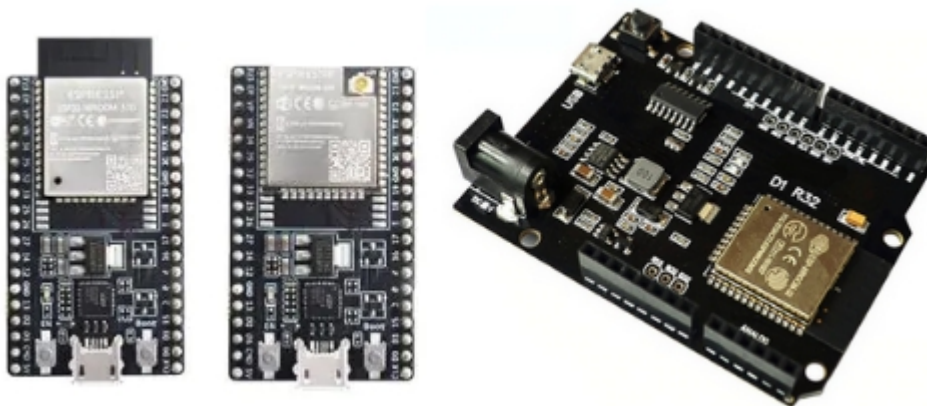


# Edukativni pristup enkriptovanom prenosu podataka u embedded i frontend razvojnim okruženjima

Ivan Gutai, Prof. dr Platon Sovilj, Marina Subotin,  
Doc. dr Marjan Urekar, Jelena Milojević, Milica Mitrović



Septembar 2021.

# Spisak korišćenih tehnologija

**ESP-NOW**, za prenos podataka preko Wi-Fi-ja

**C++**, za ulogu web servera

JavaScript + HTML5 + CSS3, za frontend

Biblioteke, uključujući i **Highcharts** (JavaScript)

- ✓ Pre IIoT-a, embedded programiranje i frontend programiranje nisu mogli da se nađu ni u istoj rečenici. Jedan od primera hardvera, koji je omogućio neprimetnu integraciju ove dve kompleksne oblasti, je Espressif-ov ESP32 MCU.
- ✓ Štampana verzija ovog rada sadrži:
  - uputstvo za konfigurisanje razvojnog okruženja za ESP32,
  - ESP-NOW primer,
  - primer kreiranja HTTPS servera,
  - smernice za prilagodljivi (eng. responsive) dizajn,
  - primer korišćenja JavaScript Highcharts biblioteke i
  - prikaz programerske prakse za upravljanje greškama (izuzecima).

# ESP32 https web server

## ESP-NOW

- ✓ ESP-NOW tehnologija je specifična za kompaniju Espressif i razvojni sistem ESP32 i omogućava bežičnu razmenu podataka.
- ✓ ESP-NOW se koristi ukoliko imamo 2 ili više ESP32 uređaja, između kojih želimo da ostvarimo komunikaciju preko Wi-Fi-ja.
- ✓ Potrebno je istaći da je struktura podataka na predajniku i na prijemniku mora biti identična.

- ✓ Primer koda:

```
uint8_t broadcastAddress[] = {0x24, 0x0A, 0xC4, 0x16, 0x71, 0x14};  
esp_now_peer_info_t peerInfo;  
memcpy(peerInfo.peer_addr, broadcastAddress, 6);  
peerInfo.channel = 14;  
peerInfo.encrypt = true;  
peerInfo.lmk[8] = 203;
```

- ✓ Ukoliko se odlučimo da koristimo enkriptovanu komunikaciju, LMK (Local Master Key) mora biti identičan i na prijemnicima i na predajnicima.
- ✓ Takođe, za Wi-Fi komunikaciju možemo izabrati kanale od 1 do 14.
- ✓ Paketi podataka od 250 bajta se šalju i primaju desetinama puta u sekundi, što ih čini pogodnim i za podatke koji se brzo menjaju.
- ✓ Podaci se dobijaju sa uređaja koji vrše akviziciju podataka, a u ovom slučaju sa BME280 senzora i relativno se sporo menjaju. Parametri koji se prate su temperatura, relativna vlažnost vazduha i atmosferski pritisak.

