THE "WIRELESS REVOLUTION" AND THE SAFE TRANSPORT, STORAGE AND HANDLING OF EXPLOSIVES AND EXPLOSIVE DEVICES.

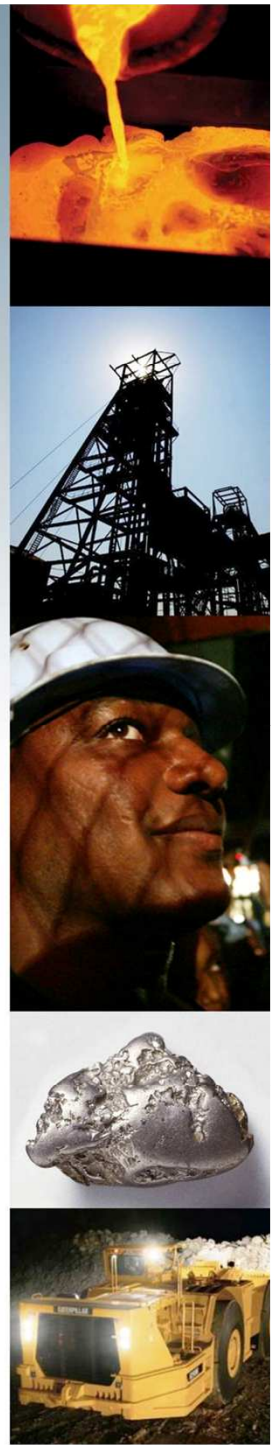
by

Stafford Smithies Ph.D.(Eng.)

Victor Solomon & Associates C.C.

Johannesburg, South Africa

"Your safety - our mission"



NEW WIRELESS TECHNOLOGIES AND THE EXPLOSIVES INDUSTRY

Are radio transmissions and explosives poor bedfellows?

This paper discusses safety of radio transmissions, including the low-power wireless devices, with:

- Explosive devices and explosives
- Electronic detonator systems
- Safety-critical electronic systems for handling, storage and delivery of explosives.

Also covered is the importance of adequate risk assessment for use of wireless systems.

THE CHANGING FACTORY ENVIRONMENT

An explosives factory early 1900's

Managing the production cycle

Automated or Computer Integrated Manufacture today

IMPORTANCE OF COMMUNICATIONS

Modern industry must deliver high quality, reliable goods, on time and at competitive prices.

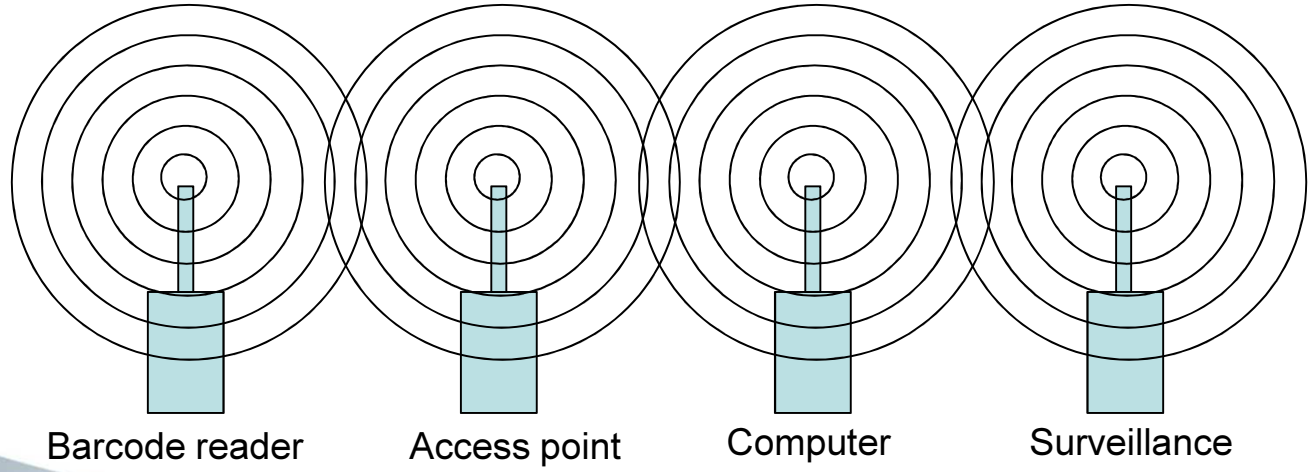
To achieve this we require:

Fast, secure, convenient and reliable communication systems.

