Sensor Alert Service (SAS)

Description and Implementation at Ft. Bragg, North Carolina and the Port of Charleston

Johnny Tolliver

ORNL

Contents

- **Introduction to SAS**
- **SAS Implementation at Ft. Bragg**
- **SAS Implementation at the Port of Charleston**
- **Other Deployments**
- **Conclusion**

Part I

Introduction to SAS

A Brief History of SAS

- **The Sensor Alert Service (SAS) is an emerging standard from OGC**
- **Nearly three years ago, the ORNL SensorNet Program realized it needed a standardized sensor alerting mechanism**
- **Finding none, we began discussing the creation of SAS under the auspices of an OGC Interoperability Experiment (IE) in September 2004**
- **The IE began in earnest in June 2005**
- **Coincidentally, IE development occurred contemporaneously with the OWS-3 Testbed**

SAS IE Results

- **After much evaluation, the SAS IE team decided to use XMPP (an IETF standard, Extensible Messaging and Presence Protocol) for message transport and TML (another emerging OGC standard) for message encoding**
- **SAS IE Interoperability demo in September 2005 using XMPP and TML**
- **Also used during the October 2005 OWS-3 Demo**
- **Draft spec written and discussed at the OGC TC meeting in March 2006 and released as an OGC Public Discussion Paper**

Numerous Improvements Made During Public Discussion Phase

- **Created a much “tighter” spec**
- **Made clear the use of XMPP Multi-User Chat (MUC) for message transport**
- **Removed ambiguities present in the old spec**
- **New message encoding format**
- **More easily extensible messages**
- **Units of measure in use made explicitly clear**

Tighter Specification

- **The spec is now much more, well, “specific”**
  - **I.e., less general**
  - **Much more likely to result in truly interoperable implementations**
- **Alert transport mechanism is now specified to be XMPP/MUC in SAS version 1.0**
  - **Was left unclear in previous spec**
  - **XMPP/MUC has shown itself to be fast and robust**
  - **Have left room for additional transports in future versions, if needed**

Ambiguities Removed in new SAS

- **Many ambiguities present in SAS IE have been removed**
  - **Now uses a "describe-provide" paradigm**
    - **The alert message format is fully described during the advertisement phase**
    - **And learned during the discovery process**
    - **Alert messages themselves can be very short yet fully understood and unambiguous**
  - **No more need for out-of-band agreements between alert producers and consumers to understand the meaning of alert messages**

Now Using O&M Formatting for Alert Messages

- **SAS IE used TML 2.0 to format alert messages**
  - **Turned out that it wasn't quite legal TML as specified in the final TML 2.0 spec**
    - **Fixing that not as easy as it sounds**
  - **Unnecessarily repeated certain values with each alert message**
    - **Made messages longer than necessary**
- **Current SAS has replaced TML with a message format that is compliant with the SWECommon model (O&M)**
- **The most basic raw alert message is now smaller and simpler than before**
    - **Better bandwidth utilization**
    - **"Faster"**
  - **Alert message contents are extensible**
  - **Faster, better, cheaper – yet fully specified and unambiguous**

