Cyber-Physical Component Verification with Global Collision Estimation Through Markov Integration

Henry Gilbert, Ruida Zeng, Michael Sandborn, Jules White, Douglas C. Schmidt
{henry.gilbert, ruida.zeng, michael.sandborn, jules.white, d.schmidt}@vanderbilt.edu
Department of Computer Science
Vanderbilt University, Nashville, USA

***Abstract*—Asserting the provenance of an item is an essential validation in any supply chain process. Unfortunately, counterfeit objects continue to proliferate as these networks grow in size and complexity. Anything from consumer luxury items to safety-critical subsystem components are targeted by counterfeiters. The reliable assertion of an item's origin and build quality remains an open problem that is expected to cost the global economy trillions of dollars (USD) in coming years. [Ghadge et al., 2021]. While institutional economic disparity is a concern, poor quality counterfeits infiltrating mission-critical systems, such as flight controllers, pose a tangible and physical risk to society. To address this issue, we propose a novel approach for detecting counterfeit items using piezoelectric signatures which result from actuating piezoelectric sensors and observing the electromechanical response. We demonstrate that the collision rate (percentage of parts that are counterfeit and probability of part type signal overlap) of piezoelectric signatures can be analytically estimated and tuned in relation to desired parameters such as a minimal false positive rate.**

***Index Terms*—component, verification, cyber-physical, markov estimation**

I. Introduction

Counterfeiting creates a cyber-physical information assurance problem in cyber-physical systems (CPSs). For CPSs, physical parts must meet stringent quality guarantees to ensure safety. When a part integrator is building a CPS, they must ensure that the cyber-information that is expected to correspond to a part (*e.g.*, certifications, tolerances) indeed corresponds to the physical part instance possessed by the integrator.

If a counterfeit part is successfully injected into a supply chain, then the cyber-information regarding the structural quality and certification may no longer hold for a set of parts, and the safety of the system can no longer be verified. Current manufacturing processes rely heavily on a distributed source of external vendors for the manufacturing of key components. An example of this is Boeing outsourcing the manufacturing of two-thirds of the 787 to external parties [Tang et al., 2009]. This manufacturing outsourcing includes safety-critical systems the plane relies on for navigation and flight control.

This segmentation between the producer and end consumer of components creates an environment that is hostile to reliable validation of the authenticity of a given part. The Global Brand Counterfeiting report for the years 2018–2020 has estimated the aggregated losses caused by counterfeiting will exceed 1.82 Trillion USD by the end of 2022 [Butticè et al., 2020]. The potential negative implications of counterfeit goods are compounded in highly regulated industries, such as pharmaceuticals. A recent paper from the journal of global health explores the devastating effects of counterfeit controlled substances [Senyo, 2022]. Specifically, life-saving HIV medication was faked with over-the-counter painkillers attempting to mimic the missing drug.

Traditional verification methods for part validity fall short of provable connections to tie digital information (e.g. database entry) to a physical part instance (e.g. drone propeller, container of medication, etc.). Thus, irrespective of other validation processes, a counterfeit part will always have a non-zero probability of being consumed undetected. Current cyber-security techniques, such as the root of trust or signing chain, are able to definitively ensure the integrity of software systems. However, such methodologies are lacking for proving that information is associated with a physical part.

Past work [Sandborn et al., 2021] addresses this problem with a cyber-physical information assurance mechanism based on building physically unclonable functions by leveraging piezoelectric transducers which act as simultaneous sensors and actuators, converting readily between mechanical and electrical energy, depending on external stimuli (e.g., vibration or voltage source). By semi-permanently attaching a piezoelectric sensor to an arbitrary part or item, the impedance identity or piezoelectric signature can be measured by inducing a vibration that is dissipated over the attached object to create a resulting electromechanical response, a signal that can serve as a type of physically unclonable function. Because of inevitable microstructural variation that is introduced in the process of producing piezoelectric elements (e.g., PZT), we expect that piezoelectric signatures can serve as globally unique and unclonable part instance identities. Essentially, a piezoelectric signature is a serial number for a part that is intrinsic to the part itself and not attached as a sticker, engraving, etc. that can be cloned and attached to another part; a piezoelectric sensor serves as an interface to measure the piezoelectric signature of a part. If the sensor is tampered with or removed, the signature is destroyed and cannot be recovered. These derived identities can be combined with cyber-information by signing with existing public key infrastructures or similar cryptographic primitives. A key unanswered question is how to design a general process that a manufacturer could use

to estimate the level of security realized when applying the piezoelectric signature technique to an arbitrary part.

This paper presents statistical processes to classify arbitrary Piezoelectric signatures to their parent part. As an implicit consequence of the proposed methodology, the classification accuracy for each manufactured part batch can be deterministically derived, and the global collision rate of a part type estimated using Markov Integration. The collision rate is defined as the probability that any two parts of the same type (i.e. category or class) generate signals that correspond to more than one part instance. The higher the probability of collisions, the easier it is for a counterfeiter (in theory) to produce a part that matches the signature of a legitimate part, allowing a counterfeit to be passed through the supply network undetected. This is shown to be the global security of a given part type. Finally, the entirety of the process can be controlled by hyperparameters that can be tuned by the manufacturer and consumer to balance between the desired level of part security and the false positive rate of flagging legitimate parts as counterfeit.

The remainder of the paper is organized as follows: Section II presents a brief introduction of the challenges in designing an Impedance-based identity System; Section III provides an in-depth explanation of the proposed solution process; Section IV includes an exploration of potential industry applications; Section V provides an analysis of the results from our industry example; Section VI provides a broad review of related work; and Section VII provides concluding remarks and lessons learned.

II. Challenges of Designing an Impedance-based Identity System for Arbitrary Part Types

A. Overview of Uncloneable Part Identities with Impedance Identities

The fundamental idea behind our approach is to attach piezoelectric sensors to rigid physical parts and measure the part's electromechanical response to an induced vibration over a range of frequencies. The impedance response value at each frequency in a contiguous interval (e.g. 500 data points) is taken together to form an impedance identity that uniquely identifies the part. Two independent entities can then assert information about the part by creating signed messages that include the part's impedance identity. Assertions can be matched to parts by measuring the unclonable impedance identity and verifying that it matches what is in the signed message.

A key component of the approach is that there are currently no known ways to manufacture a part that will have a desired impedance identity. Impedance identities are fundamentally based on a number of very difficult if not infeasible characteristics of the part and its attached sensor, ranging from microstructural variation in the piezoelectric sensor, adhesive volume and curing pattern, material structure of the part, 3D geometry of the part, etc.

Given the current state of knowledge in piezoelectric sensing and advanced manufacturing, the best case for a counterfeiter is to randomly manufacture identical quality parts to legitimate parts in the hope of randomly colliding with a legitimate part impedance identity. It is important to note that lower-quality counterfeits will inherently create different impedance identities, which forces counterfeiters to try and manufacture at the same quality as legitimate producers, contrary to the incentive to counterfeit (to produce seemingly high-quality components at a low cost). This represents an implicit defense mechanism: the impedance identity reflects the structural state of a quality part, so any deviation from this quality is detectable in the impedance identity.

For example, the manufacturer of a fuel injector for a commercial airplane may record the impedance identity of the part and imbue the physical part with a globally unique serial number. This serial number can then be combined with the impedance identity and signed with a classical cyber-security public key infrastructure so that the receiving consumer can validate the supplied serial number contained in the signed message using a private key. In this scenario, even if an attacker is able to obtain the original part parameters and the supplied serial number, they cannot obtain the same piezoelectric sensor instance that was originally attached to an authentic part of interest, and consequently cannot produce an identical impedance identity without the original, authentic component along with its corresponding sensor. In this way, there is a steep cost to an attacker to even produce similar impedance identities. The piezoelectric element and the component of interest must be carefully chosen to align with the original; we anticipate that the physical resources and time needed to achieve this alone incur a cost high enough to thwart counterfeit attempts for certain parts.

With the paper's proposed solution, a globally unique signal could be derived for the part and sent to the consumer along with the necessary parameters to classify signals from said part. This information could theoretically be made publicly available as an attacker has no way of creating a part that perfectly matches the original. Even given the underlying distribution of the original part's signals, the attacker cannot reverse the needed geometric features to produce a distribution of signals indistinguishable from the original. As the measured signal is fundamentally a 3D representation of an object projected into 2D, there is implicit information loss and noise injection with the information reduction. Thus, given the loss of perfect information, the originating 3D representation can not be ascertained.

B. Manufacturer Difficulties

This section outlines the underlying difficulties in estimating the probability that an attacker can randomly manufacture a counterfeit part that is accepted as legitimate. The underlying manufacturing process is assumed to produce a certain part type in batches of arbitrary size. For each part that a manufacturer produces, the impedance identity is measured using preselected parameters and serves as a unique cyber-physical part identifier. Assuming the identifiers are globally unique, this impedance identity can be used as a validation technique when

the consumer receives the part. This is conceptually similar to stamping parts with serial numbers, and the consumer of a part verifying the received the correct batch of serial numbers.

Thus, the problem becomes: how can we measure a part with enough information density to capture the minute differences that make every part globally unique? Then, given these measurements, how can we create a system in which counterfeit parts have a near-zero probability of being incorrectly identified as authentic? The measurement of a part's impedance identity is made possible by the piezoelectric sensor, and the technique of measuring electromechanical impedance response for parts was previously explored in [Sandborn et al., 2021]. If we can assert that a signal from a piezoelectric sensor is globally unique, the naïve solution is to simply have a central store of all authentic parts and their associated signal measurements. As the measurements are globally unique, when a counterfeit part is measured, its signal would not exist in the central store of authentic signals, and it would be correctly rejected as counterfeit.

The fundamental difficulty of part verification can be abstracted into a manufacturing process m, part type t, batch of parts t_b and a single part p. A manufacturing process would represent the entirety of the work required to generate a single part. It is assumed that for a given part type t, the manufacturing process m, is consistent across all manufactured parts of t. While all individual parts of part type t would have been created under a consistent manufacturing process, no two parts will ever be the exact same. As micro inconsistencies are introduced into the part through non-perfect manufacturing methods, each resulting part is theoretically uniquely identifiable. The core assumption of this work is that the information density contained in a Piezo signal measurement is high enough to capture these micro-inconsistencies that can be used to differentiate parts from the same manufacturing process.

C. Impedance Identity Matching & Measurement Noise

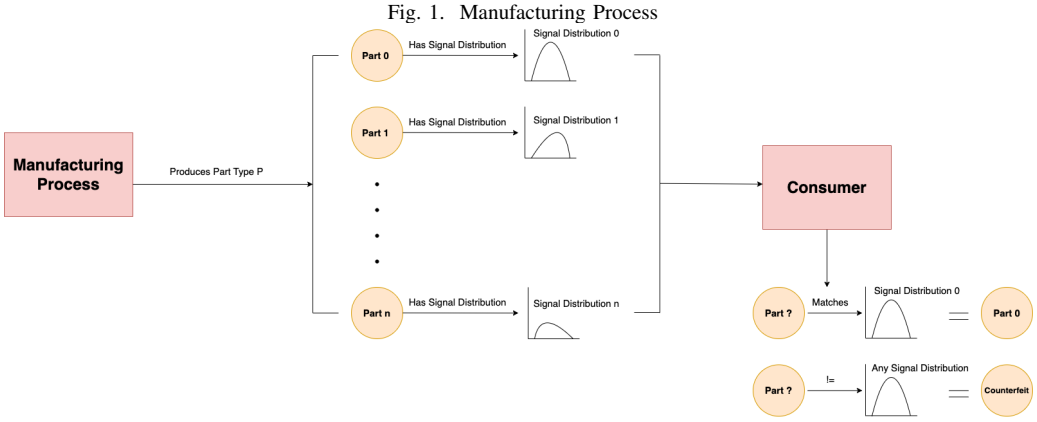
Unfortunately, electromechanical impedance measurements enabled by piezoelectric sensors are non-deterministic and vary minutely between any two measurements of the same part-sensor pair owing to ambient environment factors such as humidity, air pressure, and temperature.