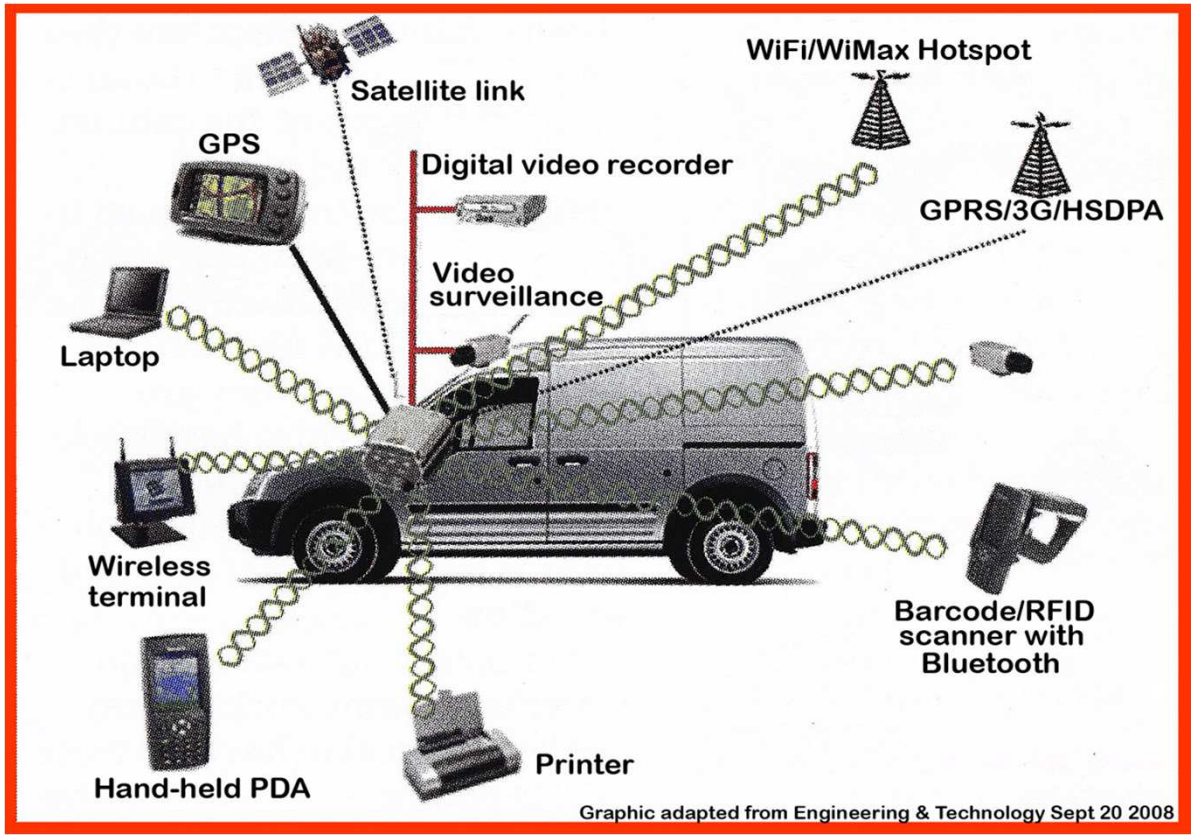
WHY A WIRELESS REVOLUTION?

Wired “peer-to-peer” business communication: telephone & telex were almost the only options just a few years ago.

Wireless systems offer convenient, secure, fast and reliable interconnection for multiple voice, data and control channels with connection to one access point.