New SAS Alert Message Format

- ***<lat lon alt datetime expiration value…>***

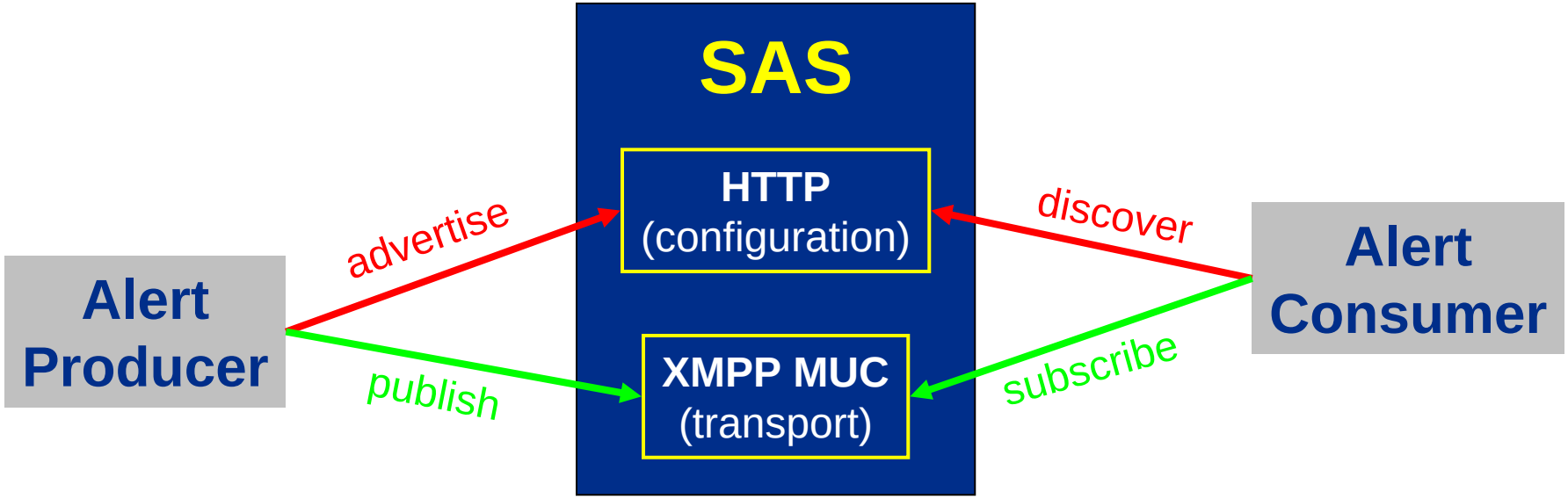
- **Units are well defined**
- **Value field is extensible**
- **Meanings of all values and units of measure are fully understood from discovery process**

New SAS Uses a Web Services Paradigm for Alert Advertisement and Discovery

- **Standard OGC GetCapabilities operation**
- **Advertise and Subscribe operations as Web Services**
- **Supports user-defined alerts (these were in previous spec but not in the SAS IE)**

