ITU Workshop on "Combating Counterfeit Using Conformance and Interoperability Solutions"
Geneva, Switzerland
28 June 2016

Combating Counterfeit ICT Conformity Assessment as a Tool

João Alexandre Zanon

Regulatory Specialist – ANATEL/Brazil

zanon@anatel.gov.br

Associate Rapporteur of ITU-T Question Q8/11

Rapporteur of CITEL Correspondence group on the Combat of Counterfeit substandard and unauthorized ICT devices

Co-Rapporteur of CITEL on Rapporteurship Fraud Control, Regulatory Non-compliance Practices in Telecommunications.

Outline

- **The Brazilian Scenario.**

- **Challenges when addressing the problem.**

- **The importance of Conformity Assessment when combating Counterfeit.**

- **Latest CITEL actives.**
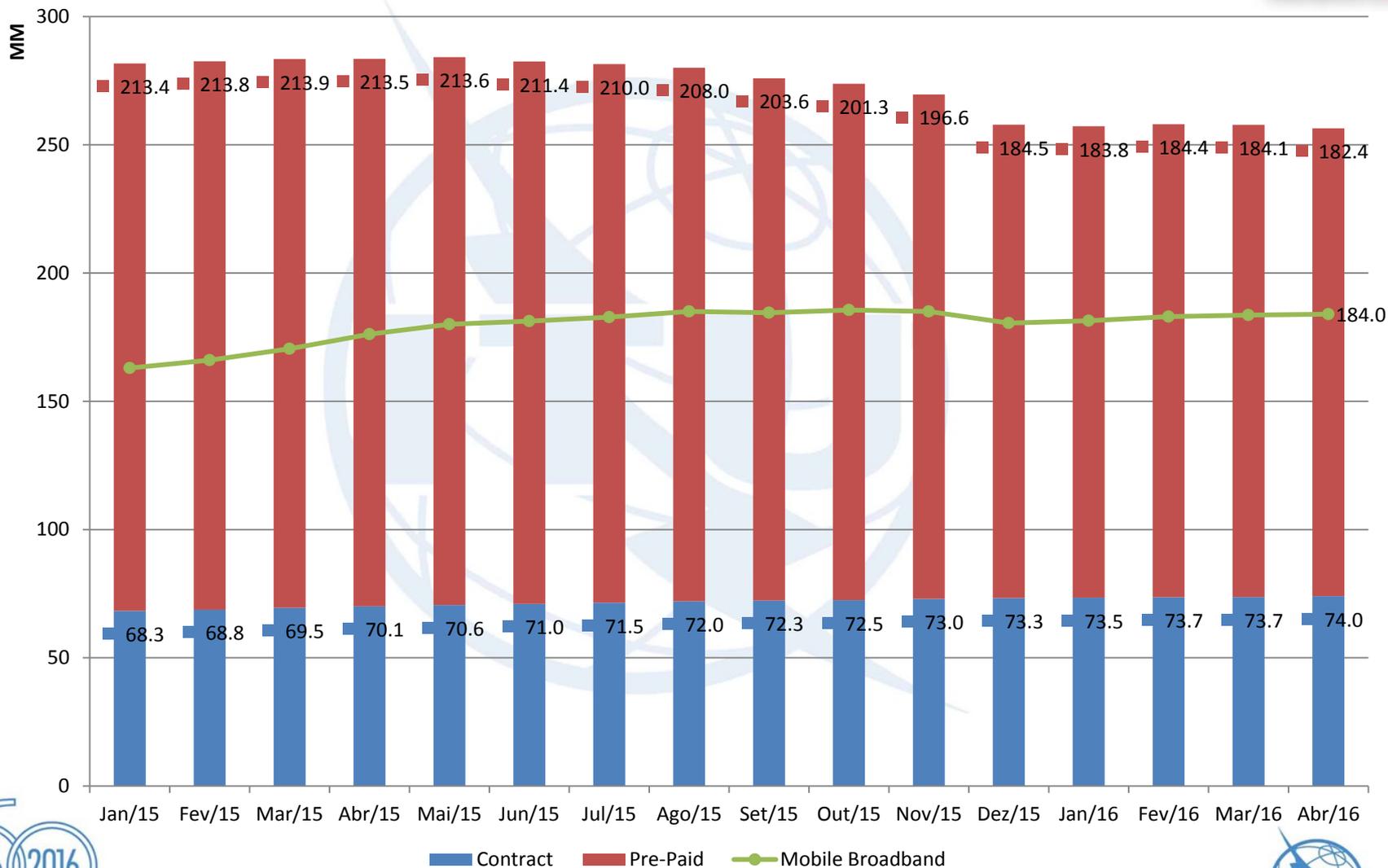
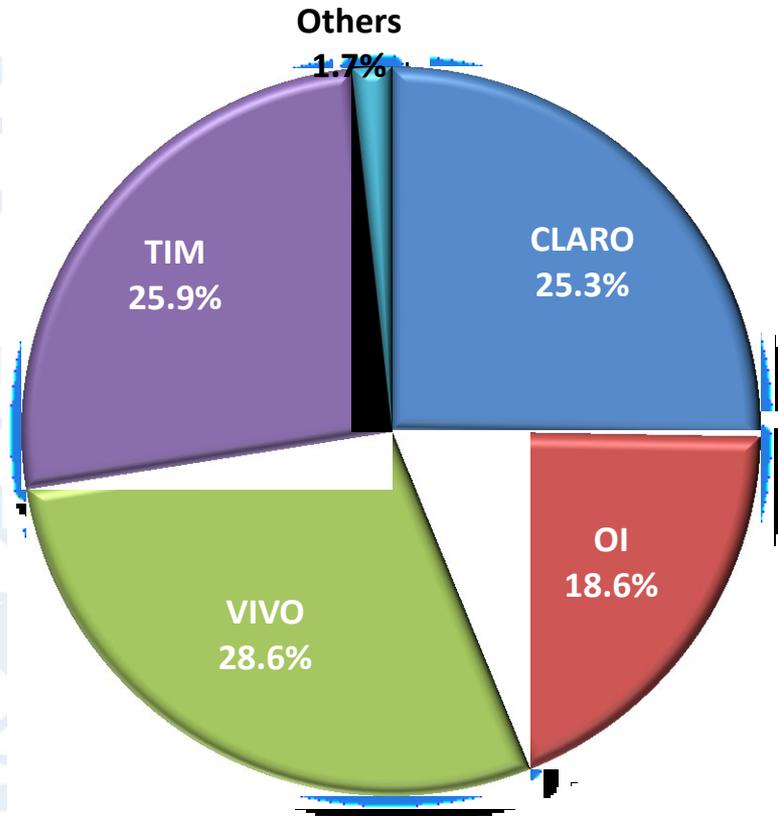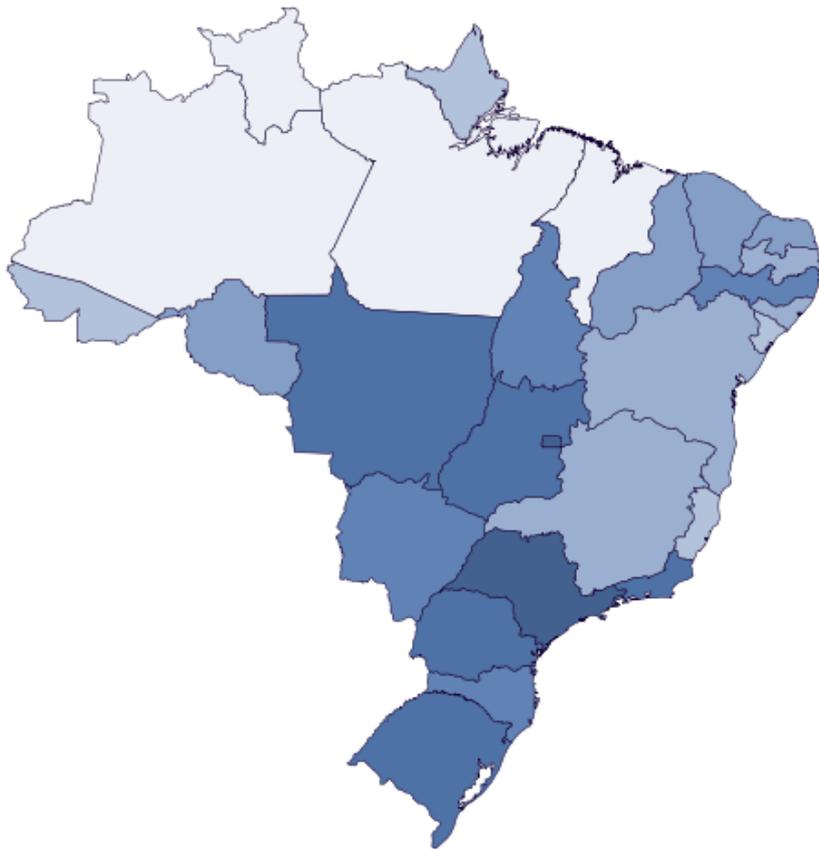- **Latest ITU actives.**

