SAND2022-3883C

Sandia National Laboratories

Exceptional service in the national interest

Synthetic threat injection using digital twin informed augmentation

Dan Krofcheck
Sandia National Laboratories

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Trusted and Trust-In AI systems

In high consequence environments, Trust between operators and AI becomes critical

Trusted systems should be:

- Resilient
- Robust
- Adaptable
- Ergonomic

Detectron 2 Object Detection

Facebook object detection API
Facilitates training collections of object detection models with pre-initialized weights

We trained 6 candidate models on our COCO formatted dataset
Model hyperparameters and training schedule were **NOT** optimized

Data separated into a 90/10 train/test split, after stratifying to minimize class imbalances

Dataset
These whole vehicle scans collected on a Multi-Energy Portal
Hand annotations for 2 classes:

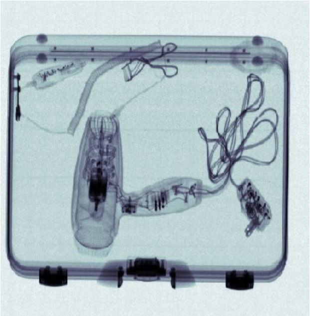
- Target A (Simple geometry SMT)
- Target B (Complex geometry SMT)

Model Name	Model Family	Model Outputs
R50-FPN-1x	Faster RCNN	Class, Score, Box
R50-FPN-3x	Faster RCNN	Class, Score, Box
R101-FPN-3x	Faster RCNN	Class, Score, Box
RN-R50-1x	RetinaNet	Class, Score, Box
RN-R50-3x	RetinaNet	Class, Score, Box
R_101_FPN_3x	Mask RCNN	Class, Score, Box, Mask

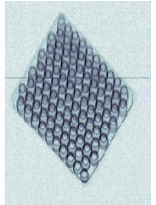
Threat Image Projection (TIP)

Using conventional published approaches (Rogers et al., 2016)
Hand cropped threats, injected following Beers law
TIPs are constrained to the cargo area

Several



Several



Many

Simple experiment:
Train the collection of models without TIP images
Train the collection of models with 100% increased observations per class using TIP.

Hypothesis:
Models should not significantly improve in this case, but we would hope they would have increased extensibility.

Rogers, T. W., Jaccard, N., Protonotarios, E. D., Ollier, J., Morton, E. J. and Griffin, L. D., "Threat Image Projection (TIP) into X-ray images of cargo containers for training humans and machines, " 2016 IEEE International Carnahan Conference on Security Technology (ICCST), 1-7 (2016).

Synthetic injection impact on model training

Table 2. mAP comparison of a two-target detection experiment, trained with all in-situ observations (No Synthetic) and then augmented with an additional 100% synthetic TIP observations per target (Synthetic).

	No-TIP		With-TIP	
Model	**Target A**	**Target B**	**Target A**	**Target B**
R50-FPN-1x	0.77	0.87	0.74	0.68
R50-FPN-3x	0.75	0.90	0.71	0.87
R101-FPN-3x	0.79	0.94	0.77	0.87
RN-R50-1x	0.72	0.90	0.67	0.79
RN-R50-3x	0.76	0.84	0.74	0.86
X101-FPN-3x	0.80	0.95	0.78	0.90

Target A: simple SMT
Target B: complex SMT

Synthetic injection impact on model training

Table 2. mAP comparison of a two-target detection experiment, trained with all in-situ observations (No Synthetic) and then augmented with an additional 100% synthetic TIP observations per target (Synthetic).

	No-TIP		With-TIP	
Model	**Target A**	**Target B**	**Target A**	**Target B**
R50-FPN-1x	0.77	0.87	0.74	0.68
R50-FPN-3x	0.75	0.90	0.71	0.87
R101-FPN-3x	0.79	0.94	0.77	0.87
RN-R50-1x	0.72	0.90	0.67	0.79
RN-R50-3x	0.76	0.84	0.74	0.86
X101-FPN-3x	0.80	0.95	0.78	0.90

Target A: simple SMT
Target B: complex SMT

Synthetic injection impact on model training

Table 2. mAP comparison of a two-target detection experiment, trained with all in-situ observations (No Synthetic) and then augmented with an additional 100% synthetic TIP observations per target (Synthetic).

