PREDIGMA

TECHNOLOGIES

reliability and security for dependable electronics

July 2019

PREDIGMA'S PURPOSE

REMOTE PREDICTIVE MAINTENANCE AND DETECTION OF CYBERATTACKS ON INDUSTRIAL ELECTRONICS

THE PROBLEM

Production downtime costs $647B/year globally *

Electrical failures account for 19% (>$120B/year) of the production downtime **

NEED SOLUTION TO ADDRESS PRODUCTION DOWNTIME DUE TO ELECTRICAL FAILURES

CYBERATTACKS – A SPECIAL CASE OF ELECTRONICS DOWNTIME

Existing software methods for cyberthreat detection are failing to address a significant number of intrusions into critical hardware.

"54% of companies experienced an industrial control system security incident within the past 12 months and 16% had experienced three or more…The average ransomware attack costs $5M" ***

NEED AN ALTERNATIVE SOLUTION TO EXISTING METHODS FOR DETECTION OF CYBERATTACKS

** https://www.isa.org/standards-publications/isa-publications/intech-magazine/2013/feb/automation-it-predictive-maintenance-embraces-analytics*
*** https://www.gepowerconversion.com/inspire/reducing-unplanned-downtime-predictive-maintenance*
**** https://www.csoonline.com*

CURRENT INDUSTRY LANDSCAPE

Current state-of-the-art Predictive Maintenance solutions are based on statistical modeling of electronics failures over extended period of time.

Majority of direct failure detection methods rely on invasive approaches such as electrical probes and/or extra circuitry adding complexity and cost to the product.

Widely-used IR sensors/cameras can detect overheating in systems but require direct line of sight – rarely possible and often too late to prevent failure.

Cyberattacks are recognized by specialized software but more often are left undetected or registered only by their destructive consequences.

THE SOLUTION

Platform for assessing the “Health Status” of industrial electronics in real-time

Based on well-known Physics

Electronic devices emit magnetic field due to their operational currents. A “normal” set of operational currents define the proper functioning of an electrical device.

Our Approach of assessment of the “Health Status”

Sensitive detection of magnetic field can map and characterize the flow of operational currents. The device “Health Status” is assessed by applying ML/AI techniques to real-time magnetic data map to predict and/or detect failures due to natural causes (e.g. aging), accidents with non-malicious intent and cyberattacks.

Corrective Action

If a problem is detected, an immediate alarm is issued, and a set of required actions is provided. The alarm is triggered by deviations in magnetic profile of electrical system that exceed predefined threshold.

THE SECRET INGREDIENT

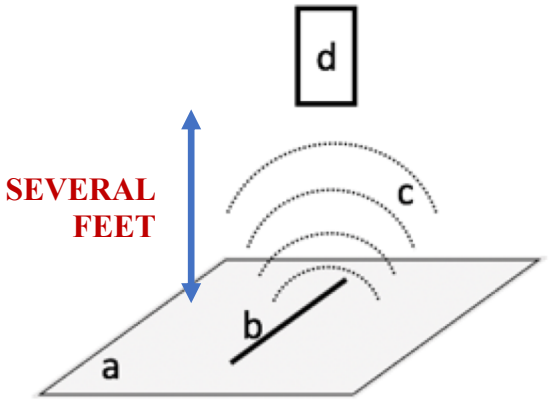
Detection of electric currents with highly-sensitive Atomic Magnetometers and Data Assessment based on ML techniques

Atomic Magnetometers, the most sensitive magnetic sensors, allow for remote (feet away) measurement on electrical circuits and systems

ML is critical in solving the complex problem of magnetic detection and interpretation of the data

Simple case example:

Detection of magnetic field created by a current in a single straight wire

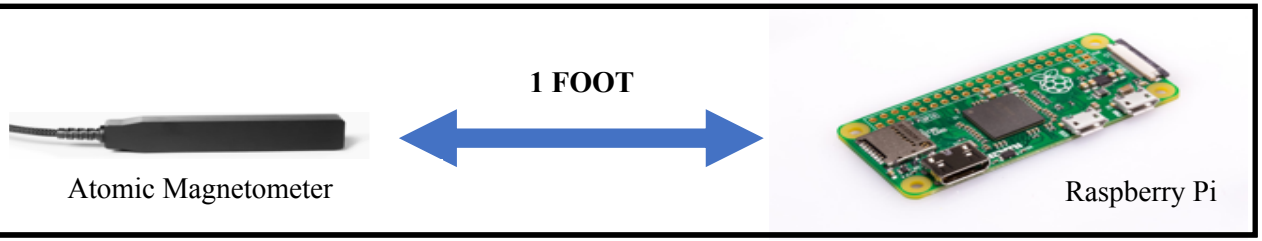


a – *electrical circuit*
b – *wire carrying current*
c – *magnetic field lines*
d – *atomic magnetometer*