WIRELESS SYSTEMS AND TRANSPORT



The Vehicle Area Network or LAN in VAN facilities - benefits for explosives vehicles?

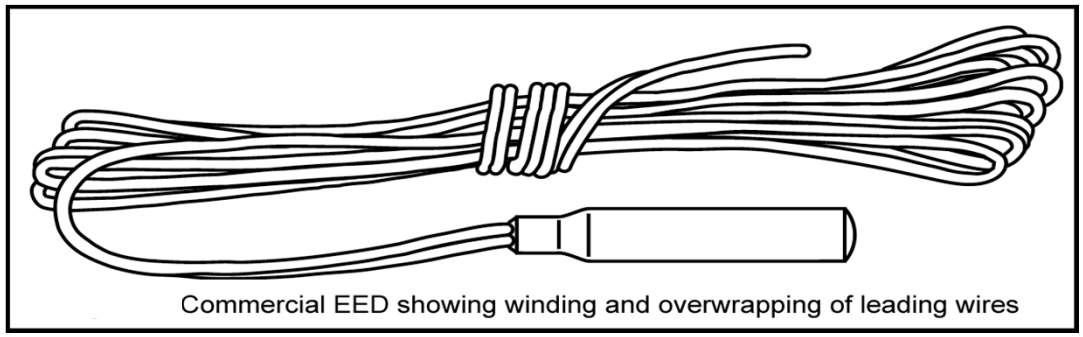
SAFETY WITH ELECTRIC INITIATORS

Sensitivities of electric initiators are listed in BSI PD CLC/TR 50426:2004

Table 1: Parameters of EED's	Type I	Type II
No-fire current in mA	180	300
Bridge wire DC resistance* in Ω	1	0,9

Type I is similar to the 40 mW device used in the USA and Type II is an 80 mW device widely used in Europe.

For packaging and transport in order to minimise RF susceptibility, leading wires are typically wrapped (and preferably shunted).



Commercial EED showing winding and overwrapping of leading wires

(From Figure 11 in BSI PD CLC/TR 50426:2004)

Caveat: Loose electric detonators with uncoiled and separated wires are an RF hazard!! Avoid radio usage!!

TRANSPORT IN THE PROXIMITY OF HIGH-POWER TRANSMISSIONS

- *Packaged Type I and Type II electric initiators:*
  - For packaged Type II electric initiators BSI PD CLC/TR 50426:2004 indicates the susceptibility is:
    - above 100 V/m (Type I will be 60 V/m) in the range 100 MHz – 1 Ghz.
    - above 300 V/m (Type I will be 180 V/m) in the range > 1 Ghz.
- *What is required:*
  - US MIL STD-461F Table VII tests up to 200 V/m for aircraft and above deck on ships and 50 V/m for ground transport over the full frequency spectrum.
  - Cenelec report CLC(SG) 819 for civil aircraft requires susceptibility >10 V/m from 100 MHz to 1 GHz and up to 200 V/m at frequencies above 1 GHz.
- *What transport mode is safe for electric initiators:*
  - Road transport should not pose any undue RF hazard.
  - Commercial aircraft – radar systems may pose a hazard with Type 1.
  - Shipping above deck – radar systems may pose a hazard with Type 1.

LOW-POWER WIRELESS SYSTEMS

- Short-range and portable devices might be very close to packaged electric initiators. (RFID systems for example).
- “Near field” coupling at < 1 wavelength distance could efficiently transfer energy to the electric initiators. (One wavelength = 300mm at 1GHz).

Poynting Antennas, Johannesburg, analysed close-proximity coupling into Type II initiators, including the folded wire condition, indicating, from the graphic:

- Safety at Tx powers below 0.7 W at 100MHz and
- Safety below 3W at 3GHz.
- At higher powers a radio exclusion distance is required.

