# Análise da Segurança das Mensagens R-GOOSE Frente a Ataques Cibernéticos de Injeção de Dados Falsos

**Fábio Bruns** * **Patrick Couceiro** * **Mayara Helena** ** **Nicolas Fulli** ** **Matheus Ayello** ** **Yona Lopes** **

* *Departamento de Engenharia de Telecomunicações, Universidade Federal Fluminense, RJ, (e-mail: fabiobruns@id,uff.br, patrickfrizzini@id.uff.br).*
** *Programa de Pós-graduação em Engenharia Elétrica e de Telecomunicações, Universidade Federal Fluminense, RJ, (e-mail: mayarahelena@id.uff.br, nicolasfulli@id.uff.br, matheus_felipe@id.uff.br, yonalopes@id.uff.br)*

**Abstract:**
This study investigates the security implications of false data injection in R-GOOSE messages within power system communication networks. By reviewing existing literature and conducting practical tests on a dedicated testbed, this research highlights the vulnerability of protection relays to cyber threats and stresses the necessity for robust security measures. Results demonstrate the potential for manipulation of message parameters, leading to communication loss between relays, thus emphasizing the critical importance of enhancing cybersecurity protocols in the power sector. The findings underscore the need for collaborative efforts among industry stakeholders, standards bodies, and cybersecurity experts to develop comprehensive security frameworks tailored to the evolving landscape of power system communication networks. Ultimately, by addressing cybersecurity challenges and fortifying protection relay systems against potential vulnerabilities, the power industry can ensure the resilience and reliability of energy infrastructure in the face of emerging cyber threats.

**Resumo**:
Este estudo investiga as implicações de segurança da injeção de dados corrompidos em mensagens R-GOOSE nas redes de comunicação do sistema de energia. Através da revisão da literatura existente e da realização de testes práticos em uma bancada de testes, a investigação destaca a vulnerabilidade dos relés de proteção às ameaças cibernéticas e sublinha a necessidade de medidas de segurança robustas. Os resultados demonstram o potencial de manipulação dos parâmetros das mensagens, levando à perda de comunicação entre relés, sublinhando assim a importância de melhorar os protocolos de cibersegurança no setor de energia. As conclusões apresentam a necessidade de colaboração entre as partes interessadas do setor, as entidades reguladoras, e os peritos em cibersegurança para desenvolver mecanismos de segurança abrangentes e alinhados ao panorama em evolução das redes de comunicação e sua integração ao sistema elétrico. Em última análise, ao abordar os desafios da cibersegurança e fortalecer os sistemas de relés de proteção contra potenciais vulnerabilidades, o setor da energia pode garantir a resiliência e a confiabilidade da infraestrutura energética face às ameaças cibernéticas emergentes.

*Keywords:* R-GOOSE; Cybersecurity; IEDs; False Data Injection; Cyberattacks.

*Palavras-chaves:* R-GOOSE; Cibersegurança; IEDs; Injeção de dados falsos; Ataques Cibernéticos.

## 1. INTRODUÇÃO

Os sistemas elétricos de potência consistem de parte essencial da infraestrutura de um país, garantindo o fornecimento de energia elétrica para permitir o desenvolvimento econômico e social. Com a contínua expansão do setor elétrico brasileiro, a complexidade da malha elétrica aumenta e os requisitos de estabilidade e performance se tornam mais críticos. Nesse sentido, a utilização de esquemas de proteção e estabilidade regionais se torna de grande valia para manter o fornecimento de energia no país.

Paralelamente, existe uma a crescente tendência de digitalização dos sistemas de energia, impulsionada pela adoção da norma *International Electrotechnical Commission* (IEC) 61850 como referência padronizadora, os sistemas de comunicação aumentam em número e em complexidade. No contexto digital, as redes de comunicação agora se encontram diretamente relacionadas ao desempenho dos sistemas de energia, portanto, conforme discutido por Hussain et al. (2023a), é essencial considerar as dinâmicas operacionais associadas .