Naturally, the measurements over the same part will be similar, but never exactly the same. As some level of randomness is now introduced into the measurements, any subsequent classification system to differentiate between authentic and counterfeit parts will sacrifice the global uniqueness of the impedance identities. As the randomness is unknown, and could theoretically cause two otherwise unique signals to overlap, any classification model must optimize the trade-off between false negatives and false positives. Specifically, the tighter the classification bounds are for a given signal, the more often correct signals will be misclassified as introduced randomness causes them to fall outside of the given bounds. Conversely, if classification thresholds are too wide, then the introduced randomness could cause two different signals to overlap, with one or both being misclassified. We define a $collision$ as the misclassification of a signal caused by innate randomness. Specifically, a single signal of a part being classified as derived from a different part. Thus, for a given part type, the probability that two different parts will yield a similar enough signal to be classified as the same part is the same as the collision rate of the system. With the 'system' being defined as all potential produced parts of a given part type. Naturally, as the number of the produced parts in a given system increases, so does the resulting system collision rate. As the number of produced parts approaches infinity, the system collision rate will approach 1 (100%). This will represent the combined entropy of a given part type's signals, and serve as an upper bound for downstream processes to accurately differentiate between authentic and counterfeit parts.

A potential solution to this would be a fuzzy matching algorithm that can handle the variance in signals that were introduced by external factors. Categorically classifying signals with limited variance is a trivial problem for most machine learning models. As such, a simple fuzzy matching algorithm would likely perform well and achieve a high accuracy score. However, while this solution is simple, it lacks interpretability. One will not be able to ascertain the underlying collision rate of a given part type or the expected performance of the model on out-of-sample signals. An out-of-sample signal is defined as a novel signal that the trained model has not seen before. The model may achieve a 98% accuracy on the given data, but how is that accuracy affected when unseen signals are introduced? Thus, simply using fuzzy-matching or any machine learning model to learn the classification will obscure the underlying collision rate of a given part type, and downstream use of the model will be unable to verify the model's performance on unseen signals.

The proposed approach will only analyze the use of piezoelectric sensors for part differentiation within a batch of parts, where each part is of the same part type, and each part was produced with the same manufacturing process. We assert that this is the upper bound for validating the proposed process. With this assertion, we are making the assumption that any deviation in the manufacturing process will always increase the variance of the resulting signals compared to the original process. Specifically, if we are able to accurately differentiate between parts of the same type, then the computed collision rate for the part type is the global upper bound. Any deviation from the original manufacturing process would increase the signal's variance and subsequently could not result in a higher collision rate. This is maintained using the above proven assumption that the original manufacturing process is the upper-bound on estimated system collision rates.

Fig. 1. Manufacturing Process



III. Proposed Process

A. Process Architecture

Each process will pertain specifically to a single batch of parts produced with a given manufacturing process. Figure 2 shows that for each batch of parts, the individual part's probability density function will be estimated using the given hyperparameters. Once all of the individual PDFs for each part instance in the batch have been derived, the meta PDF pertaining to all possible signals for a given part type will be estimated. Each individual PDF is derived by estimating the underlying distribution a part's signal is sampled from. All distributions are estimated by scaling the observed covariance in relation to the observed sampled variance proportionate to the sample size. Reference 2 for the specific formulation.

This meta PDF will be used to sample example possible signals during a Markov Simulation to estimate the collision rate for the given batch of parts. In the context of manufacturing, the producer could derive the estimated security of a given batch of parts from each part's micro-physical discrepancies, derived from the variation in manufacturing process for each part produced.

B. Part Data

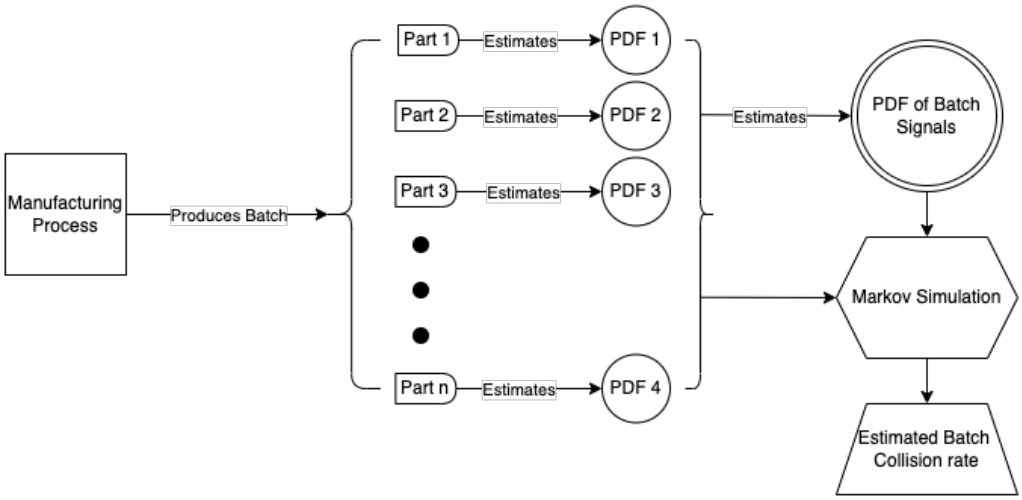
For a given part type, we will have a batch of parts of which we wish to both estimate the collision rate and derive a classification model at a desired false negative rate. The part batch represents a set of parts produced via the same manufacturing process. A concrete example of this would be a batch of 1000 GPSs produced to order. Each measured signal is the concatenation of real-valued floats recorded from a prescribed range of frequencies. Specifically, the current implementation uses frequencies in the range 10kHz-150lHz with a step size of 280, resulting in a list of 500 electromechanical impedance response values for each measurement. The part's response to a frequency depends partially on environmental factors, such as ambient vibrations. Each frequency in the given range is measured directly after the previous frequency with no break period for the previous vibrations to fully disperse. As such, measurement n is iteratively conditioned on measurements $0, \cdots, n-1$. This is acceptable as it increases the information density of the cumulative set of 500 signals. Moving forward, a part's *impedance identity* refers to this series of 500 pairs containing (frequency, response) pairs, ordered by increasing frequency.

In the Individual Part PDF estimation section, each part's set of signal measurements will be used to estimate the part's underlying PDF. As such, the measured signals from a part must be independent. To ensure this, a waiting period of one minute was enforced between subsequent measurements of a part. The waiting period allows any previously inflicted vibrations to fully disperse such that they will not affect future measurements (known as "ring down" time between measurements in the literature).

C. Individual Part PDF Estimation

This section describes how to estimate the underlying distribution from which a single part's signals are theoretically sampled. If a part's probability density function (PDF) can be accurately derived, then any novel signal can be classified against a given part by the probability it was sampled from the part's derived distribution. Whether the estimated part PDF's function is an accurate representation of the global PDF is dictated by the observed variance in the sampled signals in relation to the number of signals sampled. As this process proposed continually sampling signals until convergence, we can assert the accuracy of the estimated PDF. Naturally, a PDF integrates to 1, and every possible signal would have a non-zero probability of being derived from the PDF. To account for this, the concept of confidence bounds will be introduced. A confidence bound is the minimum probability required to classify a signal as coming from a given distribution. For example, we can require a confidence bound of 95%, meaning signal s, would need to have at least a 5% probability of being sampled from the distribution to be classified as a part's signal. As we will explore in subsequent sections, the confidence bound is a hyperparameter to balance false negatives and false positives to a desired amount, for a given part type. This is a key consequence of the proposed process that allows a manufacturer to explicitly set the batch's security (collision

Fig. 2. Proposed Process Architecture



rate) based on hyperparameters that can be theoretically given by the consumer.

As previously explained, a non-trivial amount of variance is introduced into each measurement of a part's signal. Thus, a single signal measurement for a given part is not enough to classify a new signal as coming from the given part. Rather, we can estimate the underlying PDF function of all possible signals for a specific part. Assuming the Central Limit Theorem [Kwak and Kim, 2017] applies, the PDF of a part instance will converge to a Gaussian distribution as the number of samples increases. However, as we can not take infinitely many samples for a part's signals, we must estimate the underlying distribution from a sample population. Whilst doing so, we will also account for the relative certainty of our estimated distribution using confidence intervals (CI) 1

Fig. 3. Confidence Interval Equation

$$CI = \bar{x} \pm z\frac{s}{\sqrt{n}} \tag{1}$$

With sample mean $\bar{x}$, confidence level z, sample standard deviation s, and sample count n. Note that z is a hyperparameter for the part PDF estimation process.

When given a small number of samples, the CI range would be large as the confidence for the true population's mean given the sampled mean would be low. As the number of samples increases, the CI range will correspondingly decrease as it approaches the estimation of the true population mean. Referencing the CI equations 1, the number of samples given is used to scale the projected variance for the estimated mean. Given this process is implemented by the manufacturer, two questions must now be answered:

- How small should the CI range be? - How many samples are needed to reach a desired CI range?

As the CI is fundamentally a reflection of the inherent variance in the data set, one cannot assert the desired CI range. There exists an upper limit on the shrinkage of said CI range that can only be derived from the covariance of the underlying and unknown distribution. As the ideal CI cannot be computed, then computing the needed number of samples is also intractable.

While we cannot analytically derive the optimal CI values, we can iteratively sample from the underlying distribution until a convergence of the CI ranges. Convergence of the CI being defined as the average variance of the most recent 10 samples being equal to or less than the average variance of the previous 100. To sample a part's underlying distribution, one merely takes an additional signal measurement. Thus, measurements for a part can continually be added to a growing set until the estimated CI range has converged to the theoretical upper limit based on the total population's inherent covariance. Figure 4 displays python code that implements the ideas described here.

In this example, each part starts with no previous measurements for the given manufactured part. We then continually take measurements and record the CI of the growing set. Convergence is not checked until at least 100 samples have been taken. This is done for two reasons: firstly, it allows the assumption of a normal distribution. Following conventional practice [Kim and Park, 2019], a student-t distribution would be used for subpopulations of less than 30 samples. Secondly, it makes the convergence estimation more robust and less likely to prematurely conclude convergence on a local minimum. For every sample after 100, the mean of the CI ranges from the previous 10 samples is compared to the mean of the previous 100 samples. Comparing the most recent 10 samples against the previous 100 are arbitrary hyperparameters. Under the assumption that one needs 30 or more samples for a representative Gaussian distribution, the number of samples need only be greater than 30 before convergence can be checked. Lowering the subset of samples to check would increase the variance in the number of iterations required

```
part_samples = []
ci_ranges = []
while True:

   new_part_sample = take_new_part_measurement()
   part_samples.append(new_part_sample)

   lower_ci, upper_ci = compute_ci_ranges(part_samples, supplied_confidence_bound)
   ci_ranges.append(upper_ci - lower_ci)

   if (len(ci_ranges) > 100 and
          np.mean(confidence_ranges[-10:]) >= np.mean(confidence_ranges[-100:])):
       return upper, lower
```

Fig. 4. Example Convergence Algorithm

for convergence as as the likelihood of the sample being representative will decrease.

