Secure Visual Timestamp

Author: Ivan Zilic
e-mail: i4e14@flyfish-tech.com

August 2012

Background

We all remember hacks from various action films where intruders disable Video surveillance systems by replacing live video streams with fake ones presenting normal state. This was typically done onsite, with physical access to system wiring. Despite the fact that these were scenes from films, they might even have happened in real world sometimes. At least, we have to think about the possibility.

Nowadays, popularity of IP security cameras is increasing rapidly and Internet got its place also on this field, with all its benefits and traps. The problem of fake video stream mentioned above has not vanished out with improved technology, but the weak chain link has been expanded instead, due to tremendously larger audience on the Internet space with plenty of resources and attempts time available to bad guys.

Anyway, the basic question remains: Can we be sure that the picture we have just got from remote location was really taken a moment ago ?

Solution

We can be sure that we got latest picture or video when it contains expected data unique to that particular moment – a kind of timestamp. If this timestamp data would equal to any publicly predictable sequence value (eg. time and date), then the bad guys would not have hard time to overlay this known data, too. Instead, our timestamp (*referenced as "ID" later in this document*) must contain information, which is changed frequently by a secret algorithm. A frequency of changing IDs in one minute interval, for example, gives us quick detection time.

The basic idea is to add a physical display in eye-sight of video surveillance camera(s). The current ID is shown on this display, which is contained as a part of video stream sent back to us. Afterwards, we extract ID from received video picture frame and verify it against expected ID.

In case the received ID is equal to expected one, we are sure that a true real time video has been received. (We could discuss the case when only a part of the picture would be replaced, but lets consider it out of scope for this document.)

One thing to pay special attention to is that the ID is not stolen on the communication path from ID generator to display. This can be prevented by implementing proper data encryption.

System Modules

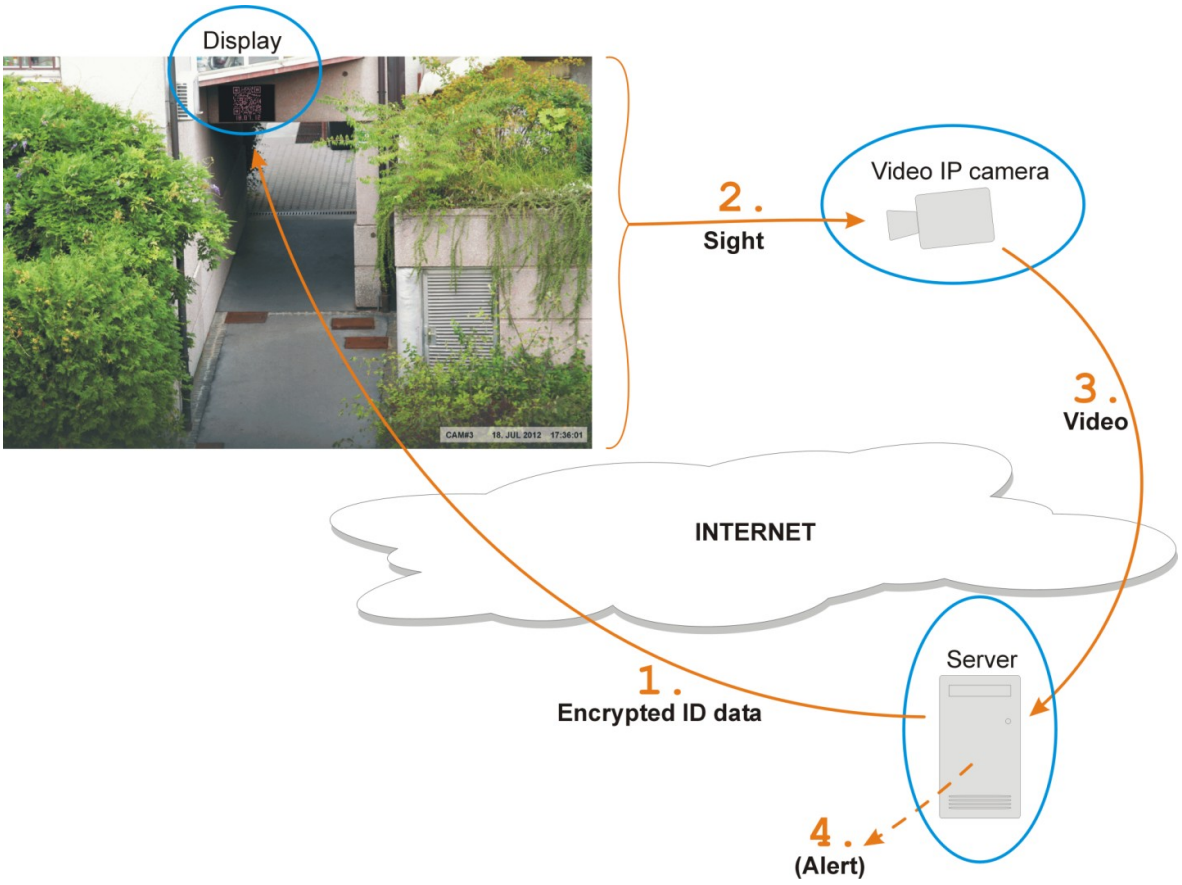
A complete system contains three main modules. First is a server in charge for providing IDs, processing received video frames and comparing IDs extracted from video against expected ones. Additionally, when applicable, it triggers the alarm.