	No-TIP		With-TIP	
Model	**Target A**	**Target B**	**Target A**	**Target B**
R50-FPN-1x	0.77	0.87	0.74	0.68
R50-FPN-3x	0.75	0.90	0.71	0.87
R101-FPN-3x	0.79	0.94	0.77	0.87
RN-R50-1x	0.72	0.90	0.67	0.79
RN-R50-3x	0.76	0.84	0.74	0.86
X101-FPN-3x	0.80	0.95	0.78	0.90

Target A: simple SMT
Target B: complex SMT

Synthetic injection impact on model training

Take away:

- We never tested on TIP images
- Models trained with additional TIP images should have more exposure to a wider array of contexts
- These models hyperparameters and training schedules were **NOT** optimized.
- The location of the TIP should affect its shape, but we did not take this into account.

Table 2. mAP comparison of a two-target detection experiment, trained with all in-situ observations (No Synthetic) and then augmented with an additional 100% synthetic TIP observations per target (Synthetic).

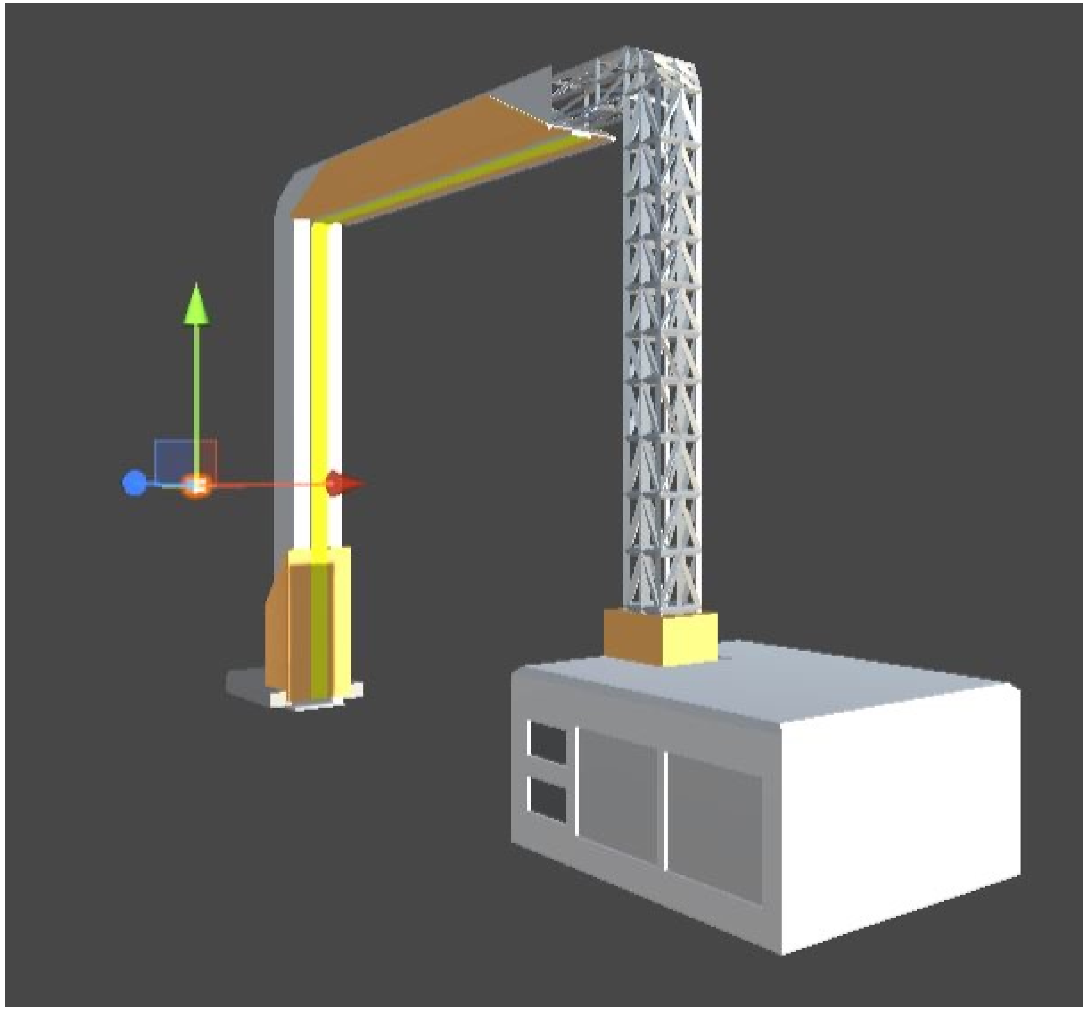
	No-TIP		With-TIP	
Model	**Target A**	**Target B**	**Target A**	**Target B**
R50-FPN-1x	0.77	0.87	0.74	0.68
R50-FPN-3x	0.75	0.90	0.71	0.87
R101-FPN-3x	0.79	0.94	0.77	0.87
RN-R50-1x	0.72	0.90	0.67	0.79
RN-R50-3x	0.76	0.84	0.74	0.86
X101-FPN-3x	0.80	0.95	0.78	0.90