If the mean of the most recent 10 samples has not decreased in comparison with the mean of the most recent 100 samples, we assume convergence and return the upper and lower bound of the computed CI. In practice, this will result in an adaptable process where signals will be continually measured for each part until the estimated part PDF has stabilized, allowing for a higher level of confidence in the overall estimated system collision rate.

The returned upper and lower bound estimation represent the mean of the underlying distribution for a given part's signals at the supplied confidence z. The covariance of the underlying distribution can be computed using Equation 2

Fig. 5. Deriving Covariance

$$cov = \frac{\sqrt{n}(upperlimit - lowerlimit)}{z_\gamma} \tag{2}$$

Once again, n represents the size of the sub population sample and z_γ the quantile derived assuming a Gaussian distribution. This assumption is valid as the convergence algorithm enforces a minimum sample size of 100, allowing the use of a normal distribution [Kim and Park, 2019].

Finally, using μ as the mean of signals values from the sub-population and Σ as the above computed covariance, the underlying distribution for a part's signals can be estimated using a Gaussian probability density function 3.

Fig. 6. Gaussian Probability Density Function

$$f(x) = \frac{1}{\sum\sqrt{2\pi}} exp[-\frac{(x-\mu)^2}{2\Sigma}] \tag{3}$$

Specifically, μ is a set of means for each measured point as such: $\mu = \{\mu_1, \mu_2, \mu_3 \ldots, \mu_{500}\}$ and Σ is the covariance matrix for each measured point as outlined in 4.

Fig. 7. Example Part Covariance

$$\sum = \begin{bmatrix} \sigma^2_{1,1} & \sigma_{1,2} & \cdots & \sigma_{1,500} \\ \sigma_{2,1} & \sigma^2_{2,2} & \cdots & \sigma_{2,500} \\ \cdots & \cdots & \cdots & \cdots \\ \sigma_{500,1} & \sigma_{500,2} & \cdots & \sigma^2_{500,500} \end{bmatrix} \tag{4}$$

Therefore, for a given part p, a corresponding PDF of the form $\mathcal{N}_p(\mu_p, \Sigma_p)$, at the supplied confidence z, can be constructed.

D. Part Classification

For each part in the batch of parts of a given manufacturing process, the corresponding PDF function will be estimated. Thus, each batch of parts will have a set of part PDFs as defined in 5.

Fig. 8. Batch PDF Set

$$P = \{\mathcal{N}_p(\mu_p, \Sigma_p) |\ \forall p \in P\} \tag{5}$$

A naïve solution for classifying a new signal s_*, would be to predict the part where s_* had the highest probability of being sampled from the part's PDF. If the set of parts P represented the entire set of all possible parts, this would be a valid solution. However, this does not account for the potential of a counterfeit part and its subsequent unknown

signal. As all PDFs integrate to 1, any signal has a non-zero probability of being derived from every PDF. Thus, even if the counterfeit was particularly poor, and the associated signal, multiple standard deviations away from any part in P, would still be classified as the part with the highest probability, even if said probability was near 0.

Clearly, there is a need to implement a cutoff point on classifications. The proposed solution is the aforementioned confidence bound. For any set of part PDFs P, a hyperparameter cb can be supplied to enforce a minimum needed probability to classify a signal against a distribution. As such the classification process for unknown signal s_* becomes the equation seen in 6.

Fig. 9. Unknown Signal Classification

$$s_* \sim \mathcal{N}(\mu_p, \Sigma_p) \quad iff. \quad \mathcal{P}[s_* \sim \mathcal{N}(\mu_{p_*}, \Sigma_{p_*})] \geq 1 - cb \tag{6}$$

Signal s_* will only be classified as a given part if the probability the signal came from the part's distribution is greater than $1 - the\ supplied\ cb$. For example, given a cb of 0.9, a signal's probability of being sampled from a given distribution would need to be greater than $1 - 0.9 = 0.1$. Thus, if signal s_* does not meet the minimum probability constraints for any of the part's distribution, it is assumed to be a counterfeit. If signal s_* matches more than one of the part's distributions, then this is a collision and will be handled in Collision Estimation. The underlying assumption of the entire process is explicitly outlined in 7.

Fig. 10. Process Assumption

$$\forall p \in P, \mathcal{P}[s_c \sim \mathcal{N}(\mu_p, \Sigma_p)] \ggg 1 - cb \tag{7}$$

Specifically, the meta distribution comprising individual part instances' distributions has very high entropy. This can be attributed to the extremely high fidelity of measurement for each part's impedance identity. As such, the resulting theoretical distribution that part signals are sampled from has an extremely large system entropy. Thus, the probability that any two randomly sampled part distributions overlap to the point of a collision should approach 0 as the magnitude of signal measurements increases.

The supplied confidence bound directly affects the classification model's ability to generalize across unknown samples. Given a lower confidence bound, the model would require a higher level of certainty that a sample came from a distribution before classifying the signals. Conversely, given a higher confidence bound, the model would require a lower level of certainty to predict a distribution for a given signal. Allowing a lower level of certainty would decrease the model's false negative rate as it would capture more outliers in a signal's distribution. However, it would also increase the probability a signal would be incorrectly matched against multiple part PDFs. Thus, increasing the supplied cb decreases false negatives, but increases false positives. Decreasing the supplied cb increases false negatives and decreases false positives.

A final point must be made on the derivation of the probability a sample came from a given distribution. Given that each PDF is a continuous multivariate normal distribution, computing $PDF\ \ f_p(s_*)$ would yield the probability density at location s_*, not the probability that s_* was sampled from $PDF\ \ f_p(s_*)$. To compute the probability of $s_* \sim \mathcal{N}(\mu_p, \Sigma_p)$ we can do as follows.

Assuming the set of all data points y that are less likely than s_* are the ones that a lower density and a higher Mahalanobis distance, then the following inequality holds 8.

Thus, for some unseen Y we would like the probability of observing it to be greater than the probability of observing s_*. Resulting in the following derivation 9.

When used in a concrete setting, this solution becomes a trivial implementation of a single function to be computed. The consumer will be provided the manufactured batch of parts, along with the manufacturer's estimated PDF for each of the parts. To validate the authenticity of each part, the consumer simply measures the part's signal before computing the probability that the signal came from each of the supplied part PDFs. Given the chosen confidence bound, the set of part PDFs will not infinitely overlap, and a single part PDF should be matched. The percentage of real part's that are classified as counterfeit should converge to the derived false negative rate of the part batch. Similarly, the percentage of counterfeit parts that are incorrectly classified as authentic will converge to the estimated system collision rate. This will be explicitly derived in the subsequent section.

E. Collision Estimation

As briefly analyzed in the above section, when using a set of part PDFs to classify a novel signal, there exists a potential for a signal to be classified as multiple parts due to an internal collision. Without confidence bounds, all part PDFs are infinitely overlapping to some degree. Enforcing a confidence bound truncates the tails of each part's PDFs and ideally creates a system in which no PDFs overlap at all. However, as shown in the Part PDF estimation section, the hyperparameter confidence bound directly controls the entropy of a part's PDF and subsequently dictates the systems collision rate. A higher confidence bounds allows less of the PDF's tails to be truncated, increasing the probability that a PDF will overlap with another PDF. Conversely, a small confidence bound increases the amount of the PDF that is truncated,

Fig. 11. Unobserved Signal Probability Inequality

$$
\begin{aligned}
(2\pi)^{-\frac{k}{2}}|\Sigma_p|^{-\frac{1}{2}}exp[-\frac{1}{2}(y-\mu_p)^T\Sigma_p^{-1}y-\mu_p)] \leq \\
(2\pi)^{-\frac{k}{2}}|\Sigma_p|^{-\frac{1}{2}}exp[-\frac{1}{2}(s_*-\mu_p)^T\Sigma_p^{-1}(s_*-\mu_p)] \\
\leftrightarrow \\
(y-\mu_p)^T\Sigma_p^{-1}(y-\mu_p) \geq (s_*-\mu_p)^T\Sigma_p^{-1}(s_*-\mu_p)
\end{aligned}
\tag{8}
$$

Fig. 12. Probability of Observation

$$
\begin{aligned}
\mathcal{Q} &= (Y-\mu_p)^T\sum_{p}^{-1}(Y-\mu_p) \\
\mathcal{Q} &\sim \int_*^2(k) \\
\mathcal{P}[(y-\mu_p)^T\Sigma_p^{-1}(y-\mu_p) \geq (s_*-\mu_p)^T\Sigma_p^{-1}(s_*-\mu_p)] &= 1-\mathcal{P}[\mathcal{Q} \leq (s_*-\mu_p)^T\Sigma_p^{-1}(s_*-\mu_p)]
\end{aligned}
\tag{9}
$$

decreasing the probability that a PDF will overlap with another PDF.

Given batch $S = \{\mathcal{N}(\mu_p, \Sigma_p) : p \in P\}$ of generated PDF functions for each part, we would like to find the expected collision rate of this system at the given hyperparameters. As shown in the Problem Setup section, the collision rate of a batch represents the upper bound on the model's ability to distinguish against counterfeit parts. Specifically, the upper bound is the probability that any new part p produced from the same manufacturing process would result in a PDF that overlaps with any other PDF, increasing the systems collision rate. As any deviation in the manufacturing process would increase the resulting relative variance of the signal in relation to the original manufacturing process, it will never increase computed collision rate.

The estimation of the system's collision will be computed on the batch level. Assuming the total number of batches for a part is unknown, it can theoretically be continual and approach infinity. While perhaps not realistic, it illustrates that a continually produced part will eventually converge to a 100% collision rate as every potential part PDF is generated. As such, batches will be assumed to be independent and the relative security of each batch will be computed individually.

Fundamentally, the collision rate of a system of PDFs is merely the overlap of all given PDFs, or the overlap coefficient. Broadly, it's the probability that two randomly sampled points from two PDFs are the same. While computing the overlap coefficient is a trivial problem for univariate Gaussian distributions, the problem becomes intractable when considering the Part PDF is a multivariate Gaussian distribution of dimensionality 500. On a high-level, computing the overlap is a series of partial-differential equations to estimate the area of of overlap of each dimension across every other dimension.

Other similarity metrics for comparing two multivariate distribution do exist, such as the KL-Divergence 10. These metrics provide a scaler to indicate similarity, which is useful for relative comparisons between distributions, but we are not able to derive the concrete probability of a system's overlap.

Fig. 13. Kullback-Leibler Divergence

$$
D_{KL}(P|Q) = \sum_{x \in X} P(x)log(\frac{P(X)}{Q(x)}) \tag{10}
$$

As an analytical solution does not exist for for computing the overlap coefficient of our part PDFs, we can reconstruct the problem into one similar to estimating the area under the curve for every part PDF against every other part PDF. Once again, an analytical solution is unable to be derived; however, we can estimate the solution using Monte Carlo Simulation. Specifically, for a set of signals, we will classify each using the above defined Signal Classification Process. A signal is allowed to not match any distribution as that represents a counterfeit part, or a part that is outside of the given batch. However, if a signal is classified as more than one distribution, then this is deemed as a collision. Thus, over a large enough sample, the relative ration of collided signals will converge to an estimation of the true system collision rate.