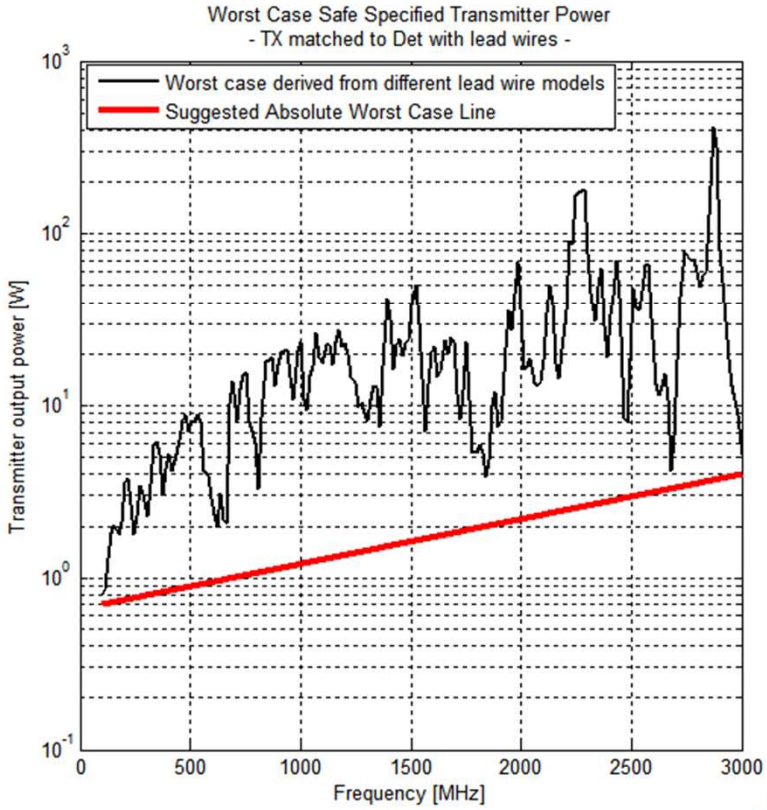


TABLE OF RADIO EXCLUSION DISTANCES FOR PACKAGED ELECTRIC INITIATORS

Table 2

Minimum recommended exclusion distance from packaged detonators				
Communication Description	ERP (W)	Freq. (Mhz)	Type I (m)	Type II (m)
Fixed communication	25	150	2	2
Mobile communication	5	150	2	2
Modem and mobile	0,5	450	0,7	0
Modems & DECT	0,5	900	0,35	0
RFID, Cellular & Tracker	2	900	0,35	0,35
Cellular & Tracker	2	1800	0,2	0,2
WiFi, Bluetoooth & Zigbee	0.1	2400	0	0

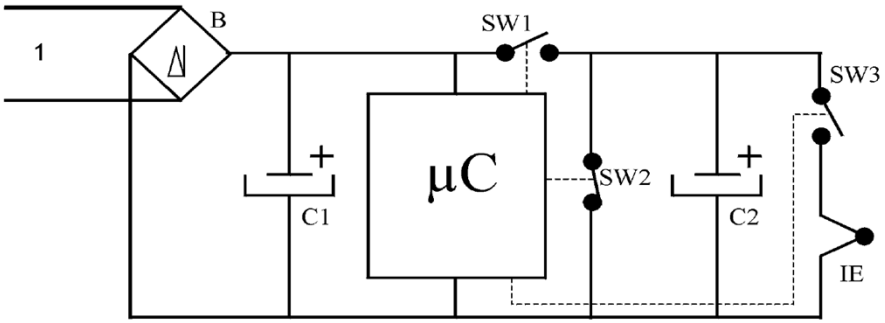
Data for Table 2 is derived from the BSI guide for distances > 1 wavelength and from the Poynting graphic for distances < 1 wavelength.

Caveats:

- **A uniform 2m exclusion is easier to adopt and manage**
- **Comply with your local regulatory requirements!**
- **Always perform a risk assessment on the operation.**

ELECTRONIC DETONATORS

- CEN/TS 13763-27 requires EMC testing for electronic detonators (EDD's) for Notified Body approval.
- There is generally no direct connection between leading wires and fusehead, making the device inherently EMI resistant.