- **What we should aim for.**

The Brazilian Scenario

Brazil - Mobile Access Numbers

Y-axis label: MM

	Jan/15	Fev/15	Mar/15	Abr/15	Mai/15	Jun/15	Jul/15	Ago/15	Set/15	Out/15	Nov/15	Dez/15	Jan/16	Fev/16	Mar/16	Abr/16
Pre-Paid	213.4	213.8	213.9	213.5	213.6	211.4	210.0	208.0	203.6	201.3	196.6	184.5	183.8	184.4	184.1	182.4
Contract	68.3	68.8	69.5	70.1	70.6	71.0	71.5	72.0	72.3	72.5	73.0	73.3	73.5	73.7	73.7	74.0
Mobile Broadband																184.0

Legend: Contract • Pre-Paid • Mobile Broadband

Mobile Density and Market Share

Mobile Density on Brazil: 124,6%

Estimated Population: 205,8M

Mobile Access: 256,4M

Apr/2016– IBGE e Anatel

Conformity Assessment
Applicable Laws and Regulations

- **Law 9.472 (July 1997) – General Telecommunications Law.**
  - Establishes that ANATEL, the Brazilian National Telecommunications Agency is responsible for issuing or recognizing the certification of telecommunication products and for issuing standards and regulations regarding their use in Brazil.