Nesse contexto, o processo de digitalização introduz novos desafios, particularmente na proteção contra ameaças cibernéticas que visam infraestruturas críticas. Entre estas ameaças, a injeção de dados falsos em mensagens *Routable Generic Object Oriented Substation Event* (R-GOOSE) surge como uma preocupação significativa, comprometendo potencialmente a integridade e a confiabilidade das operações do sistema de energia. Essa situação se torna ainda mais crítica com a introdução da tecnologia 5G para transmissão de informações no setor elétrico, conforme observado por Guo et al. (2021), onde as redes se tornam mais expostas a invasores, tornando-se necessário metodologias de segurança cibernética para a integridade do sistema.

Nesse sentido, o presente artigo explora e pesquisa as implicações de segurança da injeção de dados falsos em mensagens R-GOOSE realçando o cenário em evolução das ameaças à cibersegurança que o setor de energia enfrenta e ressalta a necessidade de medidas proativas para proteger a infraestrutura crítica. Para conduzir a pesquisa, é realizado um estudo de caso em uma bancada de testes em laboratório consistindo de: Um *Intelligent Electronic Device* (IED) GE T60 para publicação de mensagem R-GOOSE; um IED GE N60 para a assinatura da mensagem R-GOOSE; um hardware invasor para injeção dos ataques cibernéticos na rede; e um roteador Archer C80 para formar o barramento de comunicação dos testes. No estudo de caso foi realizado um total de cinco testes avaliando tentativas de ataque de mudança

O restante deste artigo está estruturado da seguinte forma. A Seção 2 é abordada a revisão de literatura realizada em trabalhos relacionados. A relevância do tópico do artigo para a literatura acerca de sistemas de segurança em redes de comunicação com o uso de R-GOOSE é discutida e o comparativo com outros trabalhos similares encontrados é apresentado. Já Seção 3 descreve brevemente a contextualização teórica fundamental para o entendimento deste projeto. Enquanto na Seção 4, o estudo de caso, sua implementação, testes e resultados são descritos. Por fim, a Seção 5 conclui o artigo e apresenta as perspectivas de trabalhos futuros.

## 2. TRABALHOS RELACIONADOS

Em levantamentos bibliográficos, a segurança aplicada a redes de comunicação para sistemas de energia tem sido amplamente discutido. O estudo Ustun et al. (2021) apresenta um mecanismo de segurança em protocolos R-GOOSE com a inserção de um vetor de inicialização no protocolo para garantir a confiabilidade. O artigo propõe detalhes sobre a implementação do campo IV e dos algoritmos de segurança nas mensagens, demonstrando como esses recursos de segurança podem ser incorporados. Além disso, são apresentados resultados de testes laboratoriais que mostram a eficácia da solução proposta. No entanto, o estudo não apresenta testes de bancada com equipamentos comerciais.

Assim também, Ribeiro et al. (2023) apresenta mecanismos de segurança a fim de validar e explorar mensagens criptografadas . Por outro lado, tem se discutido amplamente modelo de ataques em mensagens R-GOOSE. Como, por exemplo, Kharchouf et al. (2021) discute a importância de implementar técnicas de comunicação seguras para proteger os sistemas de energia contra ameaças cibernéticas, utilizando uma estrutura experimental que inclui simulações em tempo real e testes de ataques cibernéticos em mensagens R-GOOSE. O artigo também descreve a implementação de um mecanismo de segurança baseado em *Diálogo Diário de Segurança* (DDS) para garantir a autenticação, criptografia/descriptografia e controle de acesso das mensagens.

Por fim, Quincozes et al. (2021) destaca a necessidade de sistemas de detecção de intrusão especializados para proteger as subestações digitais de ameaças cibernéticas, considerando os desafios únicos apresentados pela integração de tecnologias de processamento de informações e comunicação em redes inteligentes. O trabalho discute a falta de segurança em muitos protocolos de rede de subestações digitais e a necessidade de desenvolver métodos eficazes de detecção e prevenção de intrusões para garantir a operação segura desses sistemas críticos.

Este trabalho tem como colaboração a apresentação de um ataque em um fluxo de mensagens R-GOOSE com o padrão "*Man-in-the-middle*" no qual o atacante possui acesso a rede de comunicação e consegue interceptar, gerar e adulterar os pacotes durante a troca de mensagens. O trabalho propõe um teste de bancada com equipamentos de mercado em cinco cenários distintos de alteração de parâmetros, com foco em falsa injeção de dados.