- **Alert message transport still over XMPP MUC**

SAS Block Diagram

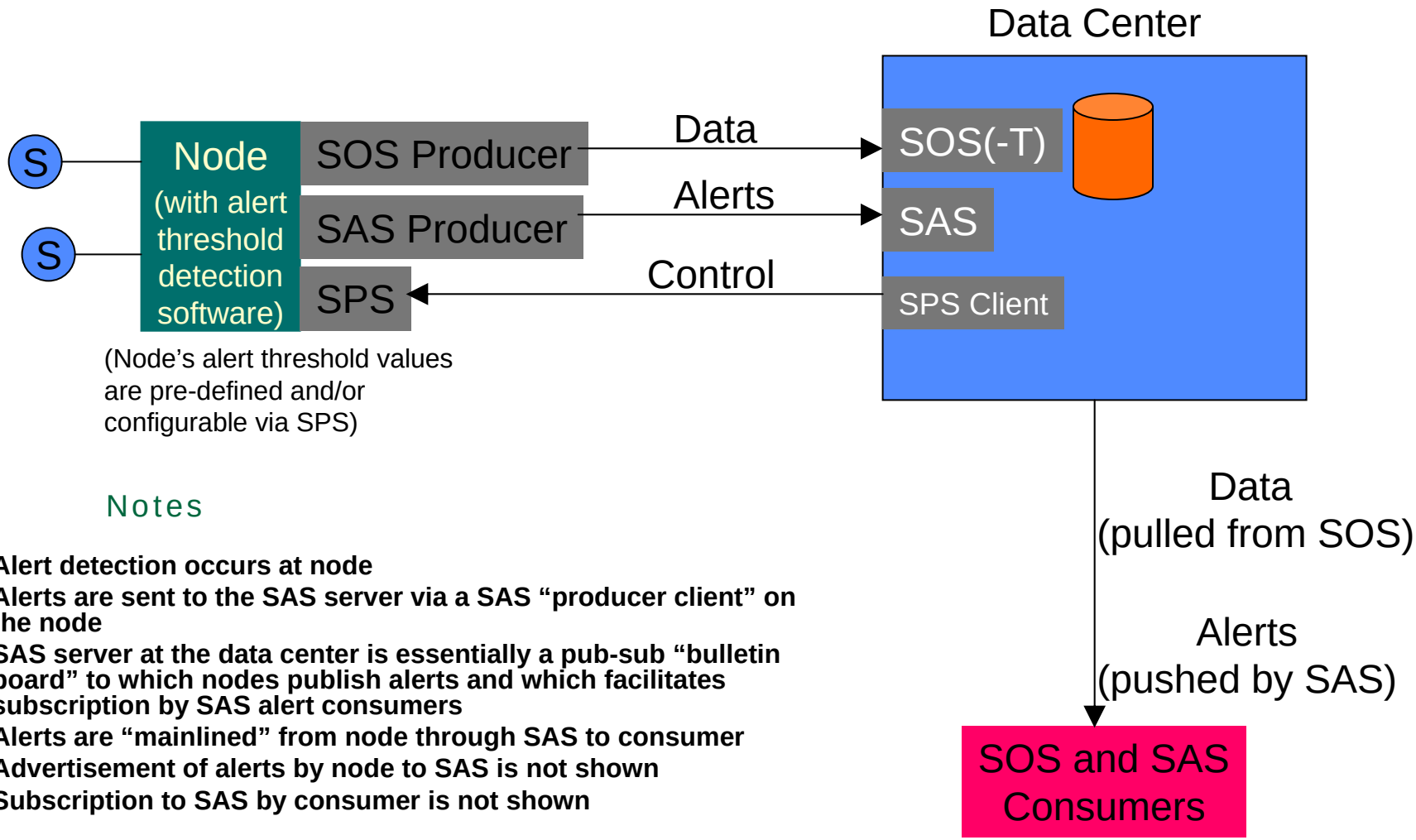


- **Describe-Provide Pattern**
  - **Describe through advertisement and discovery operations**
  - **Provide through publish/subscribe operations**

Two Main SAS Use Cases

- **Pre-defined alerts**
  - **The common SensorNet use case for in-situ sensors with pre-defined alert thresholds**
  - **Threshold values may be configurable but not through SAS**
- **User-defined alerts**
  - **Common University of Muenster use case**
  - **Threshold values set through SAS interface**