For the Monte Carlo Simulation to valid, the set of signals used to estimate the collision rate must be both large enough to converge to the true value, and representative of all potential signals for the given part type. Once again, as we are asserting that the collision rate for a given batch of parts is the upper bound of all potential collision rates, even with counterfeit. Sampling from a randomly generated normal distribution could be deemed unrepresentative. A normal distribution of signals would be indicative of the system collision rate when

compared against all possible counterfeit parts and other part types. Another potential solution would be to merely derive samples from the already computed part PDFs. This would estimate the collision rate of the current batch, but would fail to account for external part signals generated by another batch or by a counterfeit part. Both the counterfeit part and external batch signal would be derived from a novel distribution that was not considered in the original collision estimation.

Thus, to truly establish an upper bound on system collision, we would like to derive samples from a state space with the assumption it exists within a malicious environment where any signal could be counterfeit. Thus, we will instead sample from the underlying distribution of part PDFs for a given part type. Sampling from said distribution would yield a signal derived from any possible produced part for the given manufacturing process and part type. This concretely establishes the upper bound on system collision as it is the most confined case. The distribution should be representative of the given part PDFs, such that each part PDF has a proportional probability to have been derived from said distribution. Thus, signals sampled from the distribution would have the highest likelihood of causing an overlap in the set of Part PDFs, when compared to counterfeit parts or other part types as their signal would be derived from a fundamentally different distribution.

To estimate this meta distribution of potential part signals, the same process as outlined in Part PDF Estimation will be used. Specifically, all signals from all parts will be grouped together to form a single meta sub population. This is representative of the possible signals for all given PDFs and the resulting distribution would have the lowest possible entropy, enforcing the upper bound assertion. Similar the part PDFs, we must recognize that the given sub population is merely a sample of all possible signals, and as such, a confidence interval z_m will be supplied for the computation of the distributions covariance. Unfortunately, as the part signals have already been measured, the same CI convergence methodology can not be used to ensure minimal variance is introduced.

A Markov Simulation is ran over k samples, with the results being averaged and used as the estimation of the true value. Some relative metrics exist for determining the correct number of samples to take [Siekmann et al., 2011]; however, each is dependent on the relative variance found in the data set. As we recognize our data set is merely a sample from the underlying true distribution, such methods would be a underestimation of the needed number of samples. To ensure an appropriate number of runs are being performed, a similar convergence algorithm to the Part PDF Estimation can be used. Specifically, we will use a base value of 1000 sample for each run of the Markov Simulation. We will run the Markov Simulation iteratively, storing the estimated system collision rate each time. The range for a given confidence interval over the total set of estimated system collision rates will be computed after each run as well. Once a minimum of 100 runs have been completed, convergence will be checked at each iteration using the same methodology as specified in the Part PDF Estimation. Once convergence has been reached, the upper bound estimate of the system collision rate will be returned. Thus, resulting in an estimated system collision rate given part PDF confidence z_p, meta PDF confidence z_m and the collision rate confidence z_c.

As an indirect consequence of classifying part signals using an estimate PDF, both the systems collision rate and batch accuracy can concretely be estimated for future unknown signals. The supplied confidence z_p can be tuned to control the system's false negative and false positive rate. As outlined previously, there exists a negative correlation between the confidence and the systems false positive rate. Conversely there is a positive correlation between the supplied part confidence and the systems false negative rate. Both of which are analyzed and displayed in Results. Similarly, the same relationships exist between the supplied part confidence and the resulting estimated system collision. Given a lower confidence value, the barrier for classification is increased, resulting in a lower collision rate. Correspondingly, a higher confidence value increases the probability a random sample will be classified, increasing the system's collision rate. Finally, a positive correlation exists between the supplied meta confidence and the systems estimated collision rate. As the meta confidence approach 1, no additional variance is introduced into the distribution and it will converge to exactly reflect the set of part distributions. Thus, converging on the estimated accuracy of the process over the supplied part batch. Example usage of these relationships will be outlined in the subsequent section.

IV. Industry Application

A. Process Benifits

The application of signal processing for security has already been analyzed in the previous work done by Sandborn et al. [Sandborn et al., 2021]. The true novel value of the proposed process is two fold: firstly, the estimated system collision rate (security) and classification accuracy over an unknown set of signals can be concretely derived and proven to be the upper bound. Secondly, the proposed process implements key parameters as tuneable hyperparameters. Specifically, the part confidence, meta distribution confidence and part confidence bound can be controlled. As outlined in the above sections, these parameters can be controlled in direct relation to the resulting accuracy of batch classification and estimated system collision rate.

Thus, a manufacturer and consumer can work together to derive a target collision rate and classification accuracy rate for a given product. Regardless of the innate product values that may initially dictate such values, the producer can tune the aforementioned parameters to meet the required specifications. Therefore, the process can not only explicitly derive the system's accuracy and collision rate, but it allows for them to be controlled and manipulated.

Furthermore, this paper asserts the Piezo's signal measurement is a strong physically unclonable function and can be used for the generation of globally unique keys. The collision rate of a given part type within a supplied batch is analytically estimated and as it represents the collision rate between

the same part type of the same manufacturing process, the collision rate is independent to any malicious actors. This is because we've shown that the estimated collision rate from a given manufacturing process is the upper bound on the part's security. Any additional counterfeit parts injected into the part ecosystem would not increase the estimated collision rate as the counterfeit part's misclassification rate would exist significantly under the true part's misclassification rate. As such, solely deriving the part's estimated Gaussian distribution is the only validation and verification a manufacturing process would need. One could even argue they resulting derived multivariate distribution can be made public knowledge without consequence to the resulting validation rate of the part. The estimated multivariate distribution is a mere projection of the derived 3D latent space, as measured by the sensor, into an arbitrary n-dimensional latent representation. Given the original parts signal distribution, to produce a counterfeit with the ability of being misclassified, a malicious actor must be able to do two things. Firstly, they must derive the exact geometry of the original shape, down to the microscopic imperfections, from the n-dimensional distribution. As there is implicit information loss when projecting the 3D representation into a n-dimensional signal, this is fundamentally impossible. Even assuming a malicious actor somehow had perfect information of the original part, perhaps it was intercepted, they would still have to be able to dynamically manufacture a part that so closely mimicked the original, the derived signal distributions would be same. The original manufacturing process produces the same exact part with enough variance that even parts of the same batch will most likely have a zero collision rate. Thus, the counterfeiter would have to achieve a exponentially higher level of manufacturing consistency than the what produced the original part. If that were to theoretically happen, perhaps one could argue the original now becomes the counterfeit. Or, more concretely, this demonstrates the cost of circumventing the proposed process is exponentially higher than the value of any derived counterfeit.

B. Potential Constraints

The key requirement of this entire process is the ability to derive a part's signal using a Piezo electrical signal. Due to the aforementioned sensitivity in measurement, the Piezo sensor must be attached to a given part using a temporary adhesive. This is required as the sensor will output fundamentally different signal distributions relative to it's placement on a physical object. This unfortunately introduces two constraints into the productionisation of this process. Firstly, the item must be large enough to support the attachment of a Piezo senor. Each sensor measures roughly half an inch in diameter, so a prospective item must contain a flat surface at least 0.5^2 $inches$ in area. Additionally, each Piezo sensor must bought and attached to the item. Thus, the combined cost of sensors and the required labour to attach them must be significantly less than the item's value and potential loss of revenue due to counterfeiting.

The proposed process offers a robust solution to a variety of manufacturing environments. One must note that size and value constraints must be met to ensure a net economical gain from the implementation of the process.

V. Results

A. Part Signal PDF Convergence

The first step in the proposed solution is estimated the probability density function for each part. As previously explained in the Problem Setup section, the measurement derived from the Piezo electric sensor is theoretically deterministic. It is measuring the physical structure of the given part and creating a high fidelity 2D representation of the 3D object. While perhaps deterministic when measured in a vacuum, the sensor is, unfortunately, highly sensitive to external environmental factors such as humidity, altitude, temperature or any other physical unknown unknown that exists within the measuring environment. Thus, an non-deterministic amount of variance is introduced into the measurement process, and a single signal measurement from a part may not be representative of the range of signals the part would produce in varying environmental conditions. Thus, the underlying distribution that a part's signals are theoretically sampled from is instead estimated and used in subsequent analysis to parameterize a given part.

As outlined in the Individual Part PDF Estimation, a convergence algorithm is implemented to monitor the continual measurement of the part. As one can not dictate how many samples are needed to accurately derive the underlying distribution, we propose this process become a dynamic control sequence. Once the algorithm has dictated that the estimated PDF has converged, no more samples are required. While this should ideally be a fairly static process across parameterization, we must recognize that it introduces an external source of bias into our underlying process. As such, this experiment aims to understand the variance introduced by the convergence algorithm, and specifically, how consistent is the estimated number required samples.

To perform this analysis, we would like to be able to provide examples signals for each part to get an accurate estimate of the average number of required sampled. However, this experiment is restrained by the limited number of signal samples we have for each part. To artificially compensate for this, we first estimate the underlying distribution of part signals for a given part. Then infinitely sample from the derived distribution until convergence. It is true using the estimated distributions to estimate the convergence of the estimated distribution contains cyclic dependencies and non-trivial levels of variance are introduced into the results because of this. However, sampling from a high-entropy estimated distribution will only increase the number of samples the process needs for convergence. Thus, while not ideal, this establishes an upper bound on the average expected number of needed samples.

Given the only parameter that affects the part PDF, part PDF $confidence\ interval$, is applied after the values are initially estimated, this experiment does not need to be run across a

series of potential hyperparameters. Rather, each part type is run until convergence 100 times with the number of samples needed recorded for each run.

Fig. 14. Sample Convergence Analysis

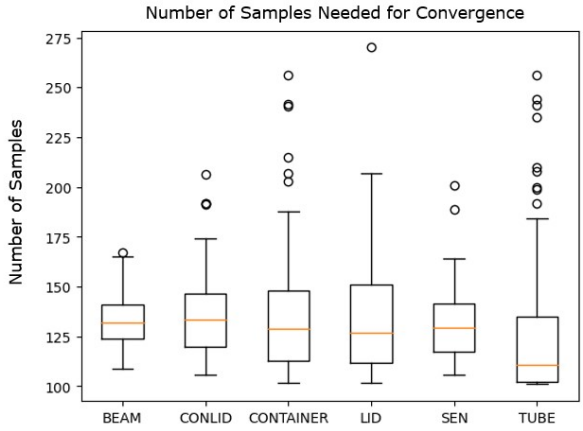


Figure 14 displays a Box plot for the 100 computed needed number of samples for each part type. The aggregate average across part type converges to a value of 129.4, with only minimal variance displayed between the final averages. The real discrepancy between part types is the variance and range of number of samples. Part types, such as BEAM, have a relatively small range of potential values with only a single outlier. Conversely, part types, such as TUBE or CONTAINER, not only have a significantly larger range, but also contain multitudes more outliers.

