

基于软件无线电的通信信号模拟与监测系统

高 飞, 李文臣, 覃 浩, 武新浩

西京学院计算机学院, 陕西 西安

收稿日期: 2025年4月25日; 录用日期: 2025年5月23日; 发布日期: 2025年5月30日

摘 要

随着无线通信技术的飞速发展, 通信环境日趋复杂, 信号种类繁多、传输方式灵活多变, 给通信系统的测试、验证与监测带来了巨大挑战。传统的信号发生与监测设备通常专用性强、灵活性差、成本高、难以适应多种通信标准与频段的快速变化。针对这一问题, 本文设计实现了一种基于软件无线电的通信信号模拟与监测系统。该系统采用C++作为开发语言, 通过编写代码设计一个自主、可控的通信信号模拟与监测平台, 并利用双缓冲区技术, 有效提高频谱和波形界面的渲染效率, 为现代无线通信系统的开发与维护提供了强有力的支持。

关键词

HackRF One, 信号处理算法, 通信信号模拟, 通信信号监测, 用户界面设计

Communication Signal Simulation and Monitoring System Based on Software Radio

Fei Gao, Wenchen Li, Hao Qin, Xinhao Wu

School of Computer, Xijing University, Xi'an Shaanxi

Received: Apr. 25th, 2025; accepted: May 23rd, 2025; published: May 30th, 2025

Abstract

With the rapid development of wireless communication technology, communication environments have become increasingly complex, with a wide variety of signal types and highly flexible transmission methods. This poses significant challenges for the testing, verification, and monitoring of communication systems. Traditional signal generation and monitoring equipment tends to be highly specialized, inflexible, costly, and poorly suited to the rapid evolution of various communication standards and frequency bands. To address this issue, this paper designs and implements a communication signal simulation and monitoring system based on software-defined radio (SDR). The system is developed in C++, creating an independent and controllable platform for communication signal simulation and

monitoring. By employing a double-buffering technique, it effectively improves the rendering efficiency of the spectrum and waveform interfaces, providing strong support for the development and maintenance of modern wireless communication systems.

Keywords

HackRF One, Signal Processing Algorithm, Communication Signal Simulation, Communication Signal Monitoring, User Interface Design

Copyright © 2025 by author(s) and Hans Publishers Inc.

This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

<http://creativecommons.org/licenses/by/4.0/>



Open Access

1. 引言

在当前这个高消耗、快节奏的时代,无线通信技术的多样化对无线通信设备通用性的要求越来越高,无线通信业务的发展面临着诸多难题与挑战。软件无线电技术(Software Defined Radio, SDR) [1]提升了无线设备的通用性,可以通过软件实现多种调制方式和频率的模拟,而无需频繁更换硬件。这种特性使得SDR能够将传统无线电设备中的大多数硬件电路转换为软件来实现,从而大大降低了开发成本和维护复杂度,并且显著提高了系统的灵活性和可扩展性[2]。但是,随着无线电技术的不断发展,频段覆盖的范围不断扩大[3]。这一趋势增加了信号处理的复杂度,要求SDR解决方案必须能够动态调整并适应各种不同的频段环境。频段的多样性不仅需要系统支持多种调制解调方式,还必须在不同的频段切换时保持稳定的性能表现。其次,目前,大多数软件无线电设备都依赖于GNU Radio [4],它是一个高度模块化、面向“流程图”的框架平台。然而,要开发出一个完全属于自己的软件无线电系统,以更好地满足特定项目的需求,这就需要进行大量的定制化开发工作。

因此,开发“基于软件无线电的通信信号模拟与监测系统”将是一个宏大的工程项目[5],需要多学科、多领域的密切合作。通过软件无线电技术,可以构建一个灵活而高效的通信系统[6],助力各类无线通信业务的快速发展。

2. 系统设计方案

2.1. 方案选择论证

2.1.1. 硬件的选择



Figure 1. HackRF One device

图 1. HackRF One 设备图

在硬件上选择了 HackRF One 作为主要的无线电设备。HackRF One 是一款开源硬件设备[7]，具有较高的性价比，支持从 1 MHz 到 6 GHz 的中频覆盖范围，设备图如图 1 所示。这使得它能够满足在不同频段范围内进行信号模拟与监测的需求。与此同时，HackRF One 的开源特性给予了更多的开发自由度，可以灵活地集成到定制的软件系统中。