Second module is a display and **its custom PCBs apply for this contest**. Display is in charge for downloading IDs and displaying them. Following the GUID and MD5 sum format length, a decision has been made that sufficient IDs combination set is achieved with 128 bits of data.

Various encoding algorithms exist for usage in automatic data recognition, from basic barcode to more sophisticated ones. There were two prerequisites set for this algorithm selection. The first was to natively support data redundancy with error correction, where the second was the possibility to reproduce it on LED matrix. QR code meets these two criteria perfectly. QR code containing 128 bits of ID data with highest error correction capabilities fits in a 29 by 29 pixels matrix.

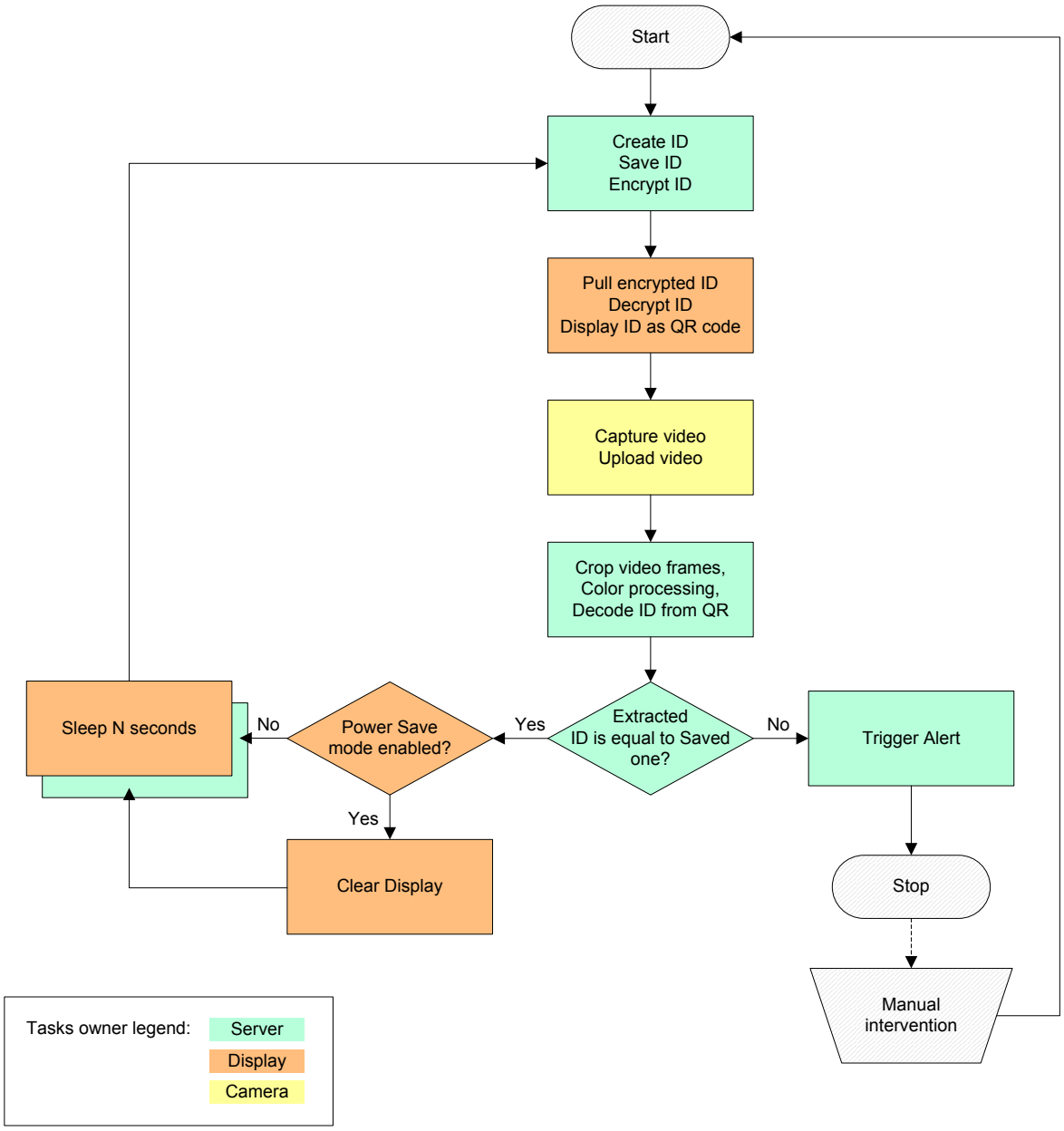
Third module is an average commercial IP video camera delivering live video stream.

