BIENVENÜE CALL 2023

Individual Assessment Report

The candidate

Heading	Description
Name of the candidate	**Benjamin LION**
Project Title	Certified IoT Application
Project Acronym	CIoTA

Final score summary

Criteria	Score
Scientific excellence of the project (35% of the final score)	3.67
Potential of the candidate (25% of the final score)	3.33
Potential outcomes of the project (20% of the final score)	4
Feasibility of the project (20% of final score)	3.37
Total score (weighted)	**14.6 / 20**

Scoring

Score	Description
0	Proposal fails to address the criterion or cannot be assessed due to missing or incomplete information.
1	Poor. The criterion is inadequately addressed, or there are serious inherent weaknesses.
2	Fair. Proposal broadly addresses the criterion, but there are significant weaknesses.
3	Good. Proposal addresses the criterion well, but a number of shortcomings are present.
4	Very Good. Proposal addresses the criterion very well, but a small number of shortcomings are present.
5	Excellent. Proposal successfully addresses all relevant aspects of the criterion. Any shortcomings are minor.

Any question can be addressed to msca-bienvenue@bretagne.bzh

Name of Applicant:	Dr Benjamin Lion	Project Number:	23-RB-BIENV-035
		Cluster:	

Consensus Recommendation:	Consensus Ranking:	Consensus Score:

Review Form/ 1

Project Number:	23-RB-BIENV-035	**Applicant:**	Benjamin Lion
Project Type:	RB-BIENVENUE		
Project Title:	Certified IoT Application		

Instructions

> **Please carefully read the evaluation guidelines before starting the review.** They can be downloaded in the *Document* section (on green banner of your portal).
>
> External experts are not representing their institutions and should evaluate proposals on their own merit. **They make an independent and confidential assessment of the application as submitted - not on its potential, if certain modifications were made, and without visiting websites that may be mentioned in the application.** The application is assessed on its own merits, according to the four criteria listed below. The candidates have been asked to structure their proposal in 4 parts that reflect the 4 criteria. However, the information related to each criterion can be found throughout the proposal. **Reviewers should therefore consider the whole proposal to evaluate each of the criteria and not only the related part.**

1. Scientific excellence of the project

> **Weighted 35% - Priority 1**
>
> • Quality of the research/innovation project
> • Originality of the scientific approach and methods
> • Originality of the application along with intersectoral/interdisciplinary/ international aspects

Strengths

> Please justify the score you have chosen.

The research goals of the project are innovative, challenging and indeed open problems whose solution can have major impact. Even the partial solution of such challenges can improve the security and safety of current IoT systems. It is correct that most of the focus in the state of the art is in the correctness of the software running on a single device, but not much is done at the system level, considering the network of devices. The proposal considers including also the execution state in a safety certification of the IoT application. These indeed would increase the assurance provides by such a certification.
The idea of bridging the gap between C, that is actually what most developers use to develop IoT applications in practice and a formal language (i.e., Gallina) in an automated manner is very important and essential for the wide adoption of the results.
The problem described applies to applications in different sectors and domain, is not limited to IT, in that sense the scope of the application is inter-sectoral.

Weaknesses

> Please justify the score you have chosen. **In case weaknesses cannot be identified, please write "No weakness found"**.

In the description, it is not clear what are the properties on which the project is focusing. The used term “safely” is ambiguous and from the description is not clear if the focus is on safety or on correctness. The use of theorem proving rather than other formal approaches (i.e., model checking) requires some justification. While proofs considering the run-time behaviour provide higher assurance, they are also much more complex to verify. There is no consideration related to performance and real-time aspects that are very common in many IoT applications.
The role of Physics in the project is not clear.

Other

> Please provide any other relevant comments in relation to the criterion.

2. Potential of the candidate

> **Weighted 25% - Priority 2**
>
> • Research records: peer-reviewed publications, conference participations (posters and talks) and proceedings, prizes and distinctions (e.g., MSCA Seal of excellence)
> • Scientific experience, knowledge and skills acquired during the fellowship
> • Value of profiles with intersectoral/interdisciplinary/ international mobility experience
> • Complementary transversal skills: project management, leadership, sector agility, communication …
>
> *The candidate's potential will be evaluated in relation to their level of experience. To avoid negative impact of career breaks (whether based on industrial, sabbatical, unemployment and/or parental leave …) on the evaluation, scientific production will be assessed on the period of effective work.*

Strengths

> Please justify the score you have chosen.