- **Resolution 242 (November 2000) – General regulations on the certification and approval of telecommunication products.**
  - Establishes that any telecommunication product, before it may be sold or used in Brazil, must have a CERTIFICATE OF CONFORMITY issued by a **Designated Certification Organization – OCD** and approved / homologated by Anatel.

  - Classifies telecommunication products in THREE Categories;

  - Establishes that ANATEL may implement Mutual Recognition Agreements for conformity assessment of telecommunication products, recognizing foreign certification bodies and laboratories as parts of its conformity assessment process.
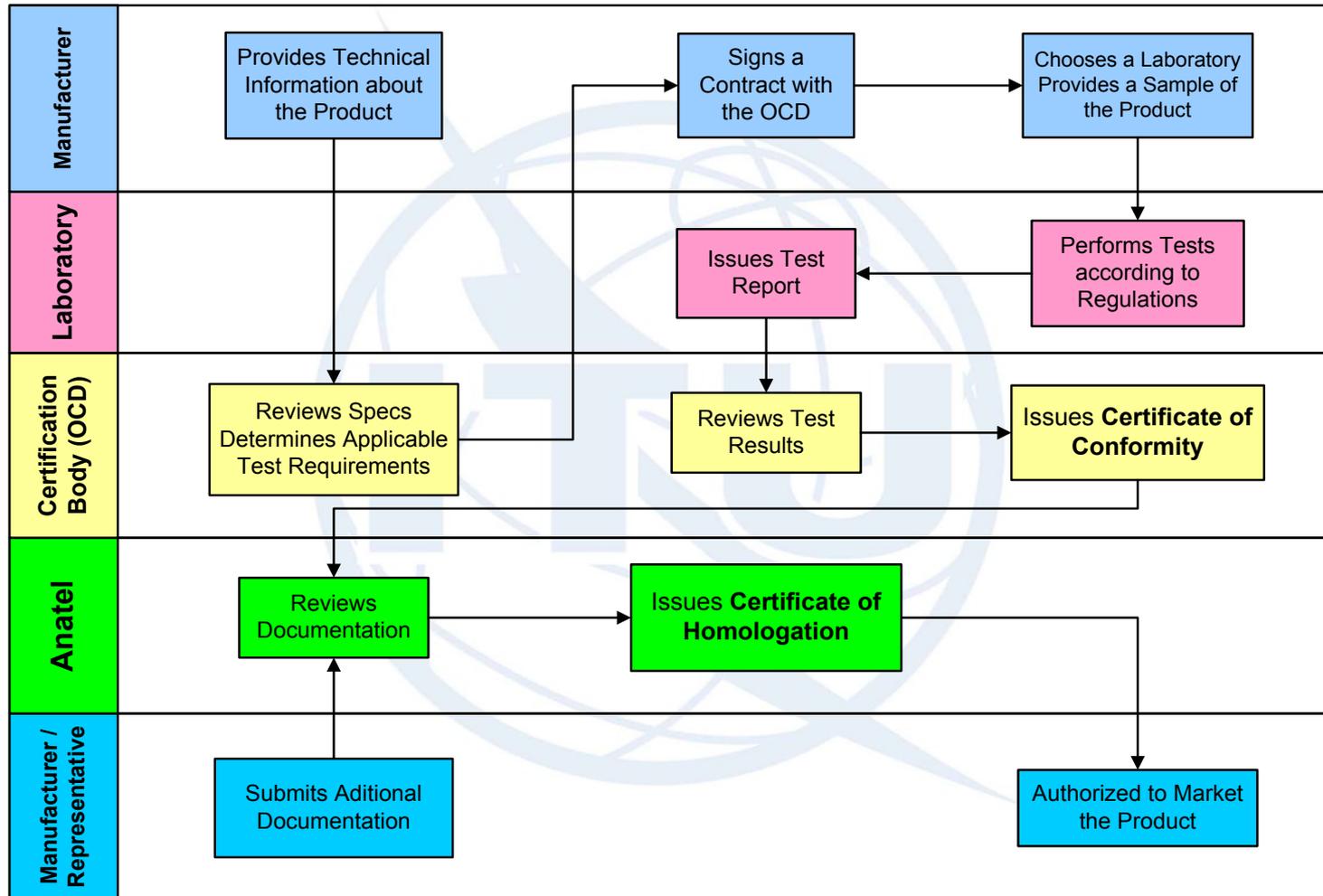
Categories of Telecommunication Products

- Category 1: Terminal equipment used by the general public to access public telecommunication networks (Ex: Telephone sets, cell phones, modems…).
  - Certification: Laboratory Testing of a representative sample;
    Factory Inspection (may be replaced by ISO 9000 certification);
    Periodic Evaluation (every year).