## 3. FUNDAMENTAÇÃO TEÓRICA

Para compreender a pesquisa desenvolvida, é necessário compreender adequadamente a norma IEC 61850, conceitos básicos de redes de comunicação e cibersegurança.

### *3.1 IEC 61850*

A norma IEC 61850 foi elaborada visando padronizar a comunicação, tendo como seu principal objetivo a interoperabilidade dos equipamentos do sistema elétrico. A Norma permite a comunicação entre os dispositivos presentes, independente dos fornecedores envolvidos. Foi inicialmente elaborada para a modelagem de subestações, mas com o

aumento contínuo dos esforços de digitalização no setor elétrico, expandiu sua modelagem de dados para incorporar diversos novos sistemas. Além disso, define inúmeros requisitos, os quais vão desde as especificações de comunicação até a descrição da linguagem a ser utilizada nos IEDs, incluindo também testes de conformidade. Dentre os protocolos propostos pela Norma, este trabalho destaca *Generic Object Oriented Substation Event* (GOOSE) e R-GOOSE.

*GOOSE:* O modelo genérico de eventos da subestação oferece a possibilidade de uma distribuição rápida e confiável dos valores de entrada e saída. Além disso, é baseado no conceito de descentralização autônoma, proporcionando um método eficiente que permite o envio simultâneo da mesma informação de evento genérico de subestação a mais do que um dispositivo físico através da utilização de serviços de multicast/broadcast. Para efeitos do modelo de evento genérico de subestação, os valores transmitidos são vistos do ponto de vista do dispositivo lógico de publicação, sendo o GOOSE o protocolo que promove essa troca de uma grande variedade de dados organizados em *Datasets*.

Além disso, a GOOSE possui o parâmetro stNum (*state number*) que é um contador simples de eventos sendo incrementado a cada mudança de evento e o valor booleano que a mensagem GOOSE carrega em sua carga útil, inserido na mensagem parametrizada, pode ser *True* ou *False*.

*IEC 61850-90-5:* A norma IEC 61850-90-5 International Electrotechnical Commission (2012), como explica Ustun et al. (2020), especifica duas soluções para a transmissão de GOOSE através de *Wide Area Network* (WAN). Em primeiro lugar, o protocolo GOOSE pode ser tunelado através de redes de comunicação de alta velocidade. Em segundo lugar, as mensagens GOOSE são incrementadas como R-GOOSE através da adição de camadas de rede e de transporte, para que possam ser comunicadas através de WANs. Dado o âmbito principal e os casos de utilização, esse documento foca na transmissão de mensagens R-GOOSE.

R-GOOSE é uma extensão do protocolo GOOSE, concebido para comunicação em subestações eléctricas conforme a norma IEC 61850, indicando sua capacidade de roteamento para diferentes redes de comunicação. Esta caraterística de roteamento permite que as mensagens R-GOOSE naveguem através de topologias de rede complexas, aumentando a flexibilidade da comunicação dentro e fora do ambiente da subestação. Adicionando assim, uma maior gama de possibilidades de comunicação e proteção para o setor elétrico como um todo. A estrutura da mensagem R-GOOSE está representada pela Figura 1.

### *3.2 Redes de Comunicação*

Uma rede é composta por dois ou mais computadores e seus elos. A rede física é composta pelo *hardware* que a compõem enquanto *software* e o modelo conceitual são a rede lógica e diferentes tipos de redes e simuladores oferecem diferentes funções.