The candidate worked abroad in a renowned institution for formal method research. He worked at different institutions and with several researchers, so he has proven ability to adapt to new contexts and research teams as well as addressing multicultural aspects. He largely fulfils the mobility requirement. He has a solid background in formal methods and languages as well as experience in using and some related tools. He has already achieved and published some results that go in the direction of the proposed research.

Weaknesses

> Please justify the score you have chosen. **In case weaknesses cannot be identified, please write "No weakness found".**

The publications are not in top conferences and journals. Considering also the time since he started to be engaged in PhD work, the number of publications is somewhat low. There is not much evidence of leadership and autonomy in the curriculum (e.g., supervisions of students, organization of workshop, activity of reviewing, etc.). The curriculum has some typos, the typos per se are not so important, but I would not expect them in a grant application.

Other

> Please provide any other relevant comments in relation to the criterion.

3. Potential outcomes of the project

> **Weighted 20%- Priority 3**
>
> • Quality of the proposed measures to exploit and disseminate research results
> • Candidate’s training objectives and capacity to acquire scientific and complementary skills that will lead to career development, reach or re- enforce a position of professional maturity/independence

Strengths

> Please justify the score you have chosen.

The potential scientific impact of the project can be high because it refers to a foundational aspect that with effects across all application domains using IoT systems. The developed technology can contribute to build better dependable systems than in turn can lead to better IoT application thus can results in a competitive advantage for the company adopting the technology. The proposed research leverages on a technology (Coq and related extensions) that has some strongholds in the region of Bretagne, thus strengthening that position. The scope and goals of the proposal fully match objectives SO7, SO9, SO17 and SO19 of the RIS3 strategy.

Weaknesses

> Please justify the score you have chosen. **In case weaknesses cannot be identified, please write "No weakness found".**

A theorem proving is not so easy to scale and it has a very steep learning curve. This may have a negative impact on the widely adoption of the techniques and methods proposed by the project. Wide adoption is important because the scope of the problem, the interconnected IoT devices, included thousands of applications and deployment so their security cannot be delegated only to people with a very specific and in-depth knowledge of the theory behind that.
In term of publications, planning only two publications, even if in top conferences, is a bit low, considering also the fact the candidate should carry on research in a well-established and experienced research group.

Other

> Please provide any other relevant comments in relation to the criterion.

4. Feasibility of the project

> **Weighted 20% - Priority 4**
>
> • Coherence and effectiveness of the work plan, including timeline and risk management
> • Credibility of the method proposed and alternative plans
> • Integration into the local environment (the region and/or the Host Institution).

Strengths

> Please justify the score you have chosen.

The project aims at building on top of Coq, that is a mature framework with a well-established community especially in France. Leveraging on existing building blocks is the best way, and probably the only way, to reach the ambitious goals of the project. The selected research team provide an ideal environment for the candidate to extend his knowledge and to carry on the proposed research.

Weaknesses

> Please justify the score you have chosen. **In case weaknesses cannot be identified, please write "No weakness found".**

One of the reasons why there is not much research at the verification of the system level behaviours is its complexity. The scale of the systems under analysis can be large as well as the expected behaviour might not always be bounded or known in advance. So, to address this research challenges is important to do it gradually considering some assumptions and possible constraints to reduce the scope of the general problem, thus limiting the complexity to a level that could be feasible. The description of the proposal does not mention any of these constraints and it does not address the complexity issues as it should.
The feasibility of translating, transparently to the programmer, any C program in an equivalent one written in a formal language is not obvious. The proposal mentions about building an extension of the “dx” tool, but that does the opposite of what it is stated in the proposal. It builds an approximation of a C program starting from a program written in Gallina. Existing IoT applications are written in C and not in Gallina.
It’s not clear how it’s possible to formally generate certificates at design time, about runtime properties (i.e., the property in figure 1 cannot be guaranteed at design time and at even at runtime, sometimes it might be satisfied other times not and this may not even be dependent only on the application itself but on other applications that may run on the device at the same time, for example).

Other

> Please provide any other relevant comments in relation to the criterion.

Complementary remarks on ethics (not part of the evaluation)

> Based on your experience are there any ethical issues that may arise from the project?
> If yes, please describe any potential ethical issue you can foresee, this will help the ethics officer during the review process to propose alternative solutions.

I don’t see any particular ethical issue that requires special attention.