- Category 2: Products not included in Category 1, that use the radio frequency spectrum. (Ex: Digital Transceivers, Antennas, restricted radiation equipment…).
  - Certification: Laboratory Testing of a representative sample;
    Periodic Evaluation (every two years).

- Category 3: Products not included in Categories 1 or 2 for which regulation is necessary to ensure network interoperability, safety and EMC (Ex: Switches Cables; Batteries; Power Supplies; Data communication Multiplexers…).
  - Certification: Laboratory Testing of a representative sample.

Brazilian Certification Process

Manufacturer	Provides Technical Information about the Product	Signs a Contract with the OCD	Chooses a Laboratory Provides a Sample of the Product
Laboratory		Issues Test Report	Performs Tests according to Regulations
Certification Body (OCD)	Reviews Specs Determines Applicable Test Requirements	Reviews Test Results	Issues **Certificate of Conformity**
Anatel	Reviews Documentation	Issues **Certificate of Homologation**	
Manufacturer / Representative	Submits Aditional Documentation		Authorized to Market the Product

CA - Enforcement activities

" All equipment that use radiofrequency to transmit signal must be certificate before being used on Brazil."

- To Identify and combat defining preventive actions to protect the market;

- To favor fair competition between all equipment manufactures;

- Protect the internal market and the end-user;

- **Pre-Market Surveillance (Type Approval):**

  - To grant access to market by compliance demonstration;

- **Post-market (Oversight):**

  - When demanded (complains).

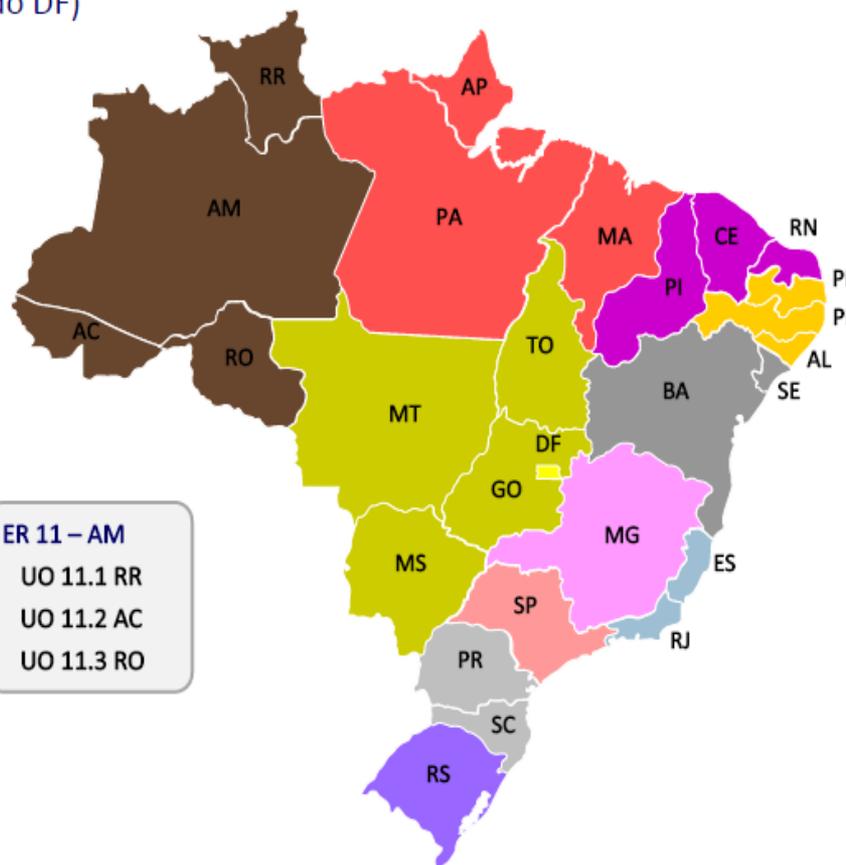 - Continues validation the equipment follows up-to-date regulations;

Working Force on enforcement

11 Escritórios Regionais

16 Unidades Operacionais (incluindo DF)

ER 01 – SP

ER 02 – RJ
UO 2.1 - ES

ER 03 – PR
UO 3.1 - SC

ER 04 – MG

ER 05 – RS

ER 06 – PE
UO 6.1 PB
UO 6.2 AL

ER 07 – GO
UO 7.1 MT
UO 7.2 MS
UO 7.2 TO

ER 08 – BA
UO 8.1 SE

ER 09 – CE
UO 9.1 PI
UO 9.2 RN

ER 10 – PA
UO 10.1 MA
UO 10.2 AP

ER 11 – AM
UO 11.1 RR
UO 11.2 AC
UO 11.3 RO

ER/UO	Número de Agentes
GR01-SP	91
GR02-RJ	46
UO021-ES	9
GR03-PR	29
UO031-SC	14
GR04-MG	41
GR05-RS	28
GR06-PE	18
UO061-AL	6
UO062-PB	8
GR07-GO	17
UO071-MT	10
UO072-MS	9
UO073-TO	3
GR08-BA	23
UO081-SE	5
GR09-CE	19
UO091-RN	7
UO092-PI	5
GR10-PA	19
UO101-MA	9
UO102-AP	3
GR11-AM	11
UO111-RO	5
UO112-AC	4
UO113-RR	5
UO001-DF	15
FIGF	3
TOTAL	**462**

SIGA - Sistema Integrado de Gestão de Aparelhos

- O "Sistema Integrado de Gestão de Aparelhos – SIGA aims to **control counterfeit, cloned, tampered and other unauthorized** mobile devices.