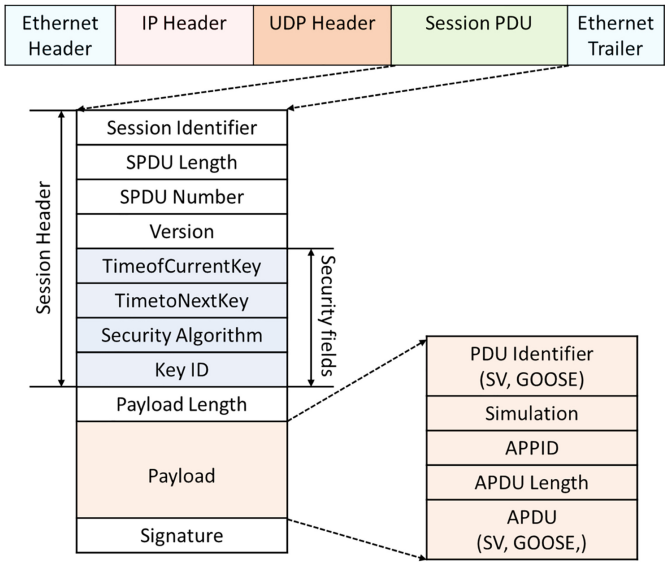


Figura 1. Estrutura GOOSE e R-GOOSE conforme esboçado por Hussain et al. (2023b).

Conforme discutido em Conovalu and Park (2016), o conceito de rede inteligente evoluiu como uma necessidade para modernizar a rede elétrica devido a uma série de deficiências que surgiram no setor da energia, tais como: o desafio de adequar a produção de energia à procura dos consumidores e a incapacidade de os consumidores gerirem eficientemente a utilização de energia. O desenvolvimento das tecnologias de informação e da comunicação alterou radicalmente o panorama das redes elétricas. O universo digital introduziu melhorias significativas nas aplicações do setor elétrico e na diversificação das fontes de energia. As redes de distribuição de eletricidade dependem fortemente de sistemas e dispositivos inteligentes que comunicam entre si.

*Camadas de comunicação - Modelo OSI e TCP:* A fim de possibilitar a comunicação entre diferentes *hardwares* e *softwares*, foram desenvolvidos modelos para a estruturação da comunicação de dados. Neste contexto, há dois modelos amplamente utilizados, o modelo OSI(1984) e o *Transmission Control Protocol* (TCP)/*Internet Protocol* (IP)(1969).

### *3.3 Cibersegurança*

A cibersegurança refere-se à prática de proteção de sistemas informáticos, redes, programas e dados de acesso não autorizado, ciberataques, danos ou roubo. Envolve várias medidas, tecnologias, processos e práticas concebidas para garantir a confidencialidade, integridade e disponibilidade de informações e recursos digitais. A cibersegurança visa a proteção contra uma vasta gama de ameaças, incluindo ataques *Man in the middle*, injeção falsa de dados, além de outras atividades maliciosas. No presente artigo, os ataques realizados no estudo de caso segue a metodologia de injeção falsa de dados.

Embora a crescente digitalização das redes eléctricas seja necessária para lidar com a evolução da procura e da produção de energia, ela levanta desafios fundamentais em matéria de segurança cibernética, especialmente se consi-

derarmos que as redes eléctricas são uma parte essencial da infra-estrutura de um país.

A cibersegurança prática em redes elétricas interligadas, segundo Krause et al. (2021), é afetada por um conjunto diversificado de desafios de segurança fundamentais. Os atacantes podem utilizar diferentes vetores de ataque para comprometer a rede de um operador de sistema de transmissão ou distribuição com o objetivo de causar apagões ou perturbações consideráveis na rede elétrica.

*Man in the middle:* Consiste na interceptação e registro de dados no meio do enlace entre dois equipamentos se comunicando, sem que as vítimas percebam. O ato do atacante maliciosamente mudar os dados inicialmente transmitidos, para outros que favorecem o atacante, faz esse ataque mudar para uma Injeção de dados falsos.

*Injeção de dados falsos:* Um ataque de injeção de dados adulterados envolve a inserção não autorizada de dados fabricados ou maliciosos sobre um sistema, ou rede com a intenção de interromper operações, manipular resultados ou comprometer a segurança. Este tipo de ataque pode levar a decisões incorretas, mau funcionamento do sistema ou acesso não autorizado a informações sensíveis. A Figura 2 ilustra um cenário de ataque de injeção de dados falsos em sistemas elétricos.