2.1.2. 软件平台的选择

基于软件无线电的通信信号模拟与监测系统的作用是通过控制 HackRF One 设备，对各种信号进行模拟，并监测各个频率范围内的信号波动，进行频谱和波形的显示。鉴于现有的解决方案中，GNU Radio 是一个常用且成熟的选择。它提供的模块化设计能够让开发者更为便捷地进行信号处理模块的拼接与功能扩展[7]。然而，GNU Radio 虽然功能强大，但其通用性设计也带来一定的冗余和优化难点。因此，针对特定项目需求，对框架进行定制化开发显得尤为重要。所以选用了 Qt 作为开发平台来代替 GNU Radio 进行编程。Qt 的良好封装机制使得 Qt 的模块化程度非常高，可重用性较好，对于用户开发来说是非常方便的，开发的界面友好。使用高性能计算机作为主控平台，运行 QT 应用程序并通过 USB 接口与 HackRF One 通信。系统使用 Qt 5.14.2 版本，代码编辑使用 Qt Creator 4.11.1 版本。

2.2. 系统架构设计

系统架构设计主要包括信号采集模块、信号监测模块、信号模拟模块、图形用户界面(GUI)模块和网络通信模块。信号采集模块通过 HackRF One 设备进行信号采集，将采集到的信号转换为数字信号并传输至信号处理模块。信号处理模块是系统的核心，负责对采集到的信号进行各种处理操作，包括调制/解调、滤波、信号增强和频谱分析。通过信号模拟模块主要负责生成各类仿真信号，如扫频噪声、射频噪声、调频噪声等，用户可以根据实验需求自定义设置各类噪声参数和干扰信号，以进行全面的信号模拟测试。

图形用户界面模块使用 Qt 框架开发，提供了一个友好、直观的交互平台[8]。用户可以通过 GUI 浏览实时频谱、信号波形，并进行各类参数配置和系统操作。网络通信模块保证了系统的便捷性和灵活性，支持通过 UDP 协议发送指令进行远程控制，实现分布式操作和管理。

2.3. 关键技术设计

2.3.1. 双缓冲区技术

双缓冲区技术[9]是为了提高频谱和波形界面的渲染效率和质量，采取了乒乓模式，乒乓操作可以看成另一种形式的流水线技术。通过分离后台绘制操作和前台显示操作，有效地减少了图形闪烁和绘制错误问题。因为大家普遍认为无线电信号和解调出的音频信号应该是连续的，实际确实也是连续的，但是电脑在处理时，无法处理一个无限长度的数据，只能对于一定长度的数据分段处理，所以有了 length 这个参数，并且做了一个循环，在没达到 length 前，不停地对 IQ 数据做解调操作并不停地把解调出的数据送入。

图 2 展示了双缓冲区技术的工作原理：

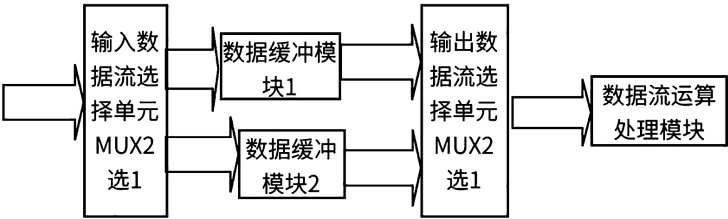


Figure 2. Working principle of double buffering technology
图 2. 双缓冲区技术工作原理图

2.3.2. 信号调制与解调

信号调制与解调算法[10]的实现是信号处理模块的核心。本文实现了多种调制/解调算法,包括振幅键控调制(ASK)、幅度调制(AM)、频率调制(FM)、相位调制(PM)等。通过调制这些信号来达到通信信号模拟/干扰的效果。例如振幅键控信号 ASK 的调制过程如下:

ASK 数字调制是将数字数据采用载波幅度调制,包括 2ASK、4ASK、MASK,信号表达式为:

$$s(t) = \sum_{m=-\infty}^{\infty} a_m g_T(t) \exp[j(2\pi f_c t + \phi_0)]$$

式中: $g_T(t) = \text{rect}\left(\frac{t-mT}{T}\right)$ 为宽度为 T 的脉冲门函数, T 为码元宽度, ϕ_0 为相位常数, f_c 为载波频率;

a_m 为输入码元。2ASK 中 $a_m = 0, 1$, 即二进制 0 对应载波振幅为 0, 二进制 1 对应载波振幅为 1。MASK 中 $a_m = 0, 1, \dots, M-1$ 。