- The project is based on Anatel Regulatory framework that dictates that **operators can only allow on the network authorized devices** and **endusers can only use authorized devices.**

- The Project is lead by Anatel with the participation of all relevant actors (**Anatel, Operators, ABR-Telecom, Manufactures, GSMA, among others**).

- The system is operated by ABR-Telecom and is **active since march 2014** collecting the relevant information from all mobile networks on Brazil.

- The system is generating the reports and alarms necessary to **map the Brazilian scenario** so that Anatel can **define the needed actions**.

SIGA Premises

- **Centralized solution:** integrated to all Brazilian mobile operators;

- **Automated solution**: allowing the input of information with low human intervention;

- **Scalable, Dynamic and Flexible:** expandable system, rules adjusted over time;

- **Multiple sources of info:** CDRs, operators systems, international databases;

- **Reliable and secure:** Minimize impacts on regular end users;

Challenges when addressing the problem.

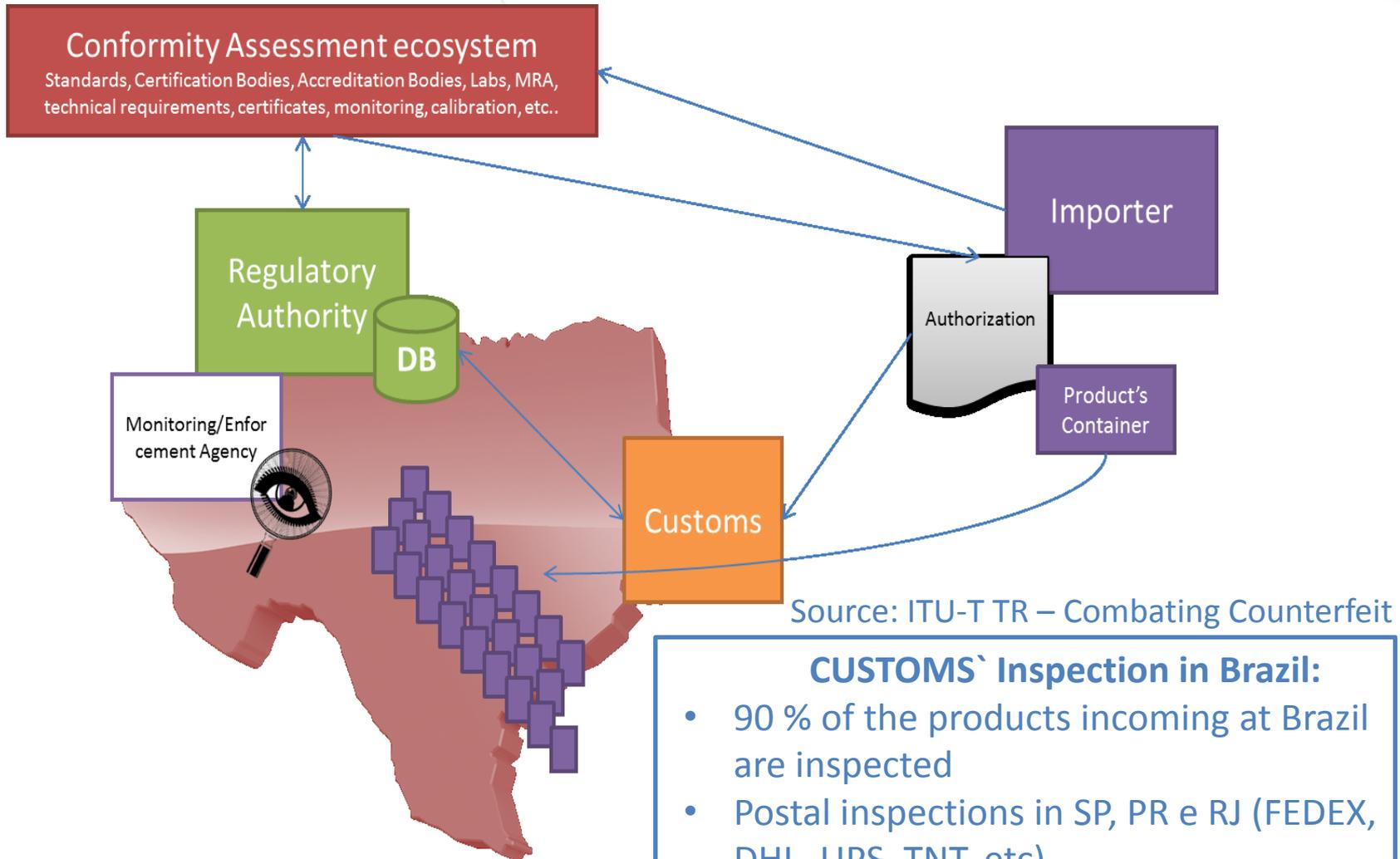# Challenges when addressing Counterfeit/Tampered/unauthorized

- **Construct a reliable reference database.**
  - Need of reliable Unique identifiers (as indicated on Res. 188).
  - Preferable use of international reference databases + national bases.

