

Live-Demo: Hardware- Angriffe in der Praxis

Erleben Sie in Echtzeit, wie die Sicherheit
von Halbleitern zusammenbricht

Fallbeispiel: Fehlerangriff

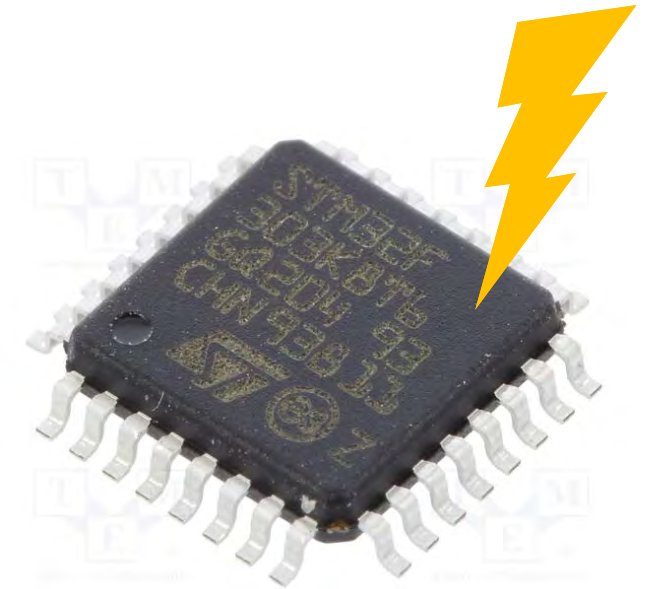
Das Ziel

Hardware:

- Kernkomponente ist ein **ST Microelectronics STM32F303**
- Gute Eigenschaften für „Mixed-Signal“ Designs (FPU, DSP, OpAmps), z.B. **Motorsteuerungen in Industrieanlagen**
- **Einzelner** ARM Cortex **M4 Kern**, max. 72 MHz

(Fiktive) Software:

- Zur Ausführung von Befehlen muss man sich mit einem **Passwort authentifizieren**



Fallbeispiel: Fehlerangriff

Das Ziel

Software Code für Authentifizierung:

- Das korrekte Passwort ist „1234“
- Das Passwort wird Zeichen für Zeichen verglichen
- Sobald ein Zeichen falsch ist, wird die Schleife verlassen
- Trigger Signale dienen zur Orientierung bei der Messung

```
void enter_password(uint8_t *user_input, uint8_t len)
{
    char passwd[32];
    char correct_passwd[] = "1234";
    uint8_t passbad = 0;

    trigger_high(); Trigger Signal

    for(uint8_t i = 0; i < sizeof(correct_passwd)-1; i++) Passwort Schleife
    {
        if(correct_passwd[i] != user_input[i]) Zeichen Vergleich
        {
            passbad = 1;
            break;
        }
    }

    trigger_low(); Trigger Signal

    if (passbad) {
        char output_bad[50];
        snprintf(output_bad, sizeof(output_bad), "Incorrect password\n");
        my_puts("Incorrect password\n");
    } else {
        show_secret();
    }
}
```

Fallbeispiel: Fehlerangriff

Das Ziel

Software Code für Authentifizierung:

- Das korrekte Passwort ist „1234“
- Das Passwort wird Zeichen für Zeichen verglichen
- Sobald ein Zeichen falsch ist, wird die Schleife verlassen
- Trigger Signale dienen zur Orientierung bei der Messung

```
void enter_password(uint8_t *user_input, uint8_t len)
{
    char passwd[32];
    char correct_passwd[] = "1234";
    uint8_t passbad = 0;

    trigger_high();

    for(uint8_t i = 0; i < len; i++)
    {
        if(correct_passwd[i] != user_input[i])
        {
            passbad = 1;
            break;
        }
    }

    trigger_low();

    if (passbad) {
        char output[32];
        snprintf(output, sizeof(output), "Incorrect password\n");
        my_puts(output);
    } else {
        show_secret();
    }
}
```

Trigger Signale

Passwort Schleife

!!! Achtung !!!