信号幅度 0, 1, 2, 3, 得到 4ASK 信号和频谱如图 3 所示, 其中(a) 为信号波形; (b) 为信号频谱。

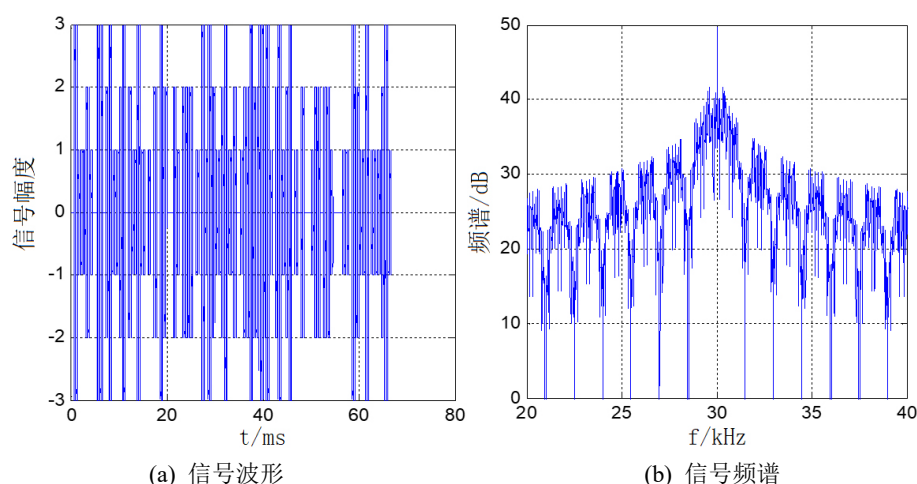


Figure 3. 4ASK signal and spectrum
图 3. 4ASK 信号和频谱

3. 系统的实现

本章将详细描述基于软件无线电的通信信号模拟与监测系统的软件设计与实现过程。软件设计包括系统的总体架构、接口设计以及关键算法的实现。流程设计则包括系统的工作流程、数据流和用户交互流程。

3.1. 系统架构设计

系统架构设计是软件开发的基础,决定了系统的整体结构和各模块的协同工作方式。该系统主要包括以下几个模块:

信号采集模块: 负责接收无线电波信号, 并通过 HackRF One 设备采集信号。

信号处理模块: 对采集到的信号进行解调、滤波和分析。

信号模拟模块: 生成各种类型的通信信号用于测试。

图形用户界面(GUI)模块: 提供用户与系统交互的界面, 允许用户设置参数并监控信号。

网络通信模块: 通过网络实现远程控制和数据传输。

3.2. HackRF One 接口设计

3.2.1. AD/DA 参数格

表 1、表 2 分别是 DA/AD 波形结构定义。

Table 1. DA waveform information format (Structure HackOutStruct)

表 1. DA 波形信息格式(结构 HackOutStruct)

No.	名称	名称	类型	备注
1	中心频率	centerFre	Float	MHz
2	采样率	FreSample	Float	MHz
3	点数	pointNum	Int	
4	功率	PowerA	Float	发射功率控制项，用最大功率
5	波形数据	waveData	Float[]	波形数据/或 byte [] 采样率 8 位垂直精度

Table 2. AD waveform information format (Structure HackInStruct)

表 2. AD 波形信息格式(结构 HackInStruct)

No.	名称	名称	类型	备注
1	中心频率	centerFre	Float	MHz
2	采样率	FreSample	Float	MHz
3	点数	pointNum	Int	
4	波形数据	waveData	Float[]	波形数据/或 byte[] 采样率 8 位垂直精度

3.2.2. UDP 控制参数格式

UDP 参数指令为“AAA--WorkX--1*2*2--2*2*2”，分别代表标志位--收发状态--电台 1 参数--电台 2 参数，其中工作状态 WorkX = 0 停止，1 电台发 2 电台收。其代码设计如下：

