==========
==========
تقرير تقييم المخاطر الأمنية والتشغيلية
التصنيف: خاص وسري (Private)
==========
==========

1. مخاطر الاستخدام العكسي (Reverse Engineering Risk):
– الخطر: وقوع الوحدة بيد جهات معادية ومحاولة استنساخ "بصمات التهديد" أو استخدامها كسلاح هجومي.
– الحل التقني: تفعيل "التشفير الذاتي" (Flash Encryption) وحرق الفيوزات (eFuse) لمنع قراءة الكود. تفعيل بروتوكول "التدمير الذاتي للبيانات" عند محاولة الفتح القسري.

2. المخاطر القانونية (Legal Liability):
– الخطر: المساءلة بسبب استخدام "أسلحة صوتية" تسبب أضراراً صحية (دوار، غثيان).
– الحل القانوني: تصنيف الجهاز كـ "معدات بحثية وعسكرية خاصة" (Non-Commercial)، واستخدام بروتوكول التصديق اليدوي (GPIO 33) لنقل المسؤولية القانونية للمشغل البشري عند التفعيل.

3. مخاطر الخطأ التقني (False Positives):
– الخطر: إطلاق هجوم صوتي في مدرسة أو مستشفى بسبب قراءة غاز خاطئة (عطر قوي مثلاً).
– الحل التقني: اعتماد "مصفوفة الثقة" (Confidence Matrix) التي تتطلب تطابق 3 مؤشرات (غاز + رطوبة + تطاير) + الانتظار الزمني (3 ثوانٍ) قبل التفعيل.

4. مخاطر الطاقة (Power Failure):

- الخطر: انقطاع التيار أثناء الهجوم مما يؤدي لتوقف المعالج.
- الحل الهندسي: الاعتماد على "الصومعة الحركية" (وحدة خارجية) بمكثفات مستقلة، وعزل دائرة الذكاء (3.3V) عن دائرة القوة (Amplifier).

==========
==========