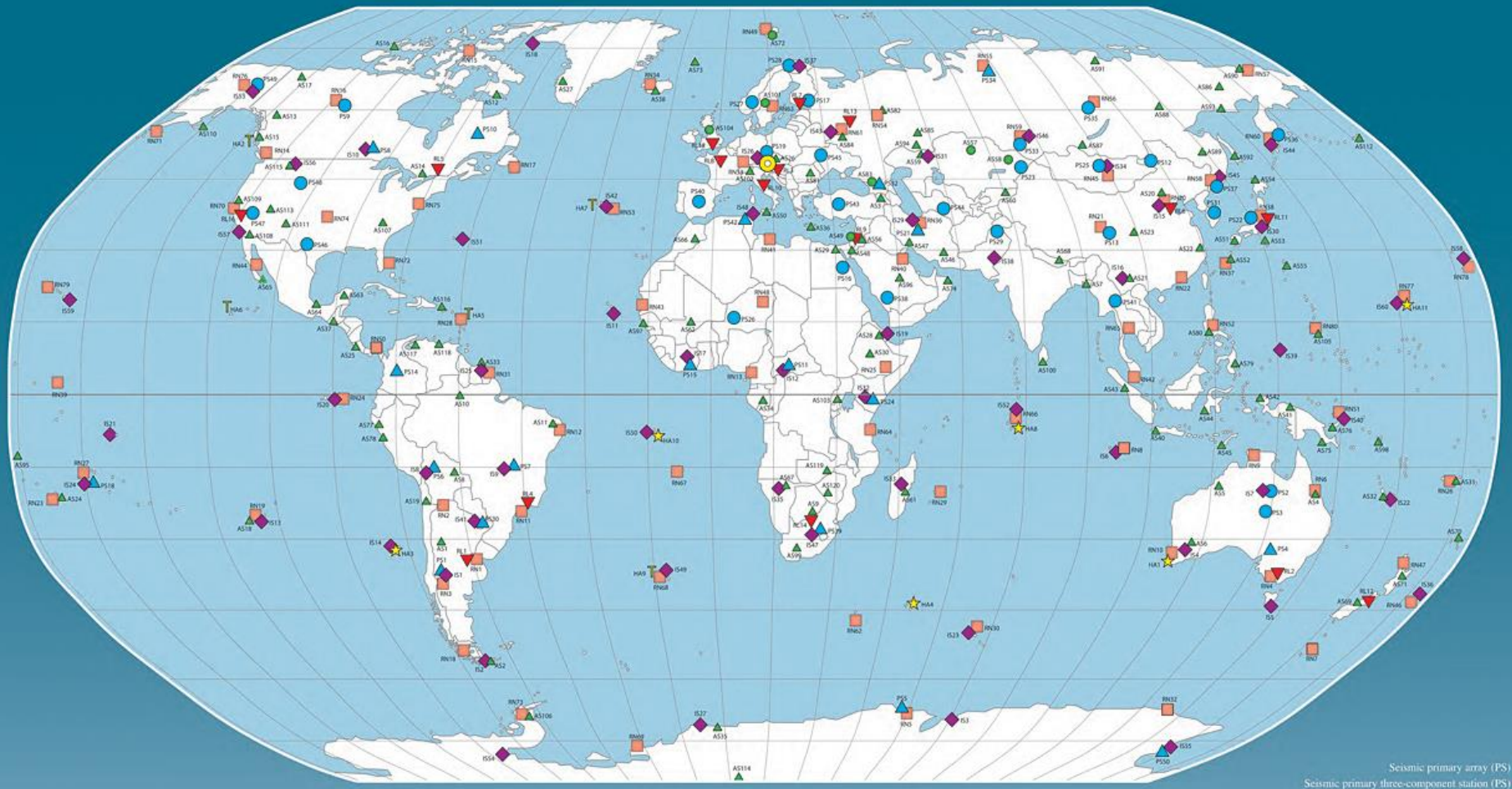
SAND2014-4537C

Authentication of Data from the International Monitoring System (IMS)