//网络发送工作状态+本地显示状态

void MainWindow::SendMessageInform (HackWave hackT0, QString numstr, double erorRate)//显示工作状态

```
{
    if (hackT0==Stop)
    {
        SendMessage(numstr+"关闭");
        ui->informSTr->setText(numstr+"-网络--关闭");
    }
    else if (hackT0==ComSend) //1
    {
        SendMessage(numstr+"电台发射");
        QString conCode=QString::number(hackT0)+"-"+QString::number(cS1.freMode)+"-
"+QString::number(cS1.modeType);
        ui->informSTr->setText(numstr+"-网控--电台发射"+"-"+conCode);
    }
    else if (hackT0==ComRec)
    {

```

```

        SendMessage(numstr+"电台接收, 误码率"+QString::number (errorRate));
        QString          conCode=QString::number(hackT0)+"-"+QString::number(cS1.freMode)+"-
"+QString::number(cS1.modeType);
        ui->informSTr->setText(numstr+"-网控--电台接收"+"-"+conCode);
    }
    else if(hackT0==EnvRec)
    {
        SendMessage(numstr+"环境监测");

        ui->informSTr->setText(numstr+"-"+网络--监测");
    }
}

```

3.3. 乒乓模式设计

乒乓模式(Ping-Pong Mode)是一种常见的通信模式设计[11], 用于在发送和接收之间高效切换, 确保系统能够在高吞吐量和低延迟的情况下进行数据传输。在基于软件无线电的通信信号模拟与监测系统中, 乒乓模式设计有助于优化信号处理和传输效率。

在实现这种乒乓模式双缓冲绘制时有以下几步:

1. 初始化缓冲区: 在系统启动时, 初始化两个缓冲区(Buffer A 和 Buffer B), 并设置初始状态。例如, Buffer A 用于接收数据, Buffer B 用于处理数据。
2. 数据接收: 开始在 Buffer A 中接收信号数据, 同时 Buffer B 中的数据进入处理阶段。接收数据的操作由信号采集模块完成。
3. 数据处理: 信号处理模块在 Buffer B 中对接收到的数据进行解调、滤波和分析。同时, Buffer A 继续接收新的数据。
4. 缓冲区切换: 当 Buffer A 接收满数据后, 系统立即切换到 Buffer B 进行新的数据接收。此时, Buffer A 中的数据进入处理阶段。
5. 重复循环: 上述步骤重复进行, 实现数据接收和处理的高效切换。系统在两个缓冲区之间不断切换, 确保数据处理的连续性和实时性。

代码实现如下:

首先定义两个 buffer,

```
static Buffer buf1;
```

```
static Buffer buf2;
```

然后通过判断标志位来获取到空闲得 buffer。

```
#define FLAG_FULL 0      //缓冲区已满
```

```
#define FLAG_EMPTY 1    //空
```

```
#define FLAG_RECVING 2  //正接收
```

```
#define FLAG_IOPlay 2   //正播放
```

```
Buffer* ApHackRF::getFreeBuffer()
```

```
{
```

```
    if(buf1.flag == FLAG_RECVING)return &buf1;
```



```

        else if(buf2.flag == FLAG_RECVING)return &buf2;
        else if (buf1.flag == FLAG_EMPTY)
        {
#ifdef _test
            if(buf2.flag == FLAG_FULL)
            {
                flushBuffer(&buf2);
            }
#endif
            return &buf1;
        }
        else if (buf2.flag == FLAG_EMPTY)
        {
#ifdef _test
            if(buf1.flag == FLAG_FULL)
            {
                flushBuffer(&buf1);
            }
#endif
            return &buf2;
        }
        return nullptr;
    }
    return nullptr;
}

```

获取到 buffer 后对改 Buffer 进行数据写入，同时清空满的 buffer，写满后又即使更换另一个以此重复。

```

Buffer* pbuf;
    pbuf = getFreeBuffer();
    if(!pbuf)return;
    if(pbuf->buflen - pbuf->writepos>=buflen*sizeof(uint8_t))
    {
        memcpy(pbuf->buf+pbuf->writepos, buf, buflen*sizeof(uint8_t));
        pbuf->writepos+=buflen*sizeof(uint8_t);
#ifdef _test
        qDebug()<<("write buf%d writelen:%d totalsize:%d\n",pbuf->bufnum,buflen*sizeof(uint8_t),
pbuf->writepos);
#endif
        pbuf->flag = FLAG_RECVING;
    }
    else
    {