This rather large difference in sample variance can be attributed to two factors. One being the part type itself. Depending on the part composition, material and manufacturing process, a large amount of variance can found between individual parts themselves. The other source of variance is the aforementioned process of sampling from the part's distribution. This almost certainly injected unnecessary variance into the results; however, as previously explained this merely increases the upper ceiling. As such, even with artificially high levels of variance, we can see the convergence methodology is relatively consistent - even the outliers fall under an estimated 300 needed samples.

Naturally, the number of needed signals for a given part will be dynamically computed during the manufacturing process and is unique to each part produced. This experiment shows that a manufacturer would be expected to need an average of 300 signals for each part to ensure the validity of down stream conclusions. However, one should note that the sample size used in this experiment is extremely small, and every part was produced through additive manufacturing. The results outlined here may not be representative of more diverse parts produced through different manufacturing processes. For example, a machined part produced through CNC milling with tight allowances should theoretically exhibit less variance between parts, when compared to additive manufacturing such as 3D printing. In this scenario, we would expect the average number of samples needed per part to linearly decrease in relation to the decreased variances across parts.

B. Part Type Collision Analysis

The fundamental aim in all research outlined in this paper is the creation of a system with high theoretical security guarantees that can be estimated given a batch of parts. This experiment aims to validate the proposed process in this paper and also explicitly analyze each hyperparameters relative impact on the estimated system collision rate. Ultimately these results will help guide the initial parameterization of the proposed process in an arbitrary production environment. Naturally, the exact performance is completely dependent on the supplied part types and the inherent variance of the manufacturing process. Regardless, the below analyzed values will illustrate the fundamental relationships, irrespective of the derived scale of values.

To model the aggregate effect of each hyperparameter against the derived variance of the estimated collision rate, a grid of potential values were tested. Specifically, the following values for each hyperparameter were used in the experiment:

To gain a broad understanding of the internal relationships between each hyperparameter and the resulting estimated collision rate, the following values will be tested - Part Dimensionality: $[2, 3, 5]$, Meta Probability Density Function Confidence Interval: $[0.95, 0.99, 0.999]$, Part Probability Density Function Confidence Interval: $[0.95, 0.99, 0.999]$, Confidence Bound: $[0.95, 0.99, 0.999, 0.9999]$.

To explicitly represent a single hyperparameter's effect on the estimated collision rate, the following base values for each will be used, when itself is not being tested - Part Dimensionality: 2, Meta Probability Density Function Confidence Interval: 0.999, Part Probability Density Function Confidence Interval: 0.999, Confidence Bound: 0.999.

Please note that for all subsequent diagrams and analysis, the part types of BEAM, LID and TUBE will rarely demonstrate any meaningful reaction to the change in hyperparameter. This is not an invalidation of the underlying process, but rather a reflection of the inherent variance in part signals. Specifically, the natural variance between individual parts is so high that even extremely distorting the derived distribution estimation for each part results in minimal to zero real overlap between distributions. As such, regardless of the hyperparameter configuration, the estimated upper collision rate will most likely converge to zero. Fundamentally, this is a strong affirmation of the underlying assumption of ultra-high information density for each of the part's signals. Observing high fidelity of distributions, even between the same part type, is an important validation of the core process assumptions. Additionally, while the remaining three parts do illustrate the

expected relationship, they only do so at very small dimensionality levels. Each signal had to be constrained to 0.4% of its potential dimensionality just so the underlying expected relations could be illustrated. Without this severe restriction, the hyperparameter effects can not be studies without millions of unique parts for each part type.

Fig. 15. Collision Rate VS System Paramters

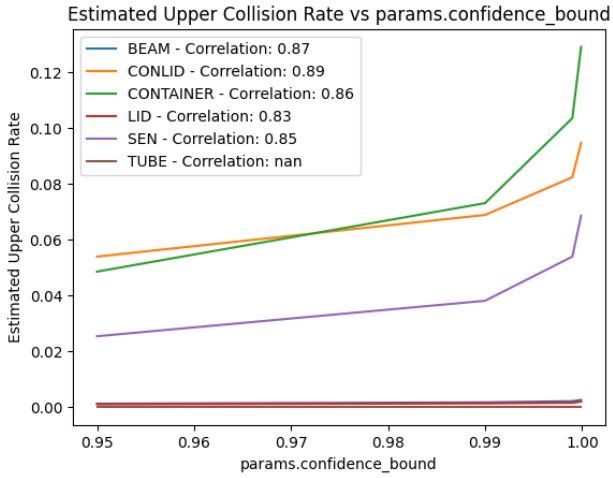


Diagram 15 illustrates the supplied confidence bound's effect on the estimated upper collision rate. As expected, an increase in the confidence bound results in a corresponding increase to the estimated system collision rate. More interestingly, the relationship exhibited is clearly exponential, with the increase in collision rate being geometrically disproportionate to the increase in the confidence bound. The can be explained as the supplied confidence bound dictates the needed minimum value for the probability of a sampled signal to be deemed as originating from one of the part's Gaussian distribution. For example, if the confidence bound is 0.95, then a minimum of 0.05% probability is needed for classification. As the confidence bound is increased, the barrier of entry for classification is decreased. However, when split in half, each side of a Gaussian distribution function is exponential. Thus, the decrease in needed classification probability will result in an exponential increase in the state space of signals that would be classified.

Diagram 16 shows the same analysis, but with the estimated collision rate being averaged across all part types. Without the relative scaling between part types, the underlying exponential relationship is clearly shown.

Diagram 17 illustrates the relationship between the supplied part probability density function's confidence interval and the

Fig. 16. Averaged Collision Rate VS System Paramters

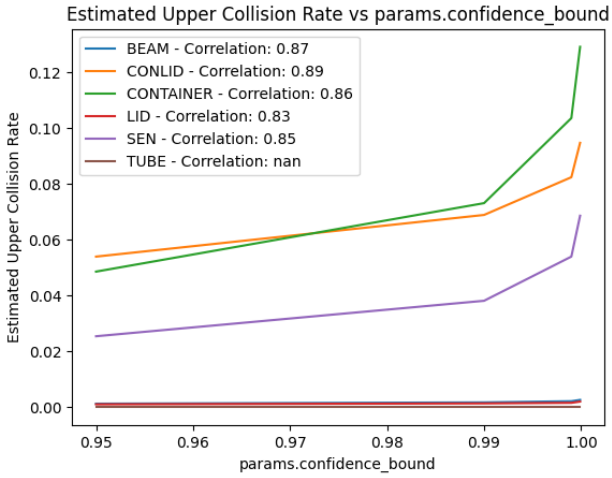
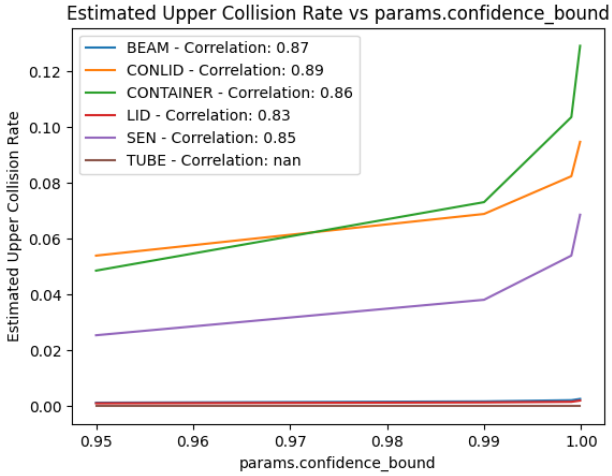


Fig. 17. Collision Rate VS Part CI



estimated upper collision rate. As expected, there is a strong positive correlation between the given confidence interval and the resulting collision rate. Once again, an exponential relationship is derived between the two. This can be reasoned by understanding that the confidence interval scales the derived covariance using a (z/t)-score, depending on the sample size. The (z/t)-score represents the number of standard deviations the sampled point is from the mean over a Gaussian or Student-T distribution. In both cases, the increasing of standard deviations results in an exponential increase/decrease in probability density. As such, a linear increase in the confidence interval will result in an exponential increase in the estimated covariance of each part's Gaussian distribution. Given limited state space, an exponential increase in covariance will directly result in an exponential increase in rate of collisions. However, please note this relationship will only be observable on smaller

levels of part dimensionality. Increasing covariance will only expand the resulting distribution in a single dimension, so as the dimensionality of a distribution increases, the relative impact of a single dimension is proportionally negated. This will be examined further in experiment: Derived System Entropy Analysis.

Fig. 18. Averaged Collision Rate VS Part CI

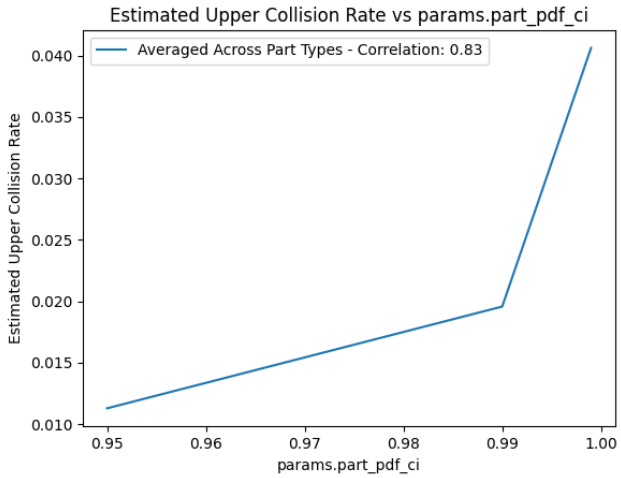


Diagram 18 describes the relationship that is naturally present when the aggregated part type collision rates are averaged together.

Fig. 19. Collision Rate VS Meta Part CI

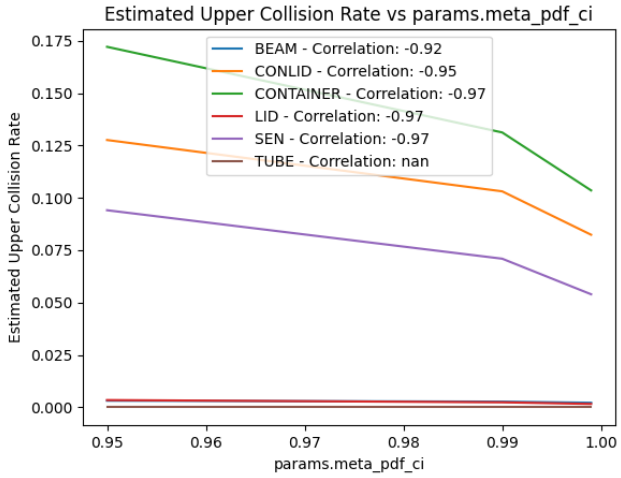
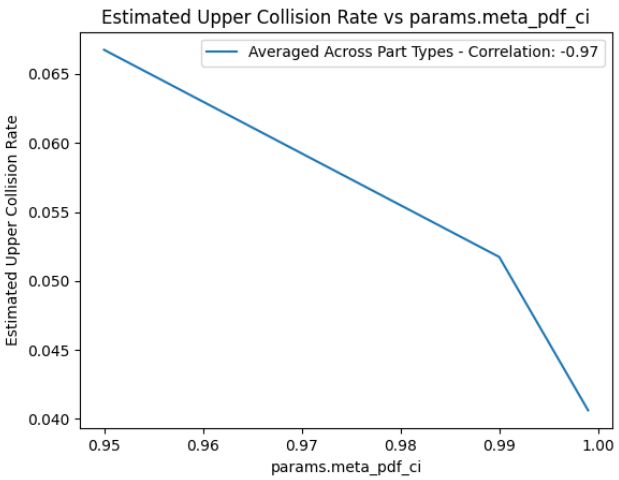


Diagram 19 illustrates the supplied Meta probability distribution function's confidence interval effect on the resulting estimated system entropy. Given a confidence interval is also supplied for the estimation of each part's probability density function, one might expect a similar positive, exponential relationship to be exhibited. Contrary to intuition, the diagram shows the exact opposite, a strong negative, inverse exponential function. Thus, the estimated system collision will become exponentially smaller as the supplied value of the meta probability density confidence interval is increased.