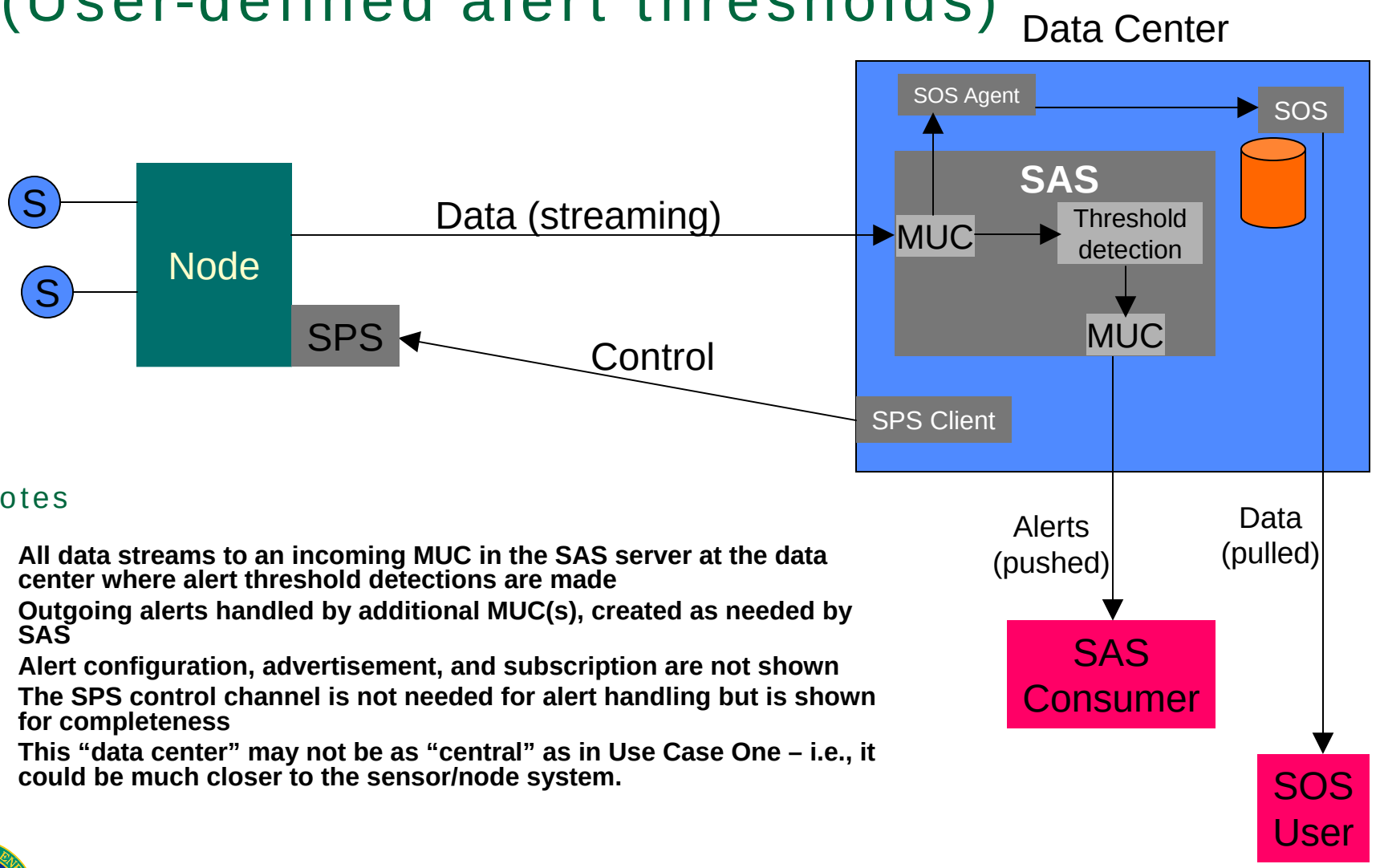
Use Case One
(Pre-defined alert thresholds)



Notes

- **Alert detection occurs at node**
- **Alerts are sent to the SAS server via a SAS "producer client" on the node**
- **SAS server at the data center is essentially a pub-sub "bulletin board" to which nodes publish alerts and which facilitates subscription by SAS alert consumers**
- **Alerts are "mainlined" from node through SAS to consumer**
- **Advertisement of alerts by node to SAS is not shown**
- **Subscription to SAS by consumer is not shown**

Use Case Two
(User-defined alert thresholds)



Notes

- **All data streams to an incoming MUC in the SAS server at the data center where alert threshold detections are made**
- **Outgoing alerts handled by additional MUC(s), created as needed by SAS**
- **Alert configuration, advertisement, and subscription are not shown**
- **The SPS control channel is not needed for alert handling but is shown for completeness**
- **This "data center" may not be as "central" as in Use Case One – i.e., it could be much closer to the sensor/node system.**

SAS Specification Status

- **Spec document is nicely done**
- **Have incorporated changes recommended since the SAS IE and the previous draft document**
- **Spec is *much* cleaner**
- **Voted out as an OGC Best Practices Paper at the June TC meeting**
- **Working toward RFC status**
- **SAS is now part of the OWS-4 SWE effort**
- **OWS-4 may bring about some more small changes**

Relation to Other Standards

- **The basic SAS is designed for sensor alerts**
  - **Uses small, bandwidth-friendly messages intended for automatic handling by a computer**
  - **Unlike CAP, SAS not really designed for human consumption**
  - **Propagation of alerts to human users is referred to as "last mile" delivery**
- **Multiple approaches to "last mile" delivery**
  - **JEP-0127 (an extension to XMPP) defines delivery of CAP alerts over XMPP**
    - **A software agent can receive SAS messages and convert them to CAP-formatted alerts for delivery over XMPP with JEP-0127 using the same basic XMPP architecture**
  - **OGC Web Notification Service (WNS) can be used as a "protocol changer" to change delivery mechanisms**