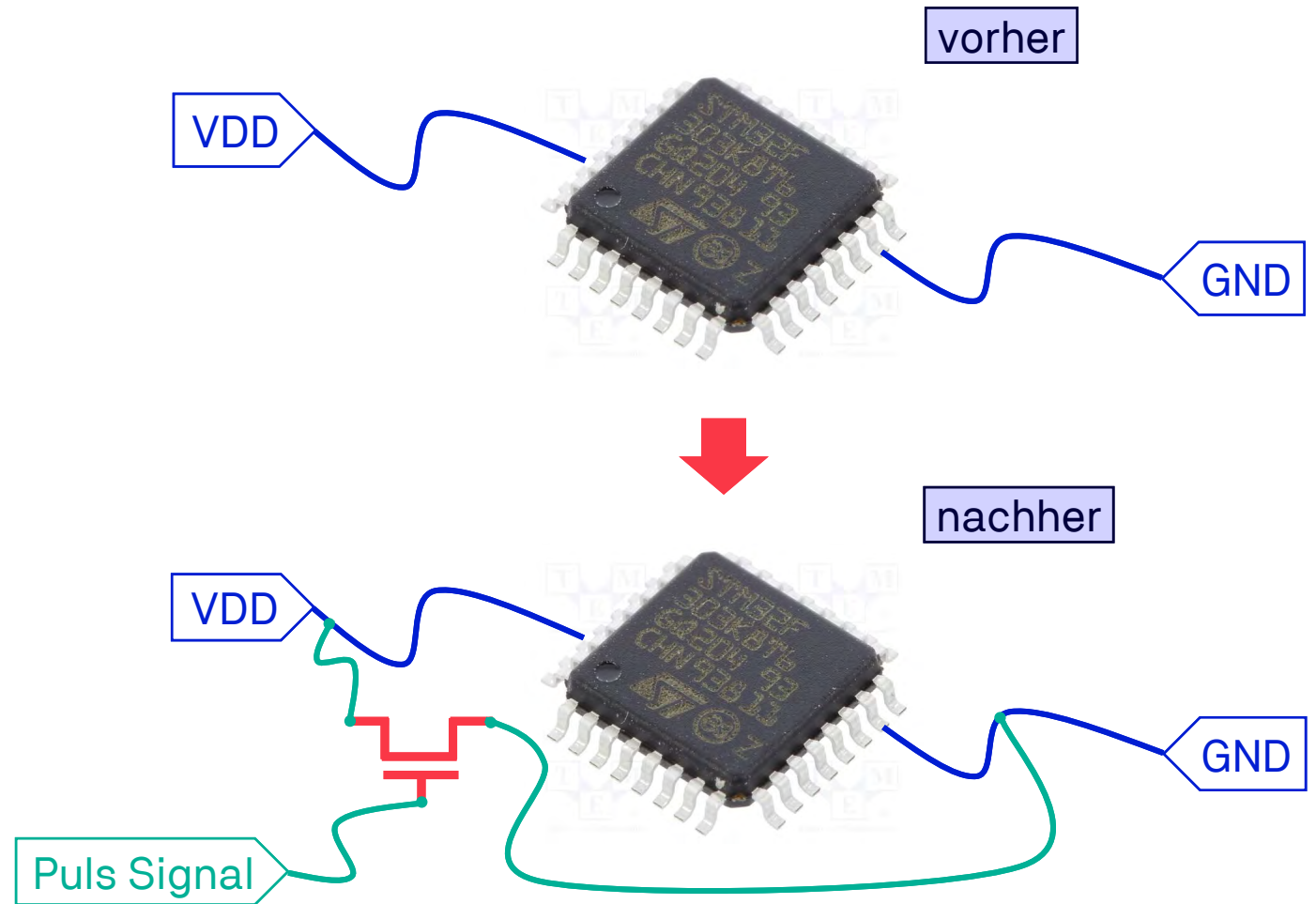
Sehr, sehr schlechter Code

Fallbeispiel: Fehlerangriff

Die Vorbereitung

