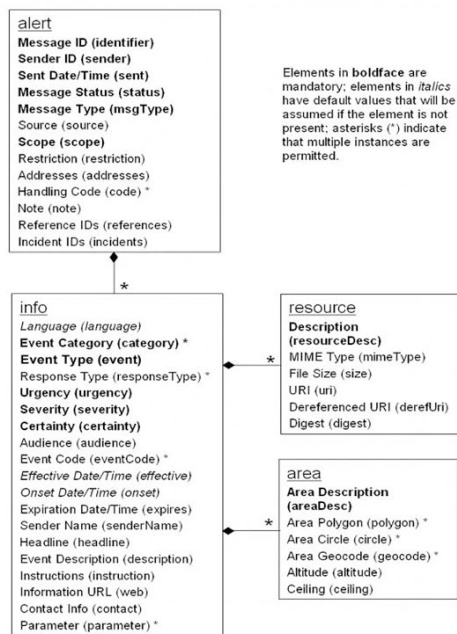


Figure 2 Document Object Model of the Alert Message

BASE INTEGRATION INTO THE PROTECTRAIL FRAMEWORK DETAILS

Please implement an Event Producer based on the Eventing Framework [WS-BaseNotification](#) and the embedded Public Event Format [OASIS Common Alerting Protocol](#). Implementation Examples are already available in Java, C#, and C++/gSoap in our [Project Repository](#).

```
<?xml version="1.0" ?>
<S:Envelope xmlns:S="http://schemas.xmlsoap.org/soap/envelope/">
  <S:Body>
    <ns3:Notify xmlns:ns2="urn:oasis:names:tc:emergency:cap:1.2"
      xmlns:ns3="http://docs.oasis-open.org/wsn/b-2"
      xmlns:ns4="http://www.w3.org/2005/08/addressing"
      xmlns:ns5="http://protectrail.eu/model/events/resource"
      xmlns:ns6="http://docs.oasis-open.org/wsr/bf-2"
      xmlns:ns7="http://docs.oasis-open.org/wsn/t-1"
      xmlns:ns8="http://protectrail.eu/wsn/extra"
      xmlns:ns9="http://docs.oasis-open.org/wsr/r-2">
      <ns3:NotificationMessage>
        <ns3:Topic
          Dialect="http://docs.oasis-open.org/wsn/t-1/TopicExpression/Full">
          urn:rixf:com.acme.intrusiondetection/events_type/intrusion
        </ns3:Topic>
        <ns3:Message>
          <ns2:alert>
            <ns2:identifier>
              urn:rixf:com.acme.intrusiondetection/intrusion/13
            </ns2:identifier>
            <ns2:sender>
              urn:rixf:com.acme.intrusiondetection/intrusion/uic
            </ns2:sender>
            <ns2:sent>2014-05-14T10:12:35.388+02:00</ns2:sent>
            <ns2:status>Actual</ns2:status>
            <ns2:msgType>Alert</ns2:msgType>
            <ns2:scope>Public</ns2:scope>
            <ns2:note>Unauthorized Intrusion detected.
            </ns2:note>
            <ns2:info>
```

```

<ns2:category>SECURITY</ns2:category>
<ns2:event>
  urn:rixf:com.acme.intrusiondetection/events_type/intrusion
</ns2:event>
<ns2:urgency>Immediate</ns2:urgency>
<ns2:severity>Severe</ns2:severity>
<ns2:certainity>Likely</ns2:certainity>
<ns2:area>
  <ns2:areaDesc>UIC in Paris</ns2:areaDesc>
  <ns2:circle>48.855283, 2.29185 0.01</ns2:circle>
</ns2:area>
</ns2:info>
</ns2:alert>
</ns3:Message>
</ns3:NotificationMessage>
</ns3:Notify>
</S:Body>
</S:Envelope>