Part II

SAS at Ft. Bragg

SAS Implementation at Ft. Bragg

- **Ft. Bragg needed to get started on a SAS implementation before the current spec was available**
- **Began working with the original SAS IE design (XMPP MUC and TML)**
- **Intergraph evaluated several commercial XMPP servers and settled on Coversant SoapBox Server 2005**
  - **An established Windows product**
  - **Good support for MUC**
  - **Commercial support**
- **Initial testing indicated performance of over 100 alert messages per second**

SAS at Ft. Bragg

- **Stretching the original expectation of SAS**
  - **Was the source of some of the changes made to the new SAS spec, in particular the need to support extensible alert messages**
- **Among other sensor systems, Bragg is using ObjectVideo, Inc. technology**
  - **Continuous analysis of live video detects anomalous events**
  - **Alert information includes a snapshot of the triggering event**
    - **Required extending the alert message format**
  - **Implemented using SoapBox MUC and (the old) TML format with additional <data> tags**

Other Alert Producers at Ft. Bragg

- **Federal Signal Intrusion Detection and Mass Notification System**
  - **Originally implemented using old TML message format**
  - **Easily converted to new format**
  - **Also uses XMPP for bi-directional control (not part of SAS)**
- **"Traditional" sensors on 3eTI node boxes**
  - **SAS alerts to be implemented using new message format**
- **Sandia National Labs Virtual Perimeter Security (VPS) system**
  - **Under development for Ft. Bragg now**
  - **Will use new SAS message format**
- **Honeywell Fire Alarm system**
  - **Being interfaced to SAS now by ORNL**
  - **Will use new SAS message format**

One Common Feature of all these SAS Deployments

- **Because of the need to get started sooner rather than later, only the SAS message format over XMPP MUC is in use**
- **The HTTP-based configuration (advertisement and discovery) is not being used**
- **Intergraph has created about a dozen pre-configured MUCs**
- **Communication of MUC addresses to producers and consumers is out of band.**
- **Expect to eventually move to a full SAS implementation at Ft. Bragg in years to come**

