On Exploitation of Smartphone Technology for Satellite Operations, Providing Ubiquitous Operations

R. Messaros and R. Bolek
Siemens AG Österreich CMT OP TN SP ADM, Siemensstrasse 90, 1211 Vienna, Austria

E. Gomez and R. Santos
ESA/ESOC European Space Agency, Robert-Bosch-Strasse 5, 64293 Darmstadt, Germany

Efficient operation of satellites mandates operational concepts which guarantee safe operation, while keeping costs low. The "lights-out" approach during the routine phase (i.e. when human involvement is limited to supervision most of the time) is consistent with the idea of lowering costs, but can pose a risk to spacecraft safety. In the "lights-out" approach staff is in charge of operations work during standard working hours only. While this is consistent with the needs of routine phase, it would leave the satellite unsupervised for long periods of time. Recent development of powerful, yet affordable mobile devices has opened up a technological window, which ESA is targeting for exploitation during the satellite operation routine phase.

An infrastructure is in the finishing stages of development, allowing remote users to interface with the Mission Control Centres. While the necessary technology for this is available for some years now, only the recent impetus in the Smartphone area allows equipping operators with non-proprietary devices, satisfying the needs of platform resources, while at the same time covering all other communication needs, thus removing the need for an extra device to be ported and maintained. The development of the recent generation of devices includes the standardised HTML5, which allows developing portable mobile applications.

Security aspects were integrated into ESA's web-enabled infrastructure right from the start, complying with international levels of network safety and authentication.

This paper furthermore describes the operational configuration as being deployed for ESA's missions, including the propagation of operational events to groups of on-call engineers, as well as supplying them with the operational context enabling them to perform the subsequent operational steps safely and efficiently.

I. Operational Background

Increasing economic pressure to bring down operational costs has led the European Space Agency (ESA) to investigate alternatives to the established concepts of mission operation. The traditional and proven infrastructure is going to be kept unchanged for good reasons for LEOP (Launch and Early Orbit Phase) operation, IOT (In-Orbit Testing) and commissioning, and contingency operation. However routine operations are an arena, in which efficient ways of operation pay off particularly well.

Recent developments in on-board automation have led to operating missions during their routine phase using time-tagged commanding and by exploiting the capabilities of on-board commanding queue management. This allows uploading and verifying command sequences several days in advance. As a result the staffing in the control

centres could be reduced from 24/7 operation to normal office hours (8 hours per day, 5 days per week), depending on the mission type.
Nevertheless, transferring operations to a lights-out way of operation bears the risk to jeopardize the mission outputs and to increase the reaction times in case of anomalies unnecessarily, as there is no monitoring outside working hours. Therefore ESA started to develop a complementary facility to produce an alert system, which conveys notifications of alert conditions occurring in ESA Ground Control infrastructure to Remote Engineers, who only need to be equipped with standard mobile phones capable of receiving SMS texts. The SMS texts shall contain the fundamental alert information itself, augmented with a basic operational context (set of TM parameters, configurable on a per-alert basis). The purpose of this operational context is to support remote engineers in determining, under which conditions alerts had been created.

II. The REALS System

This system is being developed under the name REALS (REmote ALert System), in order to open up a migration path for ESA operations towards Lights-Out Operation of missions in their routine phase, as well as operation of other ESA infrastructure (e.g. networks, ground stations).

REALS is designed to be fully integrated into the existing ESA infrastructure regarding the following problem domains:

- ESA security policy: REALS complies with the ESA Network Security Policy
- SCOS-2000 based operations concepts: The sources for events are Spacecraft Events, System Events by the generated by the MCS (Mission Control System) kernel (part of ESA's SCOS-2000 system), with the addition of REALS generated events (keep-alive mechanism flagging events). Likewise the source for TM based data, which annotates alerts, shall be based on SCOS-2000 systems (each of which can support multiple spacecraft structured in Spacecraft Domains).
- The REALS Alert Function handles events from different SCOS versions running on Linux and on Solaris.
- Integration of TM provision infrastructure ARES: ARES is designed around the ESA security policy and SCOS-2000 operational concepts. Consequentially REALS is based upon ARES, which it extends with respect to the required functionality, particularly provision of Event data.
  Event data are fundamental to the alert generation within REALS. REALS re-uses the ARES provided infrastructure and extends it with Event data and a web-interface. The web-interface supports remote engineers by supplying them with the operational context through the web-based provision of TM data that is available and accessible from within the ARES archive. ARES does not work in real-time but following a batch processing approach that ensures that data is consolidated with a configurable frequency and duration.