Review Form/ 2

Project Number:	23-RB-BIENV-035	**Applicant:**	Benjamin Lion
Project Type:	RB-BIENVENUE		
Project Title:	Certified IoT Application		

Instructions

> **Please carefully read the evaluation guidelines before starting the review.** They can be downloaded in the *Document* section (on green banner of your portal).
>
> External experts are not representing their institutions and should evaluate proposals on their own merit. **They make an independent and confidential assessment of the application as submitted - not on its potential, if certain modifications were made, and without visiting websites that may be mentioned in the application.** The application is assessed on its own merits, according to the four criteria listed below. The candidates have been asked to structure their proposal in 4 parts that reflect the 4 criteria. However, the information related to each criterion can be found throughout the proposal. **Reviewers should therefore consider the whole proposal to evaluate each of the criteria and not only the related part.**

1. Scientific excellence of the project

> **Weighted 35% - Priority 1**
>
> • Quality of the research/innovation project
> • Originality of the scientific approach and methods
> • Originality of the application along with intersectoral/interdisciplinary/ international aspects

Strengths

> Please justify the score you have chosen.

The proposed project is original and is important both theoretically and practically; formal verification has been recently adopted by many leading software/hardware companies, and it is likely that IoT developers would follow suit. Taking more runtime effects into account is beneficial, and their modelling is highly non-trivial. However, the availability of CompCert in Coq makes the task more feasible and achievable.

Weaknesses

> Please justify the score you have chosen. **In case weaknesses cannot be identified, please write "No weakness found"**.

The proposal missed some relevant projects that should be mentioned in the proposal. For example, in seL4 (in Isabelle), one gets some provable guarantees on the reliability and safety of runtime effects. Moreover, Google recently announced that seL4 would be used in KataOS.

Other

> Please provide any other relevant comments in relation to the criterion.

2. Potential of the candidate

> **Weighted 25% - Priority 2**
>
> • Research records: peer-reviewed publications, conference participations (posters and talks) and proceedings, prizes and distinctions (e.g., MSCA Seal of excellence)
> • Scientific experience, knowledge and skills acquired during the fellowship
> • Value of profiles with intersectoral/interdisciplinary/ international mobility experience
> • Complementary transversal skills: project management, leadership, sector agility, communication …
>
> *The candidate's potential will be evaluated in relation to their level of experience. To avoid negative impact of career breaks (whether based on industrial, sabbatical, unemployment and/or parental leave …) on the evaluation, scientific production will be assessed on the period of effective work.*

Strengths

> Please justify the score you have chosen.

The applicant has a good publication record with many recent journal publications. Moreover, a good sign is that the list of coauthors is diverse. The applicant worked in a strong group at CWI, Amsterdam. Through collaboration with Farhad Arbab and Carolyn Talcott, one can assume he is also well-connected in the community with many international contacts that can positively influence his future academic career.

Weaknesses

> Please justify the score you have chosen. **In case weaknesses cannot be identified, please write "No weakness found".**

The applicant does not have publications in highly selective top conferences.

Other

> Please provide any other relevant comments in relation to the criterion.

3. Potential outcomes of the project

> **Weighted 20%- Priority 3**
>
> • Quality of the proposed measures to exploit and disseminate research results
> • Candidate’s training objectives and capacity to acquire scientific and complementary skills that will lead to career development, reach or re- enforce a position of professional maturity/independence

Strengths

> Please justify the score you have chosen.

Publishing at top conferences, making the related artifacts publicly available, and seeking industrial partners to adopt the technology are appropriate ways to disseminate the research results. Possible cooperation with the industry would likely influence the applicant in one way or another. Similarly, bearing responsibility for an individual research project, being part of a bigger group, and coordinating with other academic groups will significantly impact the applicant's abilities.

Weaknesses

> Please justify the score you have chosen. **In case weaknesses cannot be identified, please write "No weakness found".**

No weakness found.

Other

> Please provide any other relevant comments in relation to the criterion.

4. Feasibility of the project

> **Weighted 20% - Priority 4**
>
> • Coherence and effectiveness of the work plan, including timeline and risk management
> • Credibility of the method proposed and alternative plans
> • Integration into the local environment (the region and/or the Host Institution).

Strengths

> Please justify the score you have chosen.

A detailed plan is described in the proposal, including appropriate work packages and timelines, that should lead to 3 high-quality publications, a highly ambitious goal. However, this is to be expected because the hosting group is strong, regularly publishing at top conferences.
Coq is a good fit for the project. It is a popular proof assistant with a vibrant community (not only) in France.