SHOW ME THE DATA

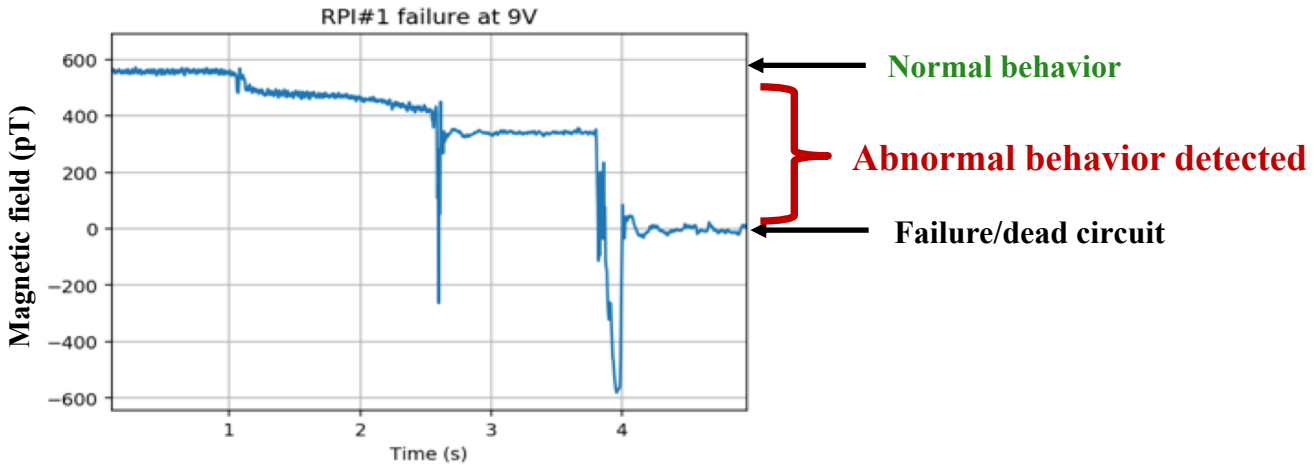
Real-world example: accelerated failure test results

Raspberry PI was forced to operate at a higher than maximum allowable voltage until it ‘burns’.



Setup

We detected remotely abnormal behavior in advance of the failure (“pre-dig-ma-tically”) in a TRUE Predictive Maintenance (PdM) Mode.



Our PdM data

MARKET SIZE

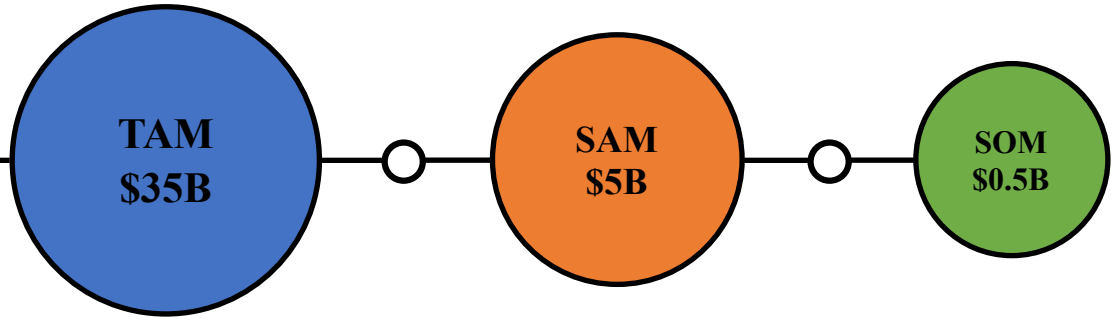
Global production downtime cost is $647B/year*