# Bežični prenos podataka

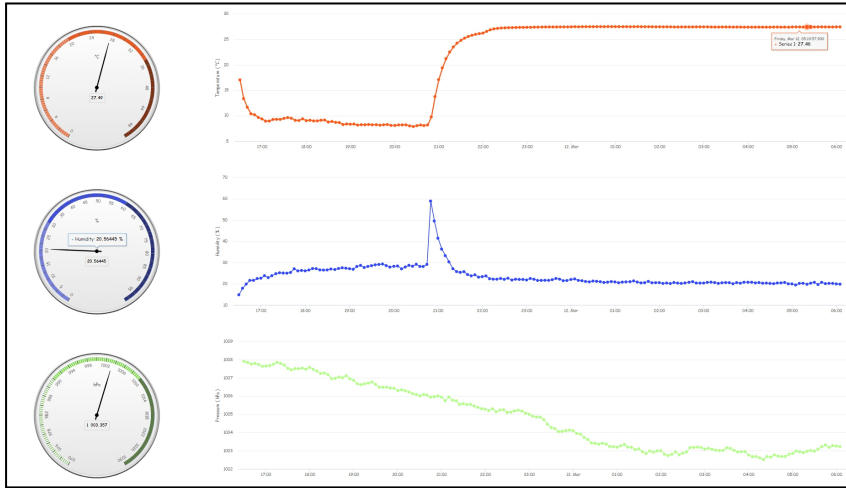
C++

- ✓ Biblioteka koja omogućava kreiranje kućnog REST (Representational State Transfer) servera je dostupna na Github-u\*.
- ✓ U Arduino IDE (Integrated Development Environment), sve dodatne biblioteke se preuzimaju na sledeći način: "Tools, Manage Libraries, search i install". Ključne reči su: "esp32 HTTPS", a zatim je potrebno instalirati **"ESP32\_HTTPS\_SERVER"** biblioteku. Iz navedene biblioteke, koristimo primer **"REST-API"**.
- ✓ Pomoću ovog primera se generiše i Self Signed sertifikat, koji je koristan prilikom razvoja i omogućava upotrebu HTTPS-a.
- ✓ Fajlove sa ekstenzijama: .html, .js, .css i ostale, je potrebno smestiti u folder: "REST-API\data\public".
- ✓ Sve može biti postavljeno na SPIFFS (Serial Peripheral Interface Flash File System), koristeći opciju iz Tools sekcije: "ESP32 Sketch Data Upload". *Kao što se fajlovi za frontend kopiraju na web server, tako se na ESP-u, fajlovi kopiraju na SPIFFS memoriju.*

\*[https://github.com/fhessel/esp32\\_https\\_server](https://github.com/fhessel/esp32_https_server)

# JavaScript + HTML5 + CSS3

## Frontend



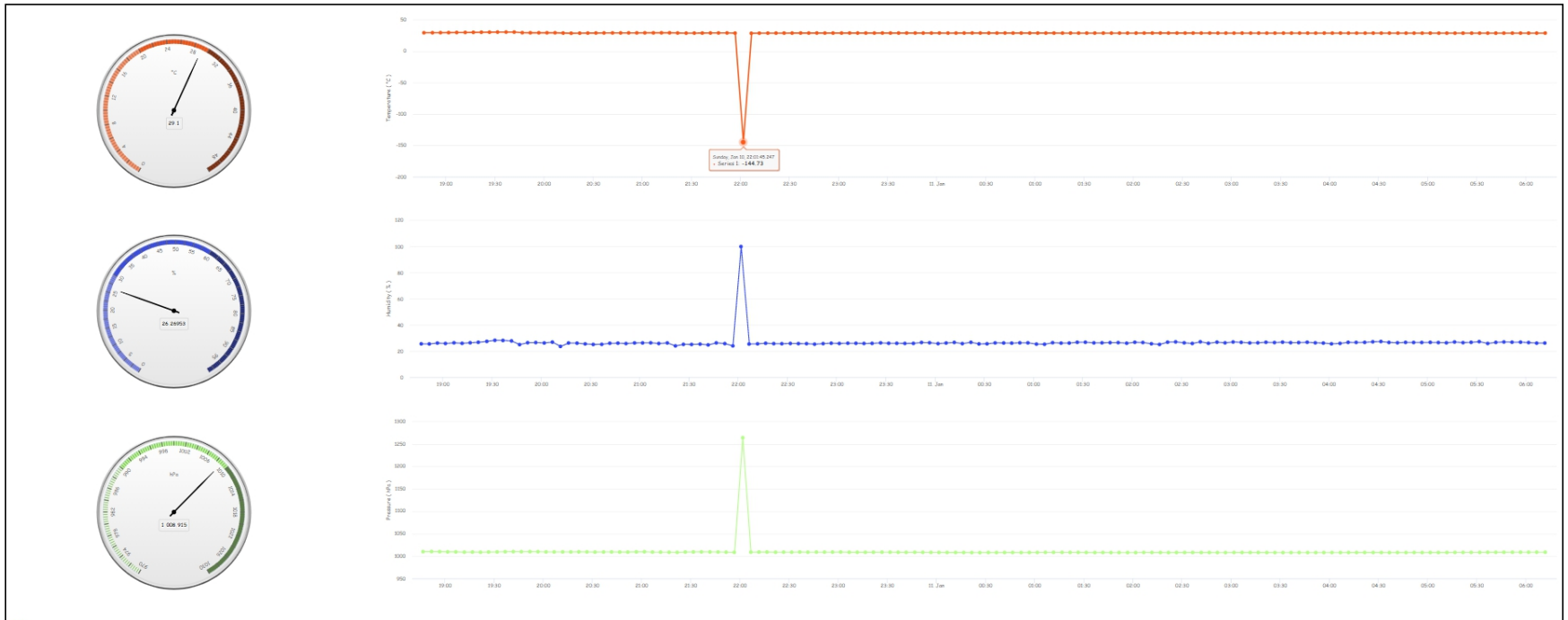
```
▼ Object 1
  ▶ BME280: {temperature: 28.11, humidity: 22.61328, pressure: 1008.238}
  ▶ MPU9250: {Accelerometer: {...}, Gyroscope: {...}, Magnetometer: {...}, Cal
  ▶ generatedNumbers: {}
    id: "MillenialDIY2020LE"
    unixTimeStamp: 1610439062
  ▶ __proto__: Object
```