Weaknesses

> Please justify the score you have chosen. **In case weaknesses cannot be identified, please write "No weakness found".**

I am unsure if all the plans are feasible, provided the proposal describes an individual 2-year postdoc project and the applicant needs to learn Coq first. It seems more like a longer-term group project, but it is unclear from the proposal whether significant group support (besides mentoring) is expected.

Other

Please provide any other relevant comments in relation to the criterion.

Complementary remarks on ethics (not part of the evaluation)

Based on your experience are there any ethical issues that may arise from the project?
If yes, please describe any potential ethical issue you can foresee, this will help the ethics officer during the review process to propose alternative solutions.

Review Form/ 3

Project Number:	23-RB-BIENV-035	**Applicant:**	Benjamin Lion
Project Type:	RB-BIENVENUE		
Project Title:	Certified IoT Application		

Instructions

> **Please carefully read the evaluation guidelines before starting the review.** They can be downloaded in the *Document* section (on green banner of your portal).
>
> External experts are not representing their institutions and should evaluate proposals on their own merit. **They make an independent and confidential assessment of the application as submitted - not on its potential, if certain modifications were made, and without visiting websites that may be mentioned in the application.** The application is assessed on its own merits, according to the four criteria listed below. The candidates have been asked to structure their proposal in 4 parts that reflect the 4 criteria. However, the information related to each criterion can be found throughout the proposal. **Reviewers should therefore consider the whole proposal to evaluate each of the criteria and not only the related part.**

1. Scientific excellence of the project

> **Weighted 35% - Priority 1**
>
> • Quality of the research/innovation project
> • Originality of the scientific approach and methods
> • Originality of the application along with intersectoral/interdisciplinary/ international aspects

Strengths

> Please justify the score you have chosen.

In principle, proving that a program is free from bugs is attractive and desired, as said by Dijkstra and emphasized by the author of this proposal.
Also, IoT is still evolving, and soon there may be dozens or hundreds of billions out there whose behavior should be controlled.
Therefore, proving that the behavior of a device is correct may be a contribution to the current and future IoT Smart Applications.

Weaknesses

> Please justify the score you have chosen. **In case weaknesses cannot be identified, please write "No weakness found"**.

In its current state, this project has some weaknesses, such as:
1) Scientific contribution: There is a lack of clarity regarding the contribution to knowledge generation. While the objective of this project is clearly defined, it is unclear exactly where in the life cycle of IoT applications the scientific contribution of this

project would be achieved. Also, usually, people assume a large number of IoT devices will make up a given application, where some of them may be faulty, and some may be compromised by an attacker. This issue is called “trustworthiness” and involves many different techniques/approaches to guarantee that the final result of the application is correct and not harmful. Again, formal proof systems usually are cumbersome to work with. Therefore, the question to be answered for IoT applications is: is formal proof better/cheaper/more practical/etc. than detecting and isolating faulty/compromised devices? This project does not address this issue. Finally, the project does not clarify precisely how CIoTA evolves Coq.

2) Methodology: the methodology and approach are not described clearly. The project makes some claims but does not explain how they will be achieved. For example, Figure 1 is unclear regarding its steps. It says there are three steps but lists I to V. After that, it calls Step I, Step II, and Step III, which are inside the first step (abstraction). It requires reading back and forth sometimes to understand what is going on.

3) IoT: the issues regarding IoT are not well characterized and even inconsistent. For example, the project mentions MQTT (by the way, the old name is not used anymore, and the protocol is just called MQTT) as a proof-of-concept experiment and affirms that devices run on batteries. However, typical devices that run on batteries do not speak TCP/IP because the stack uses a lot of memory space and consumes many CPU cycles to process. Typically, IoT devices use LPWAN communication technologies (such as LoRaWAN) to send messages to a gateway in a specific layer 1/2 protocol, which in turn is connected to the Internet and forwards the message to a server via an MQTT broker. In other words, assuming that an ESP32-powered device running on batteries will speak TCP/IP is not realistic.

4) Structure and language: the project has many English grammar problems and typos and sentences difficult to understand, which need a thorough revision.

Other

> Please provide any other relevant comments in relation to the criterion.