Target A: simple SMT
Target B: complex SMT

A digital twin for domain informed augmentation

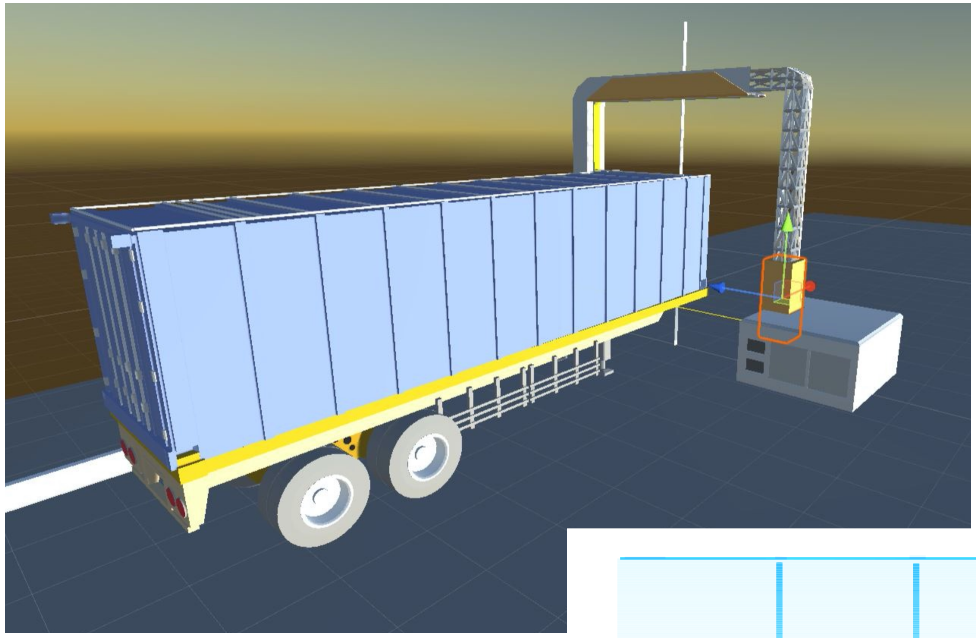
Detector
- Geometry and projection

Query
- Speed (u, s)
- Materials (a=ebc)