19% or $123B/year of production downtime is due to electrical failures**

WE ASSUME ~ 30% OF $123B COMING FROM COMPANIES READY TO MITIGATE THE PROBLEM

Predictive Maintenance Market

in reducing production downtime due to electrical failures

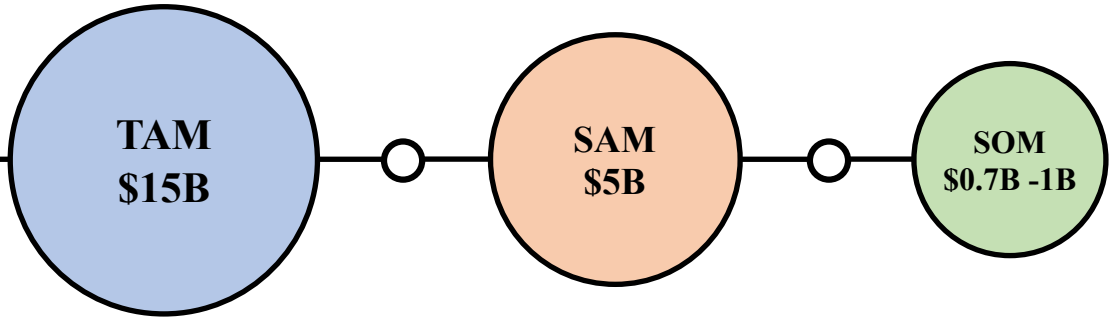


True loss from cyberattacks is hard to estimate due to underreporting

We target a market of ~10K companies which lose on average $5M/attack resulting in total loss of $50B***

WE ASSUME ~ 30% OF $123B COMING FROM COMPANIES READY TO MITIGATE THE PROBLEM

Cyberthreat Detection Market



** https://www.isa.org/standards-publications/isa-publications/intech-magazine/2013/feb/automation-it-predictive-maintenance-embraces-analytics*
*** https://www.gepowerconversion.com/inspire/reducing-unplanned-downtime-predictive-maintenance*
**** https://www.csoonline.com*

July 2019

BUSINESS MODEL: MARKET AND REVENUE

PREDICTIVE MAINTENANCE (PdM) OF ELECTRICAL FAILURE

Average factory loss is at $50M/year due to downtime.

19% or $10M/year of the loss is caused by electrical failures.

We assume a total market of ~10K factories to which we offer PdM service contract at $500K/year.

The result is $5B/year revenue for addressing 100% of the electrical failure PdM market.

As the FIRST PLAYER to provide true PdM solution in non-invasive way, easy to adopt and leading to significant cost savings, we aim to capture 10% market share or $0.5B/year.

CYBERTHREAT DETECTION

Cyberattacks lead not only to significant revenue loss but even worse – betrayed trust in customer loyalty. Total loss for the affected companies is not known due to underreporting.

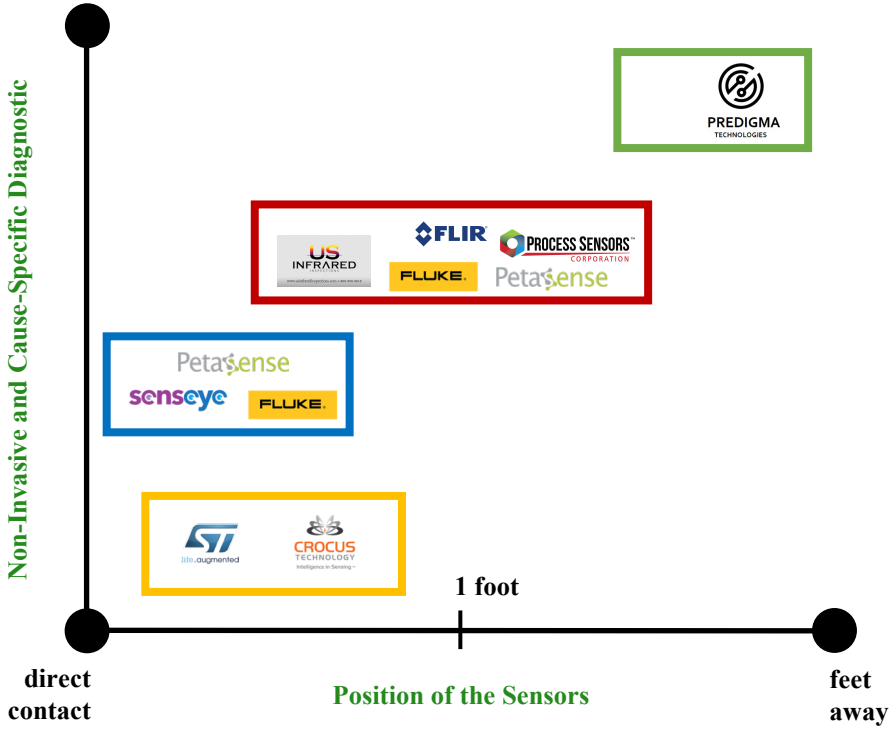
Immediate loss for a company affected by a cyberattack could be estimated at about $5M/event. Many companies suffer from more than one attack per year.