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

INTERNATIONAL MONITORING SYSTEM



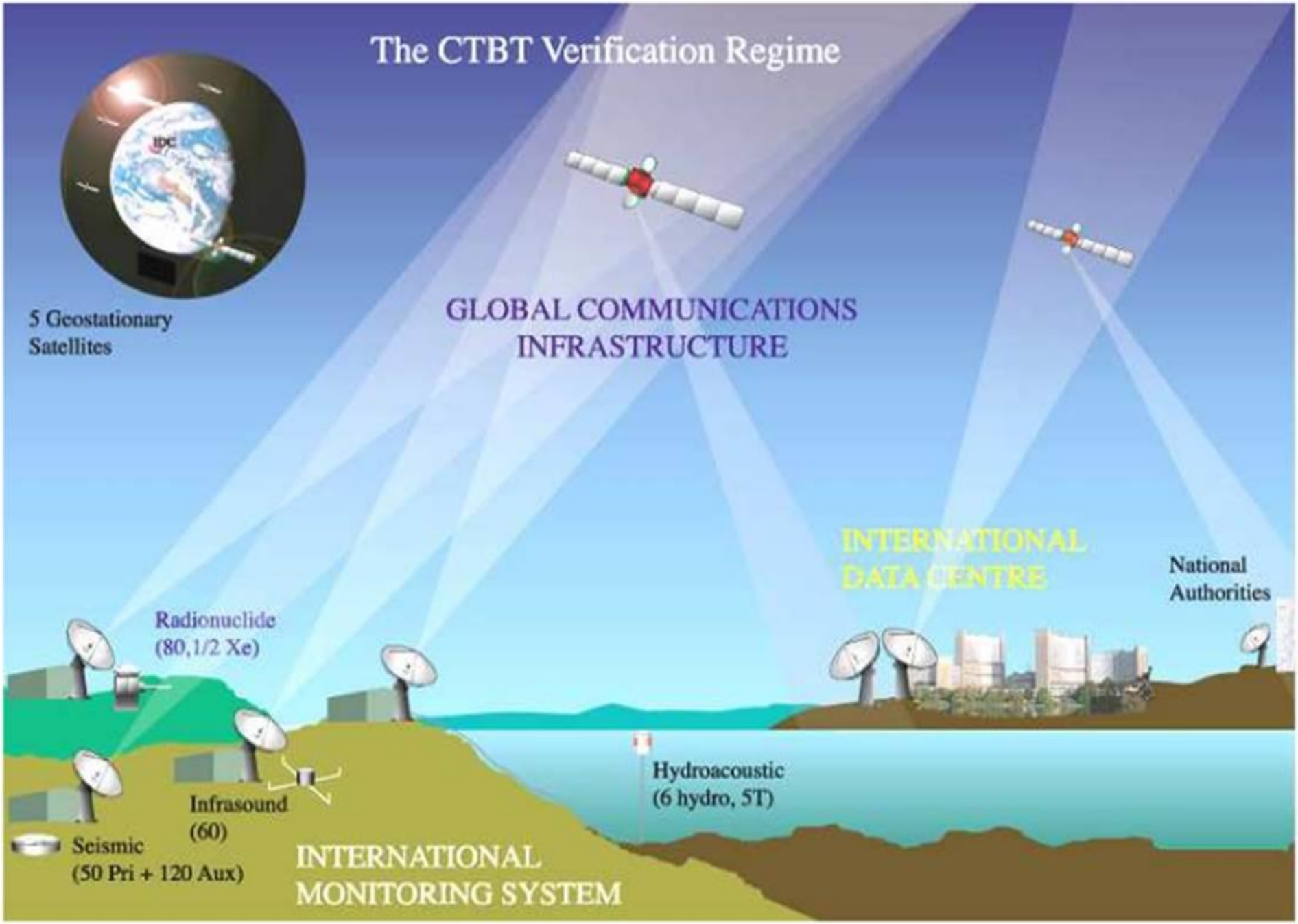
The Comprehensive Nuclear-Test-Ban Treaty (CTBT) of 1996 bans nuclear explosions in all environments.
Explosions in the atmosphere, under water and in outer space were banned in 1963. CTBT prohibits them underground as well.