2. Potential of the candidate

> **Weighted 25% - Priority 2**
>
> • Research records: peer-reviewed publications, conference participations (posters and talks) and proceedings, prizes and distinctions (e.g., MSCA Seal of excellence)
> • Scientific experience, knowledge and skills acquired during the fellowship
> • Value of profiles with intersectoral/interdisciplinary/ international mobility experience
> • Complementary transversal skills: project management, leadership, sector agility, communication …
>
> *The candidate's potential will be evaluated in relation to their level of experience. To avoid negative impact of career breaks (whether based on industrial, sabbatical, unemployment and/or parental leave …) on the evaluation, scientific production will be assessed on the period of effective work.*

Strengths

> Please justify the score you have chosen.

The candidate’s scientific production is compatible with his career stage, focused on the formal specification/proof area. He recently (2022) published two journal papers about formal methods for cyber-physical systems as the first author, as well as

three papers on the same subject at conferences. Also, he is a co-author of other papers on the same subject, as well as the first author of papers on formal methods, but with a different focus. He also has some experience with teaching and conference participation/organization.

Weaknesses

> Please justify the score you have chosen. **In case weaknesses cannot be identified, please write "No weakness found".**

The candidate's lack of research maturity in writing research projects might have negatively influenced the version submitted to this call, which may be improved in the future by the supervision of a senior researcher.
Also, since the project is focused on IoT, his experience in this area should be improved by collaborating with some who work there.
Comment: The candidate states that he does not hold a Ph.D. but also says he finished writing the thesis. His current status could be made clearer - as t indicate the thesis defense date.

Other

> Please provide any other relevant comments in relation to the criterion.

3. Potential outcomes of the project

> **Weighted 20%- Priority 3**
>
> • Quality of the proposed measures to exploit and disseminate research results
> • Candidate's training objectives and capacity to acquire scientific and complementary skills that will lead to career development, reach or re- enforce a position of professional maturity/independence

Strengths

> Please justify the score you have chosen.

As emphasized in the topic of scientific excellence, proving that the behavior of a device is correct may be a contribution to the current and future IoT Smart Applications. In that sense, the project considers giving attention to an area currently mostly overlooked by the IoT community. Also, the project considers scientific and environmental, societal, economic, and regional impacts. The impact on the candidate's research career is also given attention.

Weaknesses

> Please justify the score you have chosen. **In case weaknesses cannot be identified, please write "No weakness found".**

This project focuses on IoT, but the envisioned publication forums are in languages and formal methods. To guarantee that the contribution is relevant to this area, results must be validated by the research community of that area (for example, IEEE Internet of Things Journal, IEEE WF-IoT, etc.).

Other

> Please provide any other relevant comments in relation to the criterion.

Consider the first paragraph of Section 2.2: “The ability for programs to alter their environment is a new feature that requires rethinking of the practices of programming to increase safety of such systems, and theoretical approaches to faithfully define the notion of what such program computes.”
This statement must be taken with care because proving that a program running on a device is correct does not prevent the entire IoT system from changing the environment in a wrong or dangerous way. There is an entire data flow in IoT that starts in the sensor and goes through many instances of gateway, fog/edge, and cloud, where it is stored. Then, a model (e.g., machine/deep learning and/or a rule-based inference system) makes a decision sent to actuators that, in turn, change the environment.

4. Feasibility of the project

> **Weighted 20% - Priority 4**
>
> • Coherence and effectiveness of the work plan, including timeline and risk management
> • Credibility of the method proposed and alternative plans
> • Integration into the local environment (the region and/or the Host Institution).

Strengths

> Please justify the score you have chosen.

The work plan follows the structure of the three main phases (let us call them by this name since step is confusing) in the research methodology, which shows coherence in the methodology and implementation. These phases are: abstraction (WP1: Formal models for abstraction of runtime effects of the IoT), certification (WP2: Certification of runtime behavior), and extraction (WP3: Extraction of executables).
The candidate is already integrated with the TEA team (Time Event Architecture) of the INRIA center at the University of Rennes.

Weaknesses

> Please justify the score you have chosen. **In case weaknesses cannot be identified, please write "No weakness found".**

In the work package descriptions, tasks are not given names, which makes it difficult to grasp what they do and how they fit into the big picture.

Other

> Please provide any other relevant comments in relation to the criterion.

Complementary remarks on ethics (not part of the evaluation)

> Based on your experience are there any ethical issues that may arise from the project?
> If yes, please describe any potential ethical issue you can foresee, this will help the ethics officer during the review process to propose alternative solutions.