As FIRST TO MARKET in providing hardware-based detection of cyberattacks, we expect to capture 5-7% of TAM ($15B) or $0.7–$1B direct market opportunity.

COMPETITION

PREDIGMA'S TECH is unmatched by any existing technology for **REMOTE**, **NON-INVASIVE** and **CAUSE-SPECIFIC** electronics diagnostics.

PREDIGMA'S ML-based **HARDWARE CYBERSECURITY PLATFORM** has **NO COMPETITION** even on conceptual level.



Atomic magnetometers
remote, non-invasive and specific

Infra-red sensors
remote but non-specific

On-PCB direct sensing wires
specific but invasive; large number required to monitor an entire system

On-PCB solid-state magnetometers
could be specific but invasive; large number required to monitor an entire system

COMPATITIVE ADVANTIGES

FIRST TO MARKET based on

REMOTE measurements – several feet away

NON-INVASIVE and **PASSIVE** operation in listener mode

REAL-TIME PREDICTION of the "Health Status" of industrial electronics

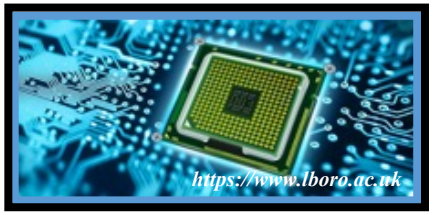
HIGHLY SENSITIVE and **SPECIFIC APPROACH** to failures and intrusions by detection of small deviations from 'normal' behavior

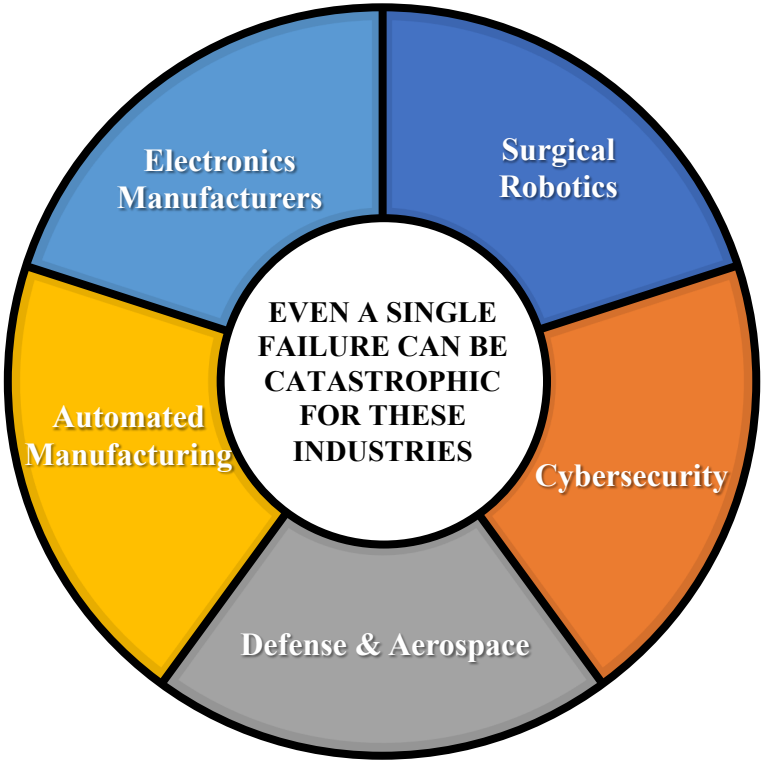
INDEPENDENT OPERATION from the electrical system's software – the main target for cyberattacks

EASY TO ADOPT by the customers – installations are external to customers hardware and software