III. REALS System Context

The high level system context is depicted on the following figure. Deployment of the entities is done using Virtual Machines. Figure 1 shows three entities for networked elements, which are separated from one another by firewall systems (indicated by red lines). In the order of decreasing protection level these are

- **Protected Entities:**
  These entities are operated on operational LAN infrastructure, which is heavily protected from the remainder of the network infrastructure. This also includes enforcement of explicit communication rules and directions.
- **Exposed Entities:**
  Infrastructure which is designed to provide access to services from the Internet is placed within exposed network parts. An outer firewall system protects this Infrastructure, which enforces the rules of communication, both between the entities on the exposed networks, as well as between the Internet and the elements on the exposed network.
- **Internet:**
  REALS operators access alarms and TM via mobile networks, placing them network-wise in the Internet. Network access is done over SSL/TLS (as part of https-URLs), in order to prevent from eavesdropping and man-in-the-middle attacks. Unauthorized access to the REALS infrastructure is prevented by exchanging credentials (time limited, revocable) in either direction.

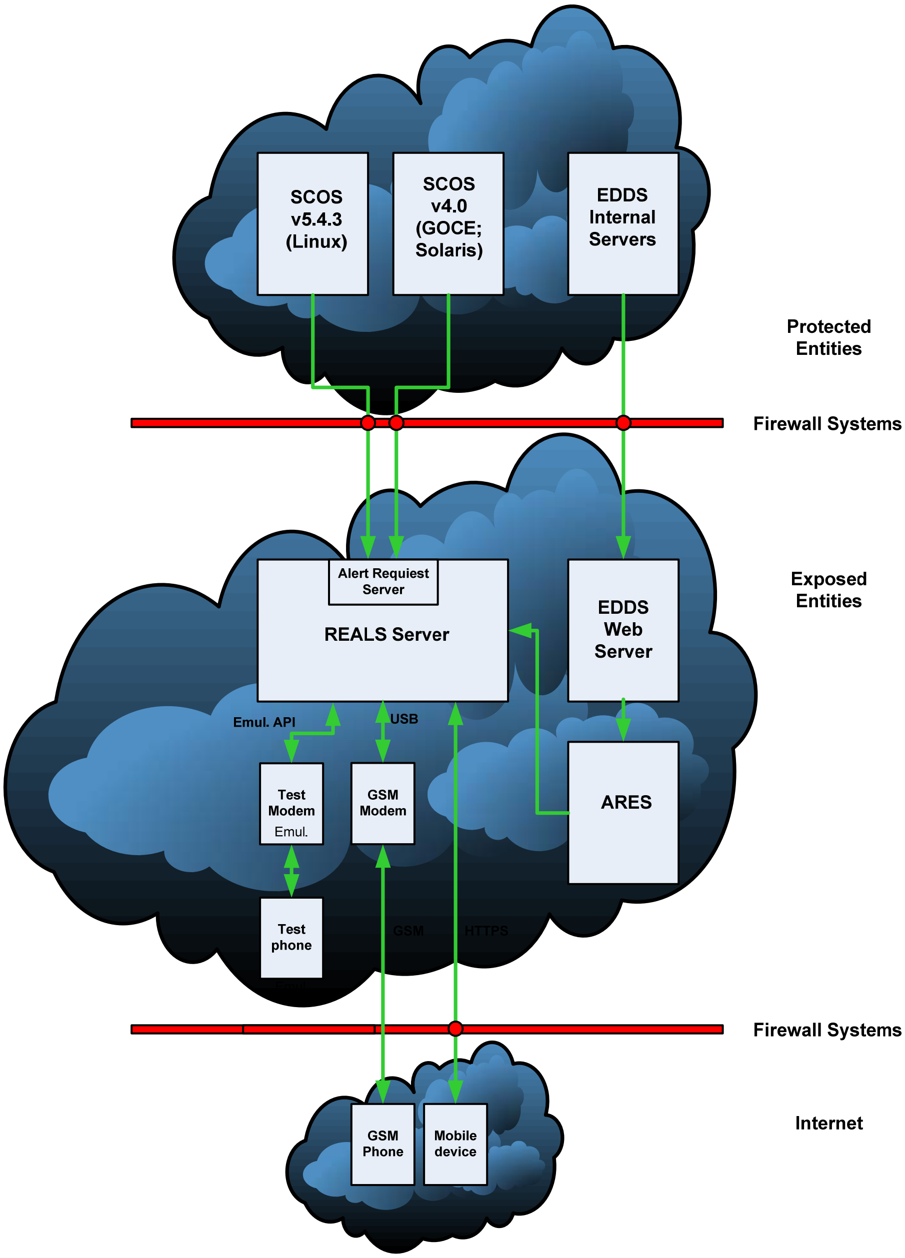

Figure 1. REALS system context.