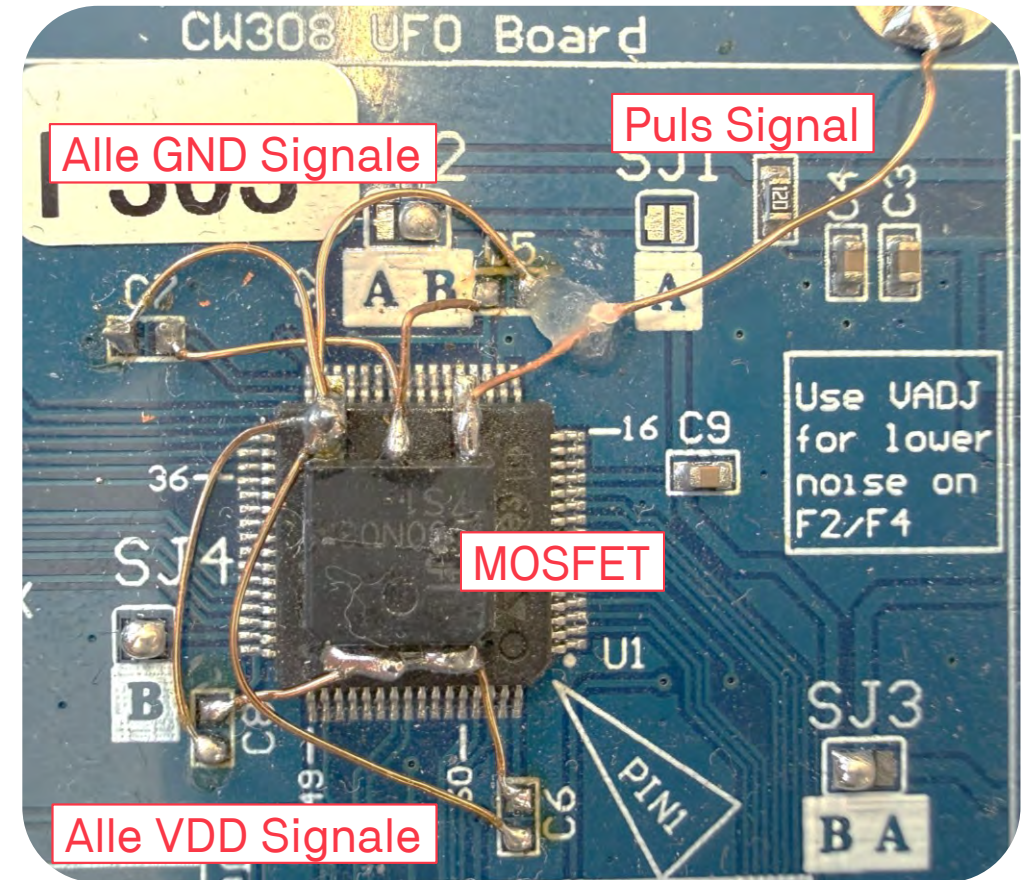
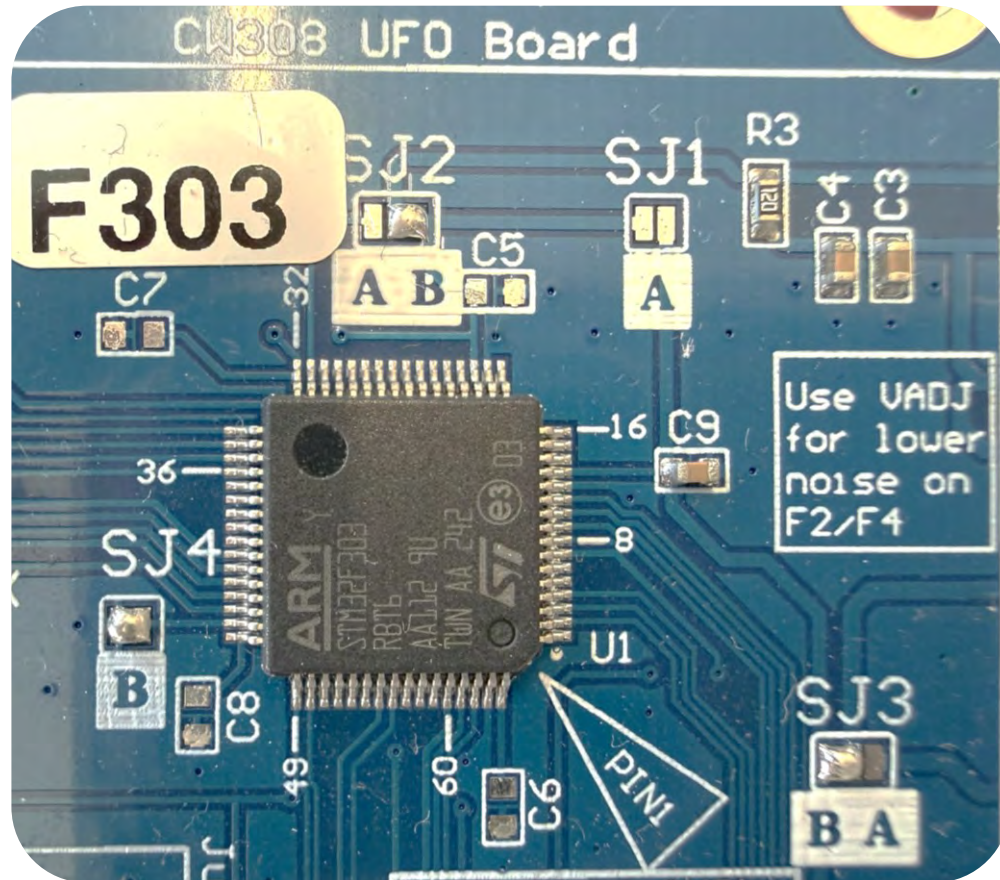
Hardware Modifikation:

- Einfachster Fehlerangriff gelingt mittels **Spannungs-Glitch**
 - Angreifer muss dazu die **Spannung kontrollieren können**
 - **MOSFET** (Schalter) an die VDD-Leitung
 - Spannung kann **sehr schnell kurzgeschlossen** werden
- für kurzen Moment keinen Strom



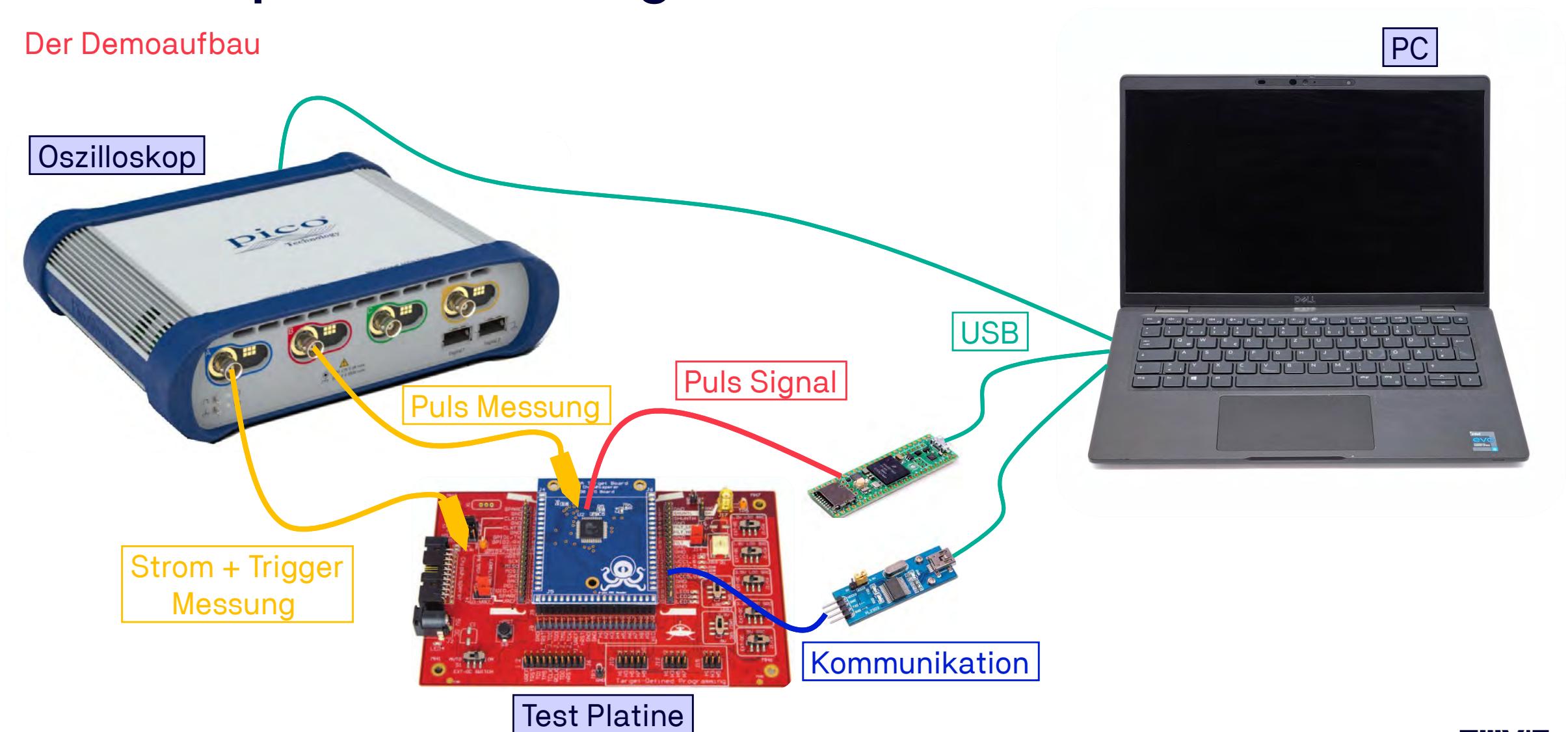
Fallbeispiel: Fehlerangriff

Die Vorbereitung



Fallbeispiel: Fehlerangriff

Der Demoaufbau



Live-Demo