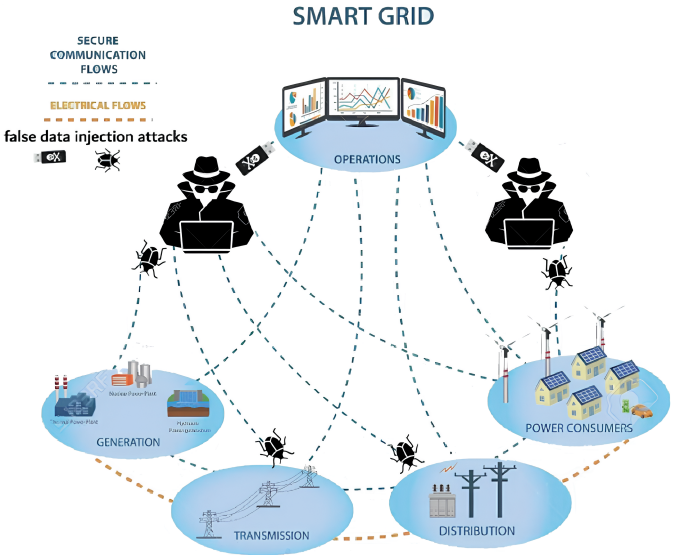


Figura 2. Exemplo de ataque cibernético de injeção de dados falso em sistemas elétricos Tahar et al. (2022).

## 4. ESTUDO DE CASO

Para analisar a segurança de relés de proteção no contexto da injeção de dados falsos em mensagens R-GOOSE, foi utilizada uma bancada de testes, conforme mostram as Figuras 3 e 4, composta por dois *Intelligent Electronic Devices* (IEDs) GE, sendo o publicador da mensagem o Multilin T60 e o assinante da mensagem o Multilin N60, Archer C80 para formar o barramento de comunicação e um *hardware* invasor por onde é injetado as informações modificadas e maliciosas, como mostra o fluxo em vermelho na Figura3 além de coletar as informações do teste. A motivação desse ataque também consiste na busca de vulnerabilidades no recebimento de mensagens dos IEDs, buscando gerar falhas de funcionamento a partir do processamento de informações adulteradas.

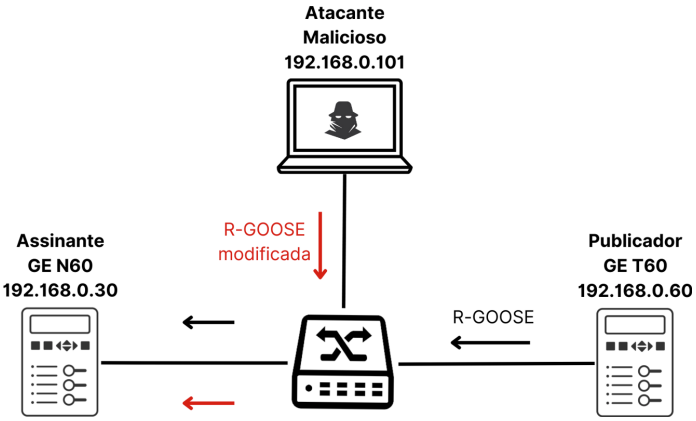


Figura 3. Topologia da bancada de testes.

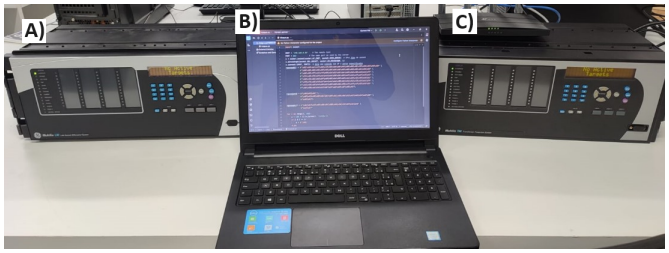


Figura 4. Arranjo físico da bancada de testes.(A) GE N60, (B) hardware invasor, (C) GE T60.

### *4.1 Metodologia*

Para a implementação da bancada de testes os IEDs e o *hardware* foram conectados ao roteador, por meio de cabos de par trançado (Cat 5e). Para parametrização dos equipamentos, foi utilizado o software Enervista do fabricante GE parametrizando uma lógica no IED publicador que envie mensagens R-GOOSE parametrizadas periodicamente no estado *False*, simulando um estado de operação estável da rede elétrica e alterado para o estado *True* mediante o clique no botão *User 1* do painel frontal.