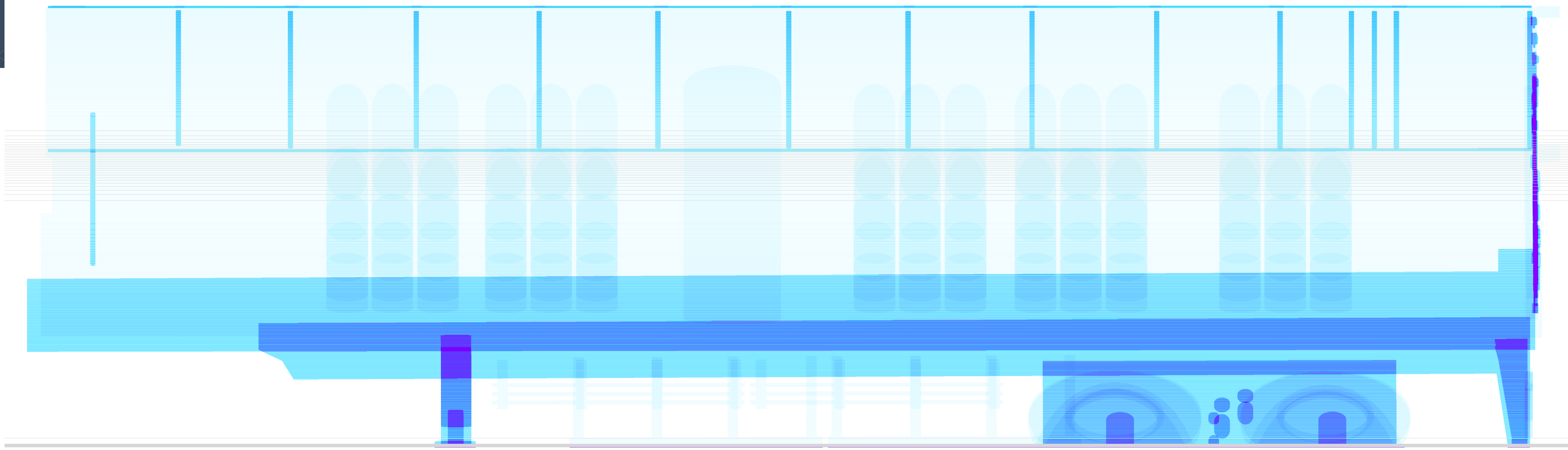


Fan Beam
- Number of rays
- Angle increment
- Min and Max angle

A digital twin for domain informed augmentation

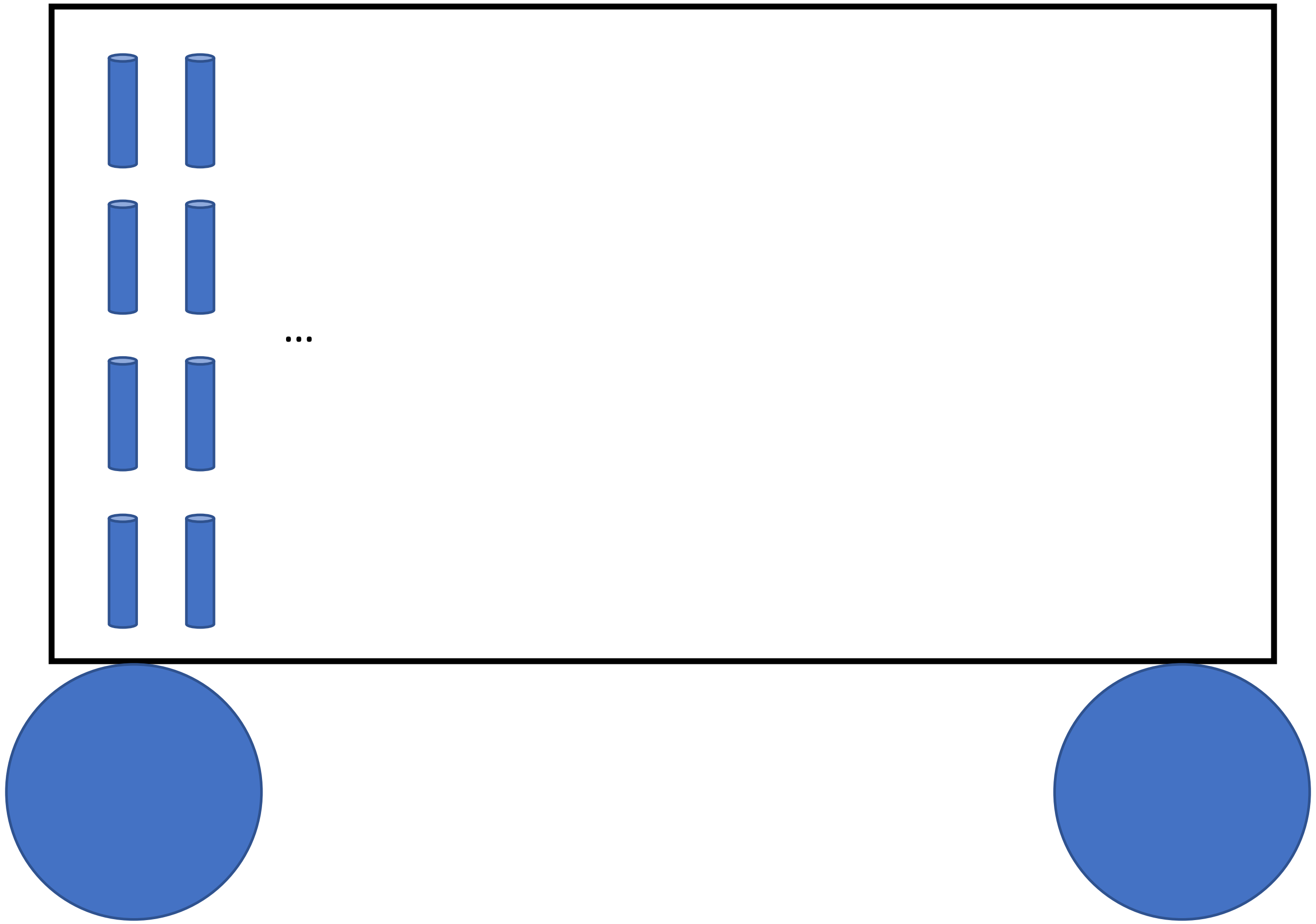


- Extensible system for visualization, testing and evaluation