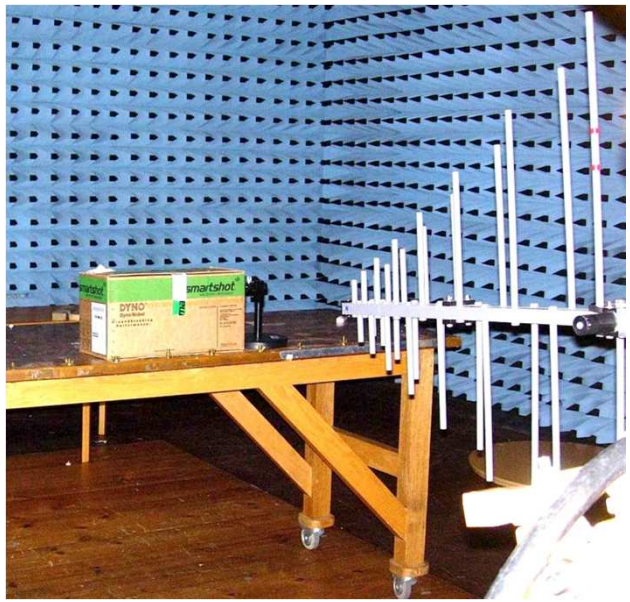
Generic two-wire EDD (from CEN/TS 13763-27, Clause 0.3)

Key:
1 - Communication line
µC - Microcontroller of application specific integrated circuit (ASIC).
B - Full wave rectifier to make the system polarity insensitive (optional)
C1 - Power supply capacitor
C2 - Firing capacitor.

Transport of EDD's

- CEN/TS 13763-27 requires a safety test at 30V/m which does not validate the product for all possible EMC transport requirements.
- Some manufacturers test the packaged product using MIL-STD-461F at 200V/m at frequencies up to 18GHz to ensure safety in transport.

Caveat: Always confirm EMC immunity of electronic detonators for transport purposes with the electronic detonator manufacturer!



Testing to MIL-STD 461F at 200 V/m
(Picture courtesy of DetNet (Pty) Ltd).

EMI AND EXPLOSIVES MATERIALS

- In an electric initiator all the RF energy is focused into tiny bridge wire or spark gap producing sufficient heat for initiation: no such mechanism exists in bulk explosives.
- In the power range to 25 W there appears to be no efficient coupling mechanism into commonly-used commercial explosives.
- There is no apparent direct coupling mechanism into shock tube detonators.
- **Caveats:**
  - **Always assume detonators are RF susceptible and keep separate from explosives!**
  - **Extremely high EM fields, such as close proximity to radar or fields in a microwave oven might cause bulk heating resulting in deflagration or detonation.**
  - **Perform a risk assessment for the planned RF system.**

SUSCEPTIBILITY OF ELECTRONIC SYSTEMS

The explosives industry is embracing automation with electronic measures for tracking and security, but what are the concerns on the safety of using wireless systems.

Electromagnetic interference (EMI) is a natural byproduct of electrical and electronic systems with deliberate and unintentional emissions that may interfere with other electronic systems.

Certification for immunity from EMI of all electrical and electronic apparatus in the supply chain is essential and typically includes:

- EM radiation through the air.
- Conducted disturbances via cables.
- Magnetic coupling.
- Electrostatic discharge.
- Power supply surges, dips and interruptions.

REGULATORY REQUIREMENTS

In Europe the Electromagnetic Compatibility (EMC) Directive and Vehicle EMC Directive govern the EMC requirements of electronic equipment for use in the EU. Electronic systems for explosives operations should comply.

- The list of over fifty European EMC test standards is comprehensive and the tests are widely used internationally.

In the USA the Federal Communications Commission (FCC) regulations, Part 15, regulate unlicensed radio-frequency transmissions, both intentional and unintentional.

- Susceptibility testing is not mandatory, but the methods and levels in MIL-STD-461F could be applied.