Ao pressionar o botão *User 1* do relé T60, é gerado um evento no *log* de eventos do IED publicador, o que ocasiona uma mudança de parâmetros no N60 de "False" para *True*, o IED assinante, também registrada em seu *log* de eventos. Portanto, para a execução e condução dos testes, após a paremetrização das lógicas e mensagens nos IEDs, é monitorado o *log* de eventos do IED GE N60 para verificar o comportamento da assinatura e recebimento das mensagens R-GOOSE.

### *4.2 Testes Implementados*

Todos os testes implementados focaram na mudança de parâmetros da mensagem e injeção de dados modificados pelo *hardware* invasor, com o intuito de avaliar o comportamento do IED assinante ao receber essas mensagens. Enquanto a outra mensagem original do publicador também estava sendo enviada em paralelo à mensagem R-GOOSE modificada.

Como mencionado anteriormente, o stNum (*state number*) é um contador simples de eventos atrelado as mensagens GOOSE e R-GOOSE sendo incrementado a cada mudança de evento. O valor que a mensagem R-GOOSE carrega, no caso do valor booleano inserido na mensagem R-GOOSE parametrizada, pode ser "True" ou "False". Em todos os testes, o *hardware* invasor foi parametrizado para enviar mensagens R-GOOSE adulteradas consecutivamente para gerar perda de comunicação. Para fins de relevância estatística com um intervalo de confiança em 95 % foram realizados 100 repetições de envio das mensagens. Os campos de alteração realizados no ataque estão realçados na Figura 5 que ilustra a mensagem R-GOOSE parametrizada sendo publicada na rede e capturada pelo *software* Wireshark.

```
R-GOOSE
  Session header
  Session user information
    Payload
      Payload length: 133
      Payload type tag: GOOSE (0x81)
      Simulation flag: 0x00 (0)
      APPID: 0x0000 (0)
      APDU length: 0x007f (127)
      goosePdu
        gocbRef: Rele60Master/LLN0$RG$GoCB01
        timeAllowedtoLive: 2000
        datSet: Rele60Master/LLN0$TT3DataSet01
        goID: TxGOOSE1
        t: May 10, 2024 12:31:11.185206949 UTC
        stNum: 93
        sqNum: 1
        simulation: False
        confRev: 1
        ndsCom: False
        numDatSetEntries: 1
        allData: 1 item
          Data: structure (2)
            structure: 3 items
              Data: boolean (3)
                boolean: False
```

Figura 5. Mensagem parametrizada com campos a serem alterados, nos ataques, realçados(figura elaborada pelo autor).

Para conduzir a avaliação desejada são estabelecidos cinco cenários de testes a serem conduzidos pelo *hardware* invasor. Um código desenvolvido em Python confecciona a mensagem R-GOOSE desejada seguindo a estrutura estabelecida por norma modificando informações da mensagem. Este algoritmo muda o pacote interceptado em seu parâmetros "stNum" e valor booleano da carga útil, buscando entender o comportamento do IED assinante. A intenção dos testes criados é avaliar se ocorre a perda de comunicação, se o IED assinante processa a mensagem modificada e muda seus parâmetros internos.

- **Teste 1:** O primeiro teste feito consistiu na mudança de estado do parâmetro do IED assinante a partir da mudança do valor booleano da mensagem e com um valor de "stNum" menor do que o da mensagem parametrizada. Ou seja, alterou-se o valor da mensagem, porém em um evento anterior ao atual;
- **Teste 2:** O segundo teste também buscou mudar o estado do IED assinante, dessa vez com um "stNum" maior do que o da mensagem parametrizada do publicador. Ou seja, alterou-se o valor da mensagem a ser recebida considerando um evento futuro;
- **Teste 3:** O terceiro teste é similar ao segundo teste, com o valor booleano da mensagem do atacante variando entre *True* e *False*, porém com o "stNum" da mensagem fixa em um valor superior ao "stNum" da mensagem correta;
- **Teste 4:** O quarto teste consistiu na mudança de estado da mensagem R-GOOSE com o valor do "stNum" sendo incrementado em cada uma das 100 mensagens enviadas e o valor booleano fixado em *True*.
- **Teste 5:** O quinto teste é similar ao quarto teste em relação ao "stNum" porém há diferenciação em relação ao valor booleano da mensagem variando entre *True* e *False* em cada mensagem nova enviada.