System modules in configuration with a single display and video camera are presented in the sketch below:



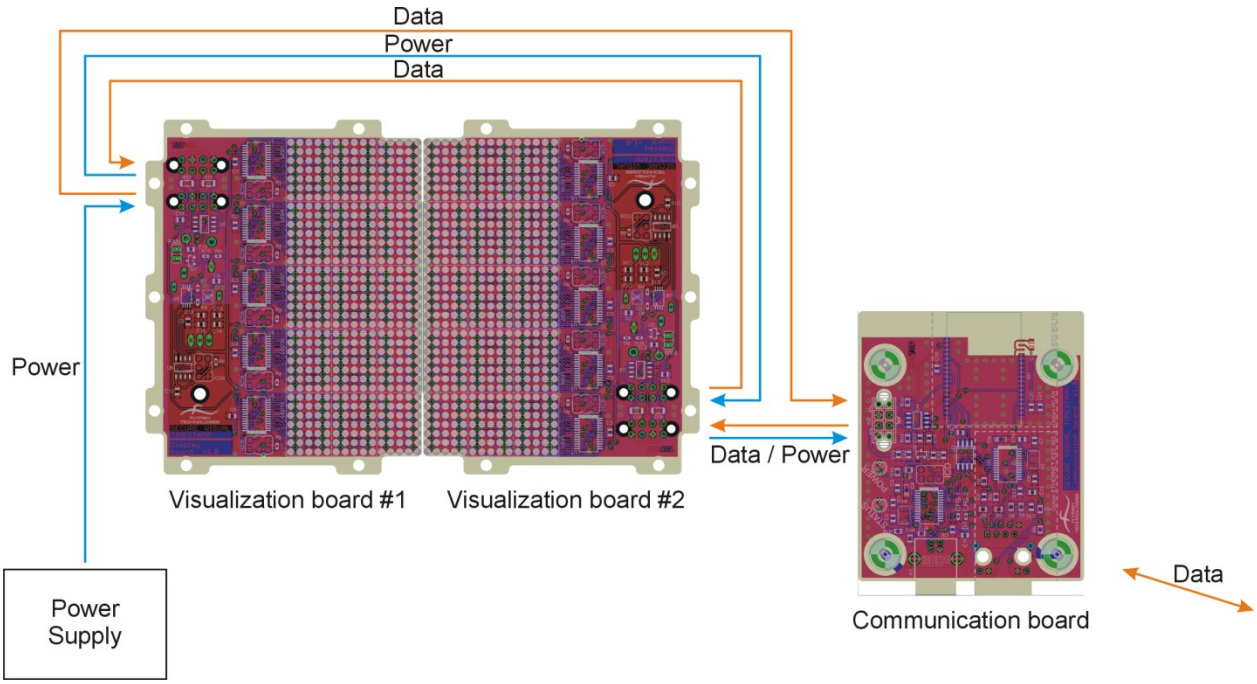
Dataflow

The dataflow chart below presents sequential data path between the system modules described above. Again, this flow includes only a single display and camera in configuration for simplicity purpose. In case of configurations with several cameras and displays, the ID is to be considered in sub-system scope, one provided for each display. Furthermore, each display is assigned to one or more companion cameras to enable proper ID compare functionality.