Sources for the Alerts are SCO-2000 systems for a range of missions, which may run on different computer architectures (Linux on x86, Solaris on SPARC). They push the Alert information to the REALS Server. The alert information is created by SCOS-2000 in real time when a parameter is out of range. It consists of the details of the out of limits parameter plus some environmental information. Telemetry and Event data are provided via EDDS (EGOS Data Dissemination System), which features a request infrastructure (EDDS Web Server, the 'Web-Shop' for requesting data) and the EDDS Internal Servers pushing the data asynchronously through the inner firewall. The ARES infrastructure stores the EDDS-provided data in a database, which is subsequently accessible to the REALS Server for further processing and delivery under operator control. Furthermore REALS handles the delivery of Alerts (including confirmation from remote on-call operators, as described in the following), as well as a web-based interface telemetry and Events.

Operational deployment of REALS is done in a redundant, hot-standby configuration, see the figure below. The concepts implemented with REALS on one hand allow REALS supplying multiple Mission Control Systems with remote Alert and Data provision, while on the other hand allowing Alert propagation to more than one parallel REALS instance, thus increasing the overall availability.

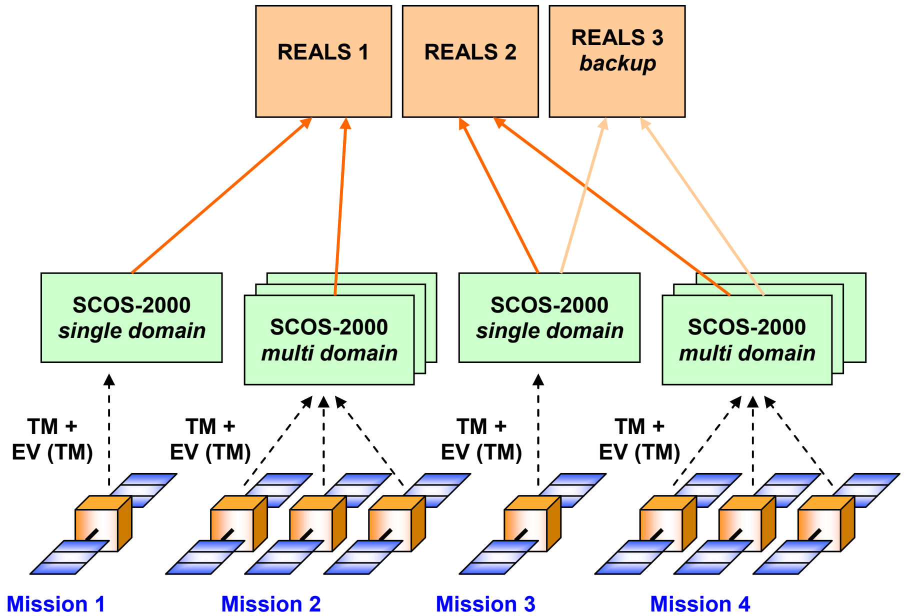

Figure 2. REALS multi-mission, multi-domain, and redundancy.

IV. REALS Functions

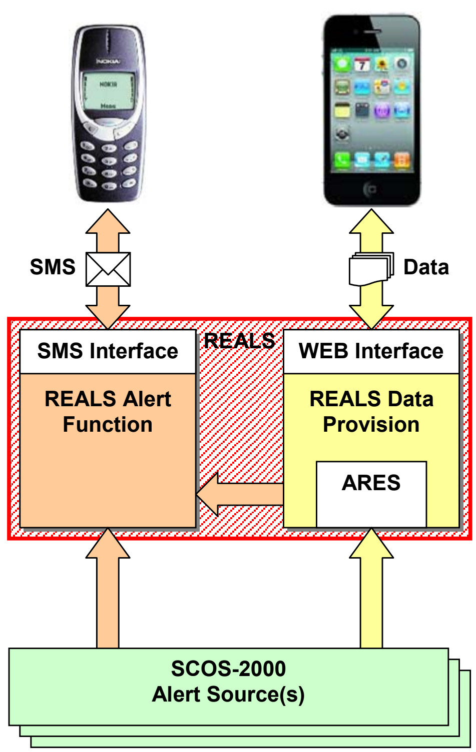

Figure 3. REALS functions and high-level architecture.