Under CTBT, a global system of monitoring stations, using four complementary technologies, is being established to record data necessary to verify compliance with the Treaty. Supported by 16 radionuclide laboratories, this network of 321 monitoring stations will be capable of registering shock waves emanating from a nuclear explosion underground, in the seas and in the air, as well as detecting radioactive debris released into the atmosphere. The location of the stations has been carefully chosen for optimal and cost-effective global coverage.

The monitoring stations will transmit, via satellite, the data to the International Data Centre (IDC) within CTBTO PrepCom in Vienna, where the data will be used to detect, locate and characterize events. These data and IDC products will be made available to the States Signatories for final analysis.
Overleaf is a listing of the 337 facilities of the international monitoring system and brief descriptions of their characteristics and capabilities.

Seismic primary array (PS)
Seismic primary three-component station (PS)
Seismic auxiliary array (AS)
Seismic auxiliary three-component station (AS)
Hydroacoustic (hydrophone) station (HA)
Hydroacoustic (T-phase) station (HA)
Infrasound station (IS)
Radionuclide station (RN)
Radionuclide laboratory (RL)
International Data Centre, CTBTO PrepCom, Vienna

Chart I, revised July 2003


The CTBT Verification Regime
5 Geostationary Satellites
GLOBAL COMMUNICATIONS INFRASTRUCTURE
INTERNATIONAL DATA CENTRE
National Authorities
Radionuclide (80,1/2 Xe)
Hydroacoustic (6 hydro, 5T)
Infrasound (60)
Seismic (50 Pri + 120 Aux)
INTERNATIONAL MONITORING SYSTEM

IMS system uses a two-factor approach to system authentication

- Geophysical Analysis
  - Background monitoring for sudden changes
  - Signal comparison with remainder of the IMS system
- Data Surety

Sandia National Laboratories

Data Surety

- Station Security
- Data Validation
- Command & Control

Sandia National Laboratories

Station Security

- Equipment co-located in a locked vault/cabinet/building
- Vault/cabinet/building armed with intrusion switch
- Status of intrusion switch
  - Reported in waveform data stream
  - Message sent on change of status in radionuclide
- Status monitored at the International Data Centre (IDC)