Display

The display contains three custom PCBs, one communication board and two data visualization boards. These two visualization boards are 100% equal in terms of hardware and also firmware.



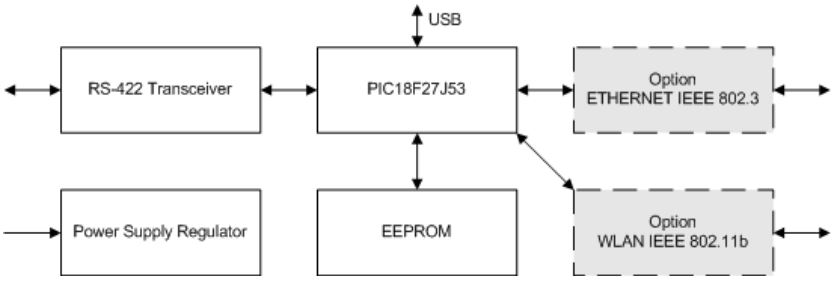
Communication board

The Communication board is in charge for downloading IDs data from the Server, decrypting it and passing the suitable pixels data further to Visualization boards.

The board general features are:

- Ethernet (IEEE 802.3) and/or WLAN (IEEE 802.11b) communication with Server, 128-bit AES encryption
- RS-422 communication with Visualization boards
- Internal EEPROM holding various status-indicating QR patterns in case of errors
- Configuration and firmware upgradeable via USB port

Block diagram of the Communication board:



Communication board Bill of Material (main parts):

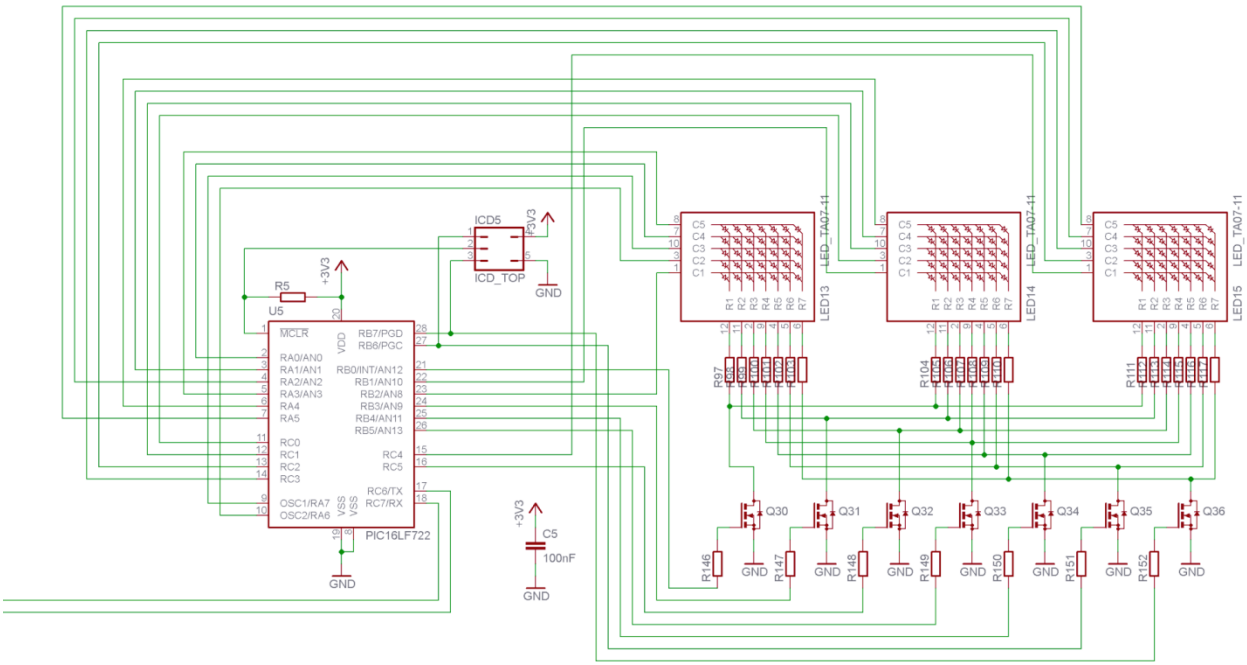
- PIC18F27J53
- ENC28J60
- MRF24WB0MA
- 25AA1024
- MAX3488
- MCP1703-3.3