The two main functions provided by REALS are:

- Alert Function
- Data Provision.

The purpose of the REALS Alert Function is to notify on-call engineers about spacecraft and ground system events. Events, which are created from an Alert Source, are pushed as XML files to the REALS Alert Application. A temporary disc space in the file system of the REALS Alert Application decouples the generation of events and the processing of events. In this way other Alert Sources can be added without any need to modify REALS. The only requirement for compatibility is the compliance to the of the XML schema. Outgoing SMS Alert messages can be configured to include up to 10 telemetry parameters for immediate assessment by the operators (a limit imposed by the 160 character size limit of SMS messages).

The full lifecycle of an Event/Alert is illustrated below. Events are raised within operational Mission Control Systems and forwarded to REALS, which stores them as Alerts it its database. Alerts are then forwarded to the first mobile phone from a sorted list of operators (configurable on a per-mission basis). Accepting the Alert (via replying per SMS) completes the life-cycle of the Alert. Timeouts of accepting the Alert or Rejecting the Alert (via replying per SMS) passes the Alert to the next person in the list, who will receive the Alert SMS. On-call operators can furthermore block classes of Alerts (in order to prevent from being flooded with consecutive Alerts).

A second mechanism will take care of ensuring that every alert is processed until an engineer rejects or accepts it. If the alert remains ignored for a configurable period of time, the spacecraft operations manager will be informed

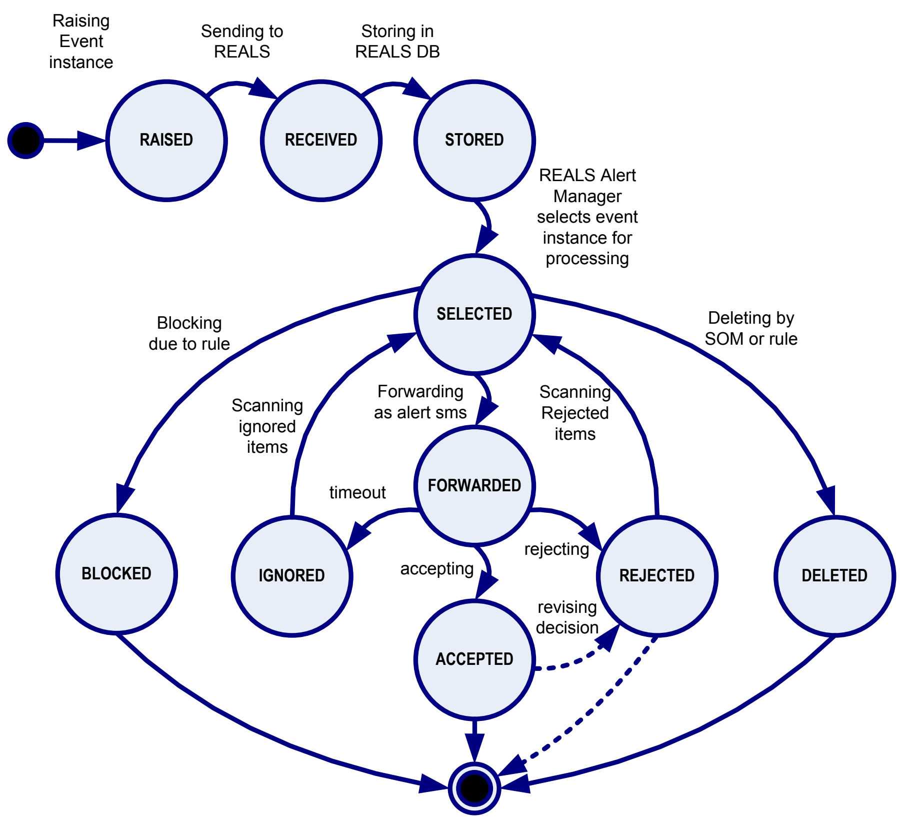

Figure 4. Event/Alert instance life-cycle.