```

XML-SOAP Message Example for an Event based on WS-Notification and CAP

TESTING

1. Upload the SOAP Test Data to the [Project Repository](#).
2. Please validate your Test Data against the WSDL [WS-BaseNotification](#) and XSD of the [OASIS Common Alerting Protocol](#) with SOAP UI Pro.
3. Please Test your solution against the Continuous Integration Environment. Send your Event to the Event Broker: <http://integration.protectrail.eu/EventProducer>
4. Please start a Integration Test with a consumer of another PROTECTRAIL member

SCHEDULING

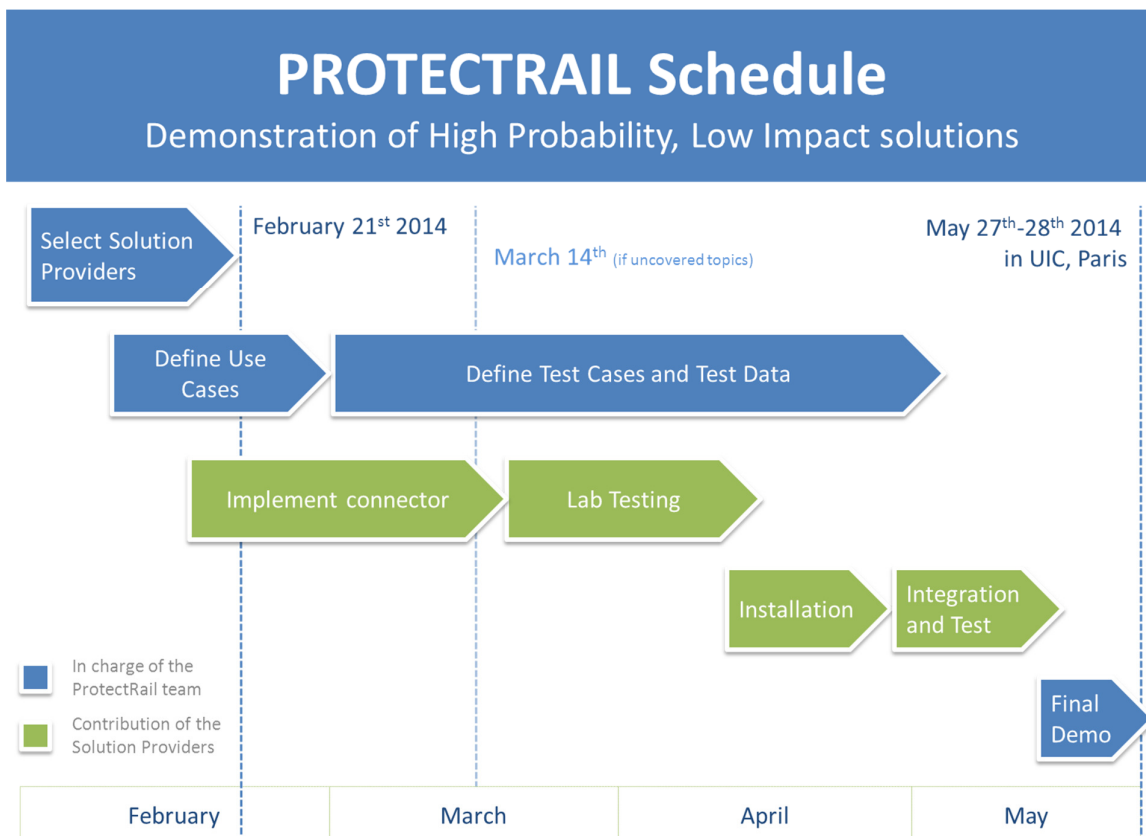


Figure 3 PROTECTRAIL HPLI Schedule



TECHNICAL QUESTIONS/SUPPORT

For any technical questions you may have regarding software use, development or integration, please contact:

Erwan Humbert

erwan.humbert@de.transport.bombardier.com

+49 30 98607 1378