Visualization board

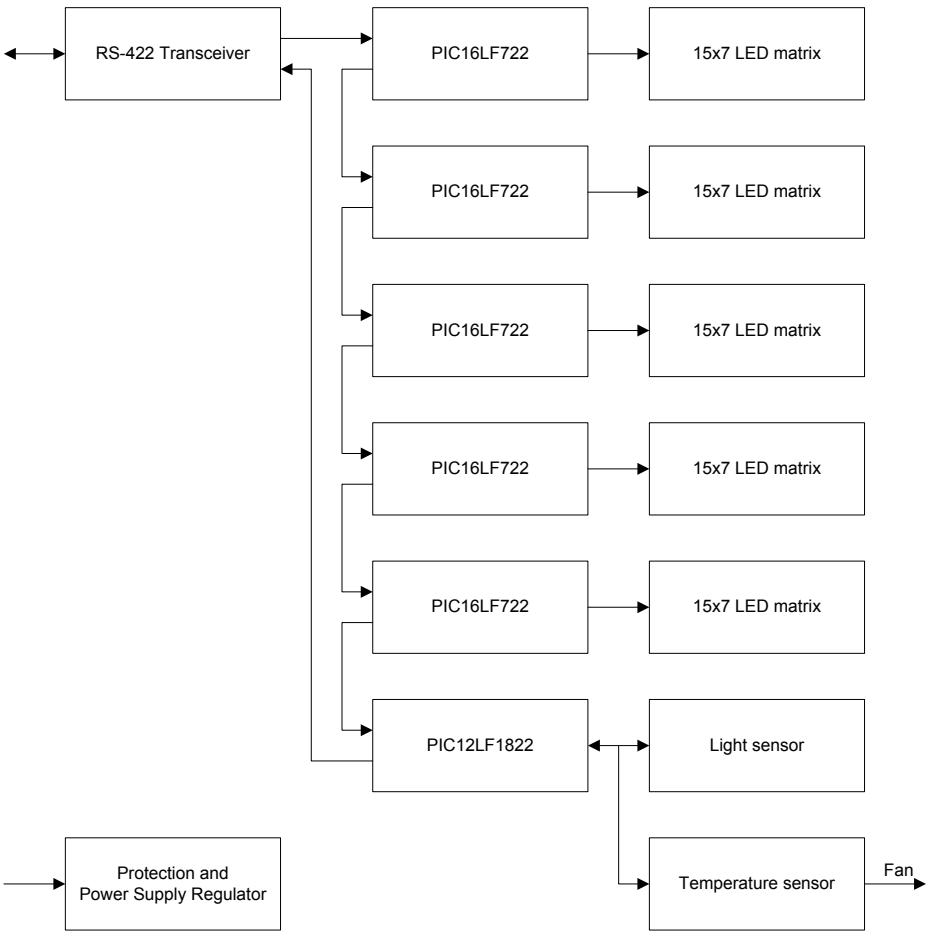
The Visualization board is in charge for displaying IDs pixel data received from the Communication board. The following features could be underlined:

- 15x35 LEDs overall matrix.
- The board contains 6 microcontrollers, five of them are equal and each is in charge for driving 15x7 LEDs matrix. The remaining microcontroller handles temperature and light sensors data.
- LEDs segments are driven from microcontrollers, without additional interface chips. The microcontrollers (industrial version) current source/sink capabilities require only reduced number of external transistors. According to chosen decent 1:7 duty cycle, one transistor for each row is sufficient.
- LEDs driving microcontrollers have plenty of processing power for the assigned roles and provide also software PWM LEDs dimming functionality within their 1:7 timeframe. PWM setting value is periodically obtained from present environment light intensity sensor.
- Communication between all 7 microcontrollers and also to remaining Communication and Visualization boards takes place in Daisy Chain topology. Address of each microcontroller in this chain is obtained during power-up initialization step, when the Communication board initiates a dedicated token packet. This topology allows 100% equal firmware for each and every LEDs driving microcontroller without need to spend any pin for any address configuration. A special attention has been paid for UART receive ISR content and priority to guarantee constant data latency along the chain, which allows precise overall consistency.
- Firmware upgradeable via RS-422 from PC through Communication board's USB port.