Q4 2011
USER
PWR
GPS
I/O 1
I/O 2


Unit First Aid Kit


Taurus
Nanometrics
USER
ON
I/O 2
I/O 1
GPS

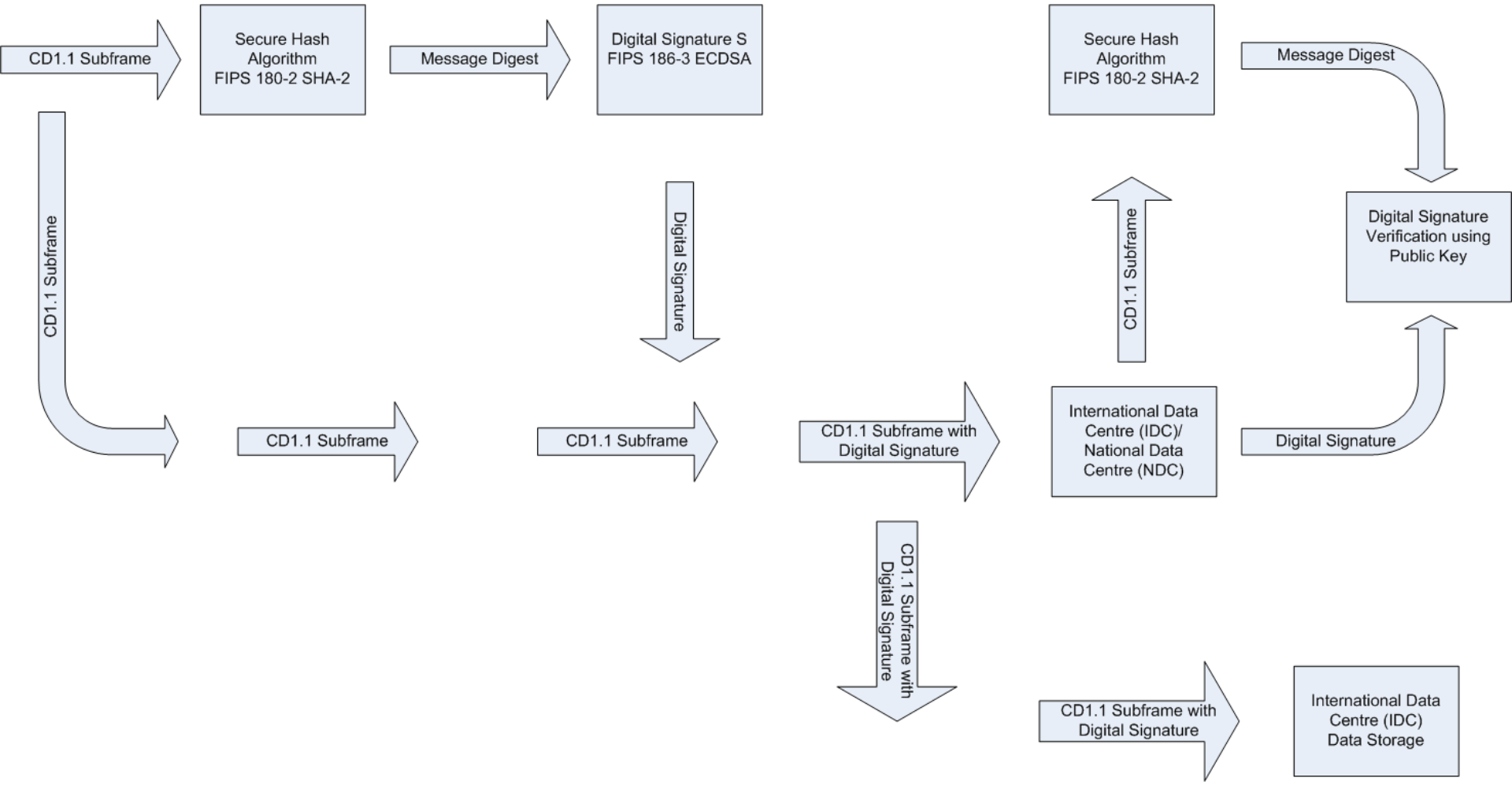

DSPEC

Data Validation

- Signatures produced from CD1.1 data using
  - FIPS 186-2 ECDSA
  - FIPS 180-2 SHA-2
  - FIPS 140
- Keys
  - Private/Public keys generated within security token
  - Public keys uploaded to Certificate Authority through PTS Secure Portal
  - Station Certificates stored on Lightweight Directory Access Protocol (LDAP)
  - IDC/NDCs retrieve Station Certificates from LDAP
  - Certification Revocation Lists document valid dates of certificates
- Data Signatures attached to frame
- Data signatures validated at IDC and NDCs
- Data from failed signatures will not used for event detection by the IDC