### *4.3 Análise dos Resultados*

Após a realização dos testes, o teste 1 foi o único que não gerou nenhuma resposta do IED assinante, mantendo o comportamento de operação estável.

Os testes 2 e 3 conseguiram mudar o parâmetro de estado do IED assinante GE N60 para "True" apesar do IED GE T60 estar publicando o valor em "False". Outra consequência dos testes foi de que após o envio das 100 mensagens foi gerada uma perda de comunicação entre os dois IEDs, conforme mostra a Figura 6.

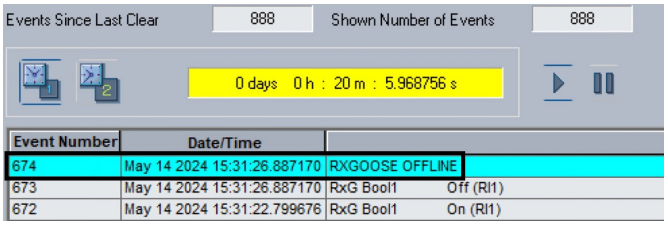


Figura 6. *Log* de eventos do IED GE N60 acusando a perda de comunicação após a conclusão dos testes 2 e 3.

No entanto, durante o teste 3 o valor booleano do *log* de eventos não retornou para *False* apesar da alternância das mensagens R-GOOSE em "True" e "False". Isso ocorreu por que o valor do "stNum" foi fixado e, portanto, o IED não reconheceu as variações de valores durante o recebimento das 100 mensagens e manteve o valor da primeira mensagem modificada recebida.

Os testes 4 e 5 conseguiram com sucesso mudar o valor de estado do IED assinante para "True" e "False" conforme as mensagens que estavam sendo enviadas, sem gerar perda de comunicação entre os IEDs após o término do envio das mensagens do *hardware* atacante. Embora fosse esperado a perda de comunicação, verificou-se que a essa perda não ocorreu no *log* de eventos e o IED não acusou mudanças no evento ("stNum") das mensagens recebidas em seus registros. Os autores não conseguiram compreender com detalhes a razão desse comportamento e esperam investigar mais a fundo o recebimento e processamento dessas mensagens pelo IED. A hipótese inicial é de que o equipamento percebe a similaridade na estrutura da mensagem mas não confere a mensagem como um todo antes de

fazer o processamento. Os autores buscaram testar essa hipótese com novos testes que destacam a mudança de novos parâmetros das mensagens. A Tabela 1 consolida objetivamente o comportamento dos resultados dos testes realizados.

Tabela 1. Consolidação objetiva dos testes realizados.

| Teste | Alterou com sucesso o valor booleano? | Ocasionou perda de comunicação? |
|---|---|---|
| **1** | | |
| **2** | ✓ | ✓ |
| **3** | ✓ | ✓ |
| **4** | ✓ | |
| **5** | ✓ | |

## 5. CONCLUSÃO

A continua expansão dos sistemas elétricos e a tendência atual de digitalização dos sistemas de energia trouxe um novo horizonte para o corpo técnico do setor. As redes de comunicação passam a se tornar diretamente relacionadas ao desempenho das aplicações e, portanto, suas dinâmicas operativas necessitam ser consideradas. A segurança cibernética torna-se uma preocupação do setor que exerce papéis críticos na infraestrutura do país e necessita garantir o fornecimento seguro e confiável de energia.

O presente artigo propôs, com o intuito de analisar a segurança de relés de proteção no contexto da injeção de dados falsos em mensagens R-GOOSE, utilizar uma bancada de testes composta, por dois IEDsGE, sendo um o publicador da mensagem e outro o assinante da mensagem, um roteador para formar o barramento de comunicação e um *hardware* invasor por onde é injetado as informações modificadas e maliciosas e coletado os resultados através do *log* de eventos do equipamento assinante. Os testes foram realizados considerando a variação nos campos do valor booleano da mensagem R-GOOSE parametrizada e de número de evento ("stNum").