- Simple representation of the physics, focusing on geometry
- Empirical alternative to closed form solutions, can recreate noisy data



A digital twin for domain informed augmentation

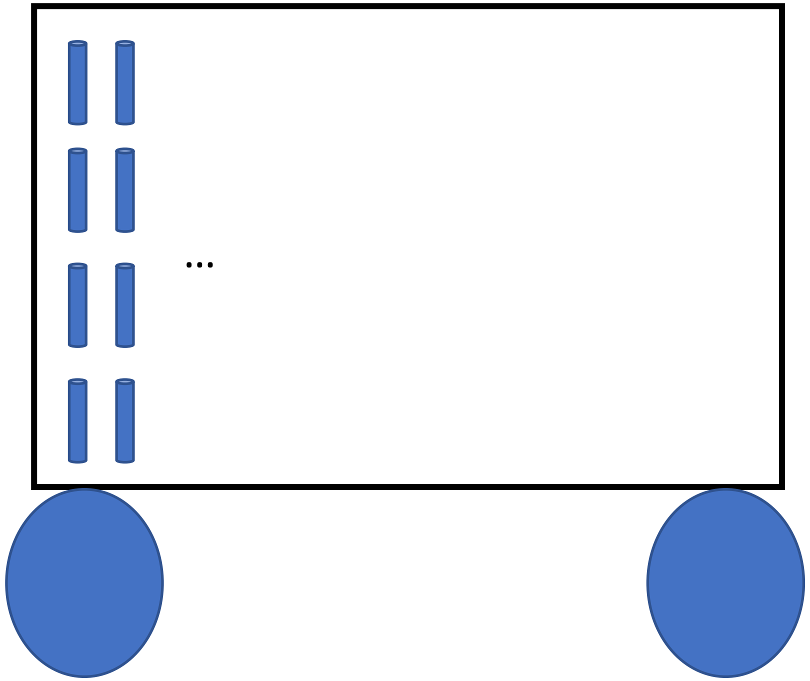
Simple experiment:



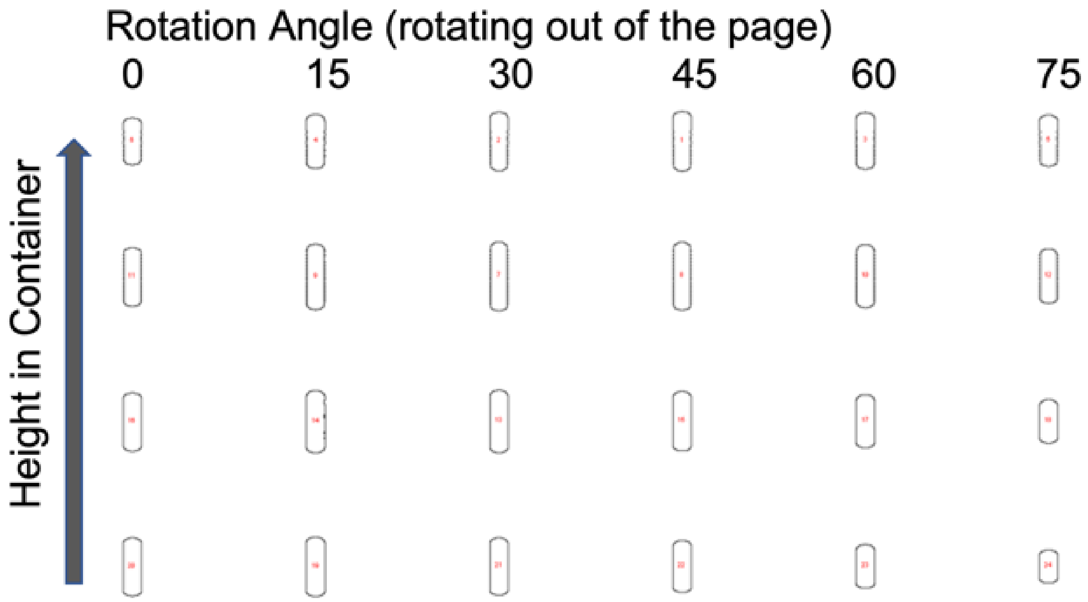
A digital twin for domain informed augmentation

Simple experiment:

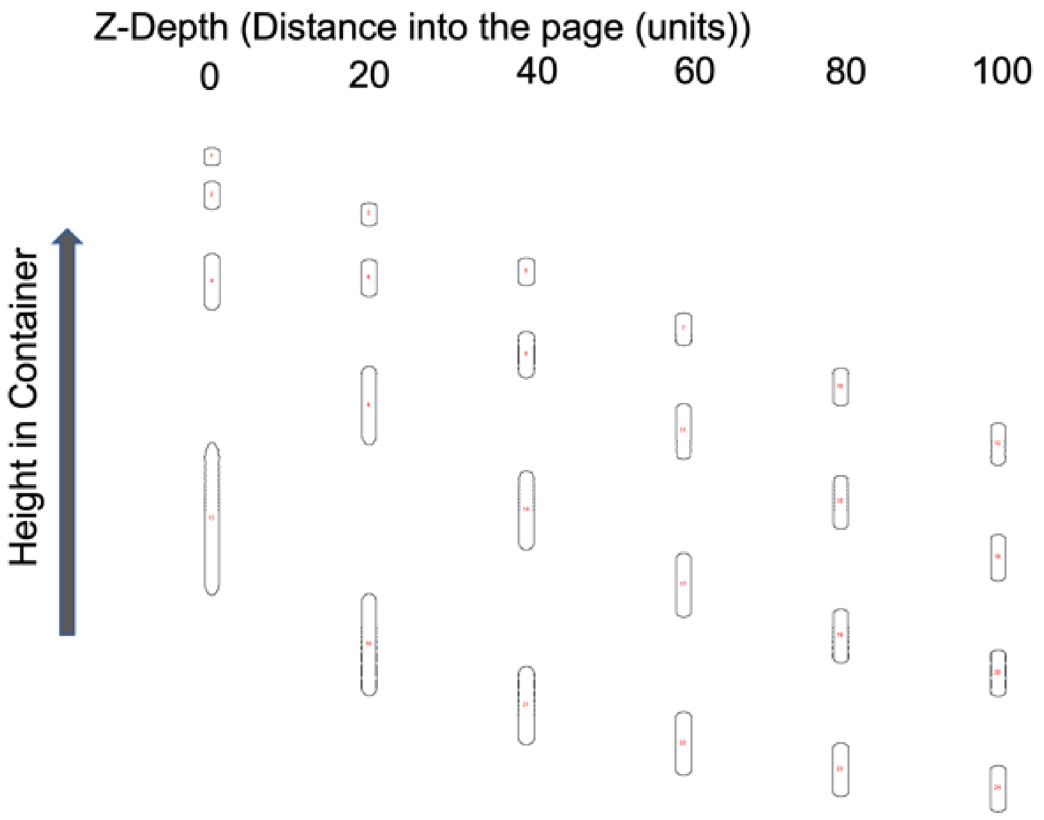
- Create an array of simple objects to scan in the digital twin
- Structure each column align a heigh gradient
- Manipulate each column to test either rotation or depth
- Measure the projected area of each object in the resulting scans