- **Identification and definition** of actions for each scenario.
  - Attack every device or focus first on voice terminals?
  - How to address the cloned/tampered problem?

- **Reduce end-user impact.**
  - Define Legacy Terminal actions (regulatory wave?)
  - Strong Educative campaign to pass information (rights and obligations) to the user.

- **Removal of terminal already on the network.**

How to control the entrance of new Counterfeit and other irregular devices?
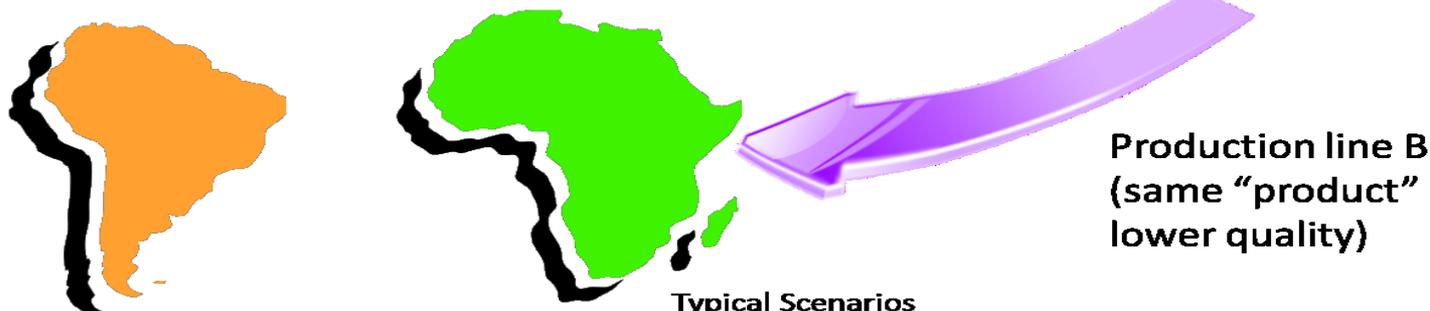
Blocking the entrance of these new irregular devices

Conformity Assessment ecosystem
Standards, Certification Bodies, Accreditation Bodies, Labs, MRA, technical requirements, certificates, monitoring, calibration, etc..

Regulatory Authority

DB

Monitoring/Enforcement Agency

Importer

Authorization

Product's Container

Customs

Source: ITU-T TR – Combating Counterfeit

CUSTOMS` Inspection in Brazil:
- 90 % of the products incoming at Brazil are inspected
- Postal inspections in SP, PR e RJ (FEDEX, DHL, UPS, TNT, etc).
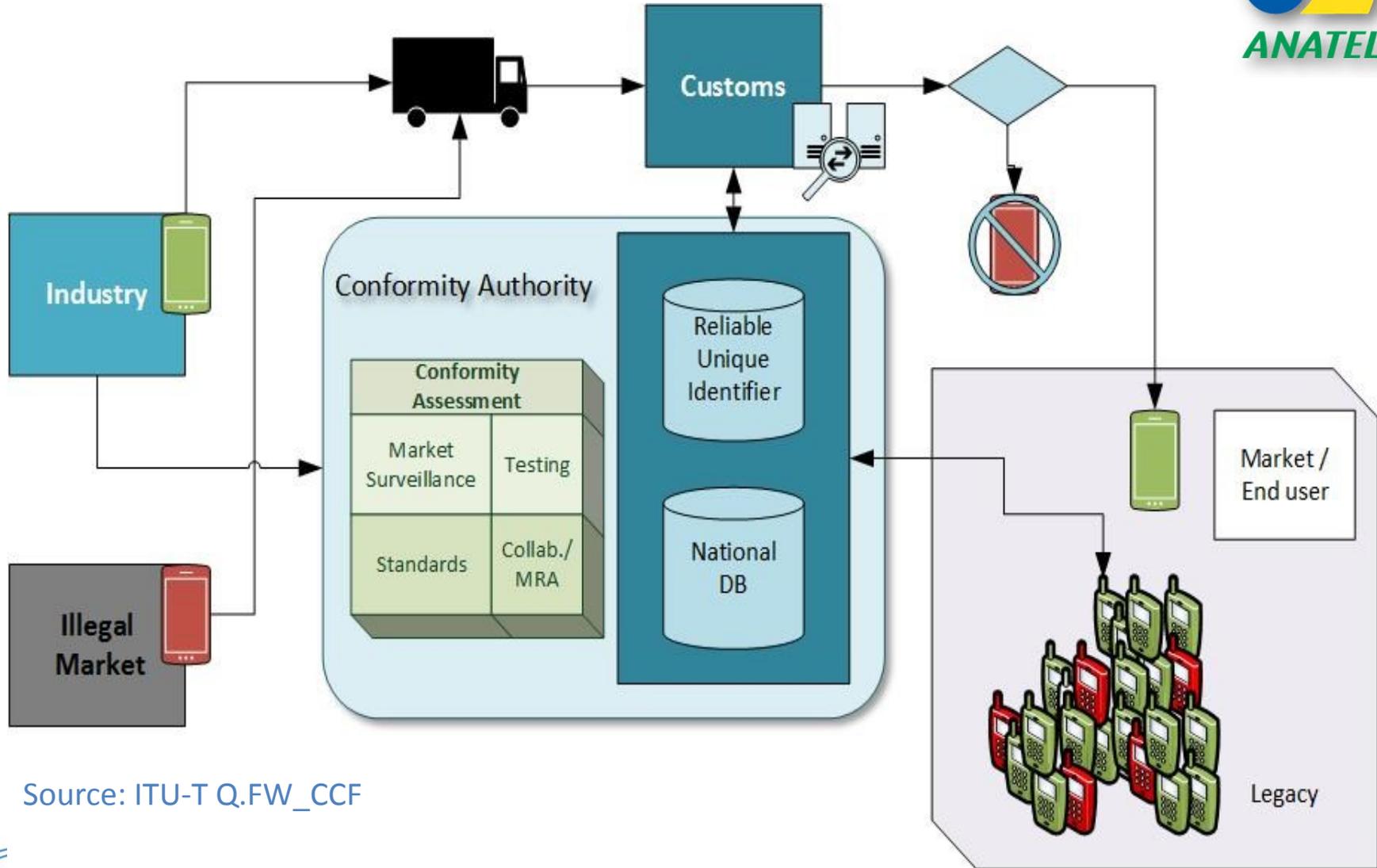- Shipping inspections – when demand.