Os resultados demonstram a vulnerabilidade de relés de proteção para mensagens não criptografadas ou assinadas. A partir da captura de mensagens da rede, é possível que um atacante replique a mensagem do publicador, e injete dados falsos diante da necessidade do ataque. Pode ser observado que ao manter uma estrutura similar e incrementar o parâmetro "stNum", em relação a mensagem do publicador, a informação é certamente processada pelo IED assinante. Esse ataque pode comprometer significativamente a aplicação afetada. Quando considera-se aplicações de estabilidade regionais ou até mesmo nacionais, essa situação se torna extremamente crítica, podendo ocasionar propagação de defeitos pela rede elétrica e apagões.

Para trabalhos futuros é proposto a ampliação dos testes realizados em outras categorias de ataques cibernéticos. Também espera-se aumentar a gama de fabricantes utilizados para a realização dos ataques e realizar propostas de mecanismos de segurança cibernéticas adequados a realidade do setor além de verificar o impacto no desempenho das mensagens frente a adoção dos mecanismos de segurança.

## AGRADECIMENTOS

Os autores gostariam de agradecer profundamente ao conselho CNPQ, à fundação CAPES, à General Electric, à KYA Engenharia e à fundação FAPERJ pelo apoio financeiro e institucional aos autores do artigo.

## REFERÊNCIAS

Conovalu, S. and Park, J.S. (2016). Cybersecurity strategies for smart grids. *J. Comput.*, 11(4), 300–309.

Guo, Y., Yan, L., Chen, Z., Zhao, Z., Bai, D., Ding, Z., and He, Y. (2021). Defending 5g iot terminals in electrical power communication and information system against cyber threats. doi:10.1109/EI252483.2021.9712987.

Hussain, S.S., Roomi, M.M., Mashima, D., and Chang, E.C. (2023a). End-to-end performance evaluation of r-sv / r-goose messages for wide area protection and control applications. doi:10.1109/ISGT51731.2023.10066414.

Hussain, S.S., Yaohao, C., Roomi, M.M., Mashima, D., and Chang, E.C. (2023b). An open-source framework for publishing/subscribing iec 61850 r-goose and r-sv. *SoftwareX*, 23, 101415.

International Electrotechnical Commission (2012). *Communication networks and systems for power utility automation - Part 90-5: Use of IEC 61850 to transmit synchrophasor information according to IEEE C37.118*.

Kharchouf, I., Saad, A., Alrashide, A., and Mohammed, O.A. (2021). Evaluating the impact of cyber attacks on secure and non-secure routable goose messages. In *2021 IEEE International Conference on Environment and Electrical Engineering and 2021 IEEE Industrial and Commercial Power Systems Europe (EEEIC/I&CPS Europe)*, 1–6. IEEE.

Krause, T., Ernst, R., Klaer, B., Hacker, I., and Henze, M. (2021). Cybersecurity in power grids: Challenges and opportunities. *Sensors*, 21(18). doi:10.3390/s21186225.

Quincozes, S.E., Albuquerque, C., Passos, D., and Mossé, D. (2021). A survey on intrusion detection and prevention systems in digital substations. *Computer Networks*, 184, 107679.

Ribeiro, F.B., da Silva, N.F., and Lopes, Y. (2023). Security mechanisms for r-goose and r-sv messaging over a 5g network. In *2023 Workshop on Communication Networks and Power Systems (WCNPS)*, 1–6. IEEE.

Tahar, B.M., Amine, S.M., and Hachana, O. (2022). Machine learning-based techniques for false data injection attacks detection in smart grid: A review. In *International Conference on Artificial Intelligence in Renewable Energetic Systems*, 368–376. Springer.

Ustun, T.S., Farooq, S.M., and Hussain, S.M.S. (2020). Implementing secure routable goose and sv messages based on iec 61850-90-5. *IEEE Access*, 8, 26162–26171. doi:10.1109/ACCESS.2020.2971011.

Ustun, T.S., Farooq, S.M., and Hussain, S.S. (2021). Initialization vector for application of iec 61850-90-5 security features on r-goose and r-sv messages. *International Journal of Electrical Power & Energy Systems*, 132, 107189.