```

```

int writebuflen = pbuf->buflen - pbuf->writepos;
memcpy(pbuf->buf+pbuf->writepos, buf, writebuflen);
pbuf->writepos = pbuf->buflen;
pbuf->flag = FLAG_FULL;

#ifdef _test
    qDebug()<<("write  buf%d  writelen:%d  totalsize:%d\n", pbuf->bufnum, writebuflen,
pbuf->writepos);
#endif
write2Buf(buf+writebuflen, buflen*sizeof(uint8_t)-writebuflen);
}

```

通过乒乓模式设计，系统能够在高效接收和处理信号的同时，保持低延迟和高吞吐量，满足各种通信应用的需求。

4. 系统测试与分析

4.1. 系统总界面

软件无线电终端系统界面如图 4 所示。包括频谱显示区、信号控制区、网络传输区。

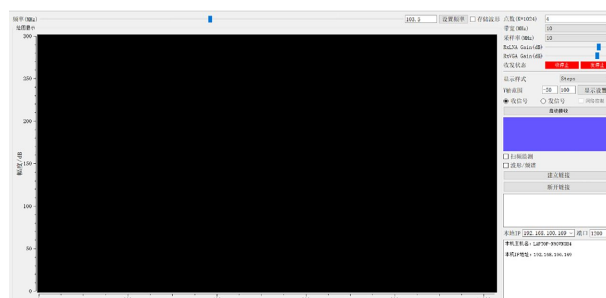


Figure 4. Software-defined radio terminal main interface diagram

图 4. 软件无线电终端主界面图

4.2. 频谱显示测试

频谱显示区可显示频率波形，拿 FM 频段举例，比如 95.5 是中央人民广播电台音乐之声，如图 5 所示，经测试显然可以正常接收。

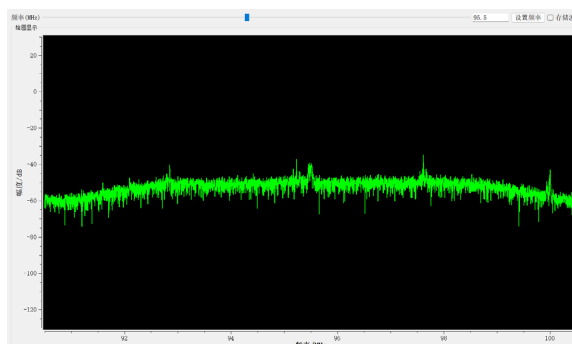


Figure 5. Spectrum display interface diagram

图 5. 频谱显示界面图

4.3. 网络传输测试

信号传输区主要建立 UDP 网络连接, 设置本地 IP 地址和端口号、用来并将传送和接收的数据显示。

点击“建立链接”按钮, 将建立 UDP 网络链接, 蓝色面板出现“网络控制”, “建立链接”按钮变灰色, 在文本显示框中显示本机主机名、本机 IP 地址、并出现“已成功绑定”并且显示绑定的端口号。点击“断开链接”按钮, “断开链接”按钮变灰色, 蓝色面板显示“网络 - 解除”, 文本框显示“已解除绑定”。

如图 6 所示, 建立连接后, 会监听来自主机的指令并执行, 收到指令后根据要求收发指定状态信号, 同时计算消息误码率。

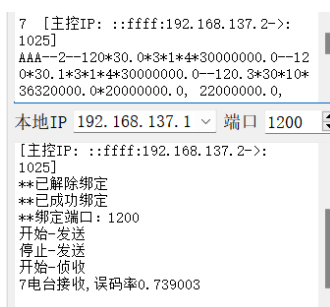


Figure 6. Network control diagram
图 6. 网络控制图

4.4. 信号模拟测试

打开软件无线电终端, 连接 HackRF one, 选择“发信号”, 出现本地参数和本地文件两种信号发送选择, 如图 7 所示, 蓝色面板显示“发射”:



Figure 7. Signal transmission diagram
图 7. 发送信号图

启动发送, 蓝色面板显示“发送 - 中”。

通过另一款软件无线点设备进行测试, 使用 Hack RF One 发送调相信号等, 另一款 USRP 进行接收, 测试结果如图 8 所示, 表明系统能够模拟各种信号。