To understand this relationship, one must understand the confidence interval's relative role when computing the estimated collision rate. Once each individual part's Gaussian distribution has been estimated, all signals across all parts and grouped and used to derive a single meta distribution. This distribution will be similarly scaled by the given confidence interval. Ultimately the meta distribution aims to encapsulate the representative state space that any newly manufactured part's distribution may be derived from. The meta distribution is used to randomly sample potential signals and check for collision in the existing batch of parts. Thus, increasing the meta's distributions confidence interval will exponentially increase the projected covariance. As such, the density of probability is more evenly distributed, and the entropy of the system will increase. However, as the original meta distribution is derived from current batch's signals, any disbursement of the probability density away from its original values will decrease the average frequency of relative samples. More concretely, as the entropy of the system increases, it becomes less likely that a synthetic signal will be sampled from a region derived from one of the parts. Thus, as sampled signals become less grounded in batch of part's distributions, the probability a signal would be classified as any of the part distribution decreases, and the system collision rate correspondingly decreases as well.

Fig. 20. Averaged Collision Rate VS Meta Part CI



Naturally, the above explained relationship is mirrored when all part types are aggregated 20 and their respective collision

rates averaged.

Fig. 21. Collision Rate VS Part Dim

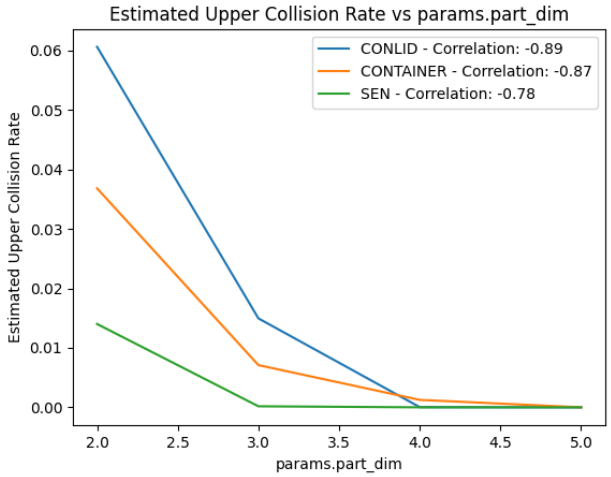
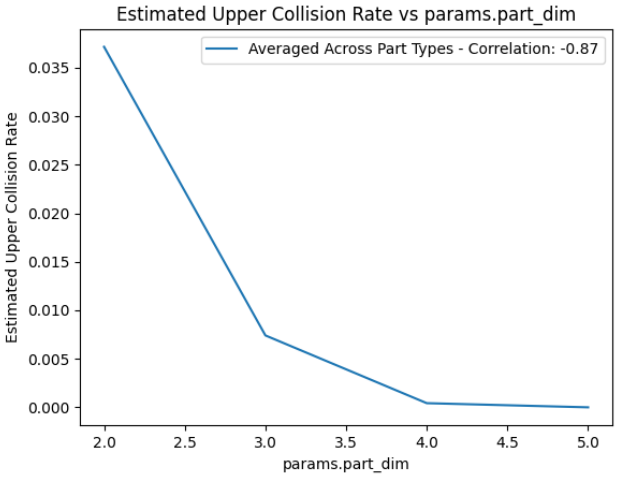


Fig. 22. Averaged Collision Rate VS Part Dim



Finally, we can analyze the remaining hyperparameter of part dimensionality 21. In support of the initial hypothesis, as the dimensionality of the part's distribution increases, the estimated collision rate of the system similarly decreases. Once again, an exponential relationship is evident between the increase part dimensionality and the resulting collision rate. This can easily be explained as each added dimension to the part's derived distribution means that for a collision to occur, the signals must be aligned on an additional dimension. The probability of occurrence is proportional to the covariance between the variants within the distribution. Additionally, increasing the dimensionality of the part's distribution increase the information density and fidelity of the resulting signals. Assuming each variant in the signal is not 100% correlated with every other variant, then increasing the dimensionality also increases the entropy of the signal. As the individual signal entropy is increased, then so is parent distribution's entropy said signal was derived from. If the distribution all part's distributions are sampled from has increasing entropy, then the resulting probability of two part's containing significantly overlapping derived distributions is inversely proportional to rate of entropy increase.

Once again, the above described relationship is illustrated when the part types are aggregated and their collision rates averaged. A final important observation is the rate of convergence to a zero collision rate. Naturally, this highly dependent on the part and part type it is being derived from; however, even averaged across all parts we see a common convergence to zero collisions given a dimensionality of 5. As explained in the Data section, each part's signal has a magnitude of 500, thus, it's resulting multivariate distribution is of dimensionality 500. Part distribution dimensionalities are only severely restricted during experimentation to demonstrate the hyperparameters effect. Regardless of other parameter values, any dimensionality above 5 was shown to consistently converge to 0. While disappointing for exploring higher dimensional behaviors, this helps validate the underlying assumption that the signal vectors have extremely high entropy and can act as a global identifier for a given part.

This experiment serves as a controlled validation of potential performance in a production system. We are unconcerned with the exact values computed in this experiment. Whether the aggregate estimated collision rate was 0.1, or 0.5 is unimportant as this is a toy example. Rather, this experiments validates our first-principals understanding of system dynamics and the reasoned theoretical relationships between the supplied hyperparameters and final collision rate. Additionally, the convergence of collision rate to 0 when given a part dimensionality of only 5 validates the assumption of the part's signal being a physically unclonable function. An increase in the part's dimensionality adds a new information channel against all existing dimensions, and results in a exponential increase in entropy. Each part's PDF entropy can then be exponentially increased an additional 495 times. While this would result in a significant decrease in computational efficiency, it shows the assumption of globally unique signals will hold true in any manufacturing process that does not produces infinite parts.

C. Monte Carlo Simulation Consistency

As the Proposed Solution section outlines, the final estimated collision rate is derived using Markov Integration through Monte Carlo Simulations. To compute the collision rate of a batch of parts, we must compute the overlap of each part's individually estimated signal distribution. While trivial in a one dimensional feature space, this problem quickly becomes intractable when projected into higher dimensions. Thus, rather than attempt to estimate the integration directly,

the relative overlap of the system of distributions will be derived through a Monte Carlo Simulation.

When performing integration estimation via any Markov Process, a fundamental question must be answered for how many samples are needed to ascertain confidence about the projected value? While some methodologies do exist for estimating the needed sample size, they are imprecise and lack theoretical guarantees regarding error rates and probability of representativeness. To compensate for this, a smaller sample size of only 100 will be used in conjunction with the aforementioned convergence algorithm. Specifically, the Monte Carlo Simulation will run iteratively, outputting the estimated upper collision rate until there has been a convergence of variance in the sample estimates. Similar to the use of the convergence algorithm when estimated a part PDF, we must recognize the levels of artificial variance this implicitly introduces into the system.

To model the aggregate effect of each hyperparameter against the derived variance of the estimated collision rate, a grid of potential values were tested. Specifically, the following values for each hyperparameter were used in the experiment - Meta Probability Density Function Confidence Interval: $[0.995, 0.999, 0.9995, 0.9999]$, Part Probability Density Function Confidence Interval: $[0.995, 0.999, 0.9995, 0.9999]$, Confidence Bound: $[0.995, 0.999, 0.9995, 0.9999]$.

To explicitly represent a single hyperparameter's effect on the variance of the derived collision rate, the following base values for each will be used, when itself is not being tested - Part Dimensionality: 2, Meta Probability Density Function Confidence Interval: 0.995, Part Probability Density Function Confidence Interval: 0.995, Confidence Bound: 0.995.

Fig. 23. Collision Rate Variance Vs Meta PDF CI

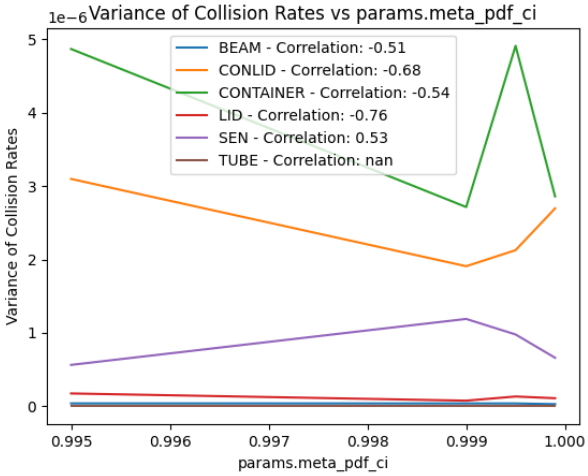
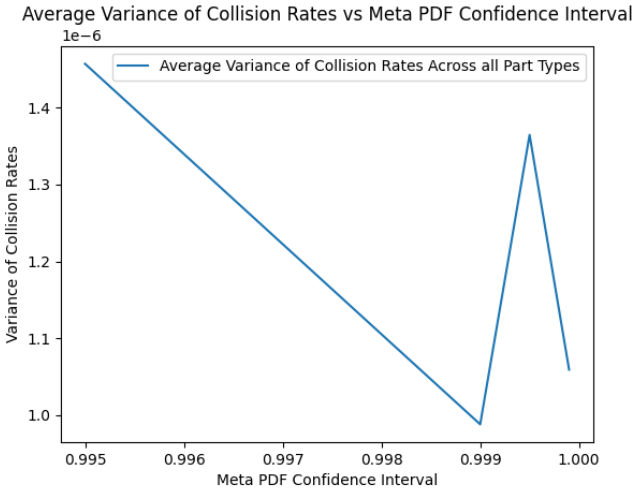


Diagram 23 illustrates the effect a varying value of the Meta PDF confidence interval had on the resulting variance of estimations for the system collision rate. As seen in other experiments, part types LID, BEAM and TUBE continue to display a direct convergence with 0% sampling due to their innate high distribution entropy. Conversely, it may seem part types CONLID, CONTAINER and SEN exhibit a strong relationship to the resulting variance given the computed correlation coefficient. However, one must take that in the context of the extremely limited sample size of only 5 points. There is a high probability the high correlation is simply random chance of the sampled points. This is supported by the fact the Meta PDF confidence interval is monotonically increasing, but the derived values for the variance, over every part type, fails to present a monotonically increasing or decreasing function. Additionally, each of the three parts seemingly displays a different function in reaction to the relative increase in the hyperparameter. Thus, the illustrated relationships are not definitive conclusions, but rather randomly sampled empirical points due to the limited sample size and the hyperparameters's minimal true effect.