Part III

SAS at the Port of Charleston and Other Deployments

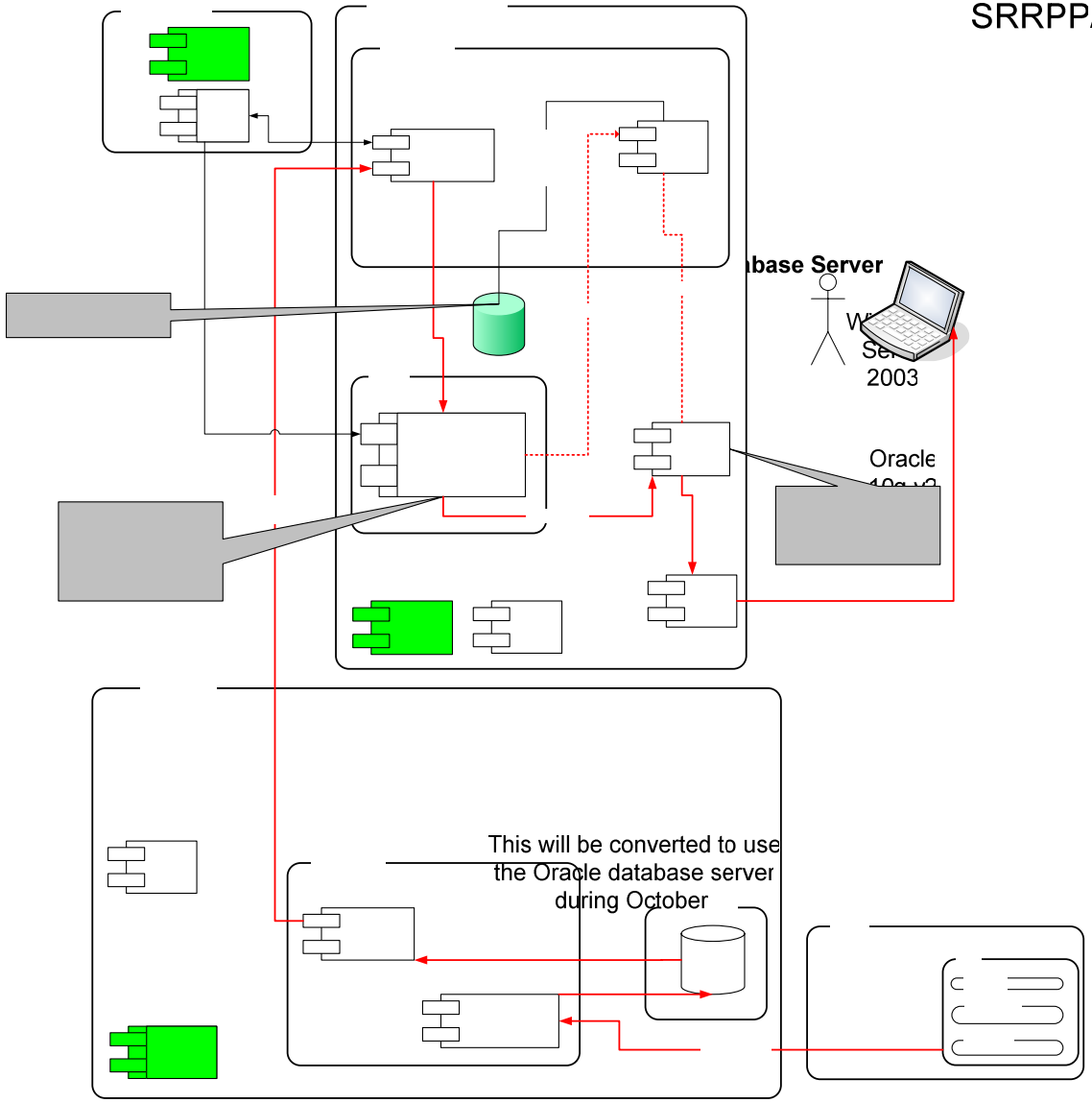
Southeast Regional Radiation Protection Project (SRRPP)

- **In conjunction with the Seahawk project and U.S. Customs and Border Patrol**
- **SRRPP got started late enough to utilize the latest SAS spec**
- **Being implemented this month and next, demo in November**
- **Will use an open source (52 North) implementation of the full SAS spec, including advertisement and discovery**
- **Initial SAS consumer will be lightweight**
  - **No automated processing or display of alerts**

SRRPP/SAS Architecture/Interface Des

8/25/2006

Johnny Tolliver



Operations Center Server

Tomcat 5 5 17

Galdos WFS
(WAR File)

SAS a
MUC
configura
data

PostgreSQL/
PostGIS
Database

Net 1 1

GPS and Sensor
Data to SDE
Conversion
and Data Export
(.Net ArcObjects)
(and SAS alert creation)

Initially SAS alerts are
created here after first
"advertising" to SAS and

Sensor
observations

SAS

OAK RIDGE NATIONAL LABORATORY
U. S. DEPARTMENT OF ENERGY

UT-BATTELLE

Other Deployments

- **ORNL Testbed**
- **Southeast Trusted Corridor Project (SETCP)**
  - **Full SAS**
  - **Beginning with the 52 North implementation**
  - **Just getting underway**
- **University of Muenster Deployments**
  - **Muenster**
  - **South Africa**
  - **Both are using the user-defined alert use case**
- **OWS-4 SWE Thread**

Conclusions

- **SAS is maturing**
  - **Spec greatly improved through the OGC standardization process**
- **We are using a mix of commercial (SoapBox) and open source (52 North) products**
- **Still missing a complete commercial SAS implementation**
  - **Although, to be fair, the spec is not standardized yet**

Conclusions, continued

- **SAS being further refined in OWS-4**
  - **Some changes to spec may yet occur**
  - **Some discussion of the need for an OGC service-wide notification standard**
- **Multiple ongoing SAS deployments**
- **Ft. Bragg and Charleston deployments are near term**
  - **Can return with a status report on their use in the near future**