The purpose of the Data Provision Function is to provide detailed telemetry information on request of on-call operators. REALS Data Provision supplies this functionality via a Web portal, which provides access to a configured sub-set of telemetry parameters. Operators can access the most recent values of telemetry parameters, as well as to historic values (limited only by the configured storage capacity within REALS). The design of the TM displays is adjusted to the limited screen resources on today's Smartphones, see Figure 5 below.

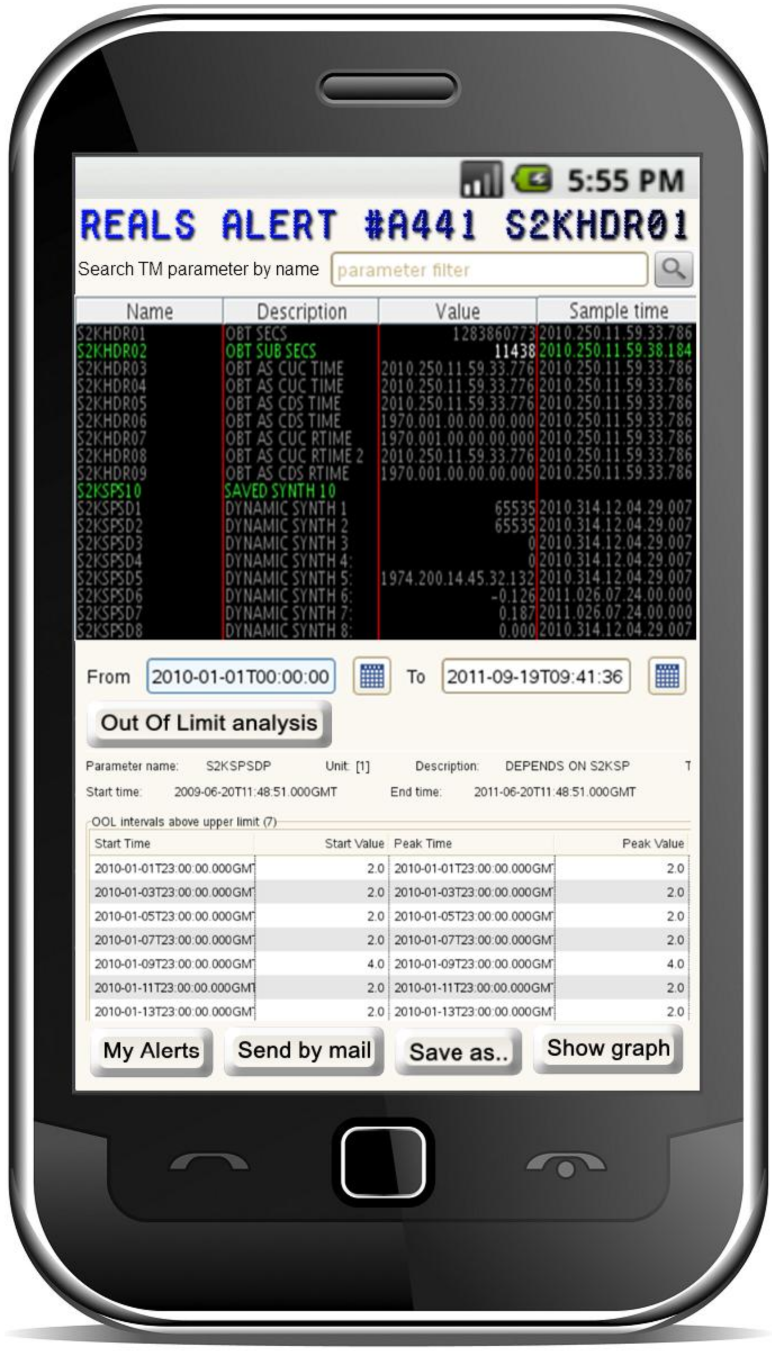

Figure 5. REALS mobile access to TM.

V. Summary

REALS provides Alert Services and remote Telemetry Access Services. As such it supplies enabler technology to increase lights-out operation periods, which helps to cut down on mission costs. REALS will be operationally validated with ESA's CRYOSAT and GOCE missions, starting from autumn 2012.