Fig. 24. Collision Rate Averaged Variance Vs Meta PDF CI



The above conclusion is supported by the averaged results across all part types 24. Very clearly, there is no true underlying relationship between the meta PDF confidence interval and the derived variance of estimations.

Similarly, the part PDF confidence interval 25 also illustrates a lack of true underlying effect on the resulting variance of estimations.

Finally, the confidence bound 26 is also shown to have to underlying effect on the variance of estimations.

Showing four diagrams to argue that a relationship does not exist may unnecessarily derived. However, it allows the

Fig. 25. Collision Rate Variance Vs Part PDF CI

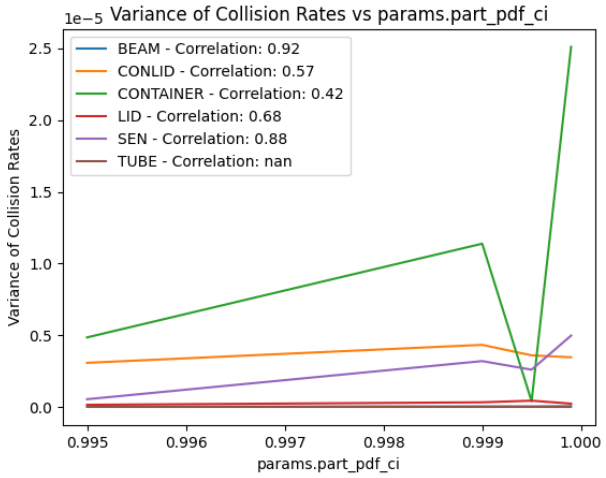
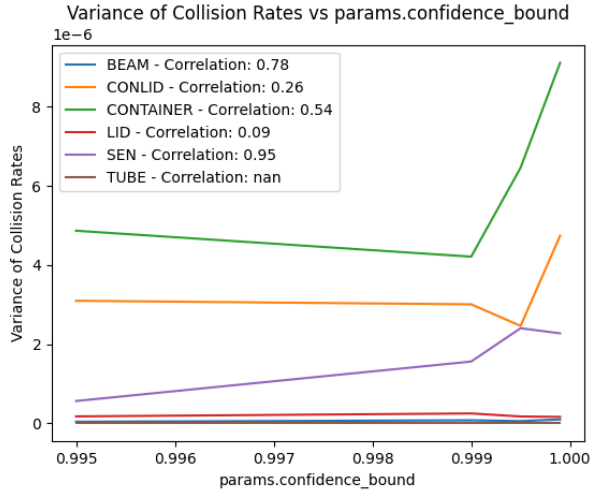


Fig. 26. Collision Rate Variance Vs Confidence Bound



validation of the proposed convergence algorithm in a generalizable context. Each hyperparameter has already been proven to have it's expected effect on the estimated collision rate in the Part Type Collision Analysis Experiment. The second-order derivative of the hyperparameter's effect is the variance it causes on the estimation process. Ideally, a change in the hyperparameter scale should correspondingly effect the scale of the estimated collision rate. However, if that same change also effects the process's ability to estimate consistent predictions, then this wold be an indicator a fundamentally incorrect dependency within the model. As this was not shown, we can conclude the process operates as expected and is able to output consistent estimations independent of the supplied hyperparameters.

Relating these results back to a concrete manufacturing process means that the even given the reasoned about system variance, the estimated collision rate will remain relatively consistent. As such, the collision rate of a part's batch can be estimated a single time, and additional computations can be avoided.

D. Derived System Entropy Analysis

The above experiments aim to understand the supplied hyperparameters impact on the performance of the proposed processes via concrete application metrics. These are worthwhile research questions, and helps to provide example performances given a variety of potential situations and parameters. However, the previous experiments are fundamentally measuring the impact of the hyperparameters via a second-order derivative indicator. Specifically, they are modeling the supplied parameters' effect via the change in process output. As the process itself is a derived estimation, the previous experiments are not explicitly capturing the direct impact of said given hyperparameters.

On the fundamental level, the hyperparameters will effect the derived entropy of the estimated distributions used for the subsequent analysis. The Part PDF Confidence Interval will scale the resulting variance of the estimated probability distribution function for each supplied part. The chosen dimensionality of the signal vector will naturally directly effect the resulting entropy as it dictates the dimensionality of the derived multivariate Gaussian distribution. Thus, the hypothesis is that an increased signal dimension will directly correspond with an increased resulting entropy. Similarly, increasing the Part PDF Confidence Interval will also directly result in an increase to the derived entropy.

To test the above hypothesis, the probability density function will be estimated for each of our six parts over a grid of varying hyperparameters. Specifically, the following ranges will be tested - Part Dimensionality: $[2, 3, 5, 10, 50, 100, 400]$, Part PDF CI: $[0.995, 0.999, 0.9995, 0.9999]$.

When analyzing the effect of the supplied part dimensionality, the part probability density function confidence interval will be kept constant at a value of 0.995. Similarly, when evaluating the effect of the part probability density function confidence interval, the part dimensionality will be kept constant at 2.

Diagram 27 illustrates the effect of the given part's probability density function confidence interval on the estimated distributions entropy. As entropy is fundamentally a measure of information bits, the exact scale is relative and unimportant. Rather, we are interested in the relative relationship that is exhibited, regardless of the concrete values. As such, we can see that across every measured part type, an increase in the supplied confidence interval results in an increase in the derived entropy of the estimated Gaussian distribution. The relative differences between part types is also unimpactful and can be explained by some parts naturally having a higher variance in measurements, and thus, a higher resulting entropy.

Fig. 27. System Entropy vs Part PDF CI

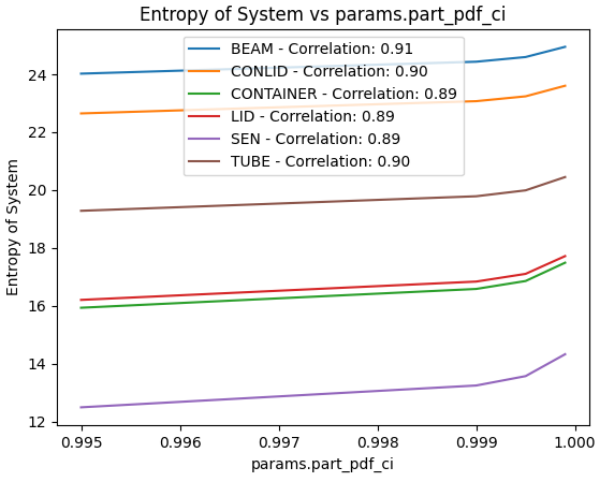
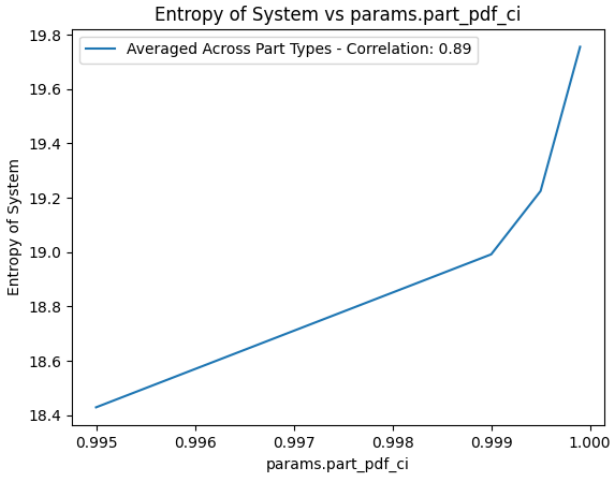


Fig. 28. Averaged System Entropy vs Part PDF CI

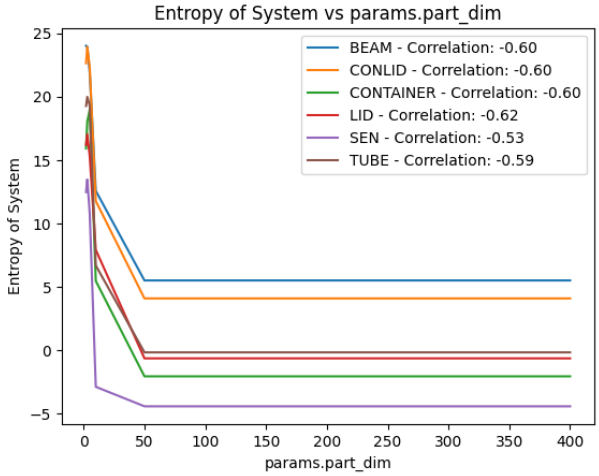


An interesting observation to note is that increase in entropy is linear for the majority of values, with only a marginal increase in scale with the final measurements. This is interesting because an increasing value in a confidence interval is not a linear relationship. Specifically, the confidence interval is derived from the z or t score, depending on data set size. The (z/t)-score represents the number of standard deviations from the mean the sampled data point is. As such, the probability density of each subsequent increase in standard deviation is an inverse exponential function within the Gaussian distribution. Thus, as the supplied confidence interval is scaled linearly, it's resulting impact on the estimated Gaussian distribution is exponential. Yet, this exponential relationship is not mirrored in derived entropy.

While perhaps initially unintuitive, this can be explained by examining what entropy is actually measuring. At the fundamental level, entropy is an indicator of randomness, lack of order, or information density of a system. Increasing the confidence interval will increase the variance, and scale of covariance in the estimated distribution. Broadly, this will widen the state space of signals that is most frequently sampled from. Conceptually, this is similar to flattening a 1-D distribution; this probability density is more evenly spread out, and the randomness of the system is increased. For a 1-D distribution, the increase in variance would result to a one-to-one increase in entropy. This is not mirrored in n-dimensional distributions as the redistribution of probability mass only happens on a single dimension, the variance. The relative covariance between variants is kept constant, thus, the system only gains novel information across a single dimension. Consequently, the entropy will not scale in a one-to-one relation with the confidence interval, and the above illustration of results is validated.

Graph 28 illustrates the same the same initial analysis, but the entropy is averaged across all part types to support a unified view of the confidence interval's effect. Without the relative scaling of each part, the averaged values seem to display a true exponential relationship between the confidence interval and derived system entropy. While perhaps seemingly contradictory to the above analysis, this can be explained by the used value of part dimensionality, which was kept constant at 2. As previously explained, the effect of an increasing confidence interval is inversely proportional to the dimensionality of the distribution as increasing the variance will increase the information density of an increasingly smaller portion of the whole distribution as it's dimensionality goes up.