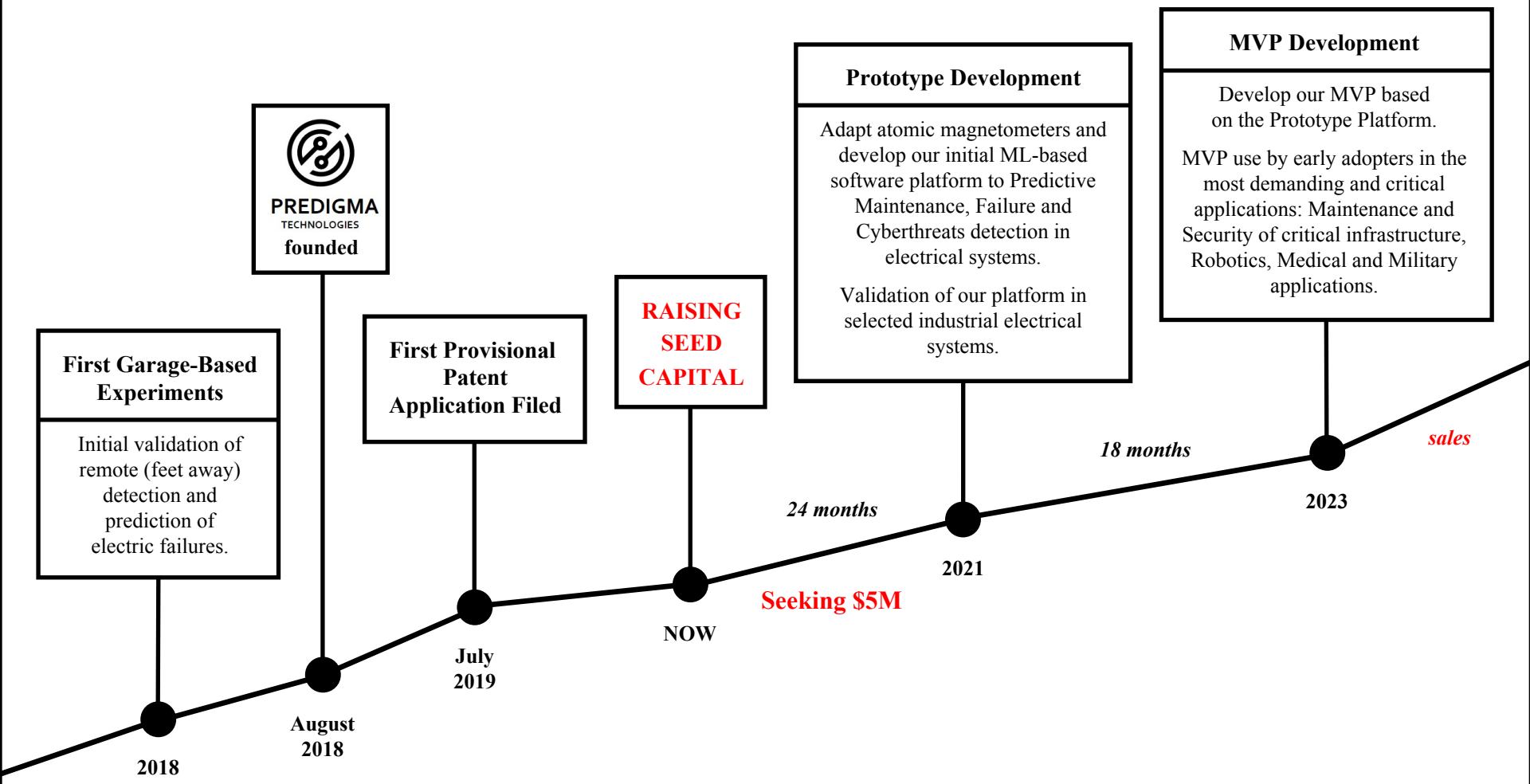
LOW IMPLEMENTATION COST – no disturbance or modification to customer's operation process

POTENTIAL CUSTOMERS





STATUS. TIMELINE. FUNDING



TEAM PREDIGMA

Slava Lebedev, PhD
CEO, co-founder

- Quantum application scientist with 12+ years experience in R&D of novel sensor technologies
- Pioneered various sensors for nuclear forensics' applications
- Developed sensors for remote explosives detection based on Raman spectroscopy

Spectral Sensor Solutions · Los Alamos National Laboratory · UCSB · University of Amsterdam · Leibniz Universität Hannover

Todor Karaulanov, PhD
CTO, co-founder

- 15+ years of experience with quantum magnetic measurements
- Developed a platform for NQR detection of explosives
- Architect of a low-field Medical MRI system
- Developed an early cancer detection platform based on magnetic field measurements

QalibreMD · IMAGION BIOSYSTEMS · Los Alamos National Laboratory · Berkeley

Evgeny Burmistrov, PhD
Director of Engineering

- Developed complex measurement systems with broad data analysis in the cloud
- Triggered number of POCs and converted them into real products
- Experienced in leading development teams with rapid prototyping and precise cost estimations

HARMAN · CROCUS TECHNOLOGY · RENESAS · SPIN MEMORY · Los Alamos National Laboratory · Lomonosov Moscow State University

PREDIGMA

TECHNOLOGIES

reliability and security for dependable electronics

Address:

PO Box 20614
Boulder, CO 80308

Phone:

805.729.2164

Email:

contact@predigma-tech.com

July 2019