- ✓ Kombinacija JavaScript, HTML5, CSS3 omogućava pravljenje dinamičkog web interfejsa. Upotrebljena je biblioteka Highcharts\*\*, koja značajno olakšava pravljenje vizuelnog dela i u zvaničnoj dokumentaciji sadrži velik broj tipova grafika, za svakog po nešto.
- ✓ Na slici je prikazan web interfejs na kom se vidi znatna promena **temperature**, a po očitavanju **relativne vlažnosti vazduha**, na srednjem delu slike se može primetiti da je uređaj premešten iz hladnije prostorije u topliju. Na donjem grafiku su prikazane vrednosti **atmosferskog pritiska** i iako deluje na prvi pogled da je promena velika, reč je o 0,1 i 0,2 mbar-a.
- ✓ U sred pisanja firmware-a i kreiranja web aplikacije, korisno je pratiti "sirove" podatke (eng. raw data). Prikazani su podaci u JSON (JavaScript Object Notation) formatu, koji se ispisuju u konzoli internet pretraživača, koji su primljeni sa hardvera.
- ✓ Vremenska oznaka 1610439062 prikazuje koliko je sekundi prošlo od 1. januara 1970. godine i predstavlja 12. januar 2021. godine u 08:11:02.

\*\* <https://www.highcharts.com/> Highcharts biblioteka je vlasnički softver, ali u edukativne svrhe se može koristiti u okviru Creative Commons (CC) Attribution-Non-Commercial licence.

Upravljanje greškama (eng. error handling) ili u preciznoj programerskoj terminologiji, upravljanje izuzecima (eng. exception handling).

## Upravljanje izuzecima



- ✓ Na slici je prikazan web interfejs u kom je zabeležen "loš" signal, koji je direktno plasiran sa hardvera. Da li ćemo koristiti termin greška ili izuzetak, proizvoljno je, a svakako ne smemo da dozvolimo da do korisnika stigne pogrešna ili nepotpuna informacija.
- ✓ Tehnički gledano, u ovom slučaju nije reč o grešci, ali je očigledno da je reč o brojevima koji su izašli van opsega. Korisnik uređaja i/ili aplikacije, to ne želi da vidi.

## Upravljanje izuzecima

- ✓ Ukoliko postoji verovatnoća da će do greške doći, to mora biti na neki način iskontrolisano, a korisniku treba da bude omogućen kontinualan ispravan rad uređaja. Treba uzeti u obzir da prilikom očitavanja vrednosti sa senzora Bosch BME280, koji omogućava merenje parametara okruženja, uključujući i atmosferski pritisak, vrednosti ne budu manje od 300 mbar ili veće od 1100 mbar. Realno, to je mnogo širi opseg od onog koji nam zapravo treba. Sve što je van navedenog opsega je rezultat nekog vida greške, npr. nepotrebnog preopterećenja sa hardverske strane, koje može da prouzrokuje povremena (eng. intermittent) očitavanja "loših" podataka sa senzora. Takođe, sve vrednosti koje su izvan tipičnog opsega za npr. atmosferski pritisak, kao što su 950 mbar ili 1050 mbar, treba da prođu obradu, pre nego što se prikažu.
- ✓ Najveći problem kod povremenih grešaka je činjenica, da ne može da se utvrdi kada će se dogoditi i kako će se one izraziti. Takav tip podataka ne sme da dođe do korisnika, pošto je pogrešan, a takođe se ne sme ni sakriti.
- ✓ Pravilno korišćenje **try...catch...finally** blokova predstavlja preduslov za kvalitetan rad sistema.
- ✓ Dobra analiza sprečava prikaz pogrešnih informacija, kao što je atmosferski pritisak u dnevnoj sobi od 1264 mbar.
- ✓ Da bi bili u potpunosti sigurni da raspolažemo sa ažurnim informacijama, preporučljivo je da se koristi vremenska oznaka (eng. timestamp), Unix tipa, ili bilo koja druga.
- ✓ Treba napomenuti da je vremenski žig vrlo bitno parče informacije i ako se pravilno koristi, omogućava da se grafici ne ažuriraju ukoliko ne postoje sveži podaci. Preduslov je pisanje odgovarajućeg algoritma.





**Hvala na pažnji**