Fig. 29. System Entropy vs Part Dim

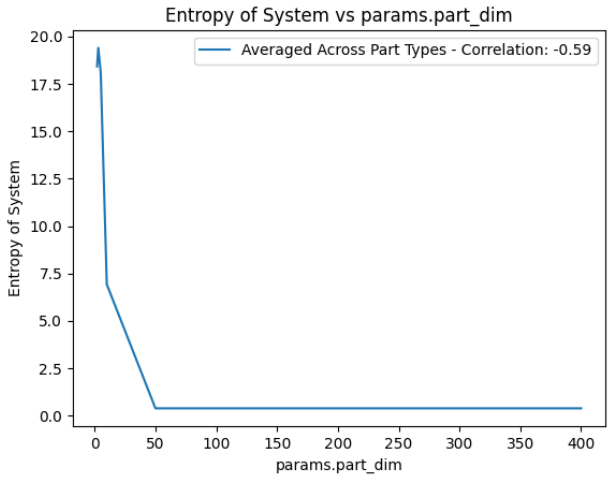


We expected the above analyzed relationship to also be present for the supplied part dimensionality 29. One might

assume that increasing the part dimensionality should result in closer to a one-to-one increase in derived entropy. However, the above diagram clearly does not reflect that. This is unfortunately a lack of data problem, rather than a true process conclusion. The core issue is the the log determinant of the covariance matrix must be calculated to derive a multivariate distribution's entropy. For the majority of the parts, only a signals were measured and stored. Thus, for the higher part dimensions, the resulting covariance matrix has significantly more columns that rows. Consequently, the covariance matrix will not have a unique solution as it is singular. The resulting determinant calculation will be 0, resulting in a negative infinity value for the log determinant of a part signal distribution's covariance matrix.

We can however, see an initial validation of our hypothesis during the first and second measurements of part dimensionality when the resulting covariance matrices weren't singular. Specifically, the above graph illustrates a strong positive relationship between the supplied part dimensionality and the resulting system entropy, as was hypothesized.

Fig. 30. Averaged System Entropy vs Part Dim



Naturally, the averaged entropy values across all part types 30 show the above described relationship with minimal deviation.

This experiments serve to validate the assumption of high-entropy systems that create globally unique part signals. When a manufacturer adjusts a given hyperparameter, the part batch's system entropy will adjust in relation to the change. Once again, this helps to validate the underlying assumptions of exponentially increasing information density that all subsequent conclusions implicitly assume.

VI. Related Work

A. Piezoelectric material

A recent industry paper from Herder et al. [Herder et al., 2014] provides a industry level overview of current Physical Unclonable Functions (PUF), methodologies and current applications. The authors create the distinguishment between strong PUFs, those made for authentication and weak PUFs, those made for simple key storage. The key difference between the two classifications being the derived domain space for each function. Finally, the paper address error-correcting and fuzzy pattern matching in the context of external variance within the physical functions. The paper concludes with an analysis of emerging validation infrastructures, such as public model PUFs and PUF implementation technologies.

Fu et al. with the Singapore Institute of Manufacturing Technology [Fu et al., 2003] proposes a novel technique for deriving lost features from transported CAD models. Once a CAD model is created in one system and transferred via data-exchange standards, many of the originating features or feature information will be lost. This then creates a bottleneck in integrated product design as the identification of design features is turned into an arduous process. To help alleviate this issue, a multiple-level feature taxonomy and hierarchy is outlined that is based on the derived characteristics of part geometry and topology entities. This establishes concrete relationships between the CAD features and the underlying geometric entities. While this might seem an orthogonal problem space to component verification, their geometric derivation system attempts to model the very characteristics our proposal asserts are globally unique. The paper operates over computer CAD designs, and thus, the data for a given geometric sequence is deterministic and the derivation of features a tractable computation. When in the context of physical domains with unknown external factors introducing unknown levels of variance, the proposed system is no longer able to ascertain the underlying geometric features using the proposed heuristic hierarchical classification.

Given the recent explosion of popularity for additive manufacturing techniques, Moroni et al. [Moroni et al., 2017] proposes a novel methodology for validating the geometric accuracy of manufactured parts. While a plethora of current tolerance practices have been standardized across the industry, most lack the fidelity to accurately validate complex or intricate parts. As such, the paper proposes the combination of traditional tolerancing with an enriched voxel-based volumetric representation schema that overcomes the specificity limitations of previous methods. Additionally, the proposed methodology creates a conceptual link between product design optimization and downstream verification of the manufactured product within the additive manufacturing chain.

B. Anti-counterfeiting

A 2008 paper from Lehtonen et al. and the Institute of Technology Management of the University of St. Gallen [Lehtonen, 2008] gives an insightful overview of current industry implementations of RFID product authentication techniques. Radio

Frequency Identification Devices (RFID) enable automatic data gathering is a wide range of industries. However, pure identification via a RFID signal does not prove the verification of the claimed identity, and additional infrastructure to support this validation is needed. An example verification methodology is the application of unique RFID transceivers onto a received batch of products. This would be done on the retail level to help deter potential tampering or theft. While a cost effective solution, this does not guarantee the validation of a given part, and given sufficient technology, the originating RFID signal can be easily spoofed.

Shiyang et al. [Liu, 2010] outlines a dual anti-counterfeit methodology to increase the implicit cost of any malicious attack vector. Specifically, the paper proposes the use of QR codes to embed biologic features, such as finger prints, and other personally identifiable information to create a dynamic and biological public key verification infrastructure. Given the implicit multi-factor authentication needed for such a verification, this process gives strong security guarantees for deference against identity falsification. While not directly applicable to product verification, the underlying ideology of using the item to be verified's own physical properties for validation is consistent with this paper proposed solution.

C. Verification of Part Information

Brandman et al. proposes the addition of a physical hash for preventing and detecting cyber-physical attacks in additive manufacturing systems [Brandman et al., 2020]. The paper argues current cyber solutions are broadly inadequate as many manufacturing environments would be unable to upgrade the physical systems to meet cyber-security requirements. A disconnected side-channel measurement system can be used to generate a physical part hash to link the manufactured part to it's digital data. This enables security insurance in the scenario where the either the network or the additive manufacturing system becomes compromised as the manufacture can revert the underlying measurement system for attack detection. Additionally, the paper suggests performing the measurement *in situ* as classifying the part against the manufacturer's design can be performed in real-time.

Turner et al. argues that recent cyber-attacks illustrate the inherent risk of physical equipment operating outside designed tolerances to produce failures [Turner et al., 2015]. This can be implicitly caused by a cyber-attack altering the underlying manufacturing design of a part to purposefully introduce weaknesses and induce failure. Such attacks are being perpetrated due to the lack of rigorous enforcement of cyber-security best practices in the manufacturing industry. The paper suggest numerous novel research avenues to support the adoption of cyber-security into physical manufacturing environments.

VII. Concluding Remarks

This paper has outlined an extension to previously proposed solution of Piezo electrical signals for part verification. Traditional part verification methods often fail to encapsulate the physical identity of an item in relation to a probable link to it's corresponding digital representation. This allows for either the physical part to be replicated along with whatever physical identifier is associated with it. By deriving a part's identity from it's physically measured Piezo electrical sensor response, the part's identification is explicitly linked with the physical part and is theoretically irreplicable.

While this methodology provides strong theoretical guarantees, the fidelity of the Piezo sensor also causes an unfortunate draw back of being highly sensitive and dependent on unknown external factors. As such, a single measurement from a part can not be used for subsequent classification or assertion of part validity. Fuzzy matching algorithms are a potential solution, but lack theoretical guarantees and fail to encompass the implicitly sampled uncertainty and the global estimation of collision rate. Thus, this paper proposes a novel signal classification process that estimates each part's distribution. This allows for the collision rate of a given part batch, representing the upper bound on part security, to be explicitly derived for each part type. As a consequence of the collision rate derivation, the classification accuracy and false positive rate is also implicitly computed. Additionally, the process is parameterized on arbitrary a set of hyperparameters. The adjust of said hyperparameters allows the explicit and granular control over the desired ratio between false negative rates, for counterfeit parts, and the estimated security, or collision rate, of the entire system.

Thus, as the classification accuracy and subsequent collision rate are derived independently outside of the part's batch, the propose solution's assertions stand even when malicious actors obtain perfect knowledge. We can define perfect knowledge as having complete information regarding a part type. For example, the specifications and the specific manufacturing process used to derive the part. As the part's geometry can not be derived from it's latent signal representation, and the counterfeit process is shown to always introduce more variance than the original manufacturing process, a malicious actor would be unable to increase the collision rate above the estimated upper bound - which is most commonly estimated at 0.

References

[Brandman et al., 2020] Brandman, J., Sturm, L., White, J., and Williams, C. (2020). A physical hash for preventing and detecting cyber-physical attacks in additive manufacturing systems. *Journal of Manufacturing Systems*, 56:202–212.

[Butticè et al., 2020] Butticè, V., Caviggioli, F., Franzoni, C., Scellato, G., Stryszowski, P., and Thumm, N. (2020). Counterfeiting in digital technologies: An empirical analysis of the economic performance and innovative activities of affected companies. *Research Policy*, 49(5):103959.

[Fu et al., 2003] Fu, M., Ong, S., Lu, W., Lee, I., and Nee, A. (2003). An approach to identify design and manufacturing features from a data exchanged part model. *Computer-Aided Design*, 35(11):979–993.

[Ghadge et al., 2021] Ghadge, A., Duck, A., Er, M., and Caldwell, N. (2021). Deceptive counterfeit risk in global supply chains. *Supply Chain Forum: An International Journal*, 22(2):87–99.

[Herder et al., 2014] Herder, C., Yu, M.-D., Koushanfar, F., and Devadas, S. (2014). Physical unclonable functions and applications: A tutorial. *Proceedings of the IEEE*, 102(8):1126–1141.

[Kim and Park, 2019] Kim, T. K. and Park, J. H. (2019). More about the basic assumptions of t-test: normality and sample size. *Korean J. Anesthesiol.*, 72(4):331–335.

[Kwak and Kim, 2017] Kwak, S. G. and Kim, J. H. (2017). Central limit theorem: the cornerstone of modern statistics. *Korean J. Anesthesiol.*, 70(2):144–156.

[Lehtonen, 2008] Lehtonen, Mikkoand Staake, T. M. F. (2008). *From Identification to Authentication – A Review of RFID Product Authentication Techniques*, pages 169–187. Springer Berlin Heidelberg, Berlin, Heidelberg.

[Liu, 2010] Liu, S. (2010). Anti-counterfeit system based on mobile phone qr code and fingerprint. In *2010 Second International Conference on Intelligent Human-Machine Systems and Cybernetics*, volume 2, pages 236–240.

[Moroni et al., 2017] Moroni, G., Petrò, S., and Polini, W. (2017). Geometrical product specification and verification in additive manufacturing. *CIRP Annals*, 66(1):157–160.

[Sandborn et al., 2021] Sandborn, M., Olea, C., White, J., Williams, C., Tarazaga, P. A., Sturm, L., Albakri, M., and Tenney, C. (2021). Towards secure cyber-physical information association for parts. *Journal of Manufacturing Systems*, 59:27–41.

[Senyo, 2022] Senyo, S. (2022). Fighting the global counterfeit medicines challenge: A consumer-facing communication strategy in the us is an imperative. volume 12 03018.

[Siekmann et al., 2011] Siekmann, I., Wagner, 2nd, L. E., Yule, D., Fox, C., Bryant, D., Crampin, E. J., and Sneyd, J. (2011). MCMC estimation of markov models for ion channels. *Biophys. J.*, 100(8):1919–1929.

[Tang et al., 2009] Tang, C. S., Zimmerman, J. D., and Nelson, J. I. (2009). Managing new product development and supply chain risks: The boeing 787 case. *Supply Chain Forum: An International Journal*, 10(2):74–86.

[Turner et al., 2015] Turner, H., White, J., Camelio, J. A., Williams, C., Amos, B., and Parker, R. (2015). Bad parts: Are our manufacturing systems at risk of silent cyberattacks? *IEEE Security Privacy*, 13(3):40–47.