Certificate of Volatility

Manufacturer: Datalogic S.r.l

Equipment Name: GRYPHON GD4520

Model: WDI4700

Purpose: Barcode reader

Date: 10/December/2019

1. Type of memory:

Volatile memory: What is the amount? What period of time does the unit need to be powered off to completely erase this memory?

SDRAM:

The system has 64 MByte of DDR SDRAM.

Data is lost in a few seconds after power down.

Non-Volatile Memory:

Type: What type(s) of non-volatile memory are included, EPROM, EEPROM, Flash memory, NVRAM, and battery backed, etc. (fill in)

Flash Memory:

16Mbyte of parallel NOR Flash.

2. Accessibility: Is it accessible by accidental/intentional keystroke, or software malfunction?

No. Flash memory is used for storing the Firmware and for storing the device configuration. the user can change indirectly the memory content by changing configuration parameters or updating the software via dedicated tools.

3. If "YES, it **is** accessible, describe location and purpose.

Purpose: typical uses for non-volatile memory location are system identification number and system configuration, boot, and initialization parameters, for example (battery-backed NVRAM on SUNs); put in for future design needs, internal depot repair, clock circuit, "nice" to have, or to flag unauthorized software, etc.

If "NO", it is not accessible, ____**X**___ (Check here).

4. *Required memory*: Is device needed for normal operation, i.e. required for this processing period?

All memory listed is required for normal operation.

5. *Removal consequences*: If device memory chip is erased, what impact will this have on operation and normal function of device?

The device will not start-up.

6. *Method of access*: How is it accessed? Is non-volatile memory location theoretically accessible with any system code, not just via the operating system or low-level booting firmware?

The system is based on a single embedded application that can access and control all the memory.

There is no possibility to run any other unknown process because the OS doesn't support this feature.

Remember: Modifying internal programming to access is not the same thing as unknowingly accessing from an accidental keyboard stroke.

7. *Warranty*: Does chip removal or EEPROM erasure void the warranty?

Yes, memory removal will void the warranty.

8. *Size*: How much memory is contained? Number of bytes, etc.

See section 1, "Type of Memory"

9. *Spacing*: Is the memory fully utilized or does it have available memory space for additional information to be placed?

Memory are used almost at 90%. The remain part are not accessible nor by external users or tools neither by the embedded application itself.

10. Can this non-volatile memory be addressed to ensure that only authorized information is resident? If yes, how?

The embedded application executes an integrity checksum at the startup. Device cannot startup in case of corruption.