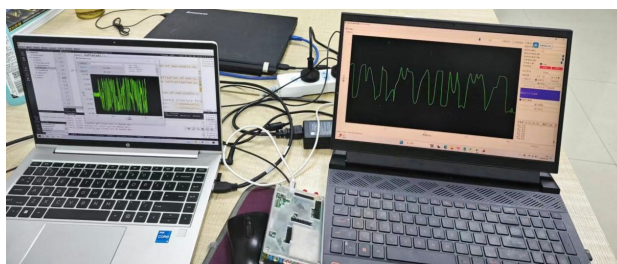


Figure 8. Phase noise test diagram
图 8. 调相噪声测试图

通过测试,全面展示了基于软件无线电的通信信号模拟与监测系统的开发与测试过程,验证了系统的功能和性能,为后续的应用和改进提供了重要参考。

5. 结束语

本论文详细探讨了利用软件无线电技术构建的通信信号模拟与监测系统的设计与实现。该系统不仅能够实时模拟多种复杂的通信信号,而且具备高效的信号处理能力,本系统的建设是复杂电磁环境建设的重要基础。结合其他信号模拟设备的使用,能够共同在复杂电磁环境领域中发挥重要作用。通过软件无线电的灵活性和可配置性,系统能够满足不同应用场景的需求。在硬件选择上,采用了 HackRF One 设备,这是一款性价比较高的开源无线电设备,支持从 1 MHz 到 6 GHz 的频段覆盖。软件开发方面,选择了 C++ 作为主要开发语言,并结合 Qt 框架进行 GUI 编程,以提升用户界面的交互性和图形渲染效率。

对于系统架构包括信号采集模块、信号监测模块、信号模拟模块、图形用户界面(GUI)模块和网络通信模块五个部分。其中,信号监测模块是核心组件之一,负责对采集到的数字信号进行实时监测和分析,确保通信质量和可靠性。此外,系统还支持使用 UDP 发送指令进行远程控制,增强了操作的便捷性。

本系统的关键技术设计,双缓冲区技术被用于提高频谱和波形界面的渲染效率及质量,有效防止图形闪烁和绘制错误。同时,系统实现了多种调制/解调算法,如 ASK、FSK、PSK 等,以及傅立叶变换算法,用于快速准确地分析信号的频率成分和特性。

实验结果显示,该系统具有高度的准确性和稳定性,能够有效模拟和监测通信信号。这一成果不仅证明了软件无线电技术在现代无线通信领域的应用潜力,也为未来无线通信技术的发展提供了有力的技术支持和研究方向。

参考文献

- [1] 夏秋,施守涵,陈懿,等. 基于 GNU Radio 和 Hack RF 的信号捕捉与通信系统设计[J]. 信息技术与信息化, 2022(9): 148-152.
- [2] 王晓平. 基于 HackRF 的无线通信平台的设计与实现[J]. 电脑知识与技术, 2023, 19(19): 113-116.
- [3] 金虹,张昊天. 软件无线电技术在军事通信的应用与发展[J]. 中国军转民, 2025(2): 24-25.
- [4] 杨泽栋. 基于软件无线电的抗干扰通信系统设计与实现[D]: [硕士学位论文]. 武汉: 湖北大学, 2024.
- [5] 郭懿萱. 基于软件无线电的通信信号调制识别系统研究[D]: [硕士学位论文]. 阜新: 辽宁工程技术大学, 2021.
- [6] 文延东,文双春,刘昱,等. 基于软件无线电的通信信号测试平台设计与实现[J]. 计算机工程与科学, 2016, 38(9): 1769-1775.
- [7] 凌玲. 基于 GNU 和 HackRF One 的短波通信平台[J]. 电子制作, 2024, 32(22): 9-12, 25.
- [8] 楚越. 基于 QT 与 OSG 的三维场景交互软件[J]. 电脑编程技巧与维护, 2024(7): 141-143, 166.
- [9] 蔡先变,尹鹏程. 缓冲区技术在 GIS 图形显示优化中的应用[J]. 计算机与现代化, 2007(8): 126-127, 130.
- [10] 齐琳. 基于软件无线电的通信信号调制模式识别算法及解调算法的研究[D]: [硕士学位论文]. 哈尔滨: 哈尔滨工程大学, 2005.
- [11] 谭超,段俊明,辛亮,等. 基于 STM32 与异步 FIFO 的乒乓模式高速数据采集系统设计[J]. 电工材料, 2023(1): 55-59, 63.