LEDs segment (15x7 LEDs) driving schematics details are presented below:



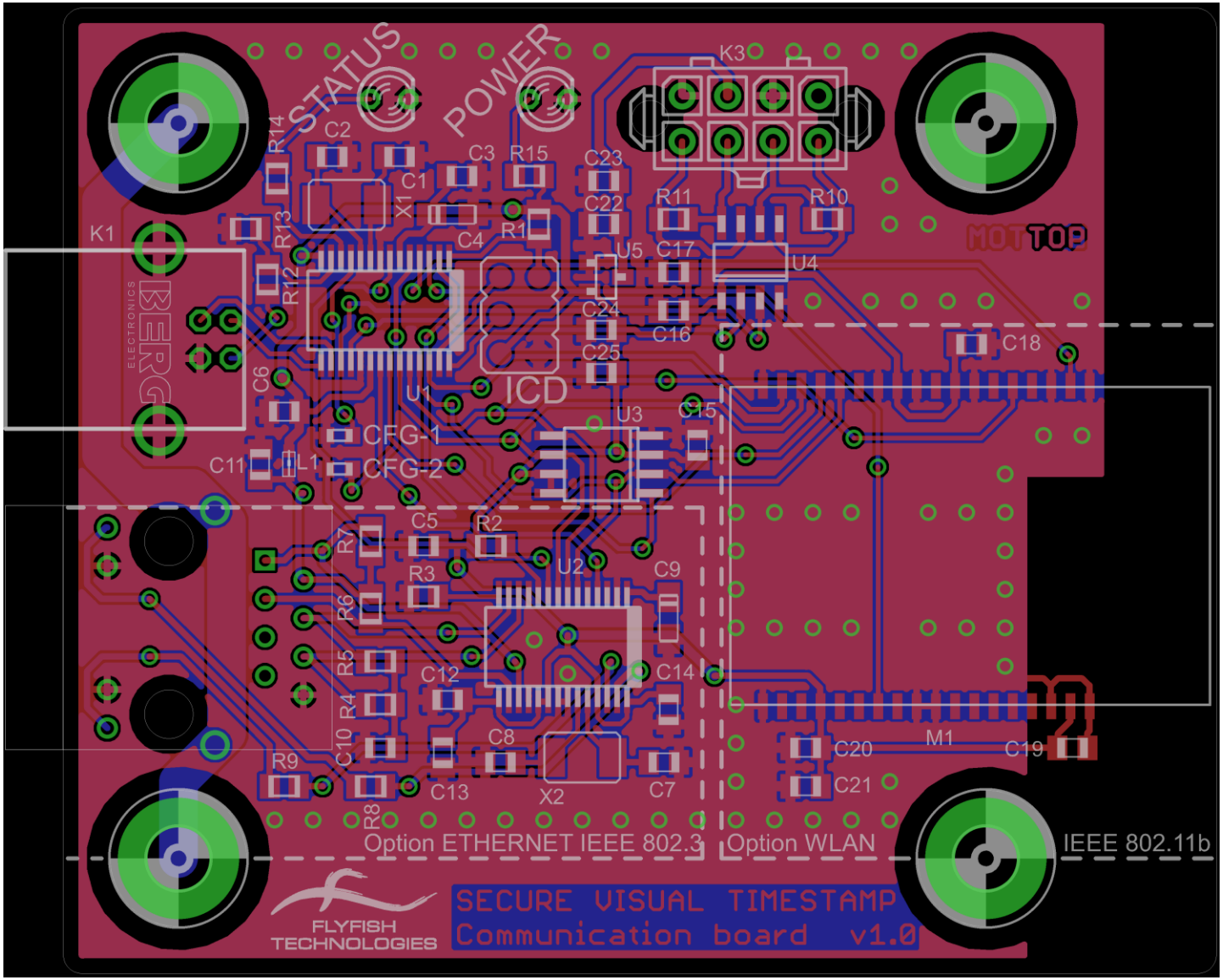
Block diagram of the Visualization board:



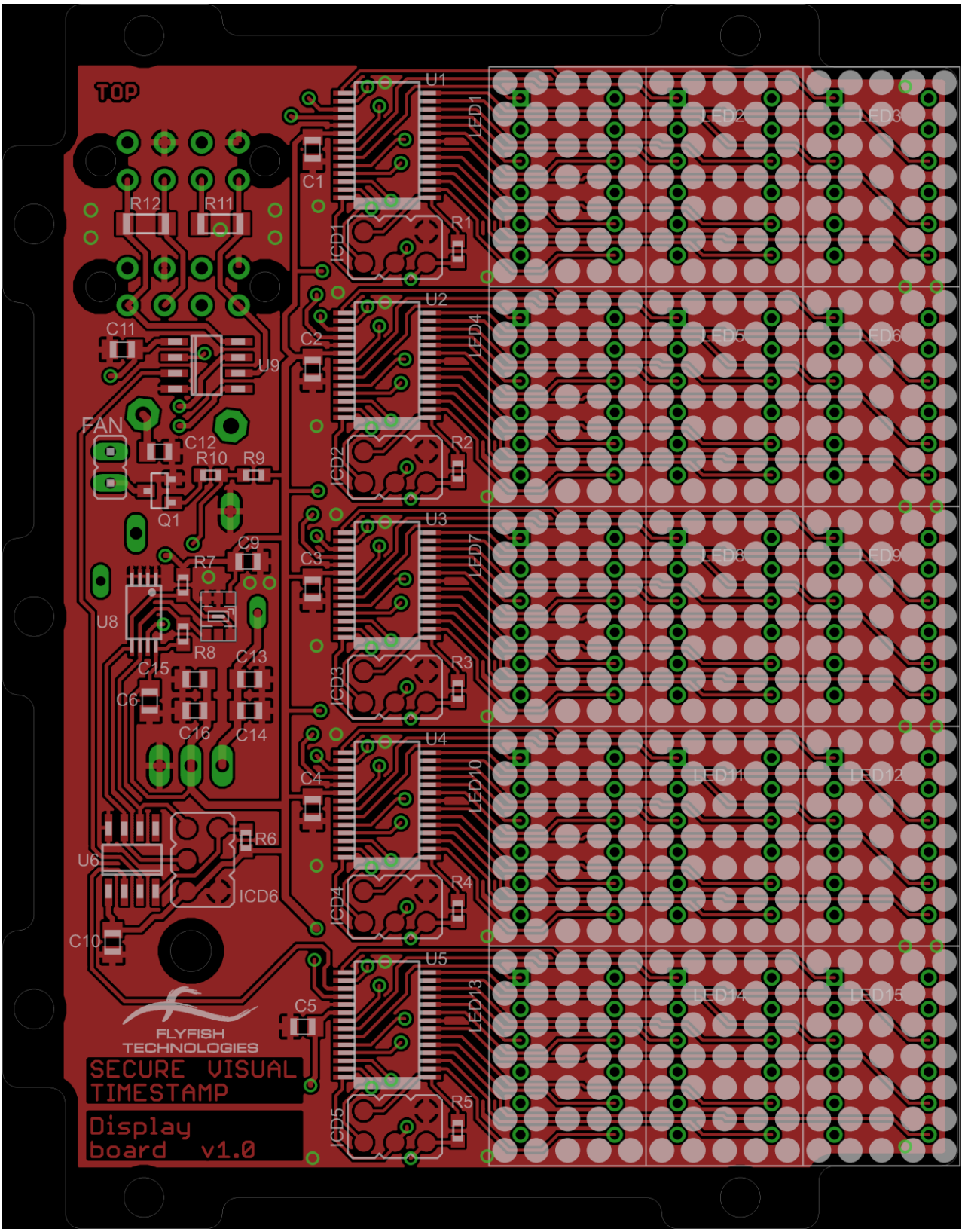
Visualization board Bill of Material (main parts):

- 5x PIC16LF722 (Industrial)
- PIC12LF1822
- MAX3488
- 15x TA07-11
- TSL2560
- MCP9805
- LM1117T-3.3