CAVEAT: Ensure that any electronic systems used in your explosives manufacturing and distribution chain have appropriate certifications and radiated power levels for your regulatory environment!
EMC certifications (not just the CE mark) are generally public documents.

MMU WITH REAL-TIME LOGGING

The AEL Mining Services Ltd Blast-*i*™ system sends GPS, date, time and delivery data on a blast site, feeding real-time wireless information to the mine control room, explosives logistics, blast designers and a global monitoring centre.

Due to radio restrictions on the blast site, the South African authorities required EMC certification of the system and a product risk assessment. Each mine on which the system is used would also, in terms of SA regulations, be required to perform application risk assessments.

In applications such as this the system should not:

- Interfere with any safety-critical process control equipment including, for example, mixing and pumping.
- Be a risk with electric initiators that might be in proximity of the vehicle during the operation.
- Be susceptible to interference from either intentional or unintentional emissions from the vehicle or at the mine.

THE BLAST-*i*^{TM} SYSTEM

(Above) MMU showing the WiFi antenna of Blast-*i*^{TM} system. The GPS antenna is on the other side of the vehicle cab.

(Above) Logging computer in cab.

(Right) The component box with a DC-to-DC converter, video server and wireless router.

Details of the Blast-i^{TM} system by kind permission of AEL Mining Services Ltd)

6. IMPORTANCE OF RISK ASSESSMENT

In an electromagnetic environment the need for risk assessment is essential as:

- The EMI sources, environment and susceptible devices and systems are unique to each set of operating conditions.
- Guidelines in this paper are not absolute and need to be validated for each case.
- Consequences of an EMI-induced event may vary from inconsequential to disastrous.
- Worker protection must be shown to be adequate or risks treated to meet the required level.

Generally a team of stakeholders under independent leadership with a subject matter expert present should perform a risk analysis.

Reference documents for RA work are IEC/ISO 31000 and IEC/ISO 31010.

RISK IDENTIFICATION TABLE

No.	CIM device or RF service	Likely area of use	Likely malfunction risk (explosives risk in red, business risk in yellow)
1	Automated guided vehicle (AGV)	Manufacturing, storage & shipping	Stoppage, delay
			Product damage
2	Robot	Process and packaging	Stoppage, delay
			Product damage
3	RFID and barcode	Storage, transport site delivery	Inventory control and security compromise
			RFID - possible hazard with EED's
4	Wi-Fi & other data communications	Manufacturing & storage	Inventory control and security compromise
5	Security cameras & sensors	Storage, transport & delivery	Compromise of operation recording & security