Sandia National Laboratories

CD1.1 Data Validation

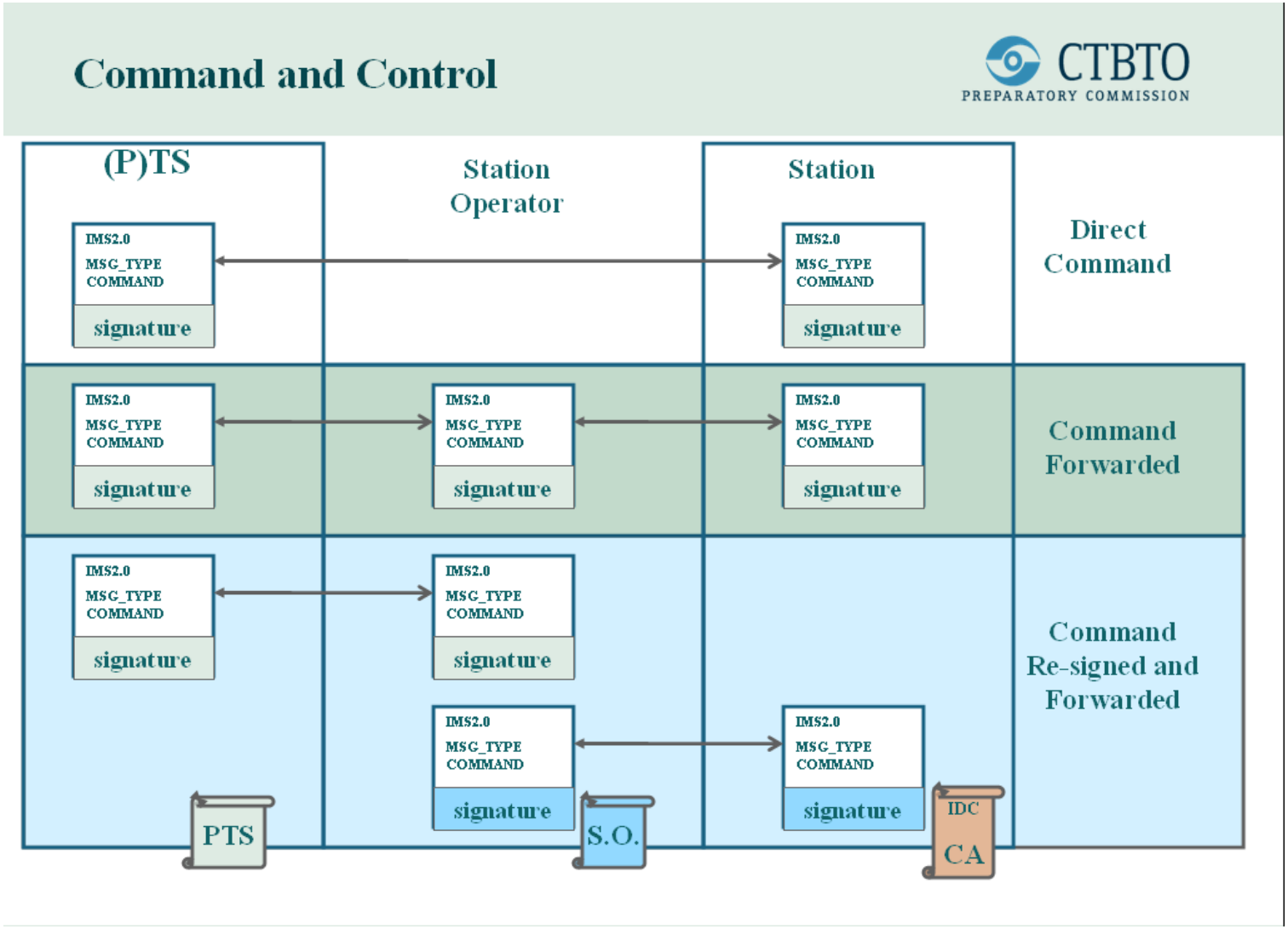


Sandia National Laboratories

Command & Control

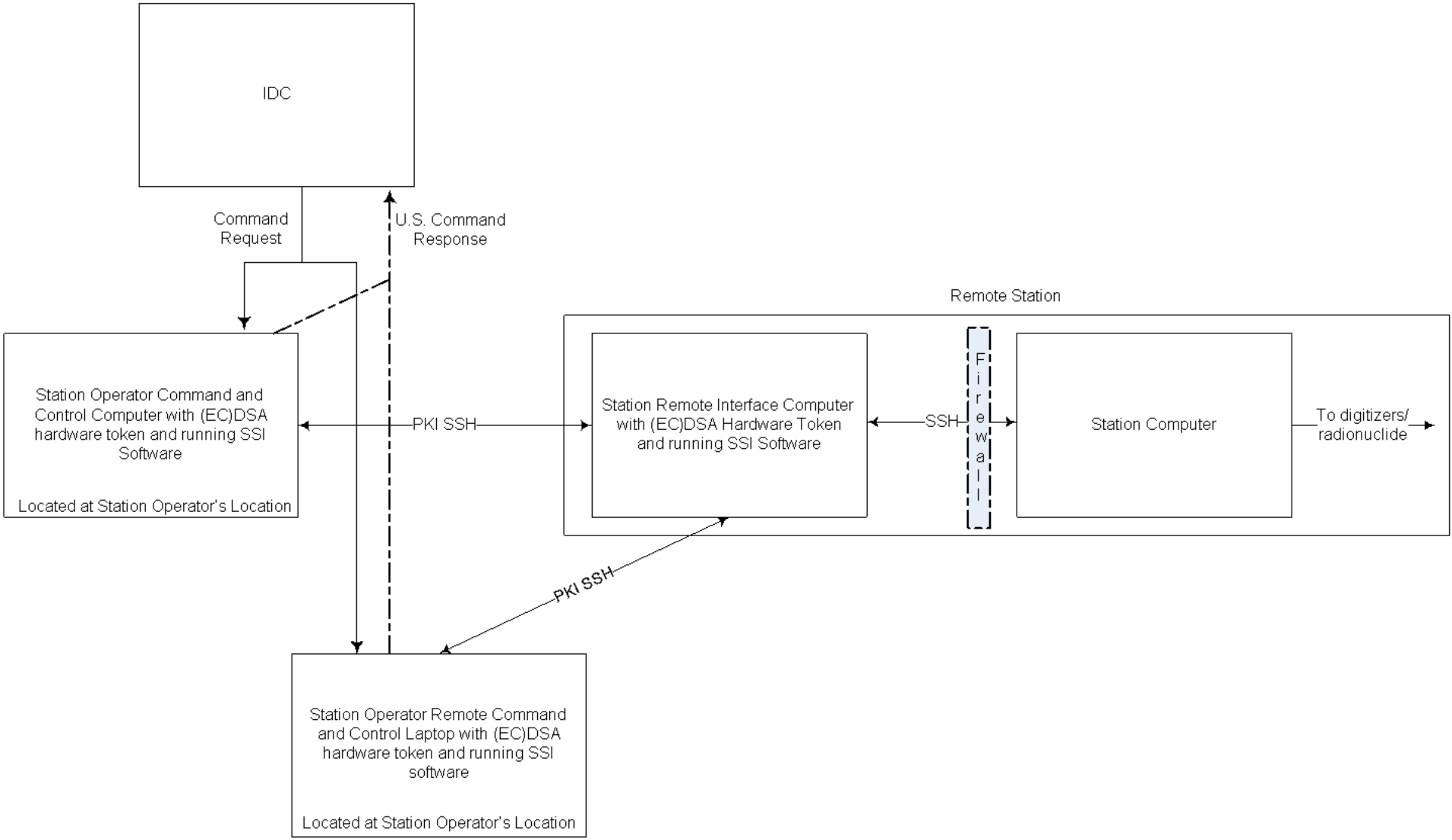
- Core Commands Authorized by PTS
  - Change in station operations
    - Calibration (waveform/radionuclide)
    - Detector Background
    - Blank Spectrum Request
  - Key Management
- Commands signed and authenticated using same requirements as data signing
- All Core Commands authenticated
- All remote commands, including remote sessions, must be authenticated at the station

Original C&C Method



Sandia National Laboratories

Proposed C&C Method



Sandia National Laboratories