Sensor informed augmentations - rotation



Sensor informed augmentations - depth



Sensor informed augmentations

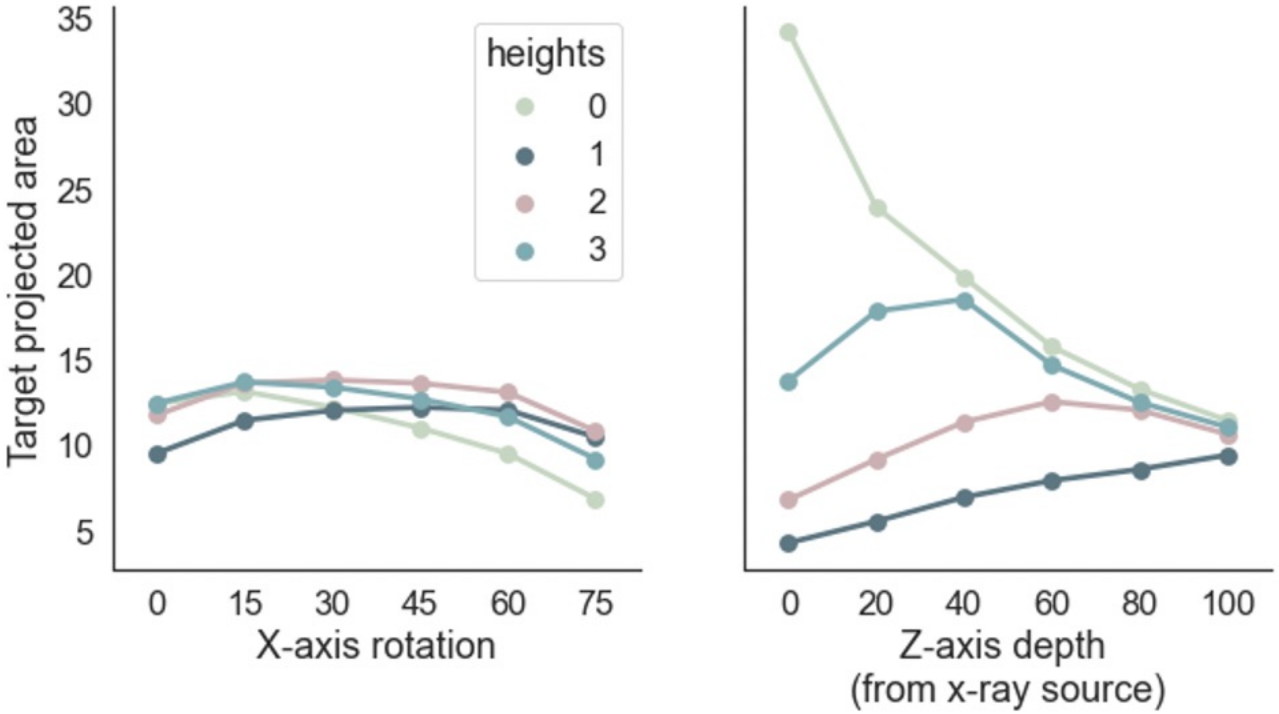


Figure 4. Projected area of the target objects as a function of rotation in the x-axis (left) and distance from the x-ray source (right).

Conclusions

Key Takeaways

- TIP can increase the generalizability of an object detection model, without too great an accuracy penalty
- More testing, and testing on context appropriate data, would address this more completely
- We proposed a simple solution to accommodate TIP augmentation based on sensor geometry
- Given a geometry, we can learn a function that maps a voxel location to a simple transform