Conformity Assessment Importance

Phenomenom of Tropicalização

Production line A

Product's origin (?)

Typical Scenarios
- **Regulations and Standards**
- **Conformity Assessment**
- **Enforcement**

Production line B
(same "product" lower quality)

Source: ITU-T TR Combating Counterfeit

Typical Scenarios
- **Lack of Regulations and Starndards**
- **Lack Conformity Assessment**
- **Enforcement uneffective**

Proposed Reference Framework

Source: ITU-T Q.FW_CCF

Multi Layer Initiatives

Multi Layer Initiatives Regarding Counterfeit

- **National:** Example **-** Brazil's SIGA and Custom Integration.
- **Regional:**
  - **CITEL CCPI:**
    - **GTPR Correspondence Group** on the Combat of Counterfeit, substandard and unauthorized mobile terminals.
    - **GTPR Rapporteurship** on Fraud Control, Regulatory Non-compliance Practices in Telecommunications and Regional Measures against the Theft of Mobile Term.
    - **Creation of a TN on Counterfeit and discussion of contributions to ITU-T Q8/11**
  - **COMTELCA:** Workshop – Combating Counterfeit (15/16 April 2015).

- **Global Wide Actions:**
  - **PP14 Resolution 188 on Counterfeit.**
  - **ITU-T TR-Counterfeit and ITU Event on combating counterfeiting ICT devices (2014).**
  - **Q.FW_CCF "Framework for solution to combat counterfeit ICT Devices".**
  - **TR-CP_BP – Technical Report - Combating Counterfeit – Best Practices.**
  - **ITU Workshop on "Combating Counterfeit Using Conformance and Interoperability Solutions"**

CITEL PCCI Initiatives

Relevant CITEL PCCI Activities

- **XXIV Meeting of PCC.I (Lima, May 2014):**
  - **Resolution 222 (XXIV-14)** - established the "Correspondence Group to Discuss Regional Measures to Combat the Spread of Counterfeit, Substandard and Unapproved Mobile Devices"

- **XXVII Meeting of PCC.I (Washington, September 2015):**
  - Proposal of the **base text for the Q.FW_CCF** based on the discussion help on CITEL Correspondence Group on Counterfeit.

- **XXVIII Meeting of PCC.I (El Salvador, June 2016):**
  - **Inter-America Contribution (IC) sent to SG11:** Result of joint seminar ITU-CITEL: Global Strategies Against Mobile Theft.
    - Proposes that SG11 address some of the points raised on the seminar (supports: Brazil, Colombia, Panama, Paraguay, Peru, USA).

