Format inspired by NWO reviewer guidelines and templates.

Identification

Proposal title: ExICSFuzz: A Fuzzing Framework for Proprietary Binaries of Industrial Control Systems via Rehosting

Overall assessment

Explain in one sentence or short paragraph how you see the entire project.

The project can enable security researchers to better test PLCs and ICSs, using fuzzing. The project has the potential for big societal impact by improving the security of critical infrastructure.

Final score. How do you assess the entire application? Please give the final score for this proposal. Consider doing this after completing the rest of the application.

The final grade for this proposal is, in your view:

eight (8)

Use the following scores in your grading:

Score	Meaning
10	Outstanding, must fund
9	Excellent, must fund
8	Very good, should fund
7	Good overall with one aspect very good, fund if room
6	Good, fund if room
5	Sufficient, fund if room
4	Insufficient, do not fund
3	Bad, do not fund
2	Very bad, do not fund
1	Does not meet academic level, do not fund

Please explain your answers. Try to exceed the length of 50-100 words per answer only when absolutely necessary.

Question 1. What is the scholarly, scientific or technological relevance of the problem? Is the problem original, timely, challenging? Is this a new line of research?

Answer:
The problem of fuzzing PLCs is timely, as fuzzing has seen a rise in feasibility and popularity in the last decade and the deployment of PLCs is ubiquitous with the surge of internet of things devices. The problem is also challenging because of the proprietary nature of PLCs and the diversity of their architectures. The project is not a new line of research, as fuzzing ICSs has been studied before [1].

Question 2. What are the innovative and original aspects of the proposal? Are the project objectives challenging and scientifically ground-breaking? Is the methodology credible?

Answer:
The project is challenging because of the diverse nature of PLCs. Generalizing over all PLCs is hard. The original and innovative aspects of the proposal are the development of a generic virtual execution engine for proprietary ISAs and the modeling of industrial peripherals. The proposal employs proven methodologies and builds on existing work, such as GHIDRA SLEIGH.

Question 3. Is the approach effective, including the practical work programme? How do you assess the program of work described in the proposal (realistic, feasible, ...)? Are the most important risks identified and effectively mitigated?

Answer:
The approach seems effective, as evidenced by the usage of proven concepts as intermediate representation, NLP models, and symbolic execution. The program of work is realistic for a four year project. The most important risks involve not being able to generalize or automate certain steps and are sufficiently mitigated by employing more manual work.

Question 4. Is the proposal well-written and are the project's objectives clearly worded? Do you expect this project will lead to significant advancement of scholarship, science, or technology (academic impact)?

Answer:
The proposal is well written. The objectives are clearly worded by dividing the project into four reasonably sized research tracks. I expect limited academic impact, as the project does not introduce new concepts and the difficulty of the project mainly comes from generalizing over unknown ISAs.

Question 5. What is your opinion on the societal impact of the proposed research? Are the expected results of the research relevant for solving a popular/economic/cultural/ technical or policy-related challenge?

Answer:
Being able to find more vulnerabilities in ICSs can have a severe positive impact on society as illustrated by the examples in the proposal. Preventing industrial incidents and protecting critical infrastructure is important.

Question 6. Are the main stakeholders of the problem clearly identified and addressed in the proposal? If any, what are the most important stakeholders the proposal does not address?

Answer:
The main stakeholders are clearly identified and addressed. The proposal addresses the needs of industry, which requires secure control systems and society which relies on the the continuity of critical infrastructure.

Question 7. Is the release of data and software artifacts clearly identified and addressed in the proposal?

Answer:
The release of data and software artifacts is clearly addressed. The project will release an open-source fuzzing framework for PLCs and a FAIR dataset. Furthermore, the project will be concluded with published papers and a technical workshop about the rehosting techniques and the fuzzing framework.

Question 8. Are the main ethical concerns clearly identified and addressed in the proposal? If any, what are the most important ethical concerns the proposal does not address?

Answer:
The proposal does not address any ethical concerns. The main ethical concern that I can think of is that the results from this project may also prove useful to hackers who are trying to find vulnerabilities in PLCs. Another possible concern is the discovery of new vulnerabilities in existing infrastructure. These should be responsibly disclosed.

Please identify at least 3 of the main strengths of the proposal:

Answer:
S1. Potential for big societal impact.
S2. Usage of proven concepts, builds on previous work.
S3. Open source contributions.

Please identify at least 3 of the main weaknesses of the proposal:

Answer:
W1. The project does not introduce new fundamental concepts, which limits academic impact.
W2. Ethical concerns are not addressed.
W3. The main challenge of the project comes from the difficulty of generalizing over unknown ISAs.

[1] Niedermaier, M., Fischer, F., & von Bodisco, A. (2017, September). PropFuzz—An IT-security fuzzing framework for proprietary ICS protocols. In *2017 International conference on applied electronics (AE)* (pp. 1-4). IEEE.