Risk Identification Table Cont'D

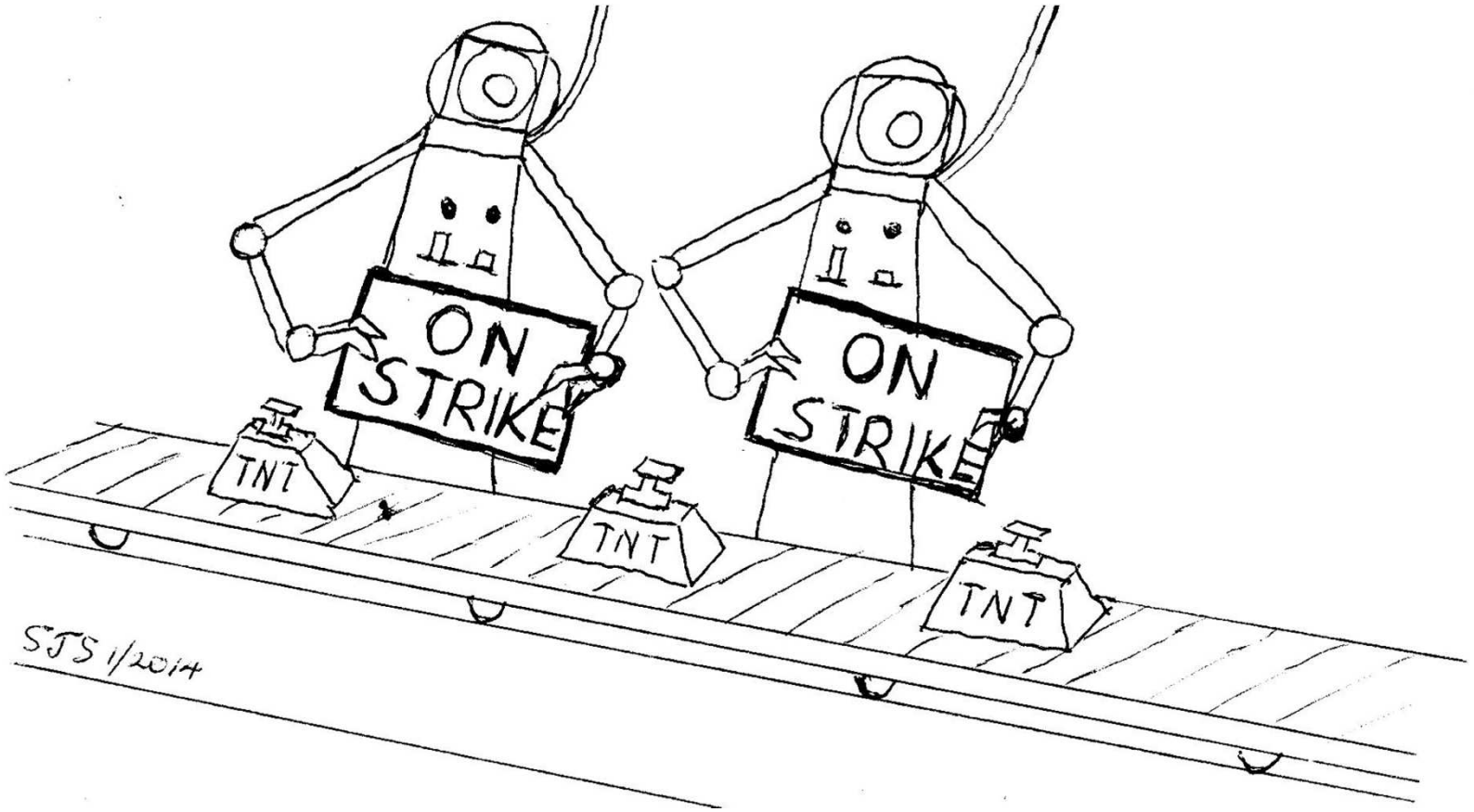
No.	CIM device or RF service	Likely area of use	Likely malfunction risk (explosives risk in red, business risk in yellow)
6	SatNav and tracking	Transport & delivery	Delays and security
			Possible EED hazard for cellular communicating
7	Radio and cellular communications	Transport & delivery	Reliability, safety and security in distribution
			Possible EED hazard
8	Ship or aircraft radar	Transport	Possible EED or EDD hazard
9	Mobile manufacturing unit (MMU)	Pumped emulsion data logging and positioning	Data to manufacturer delayed or compromised.
10	MMU	Pump and mix control	Incorrect charge or sensitization - bad blast.

The Risk Assessment will apply data from such a table to determine risk rating and actions that may be required.

TAKE HOME MESSAGES

- Low-power devices < 100 mW should pose no significant risks with packaged electric initiators. Exclusion distances may be required for higher powers.
- For electronic detonators, always consult the manufacturer/supplier for advice.
- Wireless systems up to 25 W should not pose a risk with low-sensitivity commercial explosives and shock tube product. **Obey your Regulator in this regard!**
- All electronic systems used in manufacture, storage and transport of explosives products should be adequately EMC certified.
  - Ensure all electronic equipment complies with the regulatory requirements in your area. Obtain certification documents.
  - Where systems are constructed from multiple electronic modules, the complete system should be EMC certified.
- Risk assessment when using wireless systems is of vital importance: each application is unique.

A POSSIBLE SCENE FROM THE FUTURE



On strike because of wireless interference from the non-CE certified robots in packaging!

THANK YOU

Victor Solomon & Associates c.c.

Victor Solomon & Associates c.c.