Recent ITU Initiatives

Resolution 188 adopted by Plenipotentiary (Busan, 2014) "Combating counterfeit telecommunication/ICT devices"

- Recognize that **counterfeit telecommunication/ICT devices** have become a **growing problem**;

- Recognize that **ITU and relevant stakeholders have a key role to play** in fostering coordination between the parties concerned to study the impact of counterfeit devices and the mechanism for limiting them and to identify ways of dealing with them internationally and regionally;

- **Instruct the Directors of the ITU Bureaus to assist Member States** in addressing their concerns with respect to counterfeit telecommunication/ICT devices through **information sharing at regional or global level, including conformity assessment systems**; and

- **Invite ITU Member States to take all necessary measures to combat counterfeit** telecommunication/ICT devices, to cooperate and exchange expertise among themselves in this area, and to encourage participation in industry programs combating counterfeit telecommunication/ICT devices.

http://www.itu.int/en/ITU-T/C-I/Documents/WSHP_counterfeit/PP-14%20Resolution%20on%20Counterfeit%20Devices.docx

ITU-T SG11: Protocols and test specifications

Question 8/11 Activities - Guidelines for implementations of signalling and protocols, and for addressing counterfeit ICT devices

- Rapporteur: **Isaac BOATENG –** Ghana - isaac.boateng@nca.org.gh

- Associate Rapporteur: **João ZANON –** Brazil - zanon@anatel.gov.br

- **Motivation:** ITU membership as called for assistance in addressing the growing problem of counterfeit telecommunication/ICT products and devices, which is adversely affecting all stakeholders in the ICT field (vendors, governments, operators and consumers).

- **Study Items:** What activity is needed in the ITU-T Sector to prepare common guidelines by the ITU-T and ITU-D Sectors, containing different aspects related to technical matters, in particular to address Counterfeit ICT devices?

- **Task:** Develop guidelines to address the problem of counterfeiting of ICT devices;

- **ITU-T TR-Counterfeit (rev. 2015):** Approved on November 2014, published and translated in the six languages of the Union: Covers key elements regarding the legal and regulatory nuances of the subject and also provide some use cases and experiences of countries that are already engaged in the combat of Counterfeit devices. (http://www.itu.int/pub/T-TUT-CCICT-2014)

- **ITU Event on combating counterfeiting ICT devices (November 2014):** Recognized by the participants that the whole ICT industry is affected by counterfeiting, the importance of ICTs as a tool to combat counterfeiting of not only ICT devices, but also counterfeiting of products in other industries. Also the following ITU's roles in combatting counterfeit:

  - **Multi-stakeholder cooperation** — ITU could leverage its public-private membership and relations with other organizations to foster cooperation in the area of counterfeiting;

  - **Gathering and sharing of information** — ITU could facilitate the collection, analysis and exchange of information about counterfeiting and substandard practices in the ICT sector, and about how ICTs could be used in the ICT/other industries as a fighting tool;

  - **Building capacity and raising awareness** — ITU could raise awareness among stakeholders about the negative effects of counterfeit and substandard ICT devices;

  - **Use of technical solutions** — ITU could continue the discussion on the role of IGOs in using technical standards and conformance & interoperability programs to combat counterfeit and substandard ICT devices; and

  - **Development and enforcement of adequate legal, regulatory and policy measures** — ITU could assist Member States in doing this; such measures should be comprehensive, effective and custom-tailored, yet consistent with best practices at the regional and international levels.

http://www.itu.int/en/ITU-T/C-I/Pages/WSHP_counterfeit.aspx
http://www.itu.int/en/ITU-T/C-I/Documents/WSHP_counterfeit/Final%20Report/Summary-of-Discussions-18Dec2014.docx

- **Work Items**:

  - **Draft ITU-T Recommendation Q.FW_CCF "Framework for solution to combat counterfeit ICT Devices:** Reference framework with the requirements that should be considered when deploying solutions to combat counterfeit ICT devices.

  - **Draft ITU-T TR-CF_BP "Technical Report – Guidelines on Best Practice and Solutions for Combating Counterfeit ICT Devices":** Collects information regarding difficulties, challenges and barriers faced by ITU Members, and some Best Practices and Solutions for Combating counterfeit ICT Devices.

  - **Draft ITU-T TR-Sub_Una "Technical Report on Methodologies and use cases for combating the substandard and unauthorized telecommunication/ICT devices":** Provides background information related to substandard and unauthorized ICT equipment.

- **June 2016 Meeting:**

  - **Contributions to advance the text of Q.FW_CCF and TR-CF_BP.**

  - **Revision of TR-Sub_Una scope of work.**

  - **Revision of Inter-America Contribution (IC) submitted by CITEL.**

  - **Discussions regarding Q8/11 on the next study period (WTSA-16).**

What we should aim for

What we should aim for

- **Multi Level Actions and Cooperation.**

  - Bilateral, Regional and Global cooperation.

  - International best-practices and recommendations.

- **Reduce End-user impact (specially regarding good faith / unaware user)**

  - Good communication is crucial (inform users obligations and rights).

  - Weave for legacy terminal (turnover).

  - Notify before taking any disruptive actions.

- **National multiple actions to combat Counterfeit/Tampered/Unauthorized.**

  - Structured C&I Policy and Custom Integration.

  - Solutions to remove irregular devices already on the market.

- **Reliable reference databases to our solutions.**

  - Secure unique identifier - PP14 Res. 188 Counterfeit

  - Global references databases + Country Specific databases.

Thank You!
Any Questions?

João Alexandre Zanon
zanon@anatel.gov.br

60

1956 2016

CCITT / ITU-T