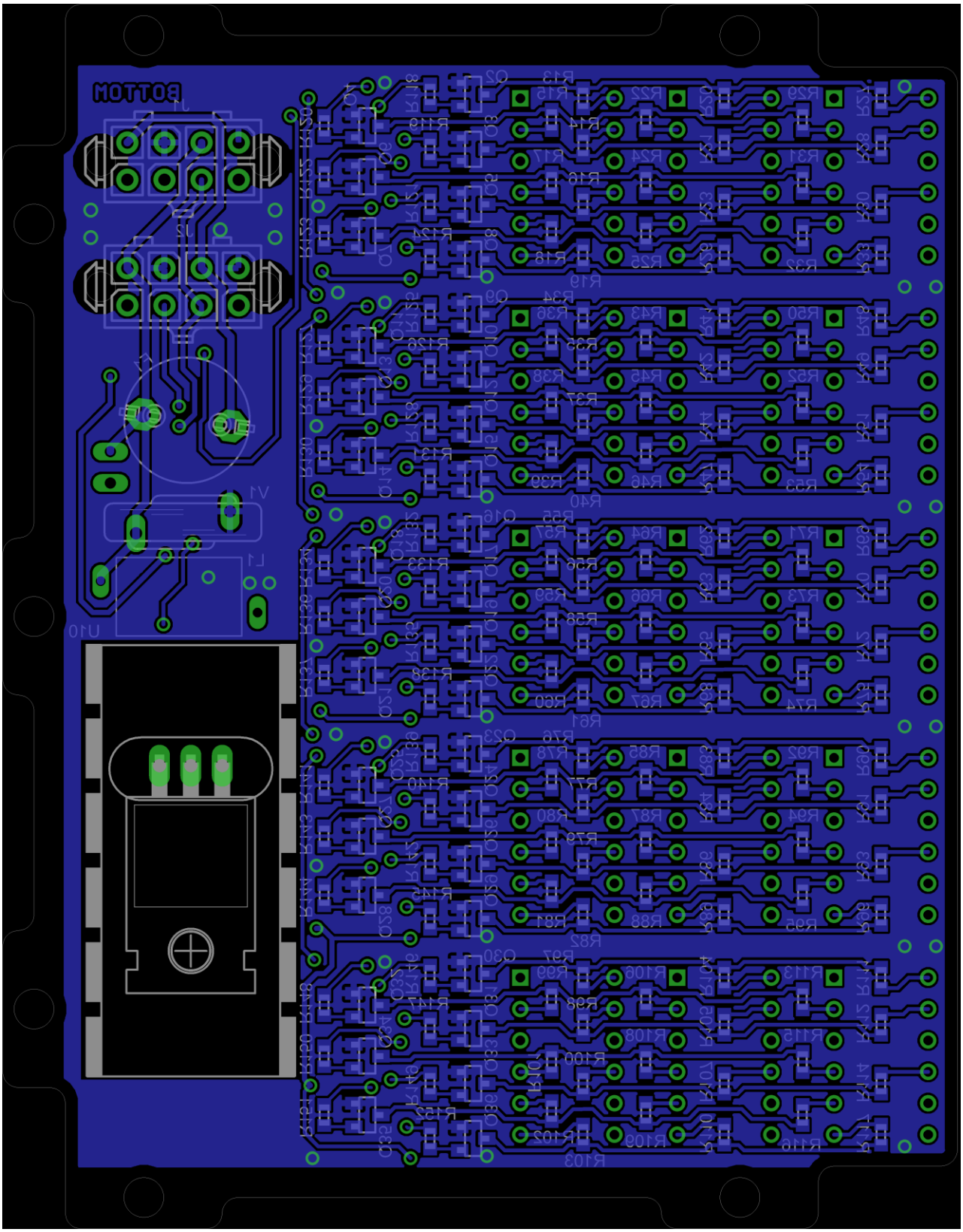
Hi-Res Communication board layout; top side and bottom signal layer (not to scale)



Hi-Res Visualization board layout; top side (not to scale)



Hi-Res Visualization board layout; bottom side (not to scale)



Appendix – Example of Test image processing

1. Complete image, before any ID extraction action

2. Crop predefined area of the image

3. Color processing including inverse effect; image becomes suitable for QR decoding algorithm